

An innovative Memristor-based Wireless Power Transfer for NFC Security

Colin Sokol Kuka

Doctor of Philosophy, PhD

University of York

York

YO10 5DD

UK

Electronic Engineering

October 31, 2021

*In memory of my father,
Thanks to my mother, wife and family for the support.*

Abstract

In traditional Wireless Power Transfer (WPT) circuits, inverters are used to produce an oscillation for the transmitter coils. This includes intrinsic energy dissipation sources due to the use of switches, necessitating an extra control circuit to ensure proper switching time. Those circuits also have limited encryption capabilities. In order to overcome these challenges, we have proposed an innovative near-field power and chaos transmission method based on the memristor and applied it to Near Field Communication (NFC) security. We adopted two Chua circuits capable of chaotic self-oscillation, avoiding the use of extra switches. Both circuits exhibit synchronised chaotic behaviour depending on parameters and an equivalent emulator for memristors, which could be used to generate distinct cryptography. Additionally, we used a chaotic memristive Colpitts oscillator. We utilised this topology for NFC to have the advantages of this circuit, which include the possibility of low-power operation and a higher frequency up to the memristor's operating limits.

By sampling the chaotic voltages generated, it is possible to create a true random number generator (TRNG). This new technique is an intriguing solution that could be used to increase the security of web applications that adopt NFC. Moreover, we worked on the development of a Python-based web server application capable of utilising the sampled voltage values and encrypting them in real time. The web server application operates similarly to a social network, with each user creating an account, logging in with their email and password, uploading notes, and logging out. The application may use any encryption algorithm and may make

use of the chaotic data obtained in real time from the circuit. We verified the functionality through various experiments and the randomness of data obtained using FIPS PUB 140-2's Security Requirements for Cryptographic Modules. The results confirm the data's true randomness.

Keywords: Chaotic Behaviour; Cryptography; Wireless Power Transmission (WPT); Memristor; Near Field Communication (NFC); Python code; Security; True Random Number Generator (TRNG); Web Server application; Wireless Power Transfer;

Acknowledgment

To begin with, I would like to express my heartfelt appreciation to my supervisor, Dr. Yihua Hu, for his early support, continued assistance, and encouragement throughout my Ph.D. studies and related research, as well as for his patience, motivation, and vast knowledge. He is an open, amiable, and cheerful person, and it is a pleasure to work with him. Our communications have always been sincere and straightforward; I never doubted his unwavering support and never felt the need to fudge the language. And it was like magic that each time I left his office, I reminded myself to work harder. His attitude toward research is also inspiring: "*As a PhD, you should aim high and try to expand your work to new areas.*" Working with him for three years will become a priceless memory in my life.

Besides my supervisor, I would like to thank Prof. Quan Xu, an academic visitor from the School of Microelectronics and Control Engineering at Changzhou University. I would like to express my gratitude for their assistance, but also for the difficult question, which prompted me to broaden my research from a variety of perspectives.

I want to express my strong feelings of gratitude towards my colleague and great friend, Dr. Mohammed Alkahtani, at the University of Liverpool. Thanks for the stimulating discussions and for sharing the experience of PhD research study. Together, we form a strong and invaluable team in our research on WPT systems and photovoltaic power management.

I would like to thank Dr. Kai Ni, now at the School of Electrical and Electronic Engineering, Huazhong University of Science and Technology, China, for being

my guide and an exemplary student at the very start of my PhD path and for continuing help from remote China. Also, I want to thank all my friends and former colleagues in the Department of Electrical Engineering and Electronics at the University of Liverpool, where I have spent two great years.

I also want to thank James Chandler, former colleague at the University Center City of Liverpool College, now at the University of Birmingham. Thanks for great help on manufacturing experimental tests.

Finally, I would like to reserve a special word of thanks to my mother: all that I am, or hope to be, I owe to you; and to my father, your spirit will always be with me. I can consistently feel your wordless love, confidence, and pride in me. I want to express my hearty appreciation to my wife and children. Her enduring love, drive, and advice unquestionably laid the groundwork for my PhD work during these years. Thank you.

Publications

We would like to inform the reader that this thesis work is based upon after this list of the author publications in academic books, journals and conferences as listed below.

Book Chapter

- Kuka Colin Sokol (Chapter 1: *Wireless Power Transmission*) (2021). Hus-sain Al-Rizzo, *ANTENNA SYSTEMS*. ISBN 978-1-83968-829-4.

Academic Journals

- Kuka C.S., Hu Y., Xu Q., Chandler J. and Alkahtani M., 2021, A Novel True Random Number Generator in Near Field Communication as Memristive Wireless Power Transmission. *MDPI -J-*, 3(1), pp.23-35.
- Kuka, C.S., Hu, Y., Xu, Q. and Alkahtani, M., 2020. An innovative near-field communication security based on the chaos generated by memristive circuits adopted as symmetrical key. *IEEE Access*, 8, pp.167975-167984.
- Kuka, S., Ni, K. and Alkahtani, M., 2020. A review of methods and challenges for improvement in efficiency and distance for wireless power transfer applications. *Power Electronics and Drives*, 5.

Conferences

- Kuka C.S., Chandler J. and Alkahtani M., 2021, Chaotic-based Security for Near Field Communication in Internet of Things devices. In *ICONS - 2021 - Widening Systems Engineering Borders WiSEB*. **Best Paper Award**

- Kuka C.S., Alkahtani M., Poliposyan G. and Alahammad M., 2020, An Innovative Memristor-based Near Field Communication Topology Adopted as Security Key. In *ICONS - 2020 - Widening Systems Engineering Borders WiSEB*.
- Wu, T., Li, W., Hu, Y., Gong, C., Kuka, S. and Lu, J., 2019, October. Parameter Dependency Analysis of Uncontrolled Generation for IPMSMs in Electric Vehicles. In *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society* (Vol. 1, pp. 3237-3241). IEEE.
- Wu, Z., Li, W., Kuka, S. and Alkahtani, M., 2019, October. Analysis of dust deposition on PV arrays by CFD simulation. In *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society* (Vol. 1, pp. 5439-5443). IEEE.

Contents

List of Tables	xxv
0.1 Principles of Wireless Power Transfer	3
0.2 Research Motivation	5
0.3 Research Objectives	6
0.4 Scope of the Thesis	7
1 Types of Wireless Power Transfer	9
1.1 Far-field Wireless Power Transfer	11
1.1.1 Microwave Coupling	12
1.2 Near-field Wireless Power Transfer	14
1.2.1 Capacitive Power Transfer	14
1.2.2 Inductive Power Transfer	16
1.3 Comparison between CPT and IPT	18
2 Inductive Power Transfer	24
2.1 Magnetic Link Design	33
2.1.1 Metamaterials	38
2.2 Inductive Power Transfer Coil Design	39
2.3 Analysis of WPT system as a two-port network.	43
2.3.1 Resonance Technique	47
2.3.2 Compensation Network	48
2.4 Power converters in Wireless Power Transfer	51

2.5	Rectifiers	54
2.5.1	Diode rectifiers	55
2.5.2	MOSFET rectifiers	58
2.6	Multi-coil WPT system	59
2.6.1	Issues related to WPT	62
2.7	WPT challenges	65
3	Near Field Communication	69
3.1	NFC vs RFID	73
3.2	NFC applications	75
3.3	NFC modes of communication	78
3.3.1	Active mode	79
3.3.2	Passive mode	79
3.4	NFC tags	82
3.4.1	NFC tags of type 1	83
3.4.2	NFC tags of type 2	84
3.4.3	NFC tags of type 3	84
3.4.4	NFC tags of type 4	84
3.4.5	NFC tags of type 5	85
3.5	NFC Data Exchange Format	86
3.6	Security issues	87
3.7	NFC Security Attacks	90
3.7.1	Skimming	91
3.7.2	Spoofing	92
3.7.3	Man In The Middle Attack	93
3.7.3.1	Relay Attack	94
3.7.4	Eavesdropping	95
3.7.5	Phishing	96
3.7.6	Data Corruption	97

3.7.7	Data Manipulation	98
3.7.8	Data insertion	99
3.7.9	Denial of Service attack	100
3.8	Thermal issue on NFC	101
4	Memristor and the Chua Circuit	106
4.1	Memristor	107
4.2	Memristor Emulator	111
4.3	Security based on chaos	114
4.4	The Chua's Circuit	116
4.4.1	Electric simulation Chua circuit	120
4.5	A new topology of WPT circuit	122
5	Memristive WPT	125
5.1	Wireless Power Transfer and Memristor	126
5.1.1	Typical Functionality	129
5.1.2	Wireless Power Transmission	132
5.2	Simulations Results	134
5.2.1	Magnetic Field	134
5.2.2	Circuit Simulation	138
5.2.3	Memristive Power Transmission	140
6	Variety of Memristive WPT	143
6.1	Memristor models	144
6.1.1	Non-ideal active voltage-controlled memristor	145
6.1.2	Theoretical analysis	147
6.1.3	Simulation and Experimental Results	148
6.1.4	Experiment	154
6.2	Low inductance Chua circuit	155
6.2.1	Array of inductors	155

6.2.2	Simulations and Experiment	158
6.3	Light dependent Chua circuit Chaos	160
6.4	Temperature dependent Chua circuit Chaos	162
6.5	Memristive chaotic Colpitts oscillator	164
6.5.1	Generalised Memristor Model	165
6.5.2	NFC built with Memristive Colpitts Oscillator	167
6.5.3	Simulations and Experiment	168
7	NFC Security Applications	172
7.1	The need of security in NFC devices	172
7.2	Experiments for Security Applications	175
7.2.1	Arduino True Number Generation	177
7.2.2	Arduino Firmata Library	178
7.3	Web server application using Python	179
7.3.1	Python libraries: Flask and SQL Alchemy	182
7.4	Statistical tests	183
8	Future Work	189
9	Conclusion	191
	Bibliography	193

List of Figures

1	The block diagram of a WPT system with the various efficiencies along the transmission path considering the non-ideal source, AD/DC converter, rectifier and inverter, compensation network and coupling factor. The receiver could be symmetrical depending on the type of load.	3
1.1	Region partition depending on the wavelength λ	10
1.2	Representation of Wireless Power Transmission: (a)Far Field WPT where the Rectenna is highlighted, and (b)Near Field WPT.	11
1.3	Photovoltaic electric energy production: sun rays made of photons hit an n-doped semiconductor which generates both majority (electrons) and other minority carriers.	13
1.4	W. Brown experiment in the invention of the rectenna or rectifying antenna: an helicopter is supplied with electric power from a microwave beam [28].	13
1.5	Recent demonstration of the Tesla experiment in Reference[30]	15
1.6	Principle of the Capacitive Power Transfer (CPT).	16
1.7	Principle of the Inductive Power Transfer (IPT).	17
1.8	Application of wireless power transfer technology listed in levels of power transmission and distance between transmitter and receiver.	19

1.9	Representation of the differences between CPT and IPT in the studies collected from journal articles. The CPT is represented with a cross and the IPT with a circle. The colour of crosses and circles depend on the efficiency of the application. The plot illustrates (a) The output power vs the distance, (b)The output power vs the size of the coils (coupled area) and (c)The output power vs the power. In (d) the plot shows the Efficiency from source to load vs the distance using the power in W as a colour code.	21
2.1	Illustration of (a) the first electric toothbrush patent [37] and (b) Braun Oral B toothbrush disassembled.	25
2.2	Pictures of (a) new generation toothbrush with mini display and in (b)the coil for the inductive power transfer and (c) the battery for inductive power transfer.	25
2.3	The phone charger (a)Palm Inc, (b)transmitter disassembled where is showing the coil and chip, (c)back part of a phone wireless used for charging and (d)receiver disassembled.	26
2.4	Qi logo in (a)the vent wireless charger and (b)the electrical specs in a phone charger.	27
2.5	Powermat Technologies is a global provider of wireless charging platforms and the first to bring wireless power technology for mobile phones to consumers worldwide[43].	28
2.6	The Aircharge wireless charging outlets on the community tables are perfectly integrated into McDonald’s furniture décor, allowing customers to top up their devices while having a meal or drink without having to bring a cable or struggle to reach power plugs [46].	29

2.7	Anycharge positions in many locations in different cities (a)-(l). Photographs of charging stations that have been built in various locations. The first row's stations ((a), (b), (c), (d)) are installed in hotels, the second row's stations ((e), (f), (g), (h)) are located in shopping centres, and the third row's stations I (j), (k), (l)) are installed in city offices [47].	30
2.8	Typical schematic for a 3 phase EV inductive charging.	31
2.9	Forms of charging technologies that can be implemented in our living environment: (a) basic residential systems in home garage or driveway; (b) parking spaces in shopping centres or large areas; (c) on-street parking in main roads of the city centres ; (d) dynamic charging systems (future technology) where roads such as motorway will have dedicated charging lanes while driving[55, 62].	32
2.10	The real inductor model has (a) resistive and capacitive effects. (b) The table shows Litz wires size vs the AWG number.	34
2.11	NiZn flexible ferrite sheet's relative permeability spectrum.	35
2.12	Application of metamaterials in WPT in Reference[78](a)-(d).	38
2.13	Required steps for the coil design in inductive power transfer.	40
2.14	Redexpert online tool for choosing the right coil for an inductive power transfer.	43
2.15	A representation of the inductive power transfer in (a) two port network model. (b) Equivalent T-model of the coupled coils in the model adopted.	44
2.16	The four basic topology for resonance and compensation network, namely a) the series-series S-S, b) series-parallel S-P, c) parallel- parallel P-P and d) parallel-series P-S.	48

2.17	Hybrid resonant topologies highlighted: the LCL configuration with the receiver in a) series, LCL-S b) parallel, LCL-P and c) doubled and d) at the receiver S-LCL; e)The LCC configuration and f) the equivalence with LCL when voltage driven [114]. Other relevant topologies such as g) LCC-LCC, h) CCL-S and i) S-CLC.	49
2.18	Schematic of the (a) Full-bridge inverter and (b) half-bridge inverter.	51
2.19	The class-E inverter (a) topology before the resonant tank and (b) waveforms of V_G turning ON S_1 and its V_{DS}	53
2.20	A receiver block diagram where has been highlighted the rectifier and its efficiency.	55
2.21	Diode efficiency function depends on the breakdown voltage and the load resistance.	55
2.22	The four typical configurations of the rectifier.	56
2.23	Waveforms generated from each configuration of the rectifier.	57
2.24	Most common voltage multiplier configurations: (a) Three stages CockcroftWalton voltage multiplier, (b) Four stages Dickson voltage multiplier, (c) Four stage Dickson voltage multiplier using CMOS technology, (d) Two stages voltage multiplier comprised of differential drive unit.	58
2.25	Four coils WPT system with the coupling factors. The couplings are marked following their value. κ_{13} , κ_{14} and κ_{24} are not visible due to their intensity values which are negligible.	60
2.26	Crosstalking example: not authorised EVs are charge because their proximity with the DWC lane.	63
2.27	Concept of autonomous vehicle tracking and guidance to reduce degraded power transfer in a DWC system.[144]	63
2.28	FOD to a chew-gum aluminium wrap which have begun to burn.	64

2.29	Challenging WPT implant in the skull which is insensitive to the exact location of the receiver [146].	65
2.30	The guideline recommended by the ICNIRP for the level of electric and magnetic field.	66
2.31	Safety level experiment (first part) for 6.6kW WPT charger.	66
2.32	Experiment (second part) continues with a human inside the parked car.	67
2.33	Schematic diagram of the proposed security key proposed in Reference [150].	67
3.1	High Permeability μ_r (400-700) flexible magnetic sheet for NFC/RFID antenna applications.	70
3.2	A comparison in terms of communication range between NFC and other types of networking.	71
3.3	First mobile phone, Nokia 6131, to have NFC technology[154].	71
3.4	Samsung NEXUS S, the first NFC-enabled Android phone, open in the back where the NFC coil can be clearly noticed[155].	72
3.5	The first contact-less payment developed by RIM [157].	72
3.6	NFriendConnector created an online social by integrating Facebook and NFC-enabled mobile phones [161].	73
3.7	NFC cards and RFID tags. The tags/receivers are very similar to each others [164].	74
3.8	Various NFC applications in healthcare; (a) NFC enabled smart watch [174]; (b) wearable bracelet prototype [175]; (c) cochlea implant with a circle indicating the NFC communication component of the implant [163]; (d) brain optogenetic implant held with fingers, the device is smaller than a US quarter. [176].	76
3.9	Type of NFC (a)modulations and coding table, (b)the Manchester coding and (c)Modified Miller coding.	78

3.10	NFC three operation modes are: reader/writer, peer-to-peer, and card emulation communications.	80
3.11	Comparison between NFC tags with chip manufacturer, memory size, used ID and cost (Reference [198]).	83
3.12	NDEF include several records, made up of a header and a payload that contains the message's content.	86
3.13	The bits and bytes of an NDEF file are shown in detail in Figure above.	87
3.14	Security risks associated with NFC technology.	89
3.15	The features of NFC communication can be used to classify NFC operation modes and security.	91
3.16	A block schematic diagram of a smartphone's and the charger. The physical equivalent of the design is shown on the right, with an image of a generic gadget put on a wireless charger.	102
3.17	The heat map on the coil surface during the charging process. In (a) and (b) Antennas in both solutions are less than 0.3 mm thick. Figure (c) shows a 45-minute time plot at the maximum temperature location.	103
4.1	The basic passive circuit components with two terminals.	107
4.2	The memristor as seen via a scanning tunnelling microscope [225].	108
4.3	(a)Initial state, (b)low-resistance state, and (c)high-resistance state of a memristor.	109
4.4	(a)Schematic depiction of a memristor device and its (b)Typical pinched hysteresis current-voltage loop.	110
4.5	Memristor device current-voltage curves (a) unipolar and (b) bipolar.	111
4.6	The memristor (a) is depicted as a block diagram and (b) as a SPICE model [235].	112

4.7	Memristor plots: charge-flux, current-voltage, current-voltage-time, and x-time curves [235].	112
4.8	Modelled memristor SPICE coding in Reference [235].	113
4.9	Typical Chua circuit rap resented with the parasitic resistance. . . .	116
4.10	Chua diode (or memristor) $v - i$ characteristic.	117
4.11	Realisation of the Chua diode with a voltage-controlled negative resistor R_N	118
4.12	In Chua's circuit, an example of a one-parameter bifurcation diagram.	119
4.13	The Chua's Circuit's behaviour as a function of the β bifurcation parameter: (a) limit cycle ($\beta = 17$); (b) period 2 ($\beta = 16.2$); (c) period 4 ($\beta = 15.7$); (d) spiral Chua's attractor ($\beta = 14.9$); (e) periodic window ($\beta = 14.31$); (f) double-scroll Chua's attractor ($\beta = 14.2$). . . .	120
4.14	Chua's circuit attractors. Two coexisting attractors during several periods of chaos (a)-(d).	121
4.15	Chua's circuit attractors. Two coexisting attractors during several periods of chaos in (a)-(g). In (h)a scroll attractor with two scrolls.	122
5.1	Memsistive circuit developed by L. Chua[255].	126
5.2	Some security applications of NFC technology. Commercial products like a security safe lock with an NFC system opening key. A BMW door opening and NFC house handle. The image was taken from a car shop in the United Kingdom and the web source [258]. . . .	127
5.3	The wireless power transfer circuit and the system built with Memristors.	128
5.4	The crypto-system model is applied to high-level security: on the left, the transmitter lock and the receiver in the Card Key.	129
5.5	Flowchart of the door opening procedure.	130

5.6	The system does not develop chaotic behaviour for all values of total inductance, but only for certain values of the coupling factor. Figure shows the operating point (OP) of the system, coupling value and the total inductance. Out of a certain range of values, the system does not develop chaos and does not oscillate.	132
5.7	Transmitter coil is (a) caved in the core in order to increase directionality and (b) receiver coil and flat core to enhance energy harvesting.	135
5.8	Structure of the receiver (brown) and transmitter (purple) in the ANSYS analysis. (a) Magnification of the 8 mH coils.	136
5.9	The Magnetic Field (a) Intensity H spread in the air, where it can be notice by the vast green color (0 dB) and (b) Vector B spread in the air, where it can be notice by the vast green color (0 dB). . . .	137
5.10	Chua circuit waveform: inductor voltage (blue) and Chua diode voltage (red); XY plot (green) on the resistor voltage.	138
5.11	The schematic of an Antoniou Circuit.	139
5.12	Chua circuit waveform magnified: XY plot (green) on the resistor, inductor voltage (blue) and Chua diode voltage (red).	139
5.13	Long time step simulation for the Memristive : inductor voltage (blue) and Chua diode voltage (red); XY plot (green) on the resistor voltage.	140
5.14	Receiver V_{MR} vs V_{LCR} shown in XY mode in 0.2 V/div and 1 V/div, respectively.	141
5.15	Receiver V_{MR} vs i_{LCR} shown in XY mode in 1 V/div and 1 V/div, respectively.	141
5.16	Receiver v_{LCR} vs i_{LCR} shown in XY mode in 0.2 V/div and 1 V/div, respectively.	141

5.17	Synchronisation of the phase portraits of a chaotic attractor: voltage in the inductor V_{LC} referred to the memristor voltage V_M in the transmitter (a) and receiver (b) coil; current in the inductor i_L referred to the memristor voltage V_M in the transmitter (c) and receiver (d) coil; the memristor voltage V_M referred to its internal voltage status V_0 in the transmitter (e) and receiver (f).	142
6.1	The schematic of (a) Chua's Memristive circuit. (b) Equivalent realisation of a non-ideal active voltage-controlled memristor.	144
6.2	Chua's memristive circuit has the (a) Double-scroll attractor phase portrait. (b) Chaotic oscillation of the memristive Chua circuit. (c) Memristive flux characteristic with the voltage of the two capacitors.	145
6.3	The behaviour in the transmitter (the Chua circuit) is a well-known double-attractor phase portrait. This plot shows the characteristic of the voltage in the coil and the voltage on the memristor.	146
6.4	Time step of the chaotic behaviour in the receiver: the memristor voltage V_M in green and internal status V_0 in red (a) and coil current i_L in red and memristor voltage V_M in blue (b).	148
6.5	Synchronisation of the phase portraits of a chaotic attractor: voltage in the inductor V_{LC} referred to the memristor voltage V_M in the receiver (a) and transmitter (b) coil; current in the inductor i_L referred to the memristor voltage V_M in the receiver (c) and transmitter (d) coil; the memristor voltage V_M referred to its internal voltage status V_0 in the receiver (e) and transmitter (f).	149
6.6	The power transmitted has a large chaotic behaviour and usually a lower value than 0.2 mW.	150
6.7	Transmitter voltage behaviour (blue) and receiver (purple) in the coil.	150

6.8	Simulation results with the synchronisation signal circled in red: LC voltage in the primary (1st plot) and the secondary (2nd plot); primary memristor voltage (3rd plot) and secondary (4th plot); the internal status of the secondary (5th plot) and the synchronisation signal (6th plot).	151
6.9	Time step of the chaotic behaviour when the receiver is disconnected (highlighted in yellow): the LC voltage V_{LC} and memristor voltage V_M in receiver and transmitter, in purple and green respectively. At the disconnection (in the 3 rd graph), the receiver memristor holds its last status as shown in the 4 th graph in blue.	152
6.10	Data transmission at 3Kbps; it is possible to notice the time of switching (highlighted in yellow) the chaotic behaviour in the LC, the memristor voltage and the internal status in the 4 th graph. . . .	153
6.11	Two attractor phase portrait in the receiver side with V_{MR} vs V_{LCR} shown in XY mode in 0.5V/div and 0.5 V/div, respectively.	154
6.12	Single attractor phase portrait in the receiver side with V_{MR} vs V_{LCR} shown in XY mode in 0.5V/div and 0.5 V/div, respectively.	155
6.13	The induced voltage in each coil as shown in Equation 6.8.	156
6.14	The system of Memristive Wireless Power Transfer built with two coils on the receiver side.	157
6.15	Planar intensity of the (a) Magnetic field between the coils (high in red and low in blue); (b) and in the surrounding area.	158
6.16	The circuit simulation of the coils array shows same chaotic behaviour such as single coil.	159
6.17	The Memristor Wireless Power Transfer Circuit built with a variable resistor which can be a LDR or thermistor.	160

6.18	Experimental study of the symmetric chaotic circuit by using light: (a)the dark is created by covering the LDR with hands, and no chaotic behaviour is shown. (b) Light goes on the LDR, enabling the chaos to start and two phase portraits are shown on the oscilloscopes. (c) A chaotic waveform is produced. (d) Real-time waveform sampling and display on the laptop.	161
6.19	Temperature experiment: (a) by holding with fingers we have increased the temperature resulting in no chaos behaviour; (b) after the temperature cooled down the chaotic behaviour started again. .	163
6.20	(a)Colpitts oscillator with memristor and (b) the generalised model of the memristor.	164
6.21	Circuit Simulations of the Memristor-based Colpitts circuit.	165
6.22	Zoom on the voltage V_L between the resistor and the inductor and the voltage V_C on the collector of the transistor.	165
6.23	Memristive Colpitts power and chaos transmission system.	167
6.24	Near-Field Communication with Memristor based Colpitts oscillators: Transmitter (squared in red) waveform.	167
6.25	Near-Field Communication with Memristor based Colpitts oscillators: Receiver (squared in blue) waveform.	168
6.26	Simulation synchronisation of the phase portraits with a single chaotic attractor: the XY plots of the transmitter (a)triangular-shaped attractor and (b)the spiral chaotic attractor. The receiver is fully synchronised and shows as well a (c)triangular-shaped attractor and (d)the spiral chaotic attractor.	169
6.27	Experiment test for single Colpitts circuits with (a) some testing parameters and (b) original parameters from Reference [286].	170
6.28	Memristive Colpitts power and chaos transmission. The experiment also shows the sampled waveform displayed in a computer monitor.	170

7.1	The IOT devices make a (a) Large use of NFC (b) A commercial NFC chip product collected from the manufacturer website [287].	173
7.2	The schematic of Memristors wireless power transfer circuit with adaptive circuit for the TRNG.	175
7.3	The experiment with a real time TRNG.	176
7.4	No chaotic waveform will generate near to zero random numbers. On the left, the Transmitter (bottom) and Receiver (top) are shown in a XY plot. The voltage for the microcontroller input and the execution of the Python code with number generation are shown on the right.	177
7.5	A chaotic waveform will generate true random numbers. On the left, it is shown the XYplot of the Transmitter (bottom) and Receiver (top). On the right, it is shown the ADC input voltage and the execution of the Python code with number generation.	178
7.6	Screenshot of the Arduino IDE uploaded with Firmata coding template.	179
7.7	The experiment set up: (a)development of the chaotic waveform; (b)sampled values of the chaos shown in Python; (c)webserver running with log in features developed with Python.	180
7.8	Use of Python and use chaotic encryption for web resources.	181
7.9	The bitmap generated form the sequence of numbers sampled which have no pattern and appear to be indistinguishable from white noise to the human eye.	184
7.10	We have used <i>rngtest</i> tests to verify the randomness of the data block. This test works on blocks of 20000 bits at a time using the FIPS 140-2. The <i>rngtest</i> is composed of five different tests: monobit, poker, runs, long run, and continuous run. The block fails the test if any of these fail.	184

7.11 The typical Flowchart of FIPS 140-2 validation which has established the Cryptographic Module Validation Program (CMVP) as a collaborative effort between the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) for the benefit of the Government of Canada. All tests conducted under the CMVP are conducted by third-party laboratories accredited by the National Voluntary Laboratory Accreditation Program as Cryptographic Module Testing (CMT) laboratories [297]. 185

7.12 The *ent* pseudorandom number sequence test in Linux OS. The *ent* is composed of five different tests: Entropy, Monte Carlo, Chi-Square, Arithmetic mean and Serial correlation coefficient. The results confirm that our sequences are true random numbers. . . . 185

7.13 Monte Carlo test; blocks of successive 48-bit numbers are used to produce (x,y) pairs, with each coordinate being a 24-bit integer. Calculating $\pi = 4q$ with q the circle ratio in the first quadrant, where the ratio q is taken by extracting pairs of random points (x, y) from our sequence, π will approach the correct value of π confirming the randomness. 187

List of Tables

1	Interesting examples of Wireless Power Transfer applications followed by year, power transmitted, frequency, efficiency and the distance achieved.	2
1.1	Theoretical maximum distance reachable by the WPT in Reactive and Radiative Region.	10
1.2	Comparison between the Capacitive Power Transfer and Inductive Power Transfer.	22
2.1	Relative permeability list of many materials. Some of them are peak values, which are obtained for a specific value of the magnetic field H and frequency indicated in the other columns. The value of the μ_R is a curve depending on the value of H. The most common materials are highlighted in bold. For redundancy, values without explicit citation come from Reference [67].	37
2.2	Inductance value formula for planar coil.	41
2.3	Inductance value formula for 3D On-Chip shape coil for PCB design.	42
2.4	Coefficient in order to calculate these 3D On-Chip Spiral Coil.	43
3.1	Differences between technologies: NFC vs RFID vs Bluetooth	79
5.1	Comparison between traditional WPT and a M-WPT system.	127
5.2	Parameters of the system proposed.	128
6.1	Internal values of the memristor model.	145

6.2	Circuit Parameters in reference to the Chua's circuit.	157
6.3	Parameters of the system proposed.	168

Declaration

I declare that this thesis is a presentation of original work and I am the sole author. This work has not previously been presented for an award at this, or any other, University. All sources are acknowledged as References.

Signed ...  ... (candidate)

Date ... March 4, 2022

Introduction

The use of wireless power transfer (WPT) for many pieces of electrical equipment is seen as a powerful new technology. Delivering power over a long distance is fascinating for the future. Wireless charging is identified as a great substitute for the wiring and batteries on many electrical devices. Wiring gives enough power, but it has the disadvantage of restricting mobility as well as having safety issues. On the other hand, batteries offer great mobility but have an initial high cost and limited life [1]. For these reasons, research in WPT is very important, and a big step forward has been made in recent years. There are several ways in which energy can be transmitted wirelessly, and they could be classified according to their working ranges, namely the far-field (long distance) and the near-field (short distance) transmission [2]. In the far-field range, the power is transmitted through microwaves, and in practise it has been developed for low-power applications, because of its low efficiency. In near-field range, a magnetic field is used to transfer power between coils in inductive coupling (electromagnetic induction or inductive power transfer, IPT). The coils of the transmitter and receiver combine to produce a transformer and they can transfer power with high efficiency over a very short range (several centimeters).

The WPT systems have a great number of applications (examples shown in Table 1), such as in electrical vehicles, where the maximum mileage run is strictly tied to the battery capacity. Increasing the quantity of batteries in each EV will be immediately reflected in their price. In addition, it is necessary to consider the amount of time spent recharging and the user's anxiety if they run out of power. In order to overcome these problems, fast wireless charging has already

Table 1: Interesting examples of Wireless Power Transfer applications followed by year, power transmitted, frequency, efficiency and the distance achieved.

Laptops	Transport	Medical Devices	E.V.	Autonomous Robot	Power Plants
2017 [11]	2018 [12]	2018 [13]	2018 [14]	2018 [15]	2018 [16]
\approx W	27 kW	\approx mW	3.5 kW	1.5 kW	11.1W
6.96 MHz	25 kHz	13.56 MHz	85 kHz	120 kHz	20 kHz
53.32%	96.7%	17%	96%	80%	0.35%
75 m	85 m	2 mm	20 cm	75 cm	7 m

been applied to vehicles for public transportation in the traditional stations [3]. This type of application is feasible due to multiple stops, waiting times, and short distances between bus stations. Therefore, the WPT has been easily adopted for electrical charging. Moreover, the research on EV wireless charging while driving or parking [4–9] has shown very attractive and market-boosting [10].

Another example is the diffusion of so-called consumer electronics. Portraying the problem of limited duration of battery life, this sector has already seen commercial achievements of these WPT systems, especially for smart-phone chargers [11].

The advantages of employing a WPT system are certainly highlighted in implantable equipment for health care [17, 18] although it is challenging to attain such applications because of the power needed to penetrate a dense medium like the skin. The wireless power delivery eliminates the need for transdermal or percutaneous wires, the latter being cumbersome and prone to infection. Packaged batteries can only power these implants for a fixed lifetime based on functionality and usage [19], with surgical interventions required each time to replace them. The WPT system leads to smaller size and lighter weight or elimination of the energy storage element that reduces the discomfort for the patient. In all these applications, transmission distances play a crucial role in efficiency, and consequently, in the correct functionality of the application. If the EV, the electronic device and the implant are far enough not to receive a certain level of power, they will not be charged, hence will not work.

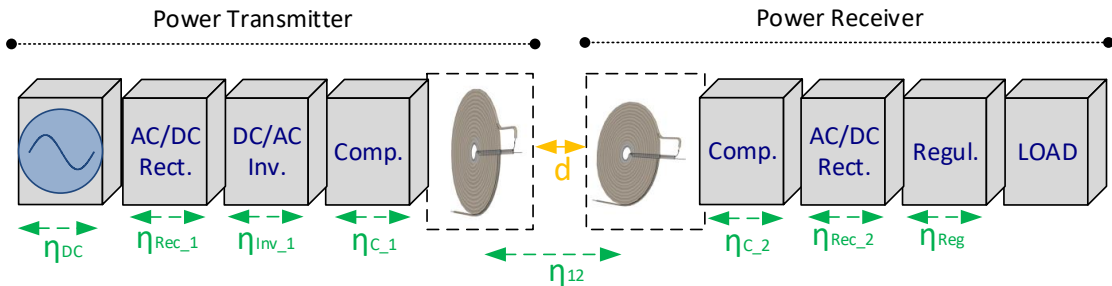


Figure 1: The block diagram of a WPT system with the various efficiencies along the transmission path considering the non-ideal source, AD/DC converter, rectifier and inverter, compensation network and coupling factor. The receiver could be symmetrical depending on the type of load.

0.1 Principles of Wireless Power Transfer

As previously mentioned, the Inductive Wireless Power Transfer (IPT) is the most widely adopted due to its high efficiency. The wireless application must be highly efficient in order for it not to lose power in other types [20]. The block diagram of an IPT system with the various components is shown in Figure 1. The system is composed of two parts: the power transmitter and the receiver. In the power transmitter section, the front-end AC-DC rectifier converts the supplied AC voltage to a direct current (DC) voltage to feed an inverter which produces a high frequency AC power output for the transmitter coil. When an alternating current (AC) is passing through a coil, referred to as the transmitter or primary coil, it generates an alternating magnetic field based on Faraday's law of induction [20]. If another coil, referred to as the receiver or secondary coil, is placed in close proximity with the transmitter, then the alternating magnetic field will induce a voltage in the receiver coil and a current will flow when there is a load connected to the coil. Therefore, power is being delivered inductively from the primary coil to the secondary coil.

A compensation or tuning network circuit is placed before the transmitting and receiving coils as a tuning block for the high frequency AC current, as shown in Figure 1. At this point, the high frequency current flows through the primary coil where it is converted into a high frequency alternating magnetic field and

when it is detected by the receiving coil, it will be converted into a high frequency alternating voltage. In the power receiver section, there is another compensation network that tunes the operating frequency to match the same frequency as the transmitter. If the load to be supplied is a DC battery, then an AC-DC rectifier converts the AC voltage from the resonant tank to a DC voltage, ready for LEDs or rechargeable batteries. In addition, it is often necessary to add a regulator to keep the voltage stable when connected to a battery or load. As shown in Figure 1, the overall system is composed of different blocks with relative efficiency, as indicated in the picture. Only by increasing the efficiency η_i of each block, however, increase the overall η_{TOT} . In general, the efficiencies depend on the power electronic design, the topology of the circuitry, and their parasitic effects.

For this reason, scientific research is focused on improving and maximising the efficiency of section η_i section of the WPT block diagram. By increasing the efficiency, it is possible to also extend the distance between transmitter and receiver. The distance is strictly related to the application, and even low efficiencies could be acceptable if they do not affect the functionality of the application. There is a trade-off between the application and the efficiency of the overall system. The design and the components of each block depend on the application of the electrical devices adopted. However, the magnetic link η_{12} has the most critical value of the overall efficiency and it is strictly related to the distance through the coupling coefficient, k_{12} , value. In the mutually coupled coils (often also indicated with “1” and “2”, primary and secondary, respectively), the higher the coupling coefficient k_{12} between them, the higher the efficiency η_{12} of power delivered to the load. Further consideration of the coil shape design and the other blocks that affect the efficiency are explained in the next chapter.

0.2 Research Motivation

The research on the magnetic field and inductive coupling are recently flourishing because of the vast number of applications. Prototypes and numerous experiments have been created for low power and high power devices. Many solutions, as shown in Table 1, have achieved good functionality. However, an issue then arises on how to identify the receiver to be charged. If there are no receivers, it will be a huge loss of power to keep wireless transferring power in the air. Therefore, another question is also raised on how to synchronise with a receiver and commercially start a payment service.

During the PhD research studies, I have been participating in Institution of Engineering and Technology (IET) young professionals meetings with companies in the Cheshire and Merseyside areas. During the activities and talks, there have frequently emerged many concerns around the development of the WPT application. In spite of the relative maturity, most of these applications have no security features and they fail to achieve these standards. Most of the businesses that researched the WPT ideology were unable to bring it to market due to a lack of security in the design of the system. Despite the fact that customers clearly value wireless charging, the power charge will be available to everyone, not distinguishing the authorised and not-authorised receivers. It is also necessary to develop a web server application that is connected in real time to a WTP system and has this data available.

Companies came to the conclusion that it is important to transmit data, especially for start-up synchronisation, where it is possible to have an acknowledgement that the receiver is present and it is charging. At the same time, there must be only one receiver, as it will be charged for the time using that service. Therefore, proprietary charging technologies would be unable to have commercial power stations unless wireless chargers were able to synchronise to only one receiver. For the above mentioned reasons, the security of wireless power transmission must be

improved to achieve selective transmission.

0.3 Research Objectives

The WPT market growth for 2019 has exceeded 1 USD billion. By 2022, wireless power is expected to achieve an aggressive growth of over 5 USD billion [21], although this is slowed down by the COVID-19 pandemic. It will most likely continue to be dominated by the consumer market, though it has the potential to expand to include the industrial and automotive markets. This future potential is related to emerging security issues.

At present, the Near Field Communication (NFC) is the most secure and widely used bidirectional WPT system. NFC is an inductive near-field WPT technology and adopts a set of international standards for portable devices. It allows the establishment of peer-to-peer radio communications, and the transfer of data between devices. NFC allows us to achieve a myriad of benefits, such as Google Wallet and other forms of contactless payments and identification. Therefore, all the research efforts are focused on the use of NFC for security improvements. The objectives of this thesis research are summarised as follows:

- Identify the technology used in for wireless power transfer and find the most secure existing product.
- Study the state-of-the art for NFC technology, list the advantages, disadvantages and propose alternative solutions.
- Study and research the memristor as a circuital element and its behaviour, and then adopt the memristive Chua circuit to produce chaotic behaviour and implement it in an NFC.
- Sensibly find the circuit parameters and propose new typologies of circuits which can be adopted in NFC.

- Sample the chaotic behaviour produced in these circuit and create a true number generator in Python.
- Adopt Python to create a HTML website and a database which can receive chaotic numbers in real time from the NFC.

0.4 Scope of the Thesis

In this part, a general overview of the WPT technology will be presented and discussed, including the motivations and objectives of the research in this thesis. An introduction and layout of research points in each chapter is provided as follows:

Chapter 0: Introduction. The research motivation and objectives of the thesis are introduced in this chapter.

Chapter 1: Types of Wireless Power Transfer. In this chapter, a comprehensive overview of the different types of WPT is provided.

Chapter 2: Inductive Power Transfer. The circuit theory and principles behind the coupled coils are first studied to show the advantages and limitations of different WPT designs. The design of major parts in the current WPT system is then summarised individually. The selection of power sources, compensation networks, and control methods are discussed with respect to applications. The latest developments in WPT applications are shown with a special focus on portable electronic devices and electric vehicles. Technical issues, limitations and potential improvements are discussed for each application.

Chapter 3: Near Field Communication. The third chapter deals with Near Field Communication (NFC) principles and applications. Still based on the WPT, the NFC has totally different applications than just charging functions. Although this is the most secure type of WPT, the NFC still presents security issues.

Chapter 4: Methodology. The traditional WPT uses switches to create an oscillation for the coil/antenna, which is not an efficient solution. This could be

done by self oscillating circuits. We also investigated devices to improve security.

Chapter 5: Memristive WPT. In this chapter, we have introduced the Memristor-based (Memristive) Wireless Power Transfer (MWPT). The system is made of two symmetrical Chua circuits able to transmit power and chaos by modifying the original design with inductors that are mutually coupled. The system has been largely simulated and experimented on to verify its functionality.

Chapter 6: Variety of Memristive WPT. In this part of the thesis, we have proposed, simulated, and experimented with two Chua circuits in chaotic communication with each other. We sampled the chaotic voltages in the receiver using various equivalent circuits for memristors. Additionally, we used an innovative technology called memristive Colpitts oscillator. We altered this circuit by adding mutually coupled inductors and observed the resulting chaos. The advantages of this circuit include the possibility of low-power operation and a higher frequency achievable up to the memristor's operating limits.

Chapter 7: NFC Security Applications. We have also worked on the realisation of a web server application in the Python language which can use the sampled voltage values and use them in real time for encryption purposes. The application can have any algorithm of encryption and use the chaotic data received in real time from the circuit. We have tested the functionality with different experiments and verified the randomness of data obtained by using Security Requirements for Cryptographic Modules FIPS PUB 140-2. The results confirm the true randomness of the data.

Chapter 8: Future work. An introduction to future research of interest and some applications.

Chapter 9: Conclusion. Conclusion of the thesis.

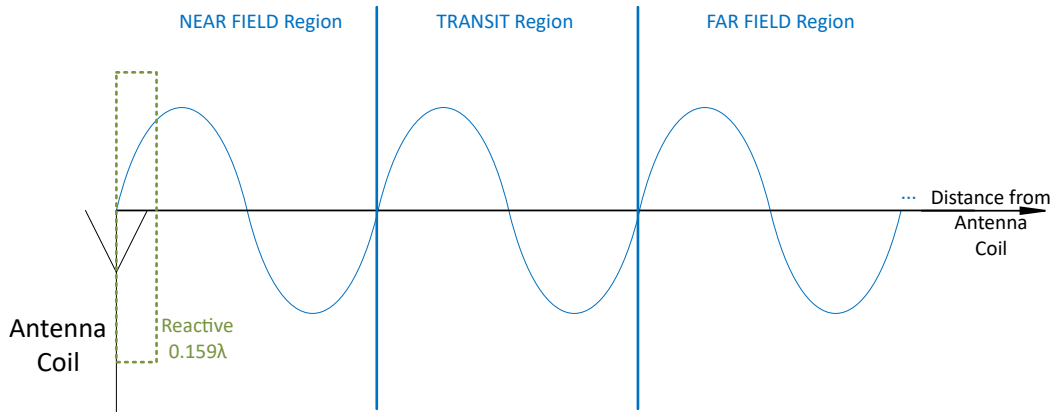
Chapter 1

Types of Wireless Power Transfer

Electrical energy can be converted into other types of energy that can be transmitted through a particular medium without the use of conductive wires. The use of radio waves to transmit information, such as sound, video, and data, is a clear example of transmitting energy wirelessly. In a radio station, a voltage signal reflecting the information is produced and then converted into an electromagnetic energy pulse, which is broadcast into the atmosphere, where it spreads in all directions. An antenna detects the electromagnetic energy signal at a lower energy frequency. This signal is then converted back into an electrical voltage signal from which the information is derived.

Depending on the distance between the transmitter and receiver, the power can also be converted into energy and then transmitted. Electromagnetic waves are generated in the surrounding media by any electromagnetic field source (point particle, dipole, antenna, or coil). The electromagnetic waves are distinguished by the properties of the fields and how these are associated with the medium in which they are travelling. These fields are normally divided into two types: the near-field and far-field, based on their distance from the source and, more specifically, the characteristics of the dominant waves in this area.

In addition, the near-field electromagnetic waves can be further subdivided into the Reactive (non-radiative) and the Radiative regions. The Reactive is

Figure 1.1: Region partition depending on the wavelength λ .

Range - Frequency	1 GHz	100 MHz	10 MHz	1 MHz	100 kHz	10 kHz
Reactive Region [m]	0 ~ 0.05	0 ~ 0.48	0 ~ 4.77	0 ~ 47.7	0 ~ 477.5	0 ~ 4775
Radiative Region [m]	0.05 ~ 0.3	0.48 ~ 3	4.77 ~ 30	46.6 ~ 300	477.5 ~ 3k	4.7k ~ 30k

Table 1.1: Theoretical maximum distance reachable by the WPT in Reactive and Radiative Region.

based on the magnetic or electric field, similarly to the electrical components. The Radiative is based on antenna functionality and where an electromagnetic (EM) wave is propagating in space. The wavelength of the field source is normally used to define these limits, as shown in Figure 1.1. As a consequence, an EM wave's wavelength, which is proportional to its energy, defines how it interacts with the surroundings. Its limits depend on the wavelength, λ [22], as shown in Table 1.1. The boundary of the radiative region is about 1 wavelength, and up to 2λ where a transition region takes place. When exceeding the 2λ distance from the transmitter, far-field area starts.

The reactive (non-radiative) region is on the very short range of $\lambda/2\pi$, and it is based on the capacitive or the mutual inductance effect of the antenna. In Figure 1.2 are shown examples of Far-Field WPT and inductive Near-Field WPT. There are used two terms to indicate the distance of the transmission: short-range and mid-range. The short-range refers to a transmission wavelength that is less than

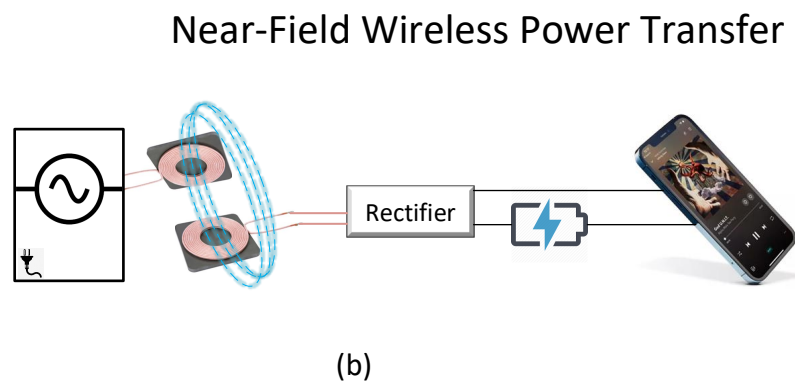
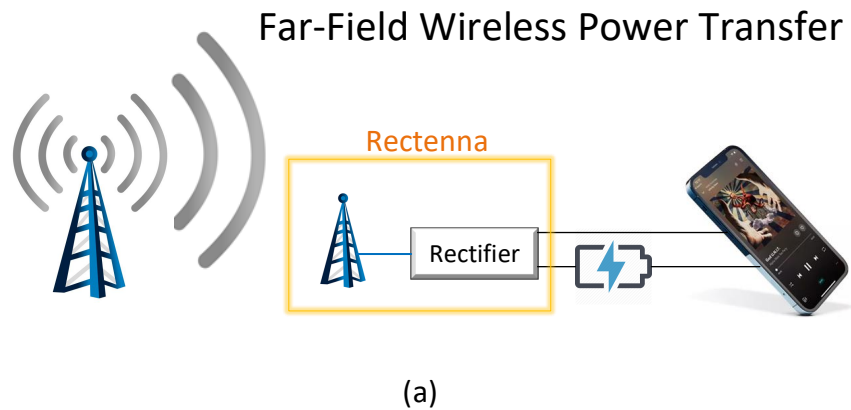


Figure 1.2: Representation of Wireless Power Transmission: (a)Far Field WPT where the Rectenna is highlighted, and (b)Near Field WPT.

the transmitter's geometry. The mid-range describes a condition in which the transmission gap is at least two to three times the size of the equipment involved in the power transfer[23].

1.1 Far-field Wireless Power Transfer

In the far-field range, the power is transmitted through microwaves, and in practice it has been developed for low-power applications, due to its low efficiency. However, despite the low intensity, the light rays are able to transmit the power. For instance, Sun rays can generate large amounts of energy in spite of travelling enormous distances (Figure 1.3). Similar to the other far-field sources, the power generation occurs in specific conditions, such as high sun exposure. A great use of this technique are the solar farms in large areas of Saudi Arabia, which are able to

generate nearly the same level of electricity per year compared to the traditional power generation stations [24–27].

However, in this example of power transmission, we are using the sun as a transmitter, which is a free inexhaustible source of energy. For this reason, most of the time the Photo-voltaic is often classified as Energy Harvesting rather than transmission. The most common far-field transmission are the Radio Frequency (RF) signals, which are continuously used to broadcast information in radio and television.

1.1.1 Microwave Coupling

The RF signals have powered very low power applications, and it is more considered as a harvesting energy solution. The ultrasound waves and vibrations are also utilised in similar applications. The waves are converted through the piezoelectric effect, and the system is considered as energy harvesting from the environment (similarly to the sun rays). Microwaves are electromagnetic waves of frequencies ranging from 1 to 30 GHz. They are widely used in today's applications, especially in communications. Microwaves, differently from radio waves, can be sent in narrow beams, allowing the transmitter to concentrate its energy on the receiver. Microwaves are emitted or radiated from an antenna fed with a high frequency current, and received in low power applications, such as mobile phones. Another antenna will then pick up the microwaves and transform them back to an electric current.

The conversion of microwaves back to electricity was the biggest barrier to overcome in order to convert back the highest amounts of power. When an antenna detects a microwave signal, it generates an alternating current of the same frequency as the microwave signal and equal to the microwave's signal strength. Since all applications and devices run on either an AC voltage of 50 Hz or 60 Hz or a constant DC voltage, the microwave antenna's high frequency current must

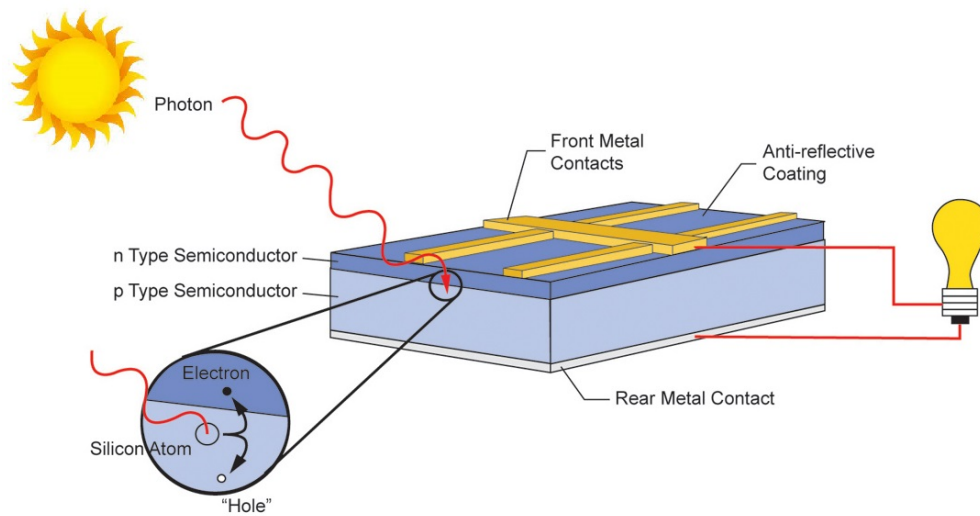


Figure 1.3: Photovoltaic electric energy production: sun rays made of photons hit an n-doped semiconductor which generates both majority (electrons) and other minority carriers.

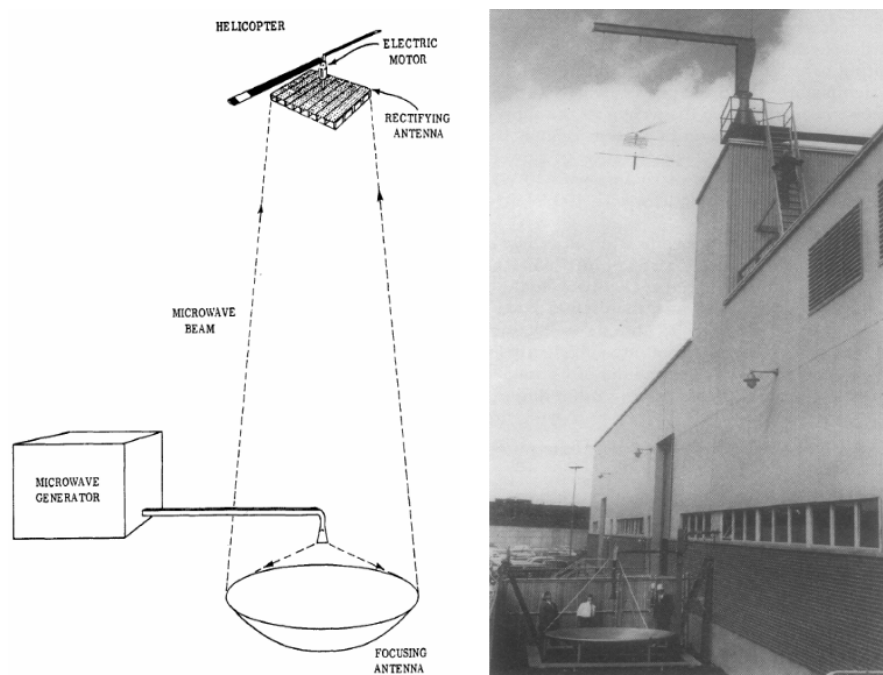


Figure 1.4: W. Brown experiment in the invention of the rectenna or rectifying antenna: an helicopter is supplied with electric power from a microwave beam [28].

be converted to a suitable voltage type. A great development of this technology was the invention of the rectenna or rectifying antenna (shown also in Figure 1.2) by W. Brown in his experiment supplying an helicopter with a microwave beam (Figure 1.4) [28]. Using a rectifier, the rectenna converts the microwave antenna's high frequency current into a DC voltage. Further advancements in the semiconductor technology coupled with the availability of Schottky-barrier diodes resulted in higher efficiencies, higher power capabilities and smaller rectenna designs[29].

1.2 Near-field Wireless Power Transfer

The two most common techniques of wireless power transmission are Inductive Power Transfer (IPT) and Capacitive Power Transfer (CPT). The most popular is IPT, which is suitable to a wide range of power levels and gap distances. CPT, on the other hand, is limited to power transfer applications with short gap lengths owing to voltage development restrictions. Despite gap distance constraints, CPT has been demonstrated to be feasible in kilowatt power applications.

1.2.1 Capacitive Power Transfer

The first methods of electromagnetic coupling were discovered by Tesla in the 1900s [30], by capacitive coupling, which is possible to use the electric field for power transfer in the near-field. However, there was a high voltage present between the transmitter and receiver, which could result in electric shock as shown in Figure 1.5. The main reason is that the experiment was based on the electric arc. The two electrodes on the capacitor are the transmitter and the receiver of the power transfer system with the air being the dielectric. During each voltage pulse, the output voltage rises to the point where the air around the high voltage terminal ionises, causing corona, brush discharges, and streamer arcs to emerge from the terminal. This event occurs only when the electric field strength surpasses the air's dielectric strength, which is around 30 kV per centimetre [30]. Because the electric

field is strongest at sharp points and edges on the high voltage terminal, the air discharges begin there. An electric arc discharges by visible light emission, high current density, and high temperature. The voltage on the high voltage terminal cannot rise above the air breakdown voltage because extra electric charge injected into the terminal from the secondary winding simply escapes into the air. Air breakdown limits the output voltage of open-air Tesla coils to a few million volts, but coils immersed in pressurised tanks of insulating oil can attain greater voltages [31, 32].

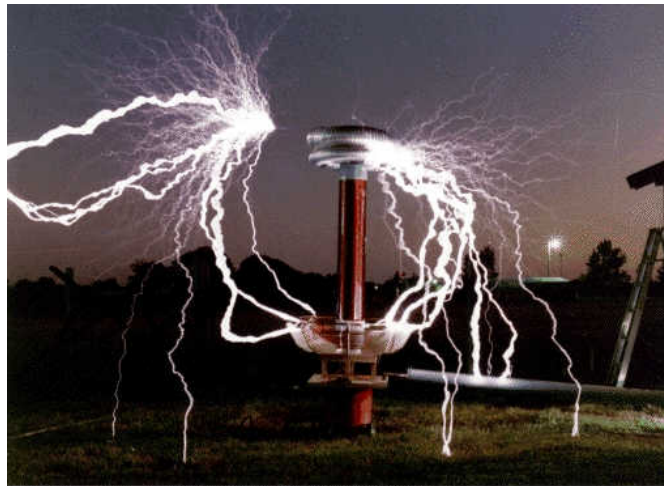


Figure 1.5: Recent demonstration of the Tesla experiment in Reference[30]

The CPT is based on this functionality, where two parallel plates (a capacitor) are on a very small distance apart because of safety issues of the above mentioned electric arc. The transmitter is attached to the first plate on each capacitor, and the receiver is connected to the second plates, as shown in Figure 1.6. Air is the dielectric forming a capacitor of:

$$C_T = \epsilon_R \cdot \epsilon_0 \frac{d}{A} \quad (1.1)$$

where d is the distance and A is the area of the capacitive plate in the transmitter and in the receiver. This value depends on the dielectric material between the plates, distance, and plate area. Therefore, this value is limited because the permittivity constant ϵ_0 of air is as small as $8.85 \cdot 10^{-12} F/m$.

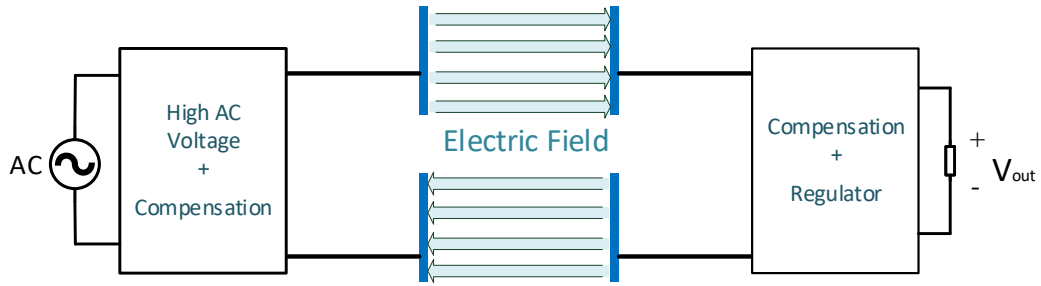


Figure 1.6: Principle of the Capacitive Power Transfer (CPT).

This design can be expanded by adding two connected capacitor plates in both sides (transmitter and receiver) with an electric field between them, as shown in figure 1.6. The created electric field causes an alternating current to pass in the receiver plates. Thus, power is being sent through the secondary plates of the receiver. The capacitive area is designed after the application, where plates can take on multiple shapes, for example, rectangular, disc, or cone, or specific architecture such as a matrix [32].

The amount of power transmitted (power loss on the components is neglected) through the capacitor electric field is thus approximately calculated:

$$P_R \propto \frac{1}{2} \cdot f \cdot C_T \cdot V_T^2 \quad (1.2)$$

where V_T is the magnitude of AC voltage in the transmitting capacitor C_T and f is its frequency. It is important to notice that V_T , f and C_T shall be as large as possible in order to deliver more power to the receiver. However, the larger the V_T and f are made, the more switching losses will occur in the electronics circuit.

1.2.2 Inductive Power Transfer

The use of a magnetic field for power transfer has the safety benefit of not using high voltages and not interacting with most biological material. As a result, the

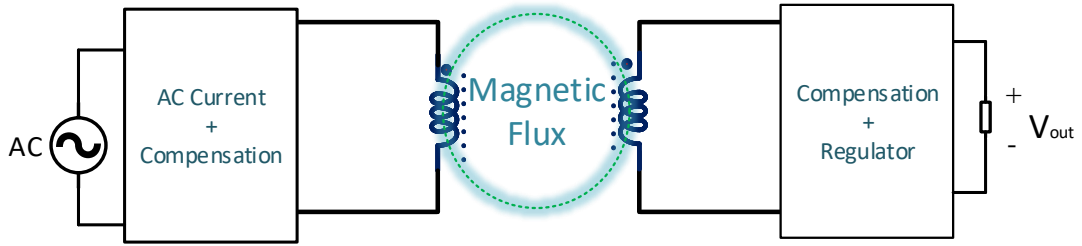


Figure 1.7: Principle of the Inductive Power Transfer (IPT).

magnetic field is used in the majority of modern near-field WPT studies and has a vast range of applications. A non-radiative magnetic field is produced by passing an alternating current (AC) through a coil known as the transmitter, as shown in figure 1.7. When a load circuit is in vicinity to the reactive area, an electromotive force (EMF) is produced in a second coil, known as receiver. In this way, the electrical power is passed from the transmitter's coil to the receiver's coil. There is a mutual inductance between the transmitting and receiving coils. This inductance is one of the most significant parameters that affects the power transmitted in inductively coupled wireless power transfer systems.

The mutual inductance M between two coils, Tx and Rx, is shown in Figure 1.7, where alternating current is guided inside coil, Tx, and induced current appears in the coupled coil, Rx. The current flowing in L_T or the transmitter coil sets up a magnetic field, which passes through the receiver coil L_R giving us mutual inductance. When the inductances of the two coils are the same and equal, L_T is equal to L_R , the mutual inductance that exists between the two coils will equal the value of one single coil (as the square root of two equal values is the same as one single value) as shown:

$$M = k\sqrt{L_T L_R} = kL \quad (1.3)$$

where k is the coupling coefficient expressed as a fractional number between 0 and 1, where 0 indicates zero or no inductive coupling, and 1 indicating full

or maximum inductive coupling. One coil induces a voltage in an adjacent coil; therefore, the transmitter L_T induces a voltage v_R^{in} in the receiver, and viceversa.

$$\begin{cases} v_R^{in} = L_R \frac{dI_R}{dt} + M \frac{dI_T}{dt} \\ v_T^{in} = L_T \frac{dI_T}{dt} + M \frac{dI_R}{dt} \end{cases} \quad (1.4)$$

The amount of power transmitted (power loss on the components has been neglected) through the magnetic field is thus approximately calculated:

$$P_R \propto \frac{1}{2} \cdot f \cdot M \cdot I_T^2 \quad (1.5)$$

where I_T is the magnitude of AC current in the transmitting coil L_T and f is its frequency. It could be noticed from this equation that I_T , f and M shall be as large as possible in order to deliver more power to the receiver. However, the larger the I_T and f are, the more switching losses will occur in a power electronics circuit. The current I_T alone will increase the conducting loss on the transmitting coils. Optimising the mutual inductance M is the most efficient option.

Research studies into the inductive power transfer in IPT has been focused on increasing the yield. Performance and reliability are sure to be improved as new designs, components, such as core, coil shapes and configurations, and ways of handling conductivity, are further researched. Finite element analysis (FEA) is a computerised method to predicting how the magnetic field is distributed in the air and how coils react to real-world forces, heat and other physical effects.

1.3 Comparison between CPT and IPT

The biggest disadvantages of the CPT are the poor coupling capacitance C_T and the safety concerns regarding the V_T , which has a huge value in nearly all the applications. Although CPT is developing quickly [33, 34], it is perceived as only suitable for low power levels over short transfer distances, while IPT is for low to high power levels spanning a larger distance range [35]. While CPT's range

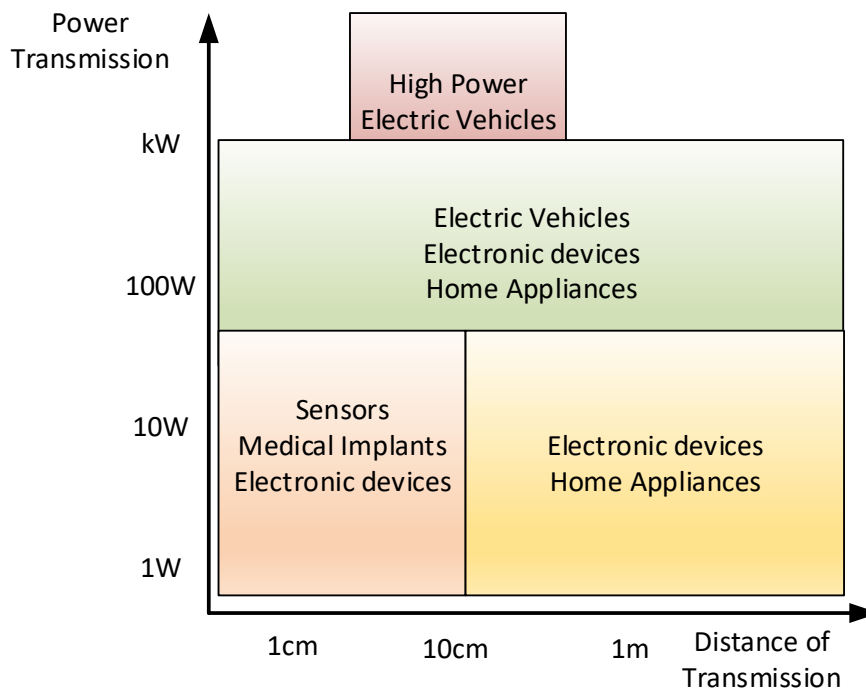


Figure 1.8: Application of wireless power transfer technology listed in levels of power transmission and distance between transmitter and receiver.

has to be restricted to short gap lengths, the safety requirements are the only limitations in terms of power. Up to date, no analytical or empirical study has been done to define the application limits between CPT and IPT, or to provide a recommendation for which concept should be utilised in particular applications of power level, gap distance, transmitter/receiver size, and cost. The applications and power levels classified into groups are shown in Figure 1.8.

A critical comparison between IPT and CPT coupling structures, typical for small gap applications focused on power density, is taken in the Reference [36]. Low-power biomedical devices and mobile device charging are two applications that CPT and IPT have in common. Despite these advancements in power levels, physical restrictions on air gaps typically prevent applications with gap lengths greater than 1 mm. The applications could be classified according to their power level.

- Biomedical implanted devices or sensors are common applications with very low power levels (less than 1 W). These applications have a poor efficiency,

a narrow gap distance, and operate at a reasonably high frequency.

- Consumer electronics, such as mobile phones, televisions, and lights, are examples of low-power (1 W up to 1 kW) applications. Some specialised biological applications may receive substantial power, but it will be less than 1 kW. The efficiency, frequency, and gap distance vary significantly in this range, although short-range high-frequency IPT strives to have acceptable efficiency and cost because it is currently marketed. Longer-range, low-power IPT systems are still being worked on.
- Automotive assembly lines, clean factories, and industrial automation applications in general are among the medium- to high-power level (bigger than 1 kW) applications that have been deployed. Electric car charging research is continuing, and interest in the technology is rising. Due to power electronics constraints, these applications often have a larger gap distance (e.g., greater than 10 cm) and a lower operating frequency.

In the 1.9 figures there are shown the empirical connections between several characteristics of IPT and CPT systems, such as power, efficiency, frequency, gap distance, coupler area, and volume. Over the previous decade or so, the graphs show the overall trends in the development of IPT and CPT separately, as well as WPT as a whole. The power transfer capability vs transmitter-to-receiver gap distance, with data point colour indicating efficiency (red-ish representing the low and blue-ish the maximum efficiency), is shown in 1.9a. The graphic clearly shows that IPT techniques work best in small to large gap areas (i.e., higher than 1 mm), whereas CPT approaches work best in very tiny to very small gap regions (i.e., 1 mm). Despite the fact that IPT appears to have a better power capability as shown in studies, it is clear that CPT power levels are growing. In their respective gap ranges, both IPT and CPT may reach higher than 90% efficiency at kilowatt power levels. The efficiency of the source to the load is shown against the gap distance in Figure 1.9b, with the data point power level denoted by colour (red

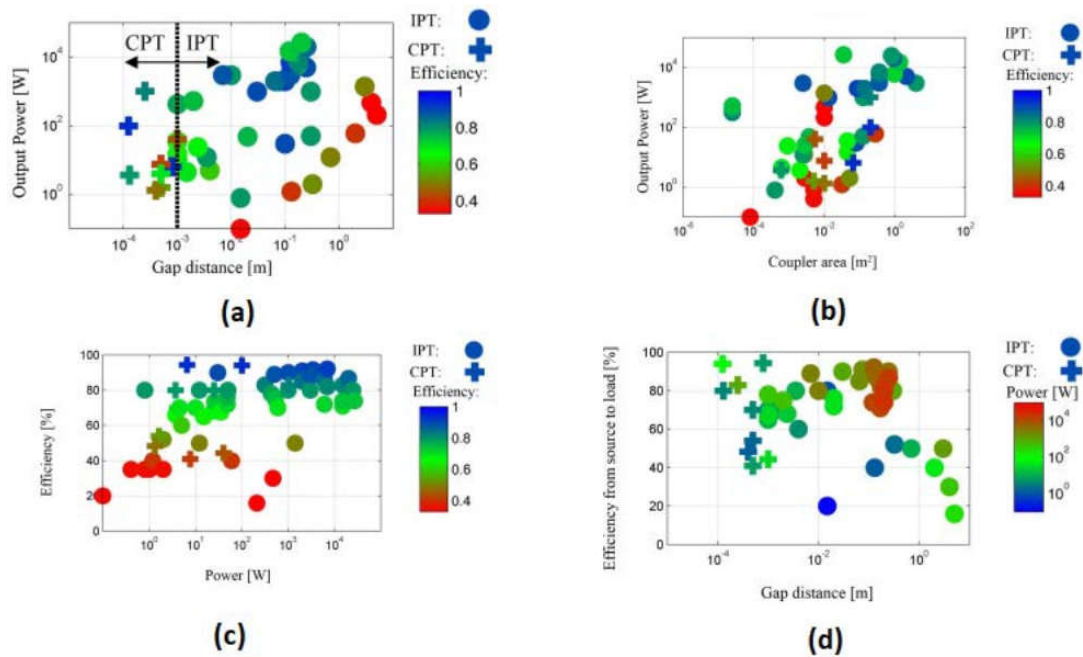


Figure 1.9: Representation of the differences between CPT and IPT in the studies collected from journal articles. The CPT is represented with a cross and the IPT with a circle. The colour of crosses and circles depend on the efficiency of the application. The plot illustrates (a) The output power vs the distance, (b) The output power vs the size of the coils (coupler area) and (c) The output power vs the power. In (d) the plot shows the Efficiency from source to load vs the distance using the power in W as a colour code.

over then 10 kW and blue lower than 1 W). The data in this graph is the same as in figure 1.9a, but the axes have been renamed. CPT is clearly better for gaps of less than 1 mm, whereas IPT is better for gaps of greater than 1 mm. Interestingly, the figure 1.9b shows that CPT is as efficient as IPT for very tiny to small gap applications, if not more so. WPT efficiency decreases as the air gap increases, whereas IPT can sustain 90 percent efficiencies for gaps as small as tens of centimetres. The efficiency vs power level is displayed in Figure 1.9c, with colour representing data point efficiency. While IPT can now transmit more power than CPT, the latter may have an efficiency advantage for applications with similar power levels. The last Figure 1.9d shows the transmitter/receiver area vs throughput power, with data point colour indicating efficiency. The cross-sectional region through which magnetic or electric fields transmit energy is known as the

Table 1.2: Comparison between the Capacitive Power Transfer and Inductive Power Transfer.

	Inductive Power Transfer	Capacitive Power Transfer
Switching frequency	10kHz ~ 10MHz	100kHz ~ 10MHz
Coupling field	Magnetic	Electric
Foreign objects (metal)	Will generate heat	Will not generate heat
Material	Litz wires, ferrites	Copper/Aluminum plates
Cost	High	Low
Safety	Excellent	Good
Size	Small	Large
Misalignment	Poor	Good
Efficiency	Excellent	Excellent
Voltage stress	Medium	High
Power level	High	Medium
Stationary or dynamic	Better for stationary	Both

coupler area. In most situations, the receiver area is specified because certain transmitters have the shape of extended pathways along which a mobile receiver can travel. Larger coupling surfaces are required when output power increases, as seen in 1.9d. Both IPT and CPT fall within this category. The area required for IPT and CPT at equivalent power levels is likewise comparable.

In addition, there is a powerfrequency capability to take into consideration. As a whole, WPT (both IPT and CPT) throughput power decreases in a linear trend (for a log scale) with increasing frequency. It is likely that this limitation is primarily determined by power electronics limitations, rather than coupling characteristics, since it affects IPT and CPT equally. As the frequency increases, the output power is limited by losses. This limitation appears in both IPT and CPT applications. The average power is increased by 10-fold in the last 10 years, with the frequency also increased by 10-fold. In part, this is attributed to the development of wide bandgap devices and the refinement of coupling structures to minimise losses. It is expected that the power-frequency empirical limitation will continue to increase with time, essentially like a Moores Law trend or variant for WPT. In table 1.2, there is a further summary between typical differences in

the development between CPT and IPT.

Summary. This chapter provides an in-depth examination of the many varieties of WPT. The chapter begins with the Far-Field, which transmits electricity via microwaves and was created for low-power applications due to its low efficiency. Near Field WPT employs two techniques: inductive power transfer (IPT) and capacitive power transfer (CPT) (CPT). The most often used technique is IPT, which is applicable to a wide range of power levels and gap distances. CPT, on the other hand, is restricted to applications requiring short gap lengths due to voltage development constraints. CPT has been proved to be feasible in kilowatt power applications despite gap distance limits.

Chapter 2

Inductive Power Transfer

The magnetic field is used to transfer power between coils in inductive coupling (electromagnetic induction or inductive power transfer, IPT). The oldest and most commonly used wireless power technique is inductive coupling. The exposed electric connections might create a short circuit or an electric shock; therefore, induction-based charging is employed as a safety measure. As a result, inductive charging for cordless products, such as electric toothbrushes and shavers, is commonly used in moist environments. The work on the inductive-based charger for electric toothbrushes began in 1968. Emanuel submitted a patent (Figure 2.1a) that demonstrates how to charge an electric toothbrush where the coils resemble more of a tightly coupled transformer rather than a loosely connected pair of coils[37]. The primary coil receives mains power, while the secondary voltage is simply rectified using a full-wave rectifier. In 1992, Inakagata, working for Panasonic Electric Works Co Ltd, in another patent [38] demonstrated how the charger or transmitter design has evolved. Rather than delivering the mains voltage directly to the primary coil, voltage is rectified into DC and inverted into a high frequency AC signal using a Colpitts oscillator. This started the era of the modern, inductively charged toothbrush. Braun Oral-B created the inductive electric toothbrush and its charger, as shown in Figures 2.1b disassembled. The battery in the electric toothbrush must be charged on a regular basis. New inductive electric

toothbrushes have many settings and also deploy a mini display. One of them has been torn down and is shown in parts in Figure 2.2, where the charging coil is clearly visible. Because the batteries charge at modest power levels over a lengthy period of time, efficiency is not an issue.

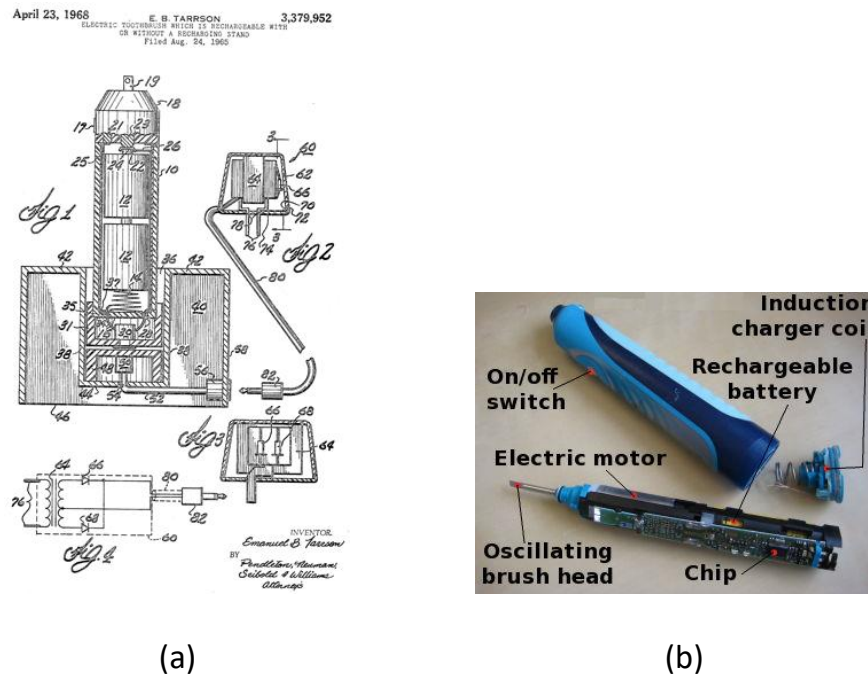


Figure 2.1: Illustration of (a) the first electric toothbrush patent [37] and (b) Braun Oral B toothbrush disassembled.

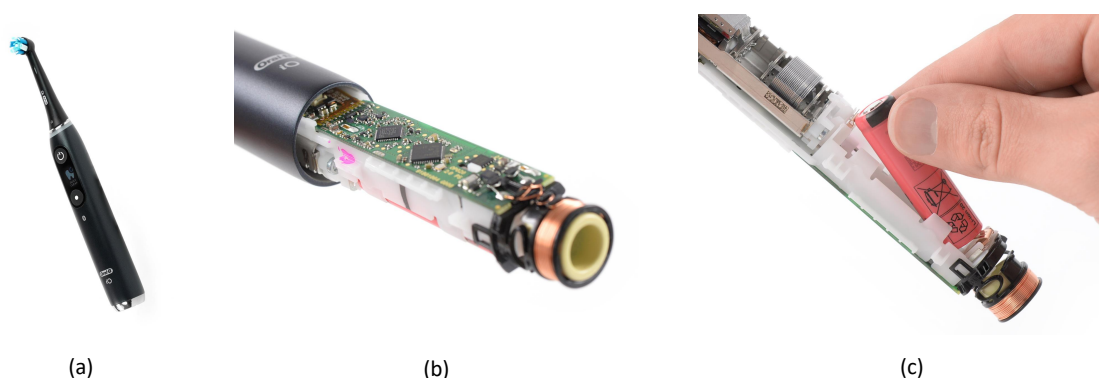


Figure 2.2: Pictures of (a) new generation toothbrush with mini display and in (b) the coil for the inductive power transfer and (c) the battery for inductive power transfer.

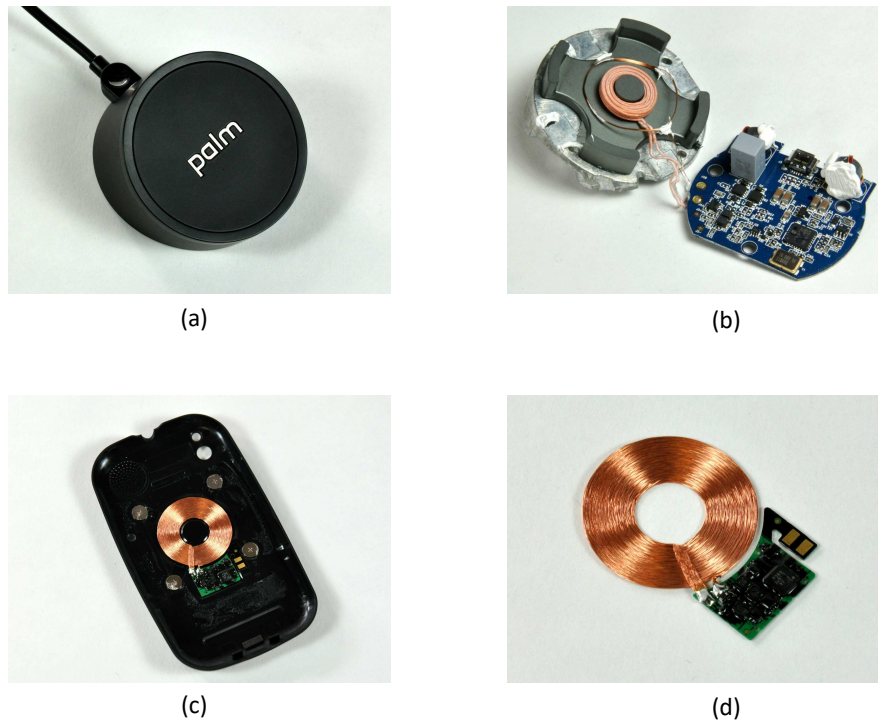


Figure 2.3: The phone charger (a)Palm Inc, (b)transmitter disassembled where is showing the coil and chip, (c)back part of a phone wireless used for charging and (d)receiver disassembled.

Inductive coupling has been extensively studied for charging low-power portable devices, such as mobile phones [39–41]. Palm Inc. (now owned by HP) was the first to offer wireless charging for cell phones. The user would set their phone on a inductive charging pad, and it would charge as if it were plugged in.

The phone charger (transmitter) is shown in Figure 2.3a, and the not-assembly version is shown in Figure 2.3b. Behind the rear cover of the mobile phone (receiver), there is a coil, as shown in Figure 2.3. It is worth noting that magnets are utilised to align the receiver and transmitter in order to produce a high coupling coefficient. For commercial competition, there is no information on the architecture of the internal circuitry that was employed. Because the phone can be charged via a USB connection with a maximum power capacity of 5 W, we can infer that the charger can supply up to 5 W. As more manufacturers released inductive chargers for portable devices, a group of electronics companies formed an organisation in 2008 to develop a global wireless power charging standard that



Figure 2.4: Qi logo in (a)the vent wireless charger and (b)the electrical specs in a phone charger.

would allow devices to be charged by chargers made by various companies.

There have been three major wireless charging organizations. In 2008, the Wireless Power Consortium (WPC) was established [42]. The Power Matters Alliance (PMA) and the Alliance for Wireless Power (A4WP) were formed in 2012. Rezence (pronounced reh-zense) is a wireless electrical power transmission interface standard created by the A4WP based on magnetic resonance principles. A single power transmitter unit (PTU) and one or more power receiver units make up the Rezence system (PRUs). The interface standard allows for power transfer of up to 50 watts across 5 cm. The power transmission frequency is 6.78 MHz, and depending on transmitter and receiver geometries and power levels, a single PTU can power up to eight devices.

In 2010, WPC proposed a Qi standard based on magnetic induction charging, and years later included the resonant mode. The WPC standard known as Qi' (pronounced chee') is represented by the logo displayed in many wireless charging devices in the front, as shown in Figure 2.4a or in the back, near to other electrical information. Many Android phones have started to support Qi 2.4b. In 2015, the A4WP and PMA united to become the AirFuel Alliance [44]. In September 2017,

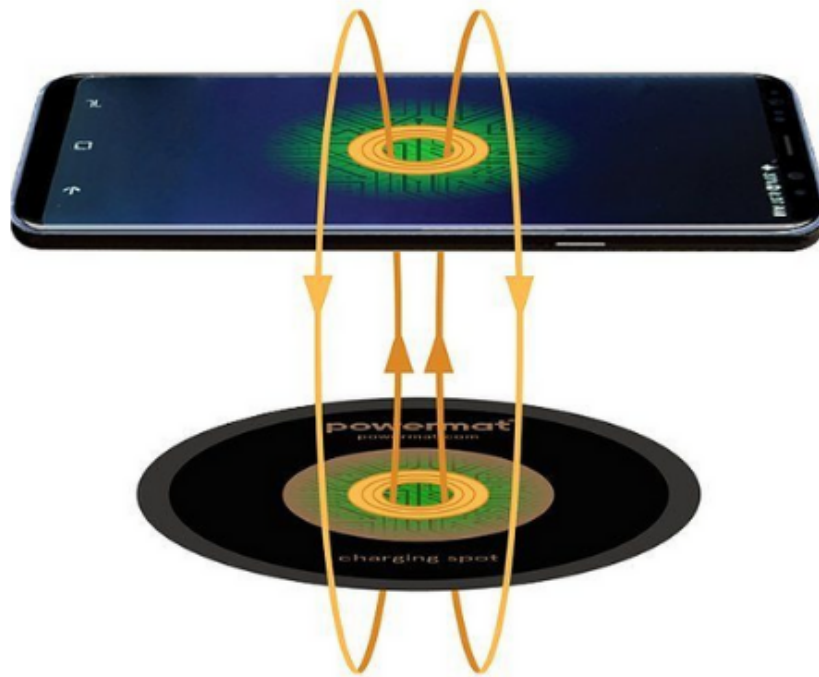


Figure 2.5: Powermat Technologies is a global provider of wireless charging platforms and the first to bring wireless power technology for mobile phones to consumers worldwide[43].

Apple stated that the upcoming iPhone 8 and iPhone X models will feature Qi, which has become the only unified wireless charging standard for mobile phones after Apple joined WPC [45].

Several trial deployments of public charging services have occurred in recent years. Starbucks began utilising resonant technology from Powermat [43] (shown in Figure 2.5) to distribute wireless chargers in selected shops in the United States in 2014. At the beginning, Powermat utilised the PMA standard, but in early 2018, it joined WPC to adopt the Qi standard. A charging kiosk was created by ChargeItSpot [48] and has been used by clothing retailers like Under Armour. A4WP wireless chargers have been implemented in Taiwan by InforCharge [49].

Aircharge, one of the numerous charging service providers, provides a Qi wire-

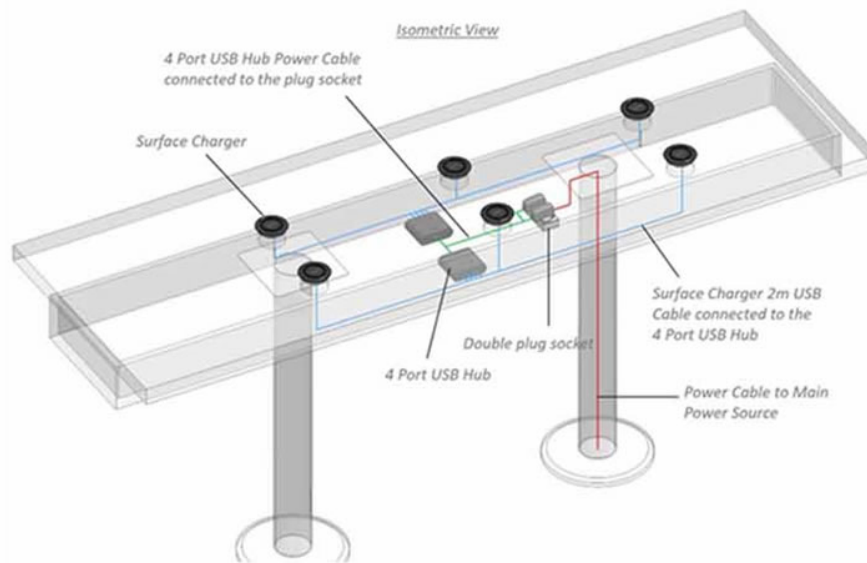


Figure 2.6: The Aircharge wireless charging outlets on the community tables are perfectly integrated into McDonald’s furniture décor, allowing customers to top up their devices while having a meal or drink without having to bring a cable or struggle to reach power plugs [46].

less charging service for McDonald’s in London[46] shown in Figure 2.6. ChargeSPOT, a Hong Kong-based company, has just launched a power bank rental business at airports in Hong Kong, Japan, and Malaysia[50]. The growth of public charging services has several major issues: consumers cannot readily identify charging sites, there is no effective way to track charging status, and the free charging service raises company expenditures. An interesting Internet of Things (IoT)-based wireless charging service system has been developed, which is called AnyCharge [47]. The charger is connected to an IoT gateway through Wi-Fi using a secure auto-connection algorithm, and the gateways are linked to the cloud server using message queue telemetry transport. The administrators can monitor and control chargers using the management platform. In addition, Android and iOS apps have been created to allow users to locate free chargers and find the shortest route to the nearest charging point. The system has initiated a large-scale experimental

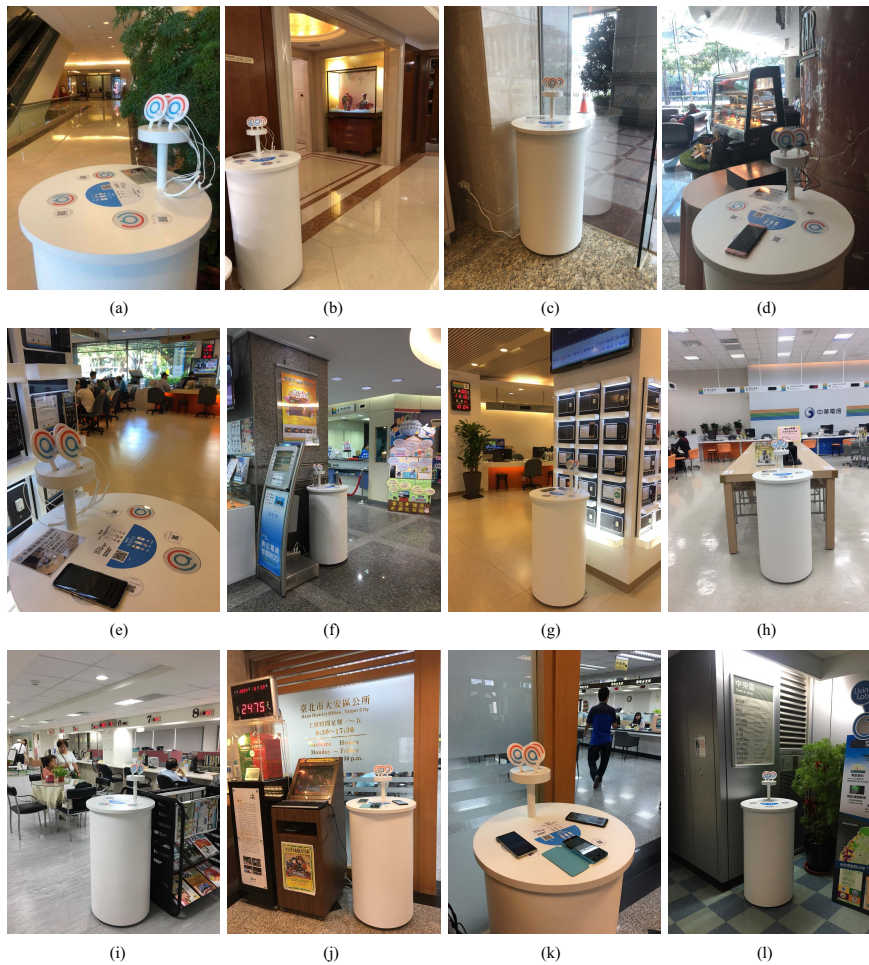


Figure 2.7: Anycharge positions in many locations in different cities (a)-(l). Photographs of charging stations that have been built in various locations. The first row's stations ((a), (b), (c), (d)) are installed in hotels, the second row's stations ((e), (f), (g), (h)) are located in shopping centres, and the third row's stations I (j), (k), (l)) are installed in city offices [47].

deployment in Taiwan, Thailand, Singapore, and Japan, as shown in Figure 2.7. This is a typical example where a WPT system needs to communicate in real time with a web server application.

As mentioned in the previous chapter, wireless charging technologies offer great solutions for electric vehicles (EV). Inductive charging [51–56] and capacitive charging [57–61] are two near-field charging technologies for EVs. However, for the reasons mentioned in the previous chapter, inductive charging is the preferred wireless technology at the moment. One of the most important concerns in these systems throughout both the design and operating stages is the max-

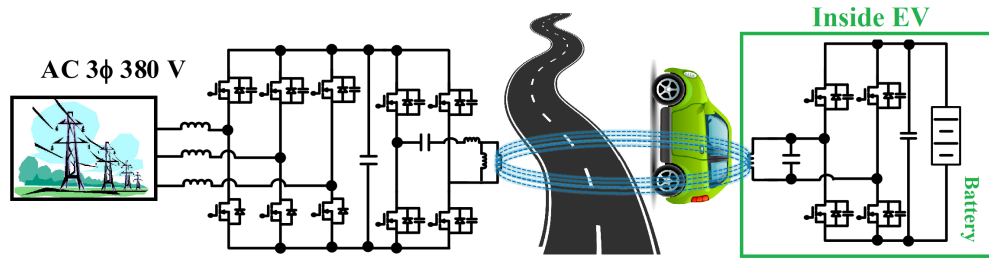


Figure 2.8: Typical schematic for a 3 phase EV inductive charging.

imisation of power transmission with high efficiency. This is accomplished by controlling the switching frequency and conversion ratio of the primary-side converter (i.e., the high-frequency (HF) AC-AC converter at the transmitter pad) as well as the secondary-side converter at the same time (e.g., full-bridge, dual-active bridge DC-DC converter, etc., at the receiver pad). The power could come straight from 3-phase transmission lines as shown in Figure 2.8. The development of an appropriate power pad for the magnetic link is one of the most important steps in the creation of a reliable and efficient WPT system for charging EV batteries. Furthermore, regulating the EV power bus voltage is critical for achieving a long battery lifespan [51, 53, 56].

Magnetic resonant charging [55, 58] is more effective than simple inductive charging. By adding compensating capacitors, we can minimise the reactive power and increase the efficiency, resulting in a large transmission distance capability (i.e., 1 to 5 m). The power delivery range attained can be as high as 100 kW [55, 58]. The forms of charging technologies, shown in Figure 2.9, that can be implemented in our living environment in four successive domains are as follows:

- basic residential systems in home garage or driveway;
- parking spaces in shopping centres or large areas;
- on-street parking in city centres main roads;
- dynamic charging systems (future technology for roads) where roads such motorway will have lanes dedicated to the charging while driving[55, 62].

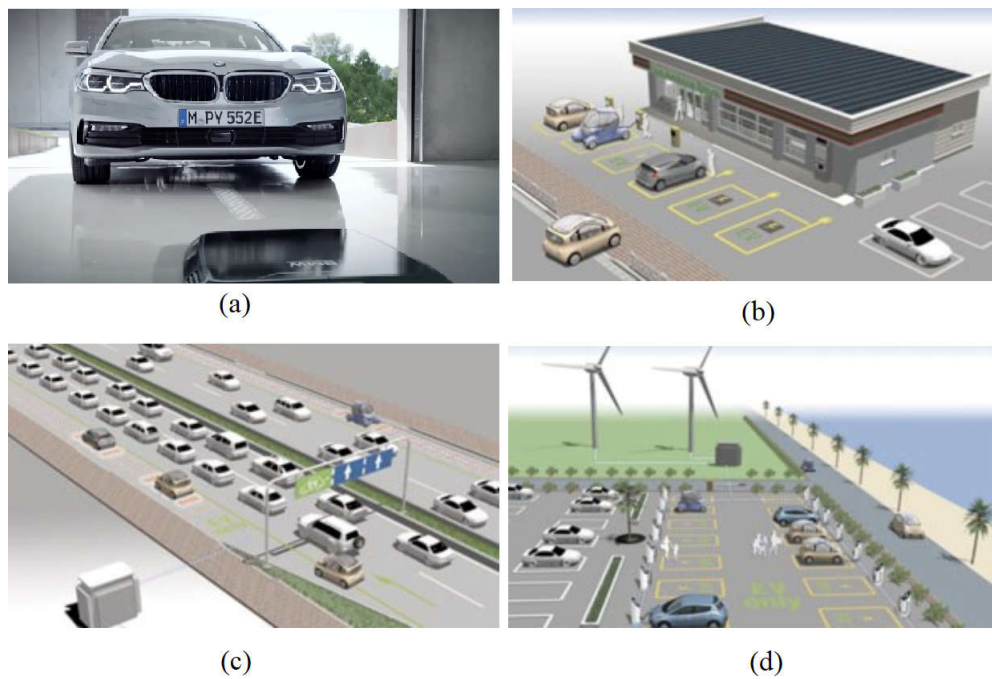


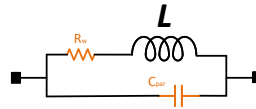
Figure 2.9: Forms of charging technologies that can be implemented in our living environment: (a) basic residential systems in home garage or driveway; (b) parking spaces in shopping centres or large areas; (c) on-street parking in main roads of the city centres ; (d) dynamic charging systems (future technology) where roads such as motorway will have dedicated charging lanes while driving[55, 62].

Solutions adopted for the first domain seem more achievable in the private sector, such as companies and car manufacturers. On the other hand, domains from two to four require government assistance. For example, the United Kingdom has approved a €300m investment spree to help triple the number of ultra-rapid electric car charge points across the country [63]. These involve the option of wireless charging options for streets, commercial vehicles like ride-sharing cars, delivery trucks, and so on. Additionally, the Oak-Ridge national laboratory (ORNL) recently showed a resonant inductive charging system with a 120 kW output, which is comparable to a Tesla supercharger [64]. It can transfer a large amount of electricity (100 kW) across a short distance (one metre) with a high efficiency of 90%. Electric vehicles may be charged automatically using wireless charging pads buried beneath highways thanks to a dynamic system. To reduce the cost and complexity of dynamic charging, higher-power charging solutions are required. In France, Qualcomm has built a 100-meter test track with a wireless charging system capable of 20 kW [65]. As a result of the potential qualities described previously, magnetic charging has received great interest and applications.

2.1 Magnetic Link Design

From the commercial devices mentioned above, it is important to increase the total efficiency of the WPT system. The efficiency deriving from the magnetic link has the most critical value, as it is related to the application distance and the environment. Coil design is the first step in WPT systems, since it determines the application, level of power transfer, efficiency, and overall performance [66]. Therefore, the inductance is considered one of the most significant factors in the WPT system. The inductance depends on the coil geometry, which includes the size of the resonator, cross-sectional area, length, and number of turns, in addition to the separation between turns and thickness or width of copper.

Inductance with no resistance, capacitance, or energy dissipation can be mod-



(a)

Current	3A	3A	5A	6A	18A	20A (polyimide film)	20A (No Silk)	40A (No Silk)	40A	70A
Strand Size (mm)	0.1	0.07	0.2	0.15	0.05	0.05	0.2	0.1	0.1	0.1
No. of Strands	75	160	25	60	1500	1740	100	1000	1000	2000

(b)

Figure 2.10: The real inductor model has (a) resistive and capacitive effects. (b) The table shows Litz wires size vs the AWG number.

elled as a perfect inductor. On the other hand, the above-mentioned components are unavoidable in real inductors, as illustrated in Figure 2.10a. Losses exist in the core materials, and the wire has a resistance of R_W . In addition, the electric field between the turns causes parasitic capacitances, C_{par} . The coil's self-resonant frequency is determined by the parasitic capacitance and self-inductance. The influence of these elements will be evident at high frequencies, and the AC resistance value will increase owing to the skin effect. As a result, the coils' quality will deteriorate. Due to the high frequency, the current will be focused on the copper conductor's surface, resulting in increased power loss that cannot be disregarded [67]. The ratio of an inductor's inductive reactance to its resistance, R_W at a particular frequency, is its quality factor, $Q = \frac{2\pi fL}{R_W}$, which is a measure of its ideality. The more the inductor's Q factor increases, the closer it gets to the behaviour of an ideal inductor. Although the parasitic capacitance effect is more difficult to calculate, the resistance is:

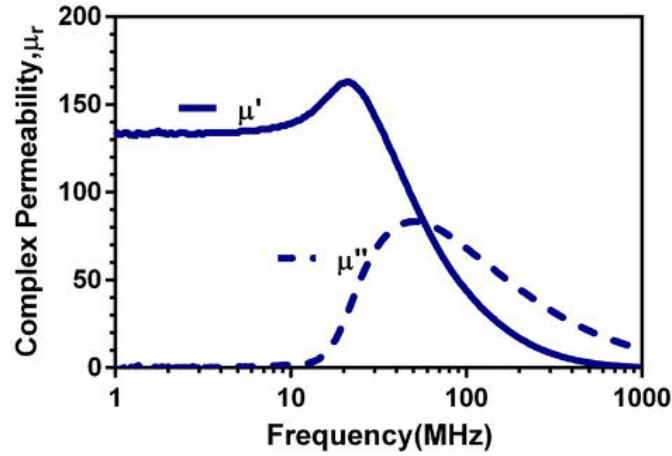


Figure 2.11: NiZn flexible ferrite sheet's relative permeability spectrum.

$$R_w = \frac{Nr}{d\sigma\delta} \quad (2.1)$$

where d is the radius of the wire, r is the radius of the coil, N the number of turns, σ is the conductivity (for copper is $5.6 \cdot 10^7$) and δ is a the skin effect quantity measured in meters:

$$\delta = \frac{1}{\sqrt{\pi\sigma\mu f}} \quad (2.2)$$

which depends on the frequency f . When the frequency increases, the skin effect will be clearer and it increases the resistance and power losses.

The transmitter and receiver coils can be comprised of various components. A magnetic core can be used to shape the flux path, increase the inductance, enhance the coupling and increment the distance. Although air is a "par excellence" medium in WPT systems, it is important to discuss the medium because more applications are trying to adopt other solutions, such as high permeability cores. Similarly to the current, the magnetic flux lines prefer the path of minimum reluctance or high permeability (the opposite of reluctance is permeability). Therefore, to increase the coupling and align the field, the preferred medium to use would be a highly permeable ferrite core (low reluctance). Permeability dispersion is the relationship between complex relative permeability and frequency. Figure 2.11 depicts a typical relative permeability spectrum of a flexible ferrite sheet [68]. The

relative permeability of a frequency-dependent system [69, 70] is given by:

$$\mu_r = \mu' - j\mu'' \quad (2.3)$$

where μ_r is the ratio of the permeability of the material versus that of the free space μ_o . The μ' and μ'' are real and imaginary parts of the relative permeability μ_r , respectively. The ratio between real and imaginary portions is known as the magnetic loss tangent:

$$\tan \delta_m = \frac{\mu''}{\mu'} \quad (2.4)$$

At the specified NFC operation frequency of 13.56 MHz, the relative permeability μ' should be more than 100 and the loss tangent $\tan \delta_m$ should be less than 0.05 to ensure high signal transmission efficiency between NFC devices and improve the transmission range [71]. The composition, microstructure, and morphology of ferrite materials, which are likewise very susceptible to processing conditions, have a significant impact on both μ' and μ'' [72]. Table 2.1 shows a list of the relative permeability of various materials at frequencies lower than 10 MHz where μ'' is equal to zero. The most common ferrite materials adopted are MnZn and NiZn (in the top part of the Table 2.1). The first one has high permeability and high saturation flux density, while the NiZn ferrite has lower permeability and high bulk resistivity. The high-permeability ferrite increases the magnetic energy storage transferred, such as inductance. The ferrite with high bulk resistivity reduces the induced Eddy and displacement currents at higher frequencies, thereby enhancing not only the coupling factor and inductance, but also the power dissipation. This makes the NiZn suitable for use at frequencies above MHz.

A decisive choice is the layout of the coil. Reducing the coil winding resistance is an important step, as it improves the quality factor and link efficiency; thus, the maximum distance achievable. Depending on the operating frequency, the winding conductor can be solid, foil, tubular, or Litz. Solid wire is a building

Medium of transmission	Relative permeability μ_R	Magnetic Field	Frequency
Electrical steel	4000	0.002 T	
Ferrite - MnZn	<i>640</i>		100 kHz - 1 MHz
Ferrite - NiZn	<i>16-640</i>		100 kHz - 1 MHz
Carbon steel	100	0.002 T	
Aluminum	1.000022		
Air	<i>1.00000037</i>		
Concrete (dry)	1		
Copper	0.999994		
Water	0.999992		
Superconductors	0		

Table 2.1: Relative permeability list of many materials. Some of them are peak values, which are obtained for a specific value of the magnetic field H and frequency indicated in the other columns. The value of the μ_R is a curve depending on the value of H . The most common materials are highlighted in bold. For redundancy, values without explicit citation come from Reference [67].

block of many types of wires, such as Litz, and understanding its behaviour is a critical step in the winding design. The power loss inside is due to the high frequency eddy currents induced in it by the varying internal (skin effect) and external (proximity effect) magnetic fields [73]. Because of its low power loss, low cost, and ease of manufacture at high frequencies, mostly above a megahertz, the solid conductor (foil wire) can be superior to other conductors or types [74]. Copper foils with a thickness close to skin depth in the multi megahertz frequency range (Cu skin depth is between 65 and 15 μm in the 1-20 MHz range) are commercially available and affordable. Another way to reduce the AC resistance is the Litz wire (twisting strands): the conductor needs to be divided into multiple insulated skin depth sized strands, with each strand seeing the same amount of magnetic flux [75], as shown in Figure 2.10b. This is a common choice of inductor wire at frequencies up to a few megahertz, above which the need for very thin strands (close to skin depth) makes the manufacturing expensive. The complete coil structures, including the number of turns, layers, distance between them, and existence of a ferrite core, are the design parameters for minimising proximity effects and AC

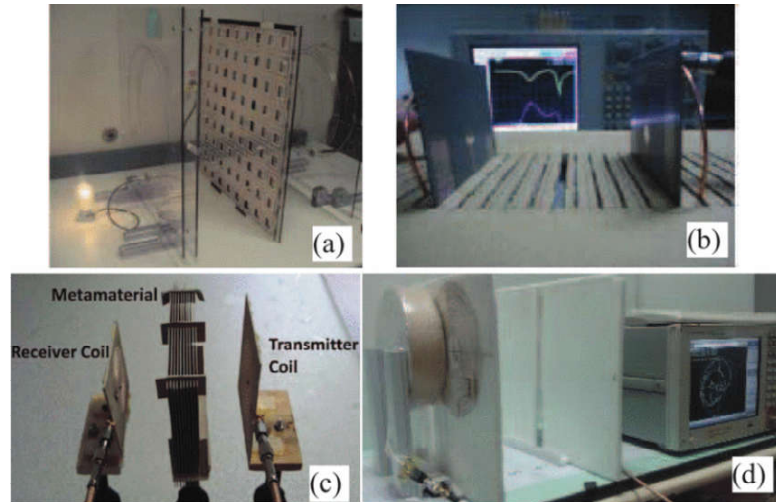


Figure 2.12: Application of metamaterials in WPT in Reference[78](a)-(d).

resistance. Based on the operating frequency range, the required diameter, and the number of wire gauges of the Litz wire can be determined [76]. In addition, superconducting materials were used to decrease the resistance and achieve a high-quality factor [77].

2.1.1 Metamaterials

Furthermore, one of the latest research improvements is artificial materials. An artificial material has been built by the scientific community with *negative permeability* and *negative permittivity* shown in Figures 2.12 from Reference[78]. This meta-material, dubbed "left-handed material," has the ability to amplify evanescent flux lines and focus the electromagnetic field[79, 80]. Therefore, the metamaterials exhibit great potential to enhance the efficiency and range of WPT systems. In [81], Wang and Teo created WPT prototypes with various metamaterial topologies for comparison, and they achieved lighting a 50cm distant 40 W bulb at 27.12 MHz. Later on, Ranaweera et al. in [82] proposed a 3-D left-handed structure, which has been used for mid-range WPT applications at 6.5 MHz, also using three-turn spiral coils with negative permeability. This experiment shows that the power delivered can be improved by 33% and 7.3% in distances, such as 1.0 and 1.5 meters, respectively. Moreover, this paper matches the purpose of

improving the efficiency and distance of WPT systems using 3-D metamaterial topology, although the metamaterials are still a research topic and not largely available. At a distance of 1.5 m, prototypes worked with double 3-D metamaterial plates in proximity of the transmitter and receiver, precisely in the front [83] and back [84] of the coils, showing an efficiency improvement of up to 80%.

2.2 Inductive Power Transfer Coil Design

The design of an IPT system has different steps. After investigating the type of material, the shape of the coil is the most important selection as it will determine the value of the inductance. We start from the power level of the secondary in order to decide the power transmitter. For example, three-phase power sources are used in EV charger applications, whereas single-phase power sources are used in consumer electronics. The IPT design may have more than two coils in order to increase the distance or the efficiency of the overall system. However, as a starting point, it should be the value of the inductance related to the coil shape and the application. Is it possible to classify the results from previous research studies as shown in Figure 2.13 the steps in the IPT geometry design linked to the application. It is also important to classify the coil types and shapes in categories as follows:

1. 2D planar coils could have a circular [77, 85], square [86–88], rectangle [89–91] shape, as shown in Table 2.2. The table also shows the formula for finding the inductance value of different types of 2D inductor.
2. 3D shapes, when the thickness of the inductor becomes not neglectable. Pancake coils [92], planar and on-chip printed spiral coils (PSC) [52, 93–95], as shown in Table 2.3, depend on the shape factors as shown in Table 2.4. Conical loop [96–99] and helix coils [100] are mostly used for charging human implanted devices, bowl-shaped transmitter coils [101], cylindrical coils [102] simply printed on the internal or plastic external ID cover. For EV charging,

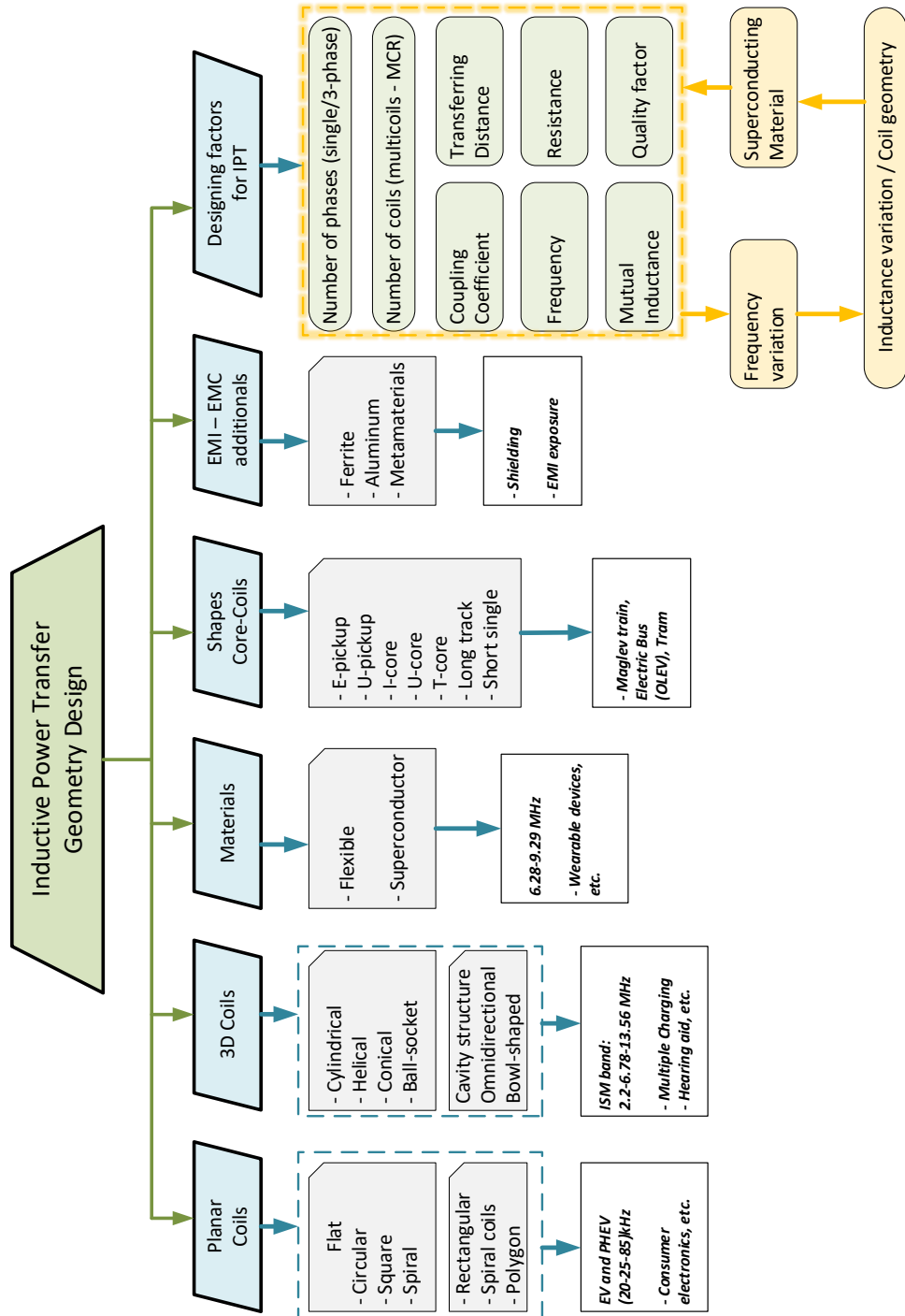


Figure 2.13: Required steps for the coil design in inductive power transfer.

coils shaped in octagon [103] and a double D shape (DD) [104] can be found.

- The materials that coils are made of like ferrites but also other types, for instance aluminum, are used in [105], or superconductors to increase the quality factor of the coils in [106].

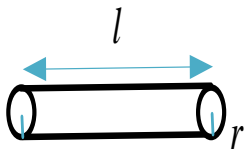
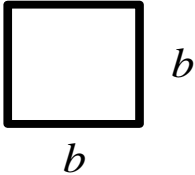
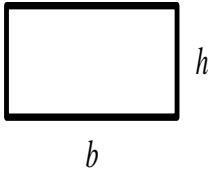
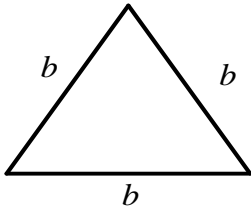
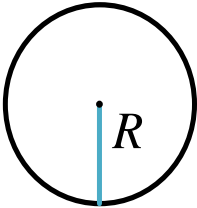
Coil shape	Inductance Formula	Comments
Straight conductor 	$L = \frac{\mu_0}{2\pi} \left[\left(\ln \frac{2l}{r} \right) - \frac{3}{4} \right]$	<ul style="list-style-type: none"> • l: length of wire • r: radius of wire
Square Loop 	$L = 2N^2 \frac{\mu_0 \mu_r b}{\pi} \left[\left(\ln \frac{b}{r} \right) - 0.774 \right]$	<ul style="list-style-type: none"> • N: number of turns • r: radius of wire
Rectangular loop 	$L = \frac{\mu_0 \mu_r}{\pi} \left[-2(b+h) + 2 \cdot \sqrt{b^2 + h^2} - h \ln \frac{h + \sqrt{h^2 + b^2}}{b} - b \ln \frac{b + \sqrt{h^2 + b^2}}{h} + h \ln \frac{2h}{r} + b \ln \frac{2b}{r} \right]$	<ul style="list-style-type: none"> • r: radius of wire
Equilateral Triangle 	$L = N^2 \frac{3\mu_0 \mu_r}{2\pi} \left[\left(\ln \frac{b}{r} \right) - 1.405 \right]$	<ul style="list-style-type: none"> • r: radius of wire
Circular 	$L = N^2 \mu_0 \mu_r R \left[\left(\ln \frac{8R}{r} \right) - 2 \right]$	<ul style="list-style-type: none"> • R: Radius of Coil • r: radius of wire

Table 2.2: Inductance value formula for planar coil.

4. Cores that increase coupling coefficient with an E-shape and U-shape [36, 107] or a dipole [108] deliver power for up to a 7-m distance. Furthermore,

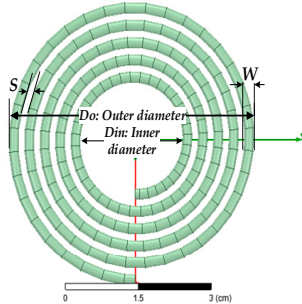
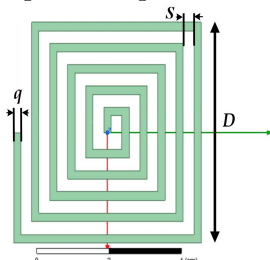
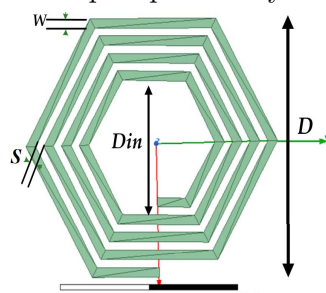
3D Coil shape	Inductance Formula	Comments
Spiral coil (Pancake) 	$L = \frac{N^2 A^2}{30A - 11D_{in}}$	$A = (D_{in} + N(W + S))/2$ <ul style="list-style-type: none"> A: Cross-Sectional area W: Wire Diameter S: Separation two turns
Square Spiral coil 	$L = 27.1^{-10} \cdot \frac{D_{3/8}}{P_{3/5}^{3/5}} (1 + R^{-1})^{3/5}$	where $R = \frac{P}{q}$ <ul style="list-style-type: none"> q: thickness coil P: Separation two turns
On-chip Spiral Layouts 	Depends on layout Table 2.4 $L = N^2 \frac{x_i D_{med} \mu_o}{2} \left[\left(\ln \frac{x_2}{r} \right) + x_3 \phi + x_3 \phi^2 \right]$	where x_i are the layout shape factors in Table 2.4 <ul style="list-style-type: none"> $D_{med} = 0.5(D - D_{in})$ $\phi = \frac{D - D_{in}}{D + D_{in}}$

Table 2.3: Inductance value formula for 3D On-Chip shape coil for PCB design.

in transportation, tracks are used as core. [109–111].

For a quick IPT design it is possible to find plenty of commercial coils. Several manufacturers have already developed specific components for wireless power transmission. One of the pioneers in this area is Würth Elektronik, a specialist manufacturer offering a wide range of coils and windings for wireless power transfer applications. Würth also offers a variety of application circuits that can help electronic designers and enthusiasts become familiar with and familiarise themselves with this relatively new technology, and the components it employs. By using the REDEXPERT online service [112], it is possible to actively choose the coils for WPT application, as shown in Figure 2.14.

Layout of On-chip Spiral Coil	x_1	x_2	x_3	x_4
Square	1.27	2.07	0.18	0.13
Hexagonal	1.09	2.23	0	0.17
Octagonal	1.07	2.29	0	0.19
Circular	1	2.46	0	0.2

Table 2.4: Coefficient in order to calculate these 3D On-Chip Spiral Coil.

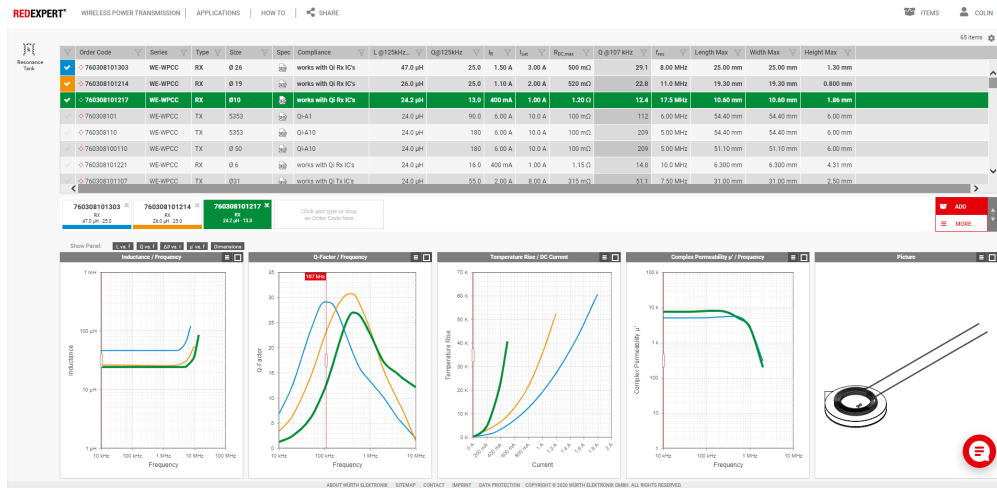


Figure 2.14: Redexpert online tool for choosing the right coil for an inductive power transfer.

2.3 Analysis of WPT system as a two-port network.

After the considerations about the coils shape design which affect the self inductances of the coils, the next sections will explain each component of the WPT system. The next paragraph will contain an analysis of the magnetic link as a two port network. We will investigate the values that are affecting the efficiency. The transmitter and the receiver coil have their inductance values shown in the previous section. The wire of each coil has an internal resistance named R_T and R_R for the transmitter and the receiver, respectively. The coil's parasitic capacitances have been neglected. In addition to the self-inductances of each coil, a third inductance exists between the two coils, which is referred to as the mutual inductance M :

$$M = k_{12}\sqrt{L_T L_R} \quad (2.5)$$

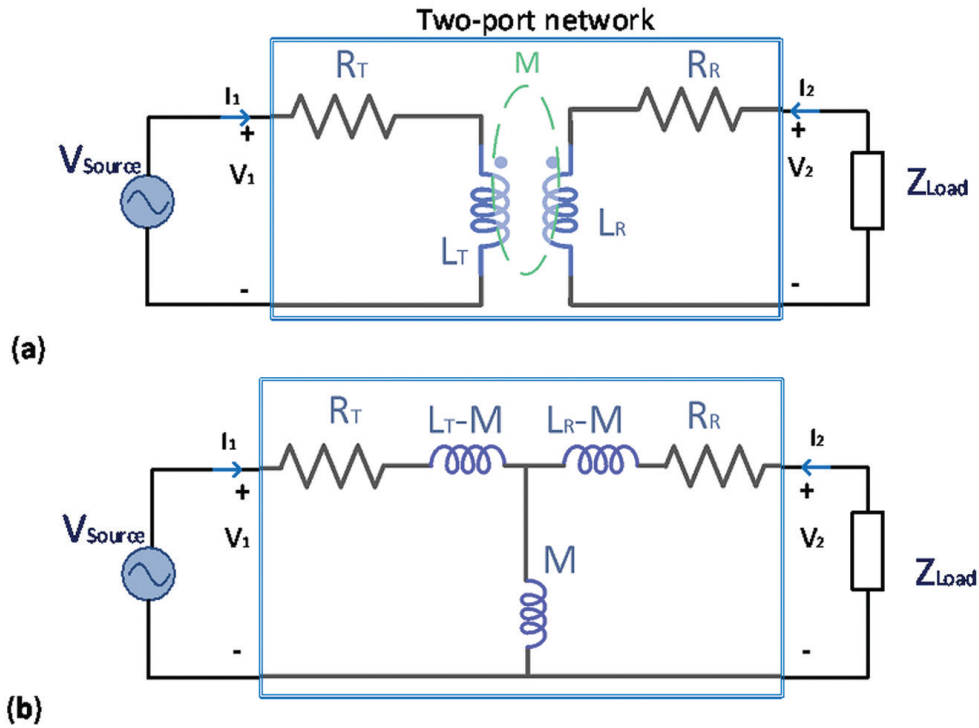


Figure 2.15: A representation of the inductive power transfer in (a) two port network model. (b) Equivalent T-model of the coupled coils in the model adopted.

where k_{12} is the coupling-coefficient and L_T , L_R are self-inductances of the transmitter and receiver coil, respectively. A two-port equivalent analysis allows to find out significant expressions for the efficiency η_{12} . In this case, it will be considered the Z-parameters of the circuit with the parasitic resistances R_T and R_R avoiding other blocks, as illustrated in Figure 2.15. The system is evaluated as:

$$\begin{vmatrix} V_{Source} \\ V_{Load} \end{vmatrix} = \begin{vmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{vmatrix} \begin{vmatrix} I_1 \\ I_2 \end{vmatrix} = \begin{vmatrix} R_T + j\omega L_T & -j\omega M \\ -j\omega M & R_R + j\omega L_R \end{vmatrix} \begin{vmatrix} I_1 \\ I_2 \end{vmatrix} \quad (2.6)$$

where the values for the Z-parameters are taken from the T-model in Figure 2.15. The impedance, as seen by the power source inverter, is a key parameter that directly contributes to the inverter, link, efficiencies of other blocks, along

with voltage gain and maximum wireless power transfer. The input impedance Z_{in} sought by the V_{Source} using the Equation 2.6 can be calculated as:

$$Z_{in} = Z_{11} - \frac{Z_{12}^2}{Z_{22} + Z_{Load}} = R_T + j\omega L_T + \frac{\omega^2 M^2}{R_R + j\omega L_R + Z_{Load}} \quad (2.7)$$

where the first part is the transmitter impedance. The second part of this impedance is an important value and it is also known as the impedance reflected from the receiver. This value is indicated with $Z_{ref,T}$ and is given by:

$$Z_{ref, T} = \frac{\omega^2 M^2}{Z_2 + Z_{Load}} = \frac{\omega^2 k^2 L_T L_R}{Z_2 + Z_{Load}} \quad (2.8)$$

where Z_2 is the impedance of the receiver, which is calculated as addition between the value of the coil's self-impedance plus an additional compensation network not shown in Figure 2.15b. The efficiency or the operating power gain G_P of an electric circuit is the ratio of power transferred to the load (considering the load pure resistive) from the power entering into the network. Thus, this gain is independent of the source impedance and is usually referred to the power transmission efficiency η_{12} .

$$\eta_{12} = G_P = \frac{P_{Load}}{P_{in}} = \frac{|I_R|^2 ReZ_{Load}}{|I_T|^2 ReZ_{in}} = \frac{R_{Load}}{R_T \frac{L_R^2}{M^2} + (R_R + R_{Load}) \left[1 + \frac{R_T(R_R + R_{Load})}{\omega^2 M^2} \right]} \quad (2.9)$$

When the operating frequency ω_0 is high enough, the denominator decreases. The high frequency ω_0 helps to achieve the maximum efficiency by counteracting for low values of mutual inductance M within certain limits. In particular, when:

$$\omega_0^2 \gg \frac{R_T(R_R + R_{Load})}{M^2} \quad (2.10)$$

The power transmission is at its maximum value where η_{12max} results:

$$\eta_{12max} = \frac{R_{Load}}{R_T \frac{L_R^2}{M^2} + (R_R + R_{Load})} \quad (2.11)$$

Equation 2.10 introduces the importance of adopting a relatively high operating frequency at the power capability, which is the most important specification for WPT applications [100, 113]. On the other hand, at higher operating frequency the power level is limited by the topology of power converters, parasitic, switching devices, and related control mechanism. As previously seen in Equation 2.8, the system depends on the type of the load Z_{Load} which in optimal conditions (maximum efficiency) could be found in a derivation of the Equation 2.11 as:

$$\frac{\delta\eta_{12}}{\delta R_{Load}} = 0 \rightarrow Z_{Load,OPT} = R_R \sqrt{1 + k_{12}^2 Q_T Q_R} - j\omega L_R \quad (2.12)$$

Where $Q_T = \frac{\omega L_T}{R_T}$ and $Q_R = \frac{\omega L_R}{R_R}$ are the quality factors of the transmitter-receiver inductances. In order to achieve the peak of efficiency Equation 2.12 and have no reactive power on the load (zero phase angle - ZPA), an impedance matching is required. In the compensation network, there is a capacitive impedance (a capacitor or a more complex circuit) to cancel the reactance ωL_R . More alternatives will be given in the next Section. The formed LC resonant tank will give a pure resistive optimum load:

$$R_{Load,OPT} = R_R \sqrt{1 + k_{12}^2 Q_T Q_R} \quad (2.13)$$

By substituting the resistive optimum load back into the Equation 2.11 and expressed in function of the coupling factor and quality factors, the maximum power transmission efficiency is given by:

$$\eta_{12max} = \frac{k_{12}^2 Q_T Q_R}{(1 + \sqrt{1 + k_{12}^2 Q_T Q_R})^2} = \frac{\Delta}{(1 + \sqrt{1 + \Delta})^2} \quad (2.14)$$

Where $\Delta = k_{12}^2 Q_T Q_R$, which is also called the figure of merit (FoM) of the system whose maximum efficiency can be at least 17% when delta is greater than

1 [23]. The latter condition is referred to as the *strongly coupled resonance regime*, which is completely different from the coupling factor k . This method is used in WPT applications, where long distance is desired in front of an acceptable power delivered. The WPT system is still loosely coupled, but can operate in strongly coupled magnetic resonance regime, only if the quality factors Q_T, Q_R are designed to be enough high. By increasing Q_T, Q_R will keep a relatively good efficiency. Quality factors can reach the value of 1000 or even higher. This value could be achieved by choosing designing coils with a lower inner resistance [52] or a high operating frequency, and this method will be introduced in the next section.

2.3.1 Resonance Technique

A largely adopted technique in the near-field magnetic coupling is the resonance, which has largely extended the potential of the near-field WPT. A capacitor is connected to the coils to form the LC resonant tank. Therefore, an impedance transformation network is made by the resonant tank at the oscillation frequency f_0 , such that the source VA is minimised and the power transferred to the load is maximized. The transmitter and receiver circuitry are made to resonate at the same frequency, as shown in the equation below.

$$f_0 = \frac{1}{2\pi\sqrt{L_T C_T}} = \frac{1}{2\pi\sqrt{L_R C_R}} \quad (2.15)$$

where L_T, L_R are the coils and C_T, C_R are the capacitors of the transmitter and receiver, respectively. By developing high-detailed transmitter and receiver coils, it is possible to achieve a high efficiency device even if the system becomes less efficient. The improvements in technology have helped to minimise parasitic effects and achieve a perfect match of operating frequencies, which has allowed for further increases in the distance between the transmitter and the receiver.

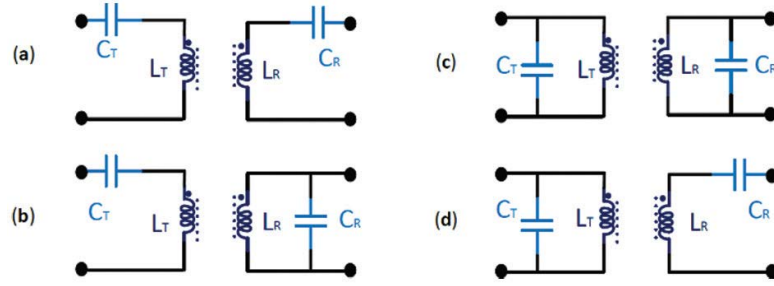


Figure 2.16: The four basic topology for resonance and compensation network, namely a) the series-series S-S, b) series-parallel S-P, c) parallel-parallel P-P and d) parallel-series P-S.

2.3.2 Compensation Network

As previously shown, an important part of the design is the choice of the resonance frequency and the network topology adopted. The chosen frequency needs to be the same in both transmitter and receiver. It is also desirable that current and voltage of the power source is in-phase, minimising the VA rating of the power supply. The easiest way is to make sure that the relationship for operating frequency f_0 is:

$$\omega_0 = \frac{1}{\sqrt{L_T C_T}} = \frac{1}{\sqrt{L_R C_R}} \quad (2.16)$$

$$f_0 = \frac{\omega_0}{2\pi} \quad (2.17)$$

where the capacitors C_T and C_R are additional components that are usually added on both sides to resonate at the same operating frequency. This condition is referred to as tuned primary-secondary or transmitter-receiver. This is done by compensation network, which creates the resonance. The mismatching of the operating frequency, due to parasitic effect, leads to a slight reduction of the efficiency in the compensation network blocks. Depending on the type of the application, there are four basic compensation topologies without considering resonant circuits [115] intermediate coils [116] or other additional capacitance and resistance [117]. These are the four basic topologies shown in Figure 2.16, called the series-series (SS), series-parallel (SP), parallel-series (PS) and parallel-parallel (PP) type of circuits. In general, the secondary coil is chosen to resonate in parallel or series.

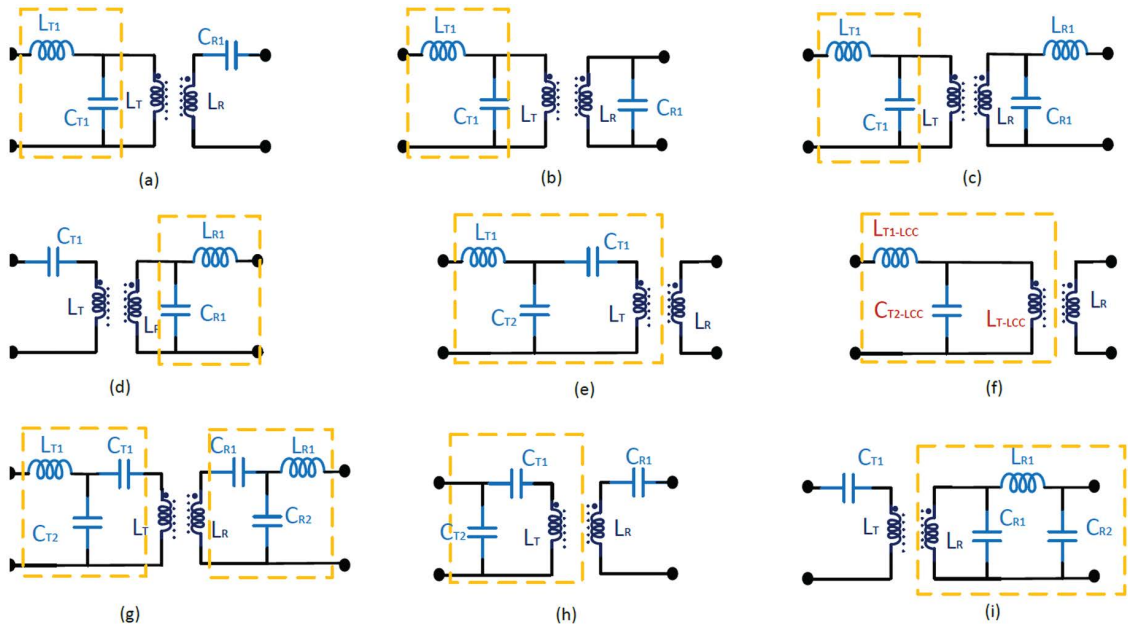


Figure 2.17: Hybrid resonant topologies highlighted: the LCL configuration with the receiver in a) series, LCL-S b) parallel, LCL-P and c) doubled and d) at the receiver S-LCL; e) The LCC configuration and f) the equivalence with LCL when voltage driven [114]. Other relevant topologies such as g) LCC-LCC, h) CCL-S and i) S-CLC.

The parallel-type secondary has voltage output type, which is suitable for large loads. Furthermore, the coil parasitic capacitance can be included in the compensating capacitor in parallel. Nevertheless, the disadvantage is that the resonant frequency depends on the value of the load (for simplicity let's consider the load resistive). On the other hand, the series-type secondary has current output type and is suitable for small values of resistive load. The choice of the secondary compensation are mostly limited on the load requirements. The primary coil could have multiple configuration depending on the number of elements. The additional elements (capacitors and inductances) will be connected with the transmitting coil L_T . The primary series needs a higher current and lower output voltage from the switched MOSFETs. In contrast, the primary parallel demands a higher voltage and a lower output current. In both cases, the higher values of current increase the MOSFET driver losses, and higher voltages increase the MOSFET capacitive losses. Because none of the basic four topologies can provide ZPA for constant

current (CC) or constant voltage (CV) in WTP applications, advanced topologies have been proposed [86, 118–120] in the resonance-compensation network between converter and transmitting coil [121, 122]. In these hybrid topologies, an extra reactance is added to the circuit, which helps for a lower switching loss compared to the S or P topologies. However, the basic four topologies are still preferred for low voltage WPT applications.

Similar to the transmitting side, the receiving side could have several variations, which are referred in capital letters, such as primary-secondary topology. The configuration of circuitries for WPT transfer are reviewed in a few recent papers [123, 124]. The LCL configuration has shown in many articles to be the most used valid alternative to the basic topologies. A very interesting correlation has been studied in [125], where $S - S$, $S - P$ are compared with the $LCL - S$, $LCL - P$, $LCL - LCL$, and $S - LCL$, respectively in Figure 2.17 a, b, c, d. Adopting voltage source inverters, which are widely employed in WPT system, the $S - S$, $LCL - P$ and $LCL - LCL$ topologies have shown a constant current in output, whereas the $S - P$, $S - LCL$ and $LCL - S$ topologies a constant output voltage. For these considerations, the ones with constant current to the load, such as the $S - S$, $LCL - P$ and $LCL - LCL$ topologies, are good candidates for battery charging applications. On the other hand, the $S - P$, $S - LCL$ and $LCL - S$ topologies are suitable for the electric appliances supplied by the power source of constant voltages. In addition, when driven by a sinusoidal voltage at the same operating frequency, the LCC topology as proposed in [114], can be simplified as an equivalent circuit similar to LCL topology. As shown in Figure 2.17 f, the value of $L_{T1} - LCC$, $L_{T1} - LCC$, $C_{T2} - LCC$, could be written in function to L_T , L_{T1} , C_{T2} and C_{T1} in Figure 2.17 e. Therefore, the load characteristic of $S - LCC$, $LCC - S$, $LCC - P$, $LCC - LCC$ (in Figure 2.17 g) is the same as that of $S - LCL$, $LCL - S$, $LCL - P$, $LCL - LCL$ respectively, under steady state at the same resonant frequency [125].

A $CCL - S$ topology introduced by Samanta et al. in [126], shown in Figure

2.17 h, reduces the inverter switch stress by half of the conventional LC parallel resonant tank. Moreover, many other papers [85, 87, 90, 127, 128] compare the characteristics of the double-sided LCC compensation topologies as it is considered the most suitable technology for electric vehicle (EV) wireless chargers. In [129] Wang et al., introduced the $S - CLC$ topology, in Figure 2.17 i, which in comparison with $LCC - LCC$ needs less compensation components, meaning lower cost, smaller dimension, and further greater potential in WPT applications.

2.4 Power converters in Wireless Power Transfer

An advantage of inductive WPT is in small sized applications and medium to high power requirements. As the magnetic link size reduces, the reflected resistance to the transmitter coil gets reduced as well. To compensate for this reduction, the operating frequency needs to increase to keep the power level up. For example, in electronic devices such as phones, wearable, and laptops, the power rating can range from 1W to about few hundred watts. For inductive WPT in the megahertz frequency region, the operating frequency is typically bound to industrial, scientific, and medical (ISM) band of 6.78, 13.56 MHz, and so on. The power converter design in the megahertz region is critical as the dynamic losses increase in the switches. There are several typically used DC-AC power inverters in the megahertz frequency range such as classes A, B, AB, C, D (ZCS and ZVS), and E. The most used inverters in the wireless power transfer applications are on switched-mode class-D and class-E inverters as they deliver the highest efficiencies.

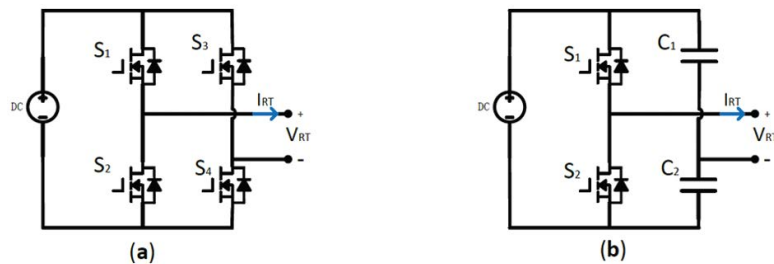


Figure 2.18: Schematic of the (a) Full-bridge inverter and (b) half-bridge inverter.

Due to easy system parameter design, most of the WPT applications adopt Class D full and half bridge inverters [130], shown in Figure 2.18. The Class D inverter employs two switches and a series-resonant LC tank, which results in a lower switching frequency compared to the Class E inverter. This topology can output twice the DC supply voltage to feed the LC resonant circuit; thus being especially suitable for low DC supply WPT applications. Obviously, the Class D resonant inverter with two switches has lower voltage stress across the switch since the peak voltage is as high as the DC supply. In the megahertz frequency range, one of the challenges of class-D inverter is the switch output capacitive losses during S2 turn-on. In recent papers, half-bridge resonant inverter has been applied to the wireless power transfer system with frequency up to 13.56 MHz [131, 132].

The series (S) transmitter coil requires high amount of current that increases switch gate driver losses. On the other hand, the parallel (P) topology reduces the current rating of the switches by circulating it through the resonant tank. However, it produces high voltages across the switches that increase the FET output capacitive losses. A combination of SP transmitter coil would take advantage of low voltage rating of S and low current rating of P coils. Class-E inverter satisfies these conditions with doubled-tuned output circuit [51]. In Figure 2.19, the basic schematic of a class-E inverter is shown. The inverter operates between the series resonance and the one in parallel with the C_S . The capacitor C_S is referred to as the shunt capacitor and it is also an important element to achieve the ZVS and ZDS conditions. Generally, the shunt capacitance C_S is made by the sum of the external capacitance C_{EXT} and the MOSFET drain-to-source parasitic capacitance C_{DS} , but this value is not usually controllable. Additionally, C_S decreases as the frequency increases. Therefore, at high frequencies, C_{DS} is dominant to C_S . As shown in Figure 2.19, the inductance L_F is referred to as the DC-feed inductance. If this inductance is large enough, the input current I_{LF} is approximately constant, which is equal to its DC component.

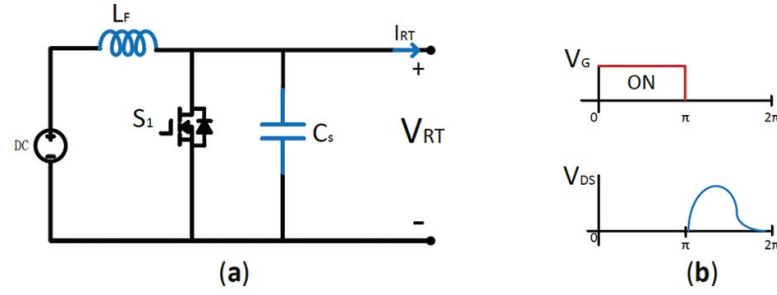


Figure 2.19: The class-E inverter (a) topology before the resonant tank and (b) waveforms of V_G turning ON S_1 and its V_{DS} .

When V_{GS} is high, on the top of Figure 2.19 b then the switch is ON, the voltage across the switch V_{DS} (bottom of Figure 2.19 b) is approximately zero (ZVS: zero voltage switching) and the current flows through the MOSFET. During the switch OFF interval, differences of currents through the DC-feed inductance and the resonant filter flows in the shunt capacitor. Not only can the Class E inverter operate at ZVS, but the voltage across the switch has a zero slope at the instant in which it is turned ON. This is referred to as zero derivative switching (ZDS). ZVS prevents the dissipation of the energy stored by the shunt capacitor when it turns on, and ZDS makes the circuit robust in the face of variations in the components, frequency, and switching instants [133, 134]. Due to this feature, the class-E inverter achieves high power conversion efficiency at high frequencies. Assuming the switch turns ON at $t = 2\pi$, the class-E inverter ZVS/ZDS conditions can be expressed as:

$$V_{DS}(t = 2\pi) = 0 \quad (2.18)$$

$$\left. \frac{dV_{DS}}{dt} \right|_{t=2\pi} = 0 \quad (2.19)$$

Due to its ZVS/ZDS feature, the MOSFET can be softly turned ON and that leads to less switching losses allowing the inverter to operate efficiently with very high frequency (MHz region). However, owing to its resonant operation principle, the device voltage and current stress are relatively higher than that for a full or half

bridge inverter, which threatens the reliability of the device. The switch voltage stress comes from the supply in addition to the inductance and the LC tank. In order to ensure the circuit reliability when implemented in a WPT system in which the load and coupling coefficient are always changing, a switch with a maximum voltage rating of at least four times the input voltage may be required. Therefore, class-E inverter is only suitable for low power and low voltage IPT systems [89, 135–138]. Enhanced gallium nitride (eGaN) device are often adopted to enhance the delivered power in the MHz frequency region [139].

2.5 Rectifiers

An import part in the WPT system is the rectifier, where it is desired to convert as much as possible magnetic field, collected from the coils or antennas, back to electrical power. In very low power solution, the design of the rectifies is crucial. The coil design is unified with the rectifier to build the rectenna. The power efficiency, seen as Power Conversion Efficiency (PCE) in the figure 2.20, is the capability of a rectifier to transform radio frequency energy into DC current. For low power, it is necessary to use very high frequencies to reduce losses. The PCE depends on the diode conduction and reverse leakage losses. The input voltage varies according to the frequency, which means the diode impedance varies, leading to a difference in the performance loss. In low input power, the efficiency is low because the input voltage dynamic is lower or equal to the forward biasing voltage of the diode.

In general, the PCE varies with the input dynamic, which in turn depends on V_j , V_{br} , and R_L , representing the diode forward voltage drop (in the pn junction), the breakdown voltage and the dc load resistance of the rectenna, respectively. As shown in figure 2.21b, the efficiency sharply decreases as the voltage swings, when a diode exceeds V_{br} , the breakdown voltage. The peak efficiency is an optimum between: the forward (junction) loss and the reverse (breakdown) leakage loss.

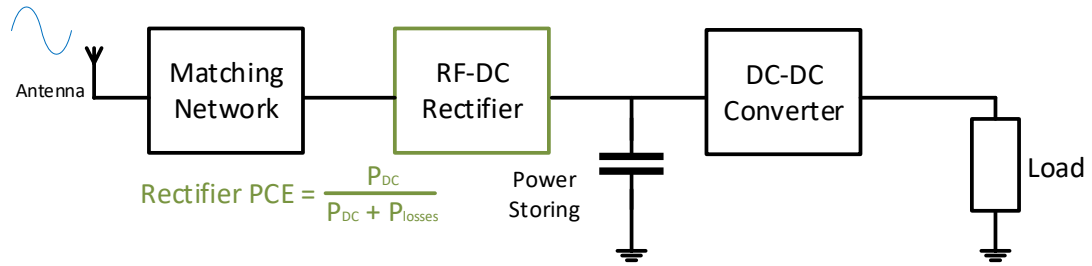


Figure 2.20: A receiver block diagram where has been highlighted the rectifier and its efficiency.

Moreover, the PCE is also affected by the production of higher order harmonics. Diodes produce harmonics and inter modulation as a result of their nonlinear nature, which reduces power conversion efficiency. Due to increased parasitic losses caused by harmonic generation, the power levels are reduced, which in turn limits the performance. As a result, all of the above-mentioned parameters follow a tradeoff depending on the requirements. High threshold voltage diodes are favoured for low power applications, whereas high reverse break down voltage diodes are preferred for high power applications.

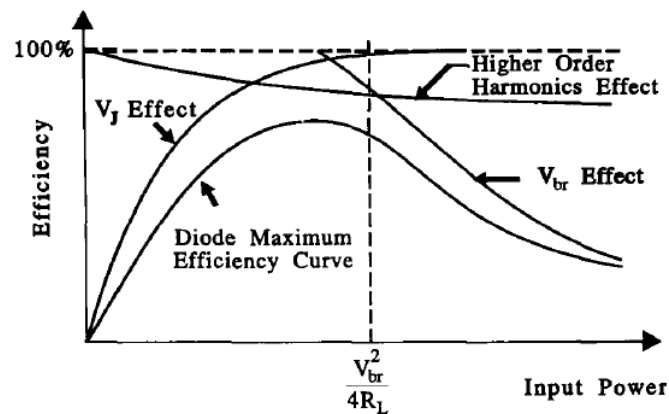


Figure 2.21: Diode efficiency function depends on the breakdown voltage and the load resistance.

2.5.1 Diode rectifiers

Diode-based rectifier circuits are the most common because they have a lower forward voltage drop compared to the CMOS circuits. In rectenna applications,

Schottky barrier diodes are widely used due to offering the best alternative to achieve higher PCE, a diode with a lower forward voltage.

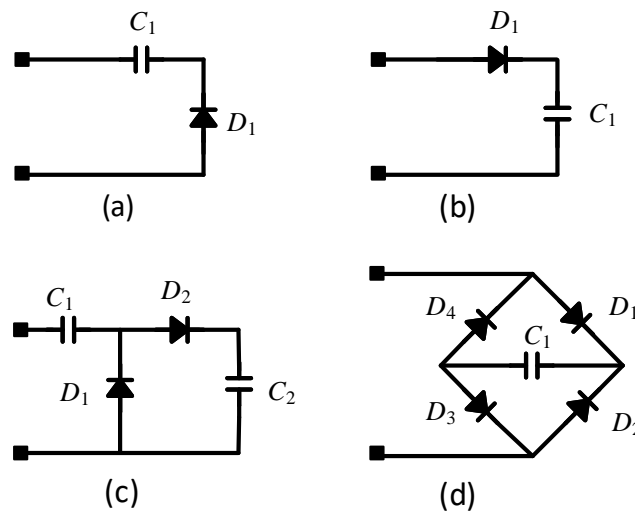


Figure 2.22: The four typical configurations of the rectifier.

The simplest rectifier circuit consists of a series shown in 2.22a (or parallel in figure 2.22b) and a parallel (or series) capacitor. The series diode circuit is also known as Villard Rectifier or DC restorer. The waveform produced is shown in figure 2.23a. The parallel version is the well-known half-wave rectifier. When AC voltage comes through D_1 , only the positive cycle goes in the output, as shown in 2.23b. Because of the reduction of the input, the full-wave rectifier, as shown in figure 2.22c, is the most popular circuit. The output voltage sees two capacitors in series (each one is storing a voltage of V_{peak}). Thus, V_{out} is twice V_{peak} , as shown in 2.23c. For this reason this circuit is also known as a single-stage voltage doubler circuit or Cockroft Walton voltage doubler.

Therefore, this topology is more stable and efficient than the halfwave rectifier. There is also the bridge rectifier, shown in figure 2.22d, which rectifies both positive and negative. The figures in 2.23 summarise the waveforms obtained. As shown in figure 2.23d, the full-wave and the Bridge rectifier double voltage have the highest output voltage.

Different configuration of circuits that convert AC to DC by increasing the

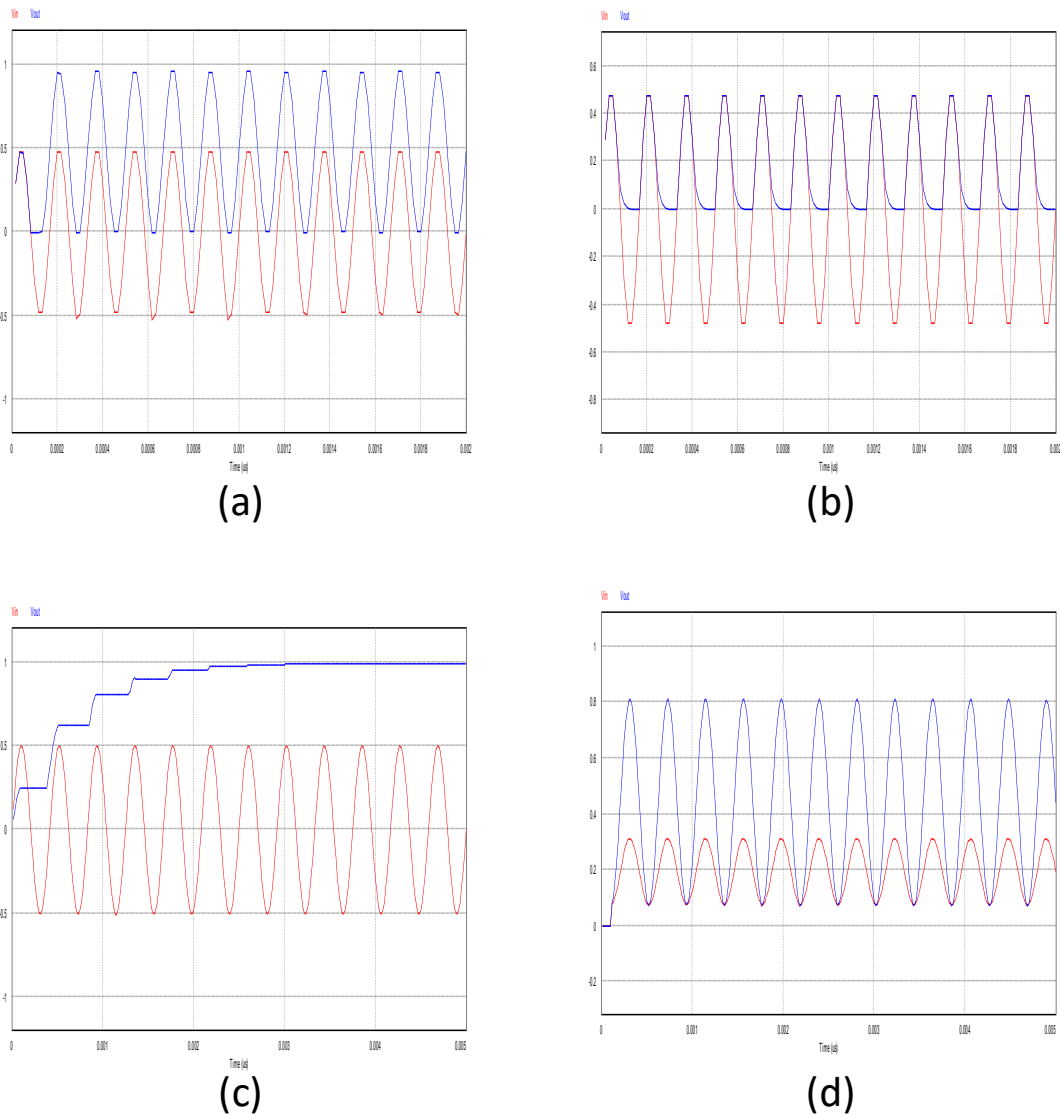


Figure 2.23: Waveforms generated from each configuration of the rectifier.

values are called voltage multiplier. The most fundamental configuration is the CockcroftWalton voltage multiplier shown in figure 2.24a. This circuit's operational principle is similar to the full-wave rectifier, but has more stages for higher voltage gain. The Dickson multiplier, in figure 2.24b, is a modification of CockcroftWalton's configuration with stage capacitors being shunted to reduce parasitic effects. Thus, the Dickson multiplier is preferable for small voltage applications. However, it is challenging to obtain high PCE due to the fact that the high threshold voltage among diodes creates leakage current; thus, reducing the overall efficiency. Additionally, for high resistance loads, the output voltage drops drastically

leading to low current supply to the load.

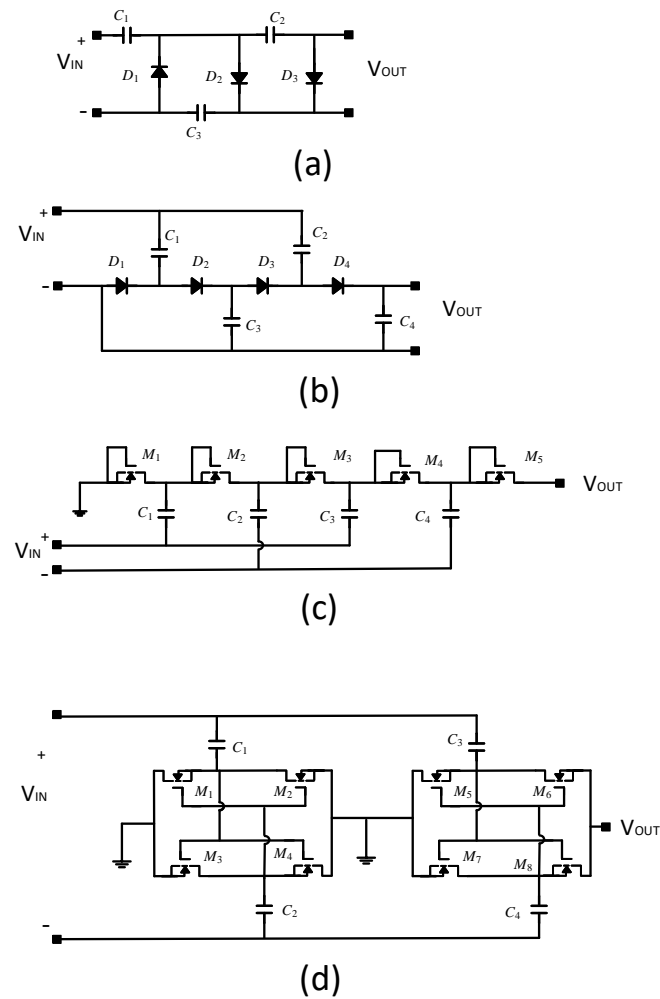


Figure 2.24: Most common voltage multiplier configurations: (a) Three stages CockcroftWalton voltage multiplier, (b) Four stages Dickson voltage multiplier, (c) Four stage Dickson voltage multiplier using CMOS technology, (d) Two stages voltage multiplier comprised of differential drive unit.

2.5.2 MOSFET rectifiers

The limitations of diodes can be overcome by MOSFET technology. The major advantage of the MOSFET is the fast switching speed. The Dickson charge pump is also designed using MOSFETs to merge it into integrated circuits, as shown in figure 2.24c. Relatively low threshold voltages and high PCEs are features of this design.

Moreover, the differential drive voltage multiplier 2.24d is widely used because of its low leakage current and potential for further modification in specific applications. The number of stages in a voltage multiplier has a close relationship with its sensitivity and efficiency. The amount of losses per stage increases as the number of stages increases. However, the trade-off consists of a higher voltage multiplication and a small threshold voltage at the first stage. On the other hand, a voltage multiplier with a few stages has less voltage drop between its stages, but it requires higher threshold voltage for all stages to work simultaneously. As a result, when a large number of stages are present, a voltage multiplier becomes more susceptible, whereas when smaller stages are present it becomes more effective. Therefore, based on the implementation goals, the optimum number of steps should be considered.

The voltage loss across MOSFET devices leads to low efficiency. This is further deteriorated by reverse leakage current. Another major disadvantage of MOSFET based circuits is that as the frequency increases, the efficiency decreases. This happens due to increased power losses from the reverse leakage current in the MOSFET.

2.6 Multi-coil WPT system

Two coil systems are used for charging both portable and heavy power devices like power-banks. An optimal alignment has the greatest coupling co-efficient where the coils are the same size and parallel to each other. The mutual inductance declines as the ratio of the two coils' primary magnetic field decreases, particularly when there is a broad separation between the two coils.

Multiple coils in the transmitter, receiver, or in the middle are adopted essentially for two main reasons: (a) more degrees of freedom to maximise the efficiency and desensitise the link gain with the coupling factor; and (b) highly coupled transmitter-repeater or repeater-receiver links work greatly as impedance

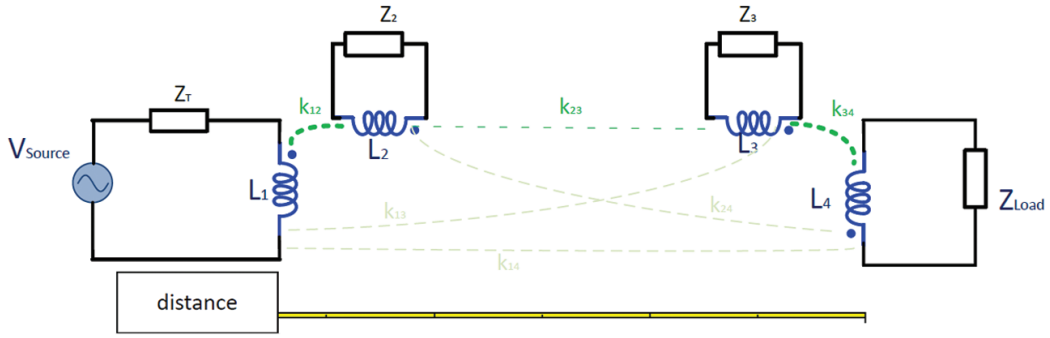


Figure 2.25: Four coils WPT system with the coupling factors. The couplings are marked following their value. κ_{13} , κ_{14} and κ_{24} are not visible due to their intensity values which are negligible.

matching elements on both sides. Although this last configuration requires four or more coils, it offers better efficiency-distance than a three-coil system [9]. For this reason, the three coil WPT is not very popular, unless the application has no space for additional coils.

Let us consider a four-coil resonator system with two intermediate repeater coils called “2” and “3” where an impedance (capacitor) compensation Z_2 and Z_3 are connected to form LC resonators. As shown in Figure 2.25, the transmitter and receiver are referred as “1” and “4” respectively. It has been considered that the transmitter R_T and the load impedance Z_{Load} have relatively low quality factor of $Q_T = Q_1$ and $Q_R = Q_4$. Considering only the parasitic resistance, much higher quality factor Q_2 and Q_3 can be achieved. With this new nomination, k_{23} will be much lower than k_{12} and k_{34} , because the distance between the intermediate coils are usually larger than the geometry of the coils. In this way, the cross coupling effect could be neglected because of either low quality factor Q or the small coupling coefficient depicted in the Figure 2.25 in yellowish green. Similar to the two-coil system, the figure of merit could be written as a generic Δ_{ij} for any two of the four coils:

$$\Delta_{ij} = \kappa_{ij}^2 Q_i Q_j \quad (2.20)$$

calling i and j the number of the referred coils. An important equation in designing of a multi-coils system comes from the impedance, which is reflected from the all coils to the primary transmitter. Considering the Equation 2.8 introduced in a two coil system, it is possible to write for each coil the reflected impedance:

$$\begin{cases} Z_{ref,3} = \frac{\omega^2 k_{34}^2 L_3 L_4}{Z_4 + Z_{Load}} \\ Z_{ref,2} = \frac{\omega^2 k_{23}^2 L_2 L_3}{Z_3} \\ Z_{ref,1} = \frac{\omega^2 k_{12}^2 L_1 L_2}{Z_2} \end{cases} \quad (2.21)$$

Combining these equations in the equation 2.21c, it is possible to obtain the impedance reflected in the primary transmitter:

$$Z_{ref,1} = \frac{\omega^2 k_{12}^2 L_1 L_2}{\frac{\omega^2 k_{23}^2 L_2 L_3}{\frac{\omega^2 k_{34}^2 L_3 L_4}{Z_4 + Z_{Load}} + Z_3} + Z_2} \quad (2.22)$$

where simplifying we obtain:

$$Z_{ref,1} = \frac{\omega^2 \left(\frac{k_{12} k_{34}}{k_{23}}\right)^2 L_1 L_4}{Z_4 + Z_{Load}} = \frac{\omega^2 k_{TOT}^2 L_1 L_4}{Z_4 + Z_{Load}} \quad (2.23)$$

In this equation we can notice that the reflected impedance of the all system depends only on the total coupling coefficient and the value of receiver impedance. Moreover, the WPT system can be seen as an equivalent total coupling coefficient defined by:

$$k_{TOT} = \frac{k_{12} k_{34}}{k_{23}} \quad (2.24)$$

It is a design rule making sure that the following condition can be met:

$$k_{TOT} = \frac{k_{12} k_{34}}{k_{23}} = 1 \quad (2.25)$$

the reflected load will be matched, and we will have the maximum power transferred. In such a way, the four-coil system creates the possibility to extend

the distance from the primary to the load using more and more coils. In order to maximise the transmission distance, the mutual coupling coefficient between the repeaters could be minimized. Additional intermediate coils are still loosely coupled between them, but they will result in an increase in the total coupling coefficient of the system. For example, even if the coefficient κ_{23} between the intermediate coils is loosely coupled to 0.01, because of the long transmission distance, the equivalent coupling coefficient κ_{TOT} of the whole system can still be adjusted to the maximum 1, when both κ_{12} and κ_{34} are coupled to 0.1.

However, the matching impedance of such a system is not endowed with a high overall efficiency because it is restricted by the merit factor given by Equation 2.22. Nonetheless, the four-coil system still offers (in terms of efficiency-distance) a better solution than the two-coil systems, when the distance is much bigger than the coil size.

2.6.1 Issues related to WPT

Power transfer over short transmission distances is commonly achievable with a good coupling coefficient, which depends on the medium between coils (whether it is air or any material with a permeability of 1 or above). In addition, the best coupling coefficient is obtained when the coils have the same dimensions, negligible gap and they are perfectly aligned. The misalignment between the transmitter and the receiver has been the first challenge to overcome in this technology. Therefore, the charging appliances are usually fabricated to a similar size in order to have a visible match. Although the system efficiency and power transferred can be maximised, the following problems can arise in these systems.

Cross-talking or localised charging, happens if the transmitter is much larger than the receiver. The magnetic flux path should only occur between the transmitter coil and the receiver coil[140]. Only the transmitter coil that is closest to the receiver is powered on, with others around it in standby mode. This type

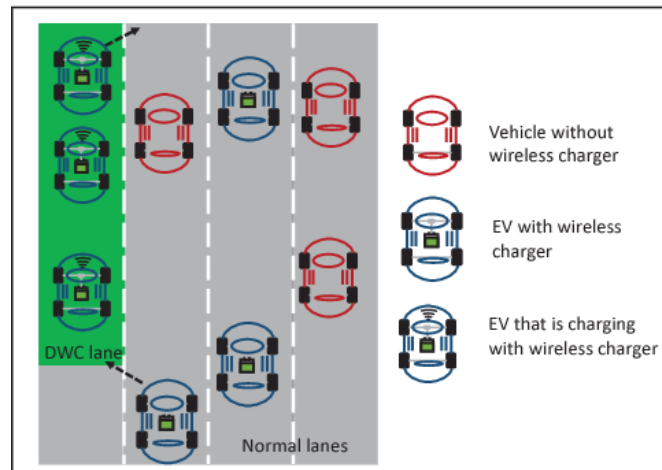


Figure 2.26: Crosstalking example: not authorised EVs are charge because their proximity with the DWC lane.

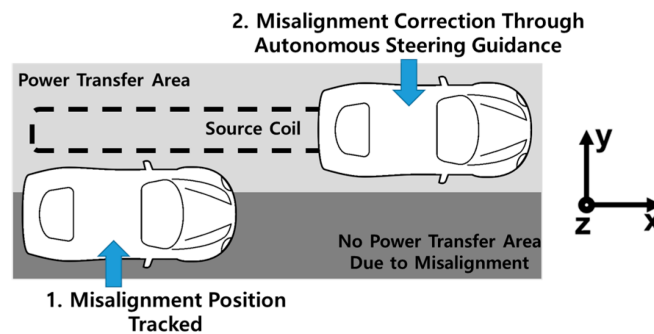


Figure 2.27: Concept of autonomous vehicle tracking and guidance to reduce degraded power transfer in a DWC system.[144]

of WPT is mostly used in dynamic wireless charging (DWC) applications where power consumption by each transmitter coil can be monitored to roughly identify the position of the receiving coil[141, 142]. An example is the reference [143], which is shown in Figure 2.26 as a non authorised vehicle outside the charging lane will be charged.

Not-alignment between primary-secondary coil is usually measured in degrees, from perfectly aligned 0° up to the coils being orthogonally positioned relative to each other. Beyond the same size mentioned previously, another solution could be the adoption of a movable transmitter coil to align it with the position of the receiving coil, which is detected through certain sensors. The transmitter coil will be moved to the place right beneath the receiving coil. This solution has great



Figure 2.28: FOD to a chew-gum aluminium wrap which have begun to burn.

potential in stationary EV charging because precisely adjusting the position of the vehicle is relatively difficult, especially when the receiving coil is very small. The misalignment between the coils is detected using sensors and the vehicles position is then adjusted by appropriate autonomous steering until the degraded power transfer in the DWC is restored to an optimum level as shown in Figure 2.27.

The **foreign object detection** (FOD) near the transmitter coil or pad causes safety issues because of the eddy current created inside metallic objects. An increased temperature can be observed in daily metal objects such as coins, keys, and metallic packaging materials [145, 146]. Actually, the feature of foreign object detection (FOD) is part of some industry standards, such as WPC1.1 [146]. In figure 2.28 is shown the effect of a commercial chew-gum in its typical aluminium wrap. Eddy currents have increased the temperature and a small fire has started. The detection is often achieved using a magneto resistance or temperature sensor. Another method is to turn on and then off the transmitter coil, and the presence of FOD will change the characteristic of the power decay time in the transmitter. In the case of FOD, the transmitter is shut down for safety reasons.

A particular note should be taken for the misalignment in biomedical implants, where the receiver has dimensions of millimeters, often not anchored and completely hidden inside the patient body. Most of the time it difficult to find the exact receiver location. Moreover, the medium is not air but human tissue: by taking into account the higher absorption rate, in [147] an optimal design scheme was

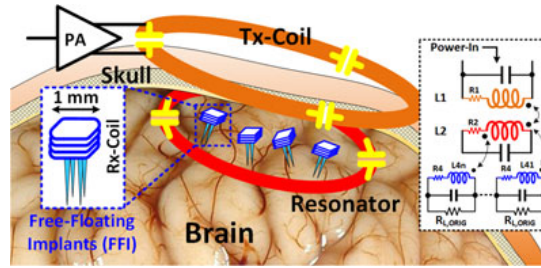


Figure 2.29: Challenging WPT implant in the skull which is insensitive to the exact location of the receiver [146].

proposed by using a large external transmitting coil, which can effectively energize the implant in the brain tissue as shown in the Figure 2.29. In the radiative near-field region for the millimeter-scale receiver, there are research applications such as a cardiac implant [146, 148]. Relative high efficiencies can be obtained when the system operates in the low-gigahertz range, which is suitable for biomedical implantable system.

2.7 WPT challenges

There are three main developments still to be largely researched. These have been investigated in some research papers, but further studies are still needed. The three challenges can be classified as follows:

EMI. Metallic shields are used to reduce the high frequency magnetic fields around the system and reduce the electromagnetic interference (EMI). However, in addition to the magnetic core losses, there will be Eddy current losses inside the coil conductor and the metallic shield, which bring up the significance of efficient coil design in WPT systems. In general, the three-phase WPT charging system is an alternative to the single-phase WPT charging systems, due to the great benefits of EMI reduction. This happens because the output phase voltage in a six-step inverter has even harmonics, third harmonics, and multiples of third do not exist. However, the harmonic voltages of the fifth, seventh, and other non-triplet odd multiples of fundamental frequency can act as EMI sources. Therefore, an EMI filter is still required without increasing complexity.

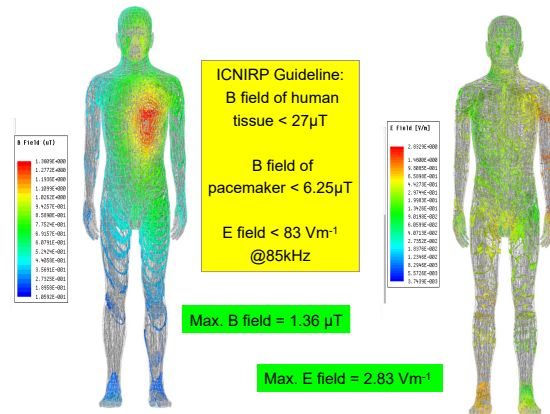


Figure 2.30: The guideline recommended by the ICNIRP for the level of electric and magnetic field.

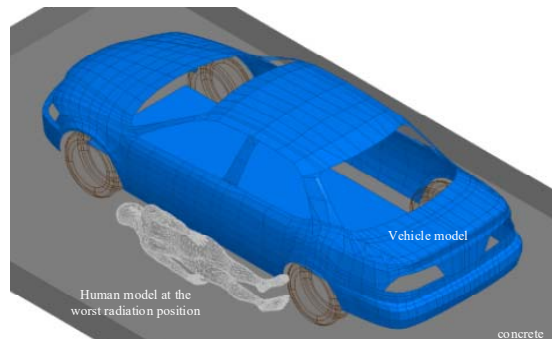


Figure 2.31: Safety level experiment (first part) for 6.6kW WPT charger.

Safety. The human exposure to electric and magnetic fields in the transfer space must be considered in any WPT topology. The guideline (shown in Figure 2.30) for the level of electric field is 83 V/m and the magnetic field is 21 A/m [107], as recommended by the International Commission on Non-Ionizing Radiation Protection (ICNIRP) [149]. Medium and high-power WPT charging applications create high levels of field in the coils' proximity. Thus, the safety of people nearby the charger becomes a fundamental requirement. The Figures 2.31 and 2.32 show an investigation into a 6.6 kW WPT charging system for EVs [107]. The coil size is $500 \times 500\text{ mm}$ and a car is parked in the charging position above the coil. The worst position for a human is to lie on the ground close to the coil, as shown in Figure 2.31.

Security. The power encryption in WPT was initially applied to [150, 151]. The energy is encrypted in the WPT system by chaotically adjusting the power

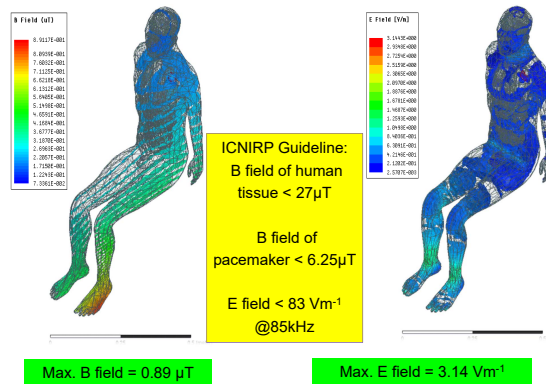


Figure 2.32: Experiment (second part) continues with a human inside the parked car.

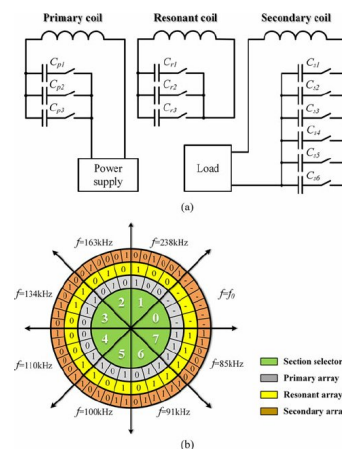


Figure 2.33: Schematic diagram of the proposed security key proposed in Reference [150].

source's frequency. The authorised receptor may then receive the energy by changing the circuit at the same time to decode the encrypted energy using the security key acquired from the power supply, but the unauthorised receptor cannot get the energy unless they know the security key. The power supply encryption is based on the variation of transmitting frequency, which results in the resonance of an unallowed receiver. A capacitor array creates the variation of the frequency and matches it with the receiver for the maximum power delivered, as shown in Figure 2.33. Hence, the transmitted power can be packed with different frequencies and delivered to the receiver in a specified time slot.

Summary. The circuit theory and principles underlying magnetically linked coils are first examined in order to demonstrate the advantages and disadvan-

tages of various WPT configurations. The present WPT system's primary components are then summarised individually. The application-specific selection of power sources, compensation networks, and control mechanisms is discussed. The most recent advances in WPT applications are demonstrated, with a particular emphasis on portable electronic gadgets and electric cars. Each application's technical challenges, limits, and prospective enhancements are examined.

Chapter 3

Near Field Communication

In order to improve security in the WPT systems, it is necessary to investigate the existing secure WPT products using this technology. The most widely used technique for secure WPT is the Near Field Communication (NFC) technology, where devices interact by inductive coupling between transmitter and receiver coils through generation of magnetic fields.

Thin NFC sheets, composed of soft magnetic materials, are put between antennas and metal cases of wireless devices like phones and tablets to prevent eddy currents from degrading antenna gain and radiation efficiency. Magnetic materials with excellent features, such as high permeability (shown in Figure 3.1), low magnetic loss, and high resistivity, are highly sought to improve the efficiency of wireless power transfer.

NFC also has a collection of communication protocols that allow two electronic devices to communicate across a distance of a few cm. NFC provides a low-speed connection that is easy to set up and may be used to bootstrap more powerful wireless connections. NFC devices can be used as electronic ID cards and key-cards. They are utilised in contact-less payment systems, and they let you pay with your phone instead of or in addition to credit cards and electronic ticket smart cards. NFC may be used to transfer tiny files like contacts, as well as to establish quick connections for exchanging bigger media like photographs, movies, and other files.



Figure 3.1: High Permeability μ_r (400-700) flexible magnetic sheet for NFC/RFID antenna applications.

The NFC is one of the many types of networks for transferring data. Networks may be characterised by many properties or features such as physical capacity, user authorisation, organisational purpose, access rights, amongst others. Another different classification method relies on the physical extent or geographic scale. In networking, the NFC is part of the Nanoscale communication network (as shown in Figure 3.2 in comparison with the communication range). They use physical principles that are different from macroscale communication methods and contain important components, such as the message carriers. Nanoscale communication can also communicate with very small sensors and actuators, such as those present in biological systems, and it can also function in harsher environmental conditions than the traditional communication [152].

This developing technology, officially known as near field communication (NFC), was standardised in 2004 and is progressively changing the consumer electronics sector by facilitating electronic transactions, mobile payments, data transmission, and so on. NFC was initially disclosed in 2002 by a Sony-NXP Semiconductors joint venture [153]. NFC has grown in popularity and evolution over the last decade, and is now being integrated into many more elements of our everyday

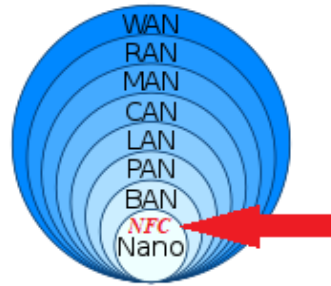


Figure 3.2: A comparison in terms of communication range between NFC and other types of networking.

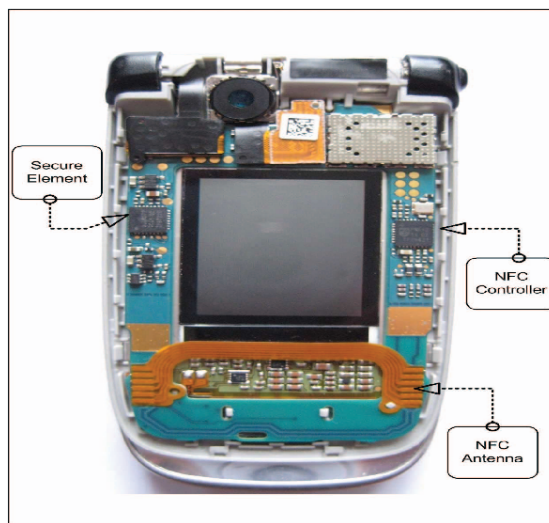


Figure 3.3: First mobile phone, Nokia 6131, to have NFC technology[154].

lives than ever before.

The NFC Forum was created in 2004 by a joint effort between Sony, Philips, and Nokia to help improve NFC technology. In 2006, Nokia introduced the Nokia 6131 shown in the Figure 3.3, the first NFC-enabled handset [155, 156]. NFC technology had a new application and this was used in 2006 to help impaired users in libraries that have enabled handicapped patrons. M-Biblio at the University of Bristol launched NFC-enabled QR codes in 2011 to allow students to use library resources[156].

In 2010, Samsung released the first NFC-enabled Android phone (the Samsung NEXUS S) [155]. In the figure 3.4, it shows the phone with cover lid removed. As it can be seen, the lid has the NFC sheet which connects to the two contacts circled in green. The Research in Motion/BlackBerry Limited's (RIM) payment card



Figure 3.4: Samsung NEXUS S, the first NFC-enabled Android phone, open in the back where the NFC coil can be clearly noticed[155].



Figure 3.5: The first contact-less payment developed by RIM [157].

received the PayPass capability in 2011 from VISA and became the first contactless payment [157], as shown in Figure 3.5. Other examples of the early uses in 2012 are: Samsung TecTile Programmable NFC tags in 2012, Sony's Xperia smart tags, NFC allow Smart Objects in 2011, Wallet in 2011, and Google, Verizon, and T-combined mobile's endeavour to deploy mobile wallets. In 2011, NFriendConnector [158] combined Facebook and NFC-enabled mobile phones to create online social connections. Users' real-life social network and their online accounts are becoming increasingly entwined, with online connections tracking genuine social acquaintances and exchanges as shown in Figure 3.6.

Starting with the iPhone XS, all new Apple devices include NFC enabled capability (Apple Pay).[159]. Since 2010, technological heavyweights such as Google, Apple, Samsung, NXP and others have released new intriguing NFC applications every year in the communication industry. Industry participants are continually



Figure 3.6: NFriendConnector created an online social by integrating Facebook and NFC-enabled mobile phones [161].

offering new advancements and enhanced technology in NFC enabled gadgets, bringing the worldwide market to \$4.80 billion in 2015 and forecasting a 47.42 billion dollar market by 2024[160].

3.1 NFC vs RFID

All communications based on near-field magnetism between transmitting and receiving devices use the inductive coupling concept. The above-mentioned idea also applies to inductive coupling-based RFID systems. Even yet, there are some distinctions between NFC and conventional RFID systems in terms of other components such as network systems and protocols(Figure 3.7).

NFC is a subclass of RFID technology that works across a wide range of frequencies with three unique bands low, high, and ultra-high frequencies. The operational range of NFC and RFID technology differs significantly. RFID has a range of metres, but NFC has a range of three to five centimetres. All RFIDs work on the same concept of one-way data transfer from the tag to the receiver, with no power transmission in the opposite direction [162, 163]. The RFID transmitter sends an interrogating signal to the tag via the antenna, and the tag responds with its unique information. RFID tags are either active or passive. Active RFID tags have their own power source, allowing them to transmit at up to a 100-meter read range. Active RFID tags are excellent for a variety of sectors where asset location



Figure 3.7: NFC cards and RFID tags. The tags/receivers are very similar to each others [164].

and other logistical enhancements are crucial. RFID tags that are passive do not have their own power source. Instead, the RFID reader transmits electromagnetic energy to them, which powers them. Passive RFID tags have a read range of up to 25 metres since the radio waves must be powerful enough to power the tags. Passive RFID tags primarily operate at three frequency ranges:

- Low Frequency (LF) 125 -134 kHz
- High Frequency (HF) 13.56 MHz
- Ultra High Frequency (UHF) 856 MHz to 960 MHz

Near-field magnetic transmission is used in RFID, which is one of the oldest technologies. The first commercial use of RFID was an electronic items surveillance system (EAS) in 1960, which employed a one-bit tag to detect the presence or absence of the tag. More work on RFID systems was done using microwave and inductive systems between 1970 and 1980, and in the late 1970s, the size of RFIDs was reduced using low-power complementary metal-oxide semiconductors (CMOS) logic circuits. RFID applications such as animal monitoring, business, electronic toll collection, and automation became commonplace after 1980, thanks to the fast advancement of personal computer (PC) technology. The first effective use of RFID technology in the world was the electronic toll collecting systems in the 1990s [165]. RFID is being used in a variety of commercial applications, including the Internet of Things (IoT), such as automobiles, agriculture, transportation, medical systems, payment cards, supply chains, tracking, identification

applications, and short-range interactions [166, 167]. However, RFID technology cannot enable communications that need initialization on both ends (e.g., peer-to-peer communications, as will be mentioned below). NFC, which also supports peer-to-peer connections, is a perfect solution to RFID's limitation.

NFC is a near-field communication technology that allows for secure communication between devices over a short distance. NFC is a short-range (less than 10 cm) wireless communication technique that uses high frequency (HF) radio waves with a narrow bandwidth[168]. An antenna, a reader, and a tag are the three essential components of NFC. A reader (transmitter) delivers a signal at the standard NFC frequency of 13.56 MHz, which the tag antenna receives and analyses, and replies with the desired information back to the reader, which is then decoded and stored[153, 169].

NFC has been used in a variety of applications since 2004. This technology is used in Nokia, Apple/Google/Samsung pay transactions, wireless energy/data transfer, and wireless key card entry, to name a few examples [170]. Despite the fact that the NFC tag is passive, it may send data in both directions. NFC technology can handle a variety of data transfer speeds, with the most common three being 106, 212, and 424 Kbps [171]. There's also an 848 Kbps rate, although it does not comply with NFC specifications.

3.2 NFC applications

Nowadays, around one-third of the world's population owns a smartphone, and this number is expected to rise dramatically in the coming years. Since its introduction, several NFC applications have been developed and have become a part of our daily life. The use of NFC technology in contactless mobile payments has resulted in tap-and-go tasks. When using an NFC-enabled device, the user simply touches or presents the phone to the NFC-enabled device to transfer or share data without the need for a physical connection. NFC has been established to be compatible

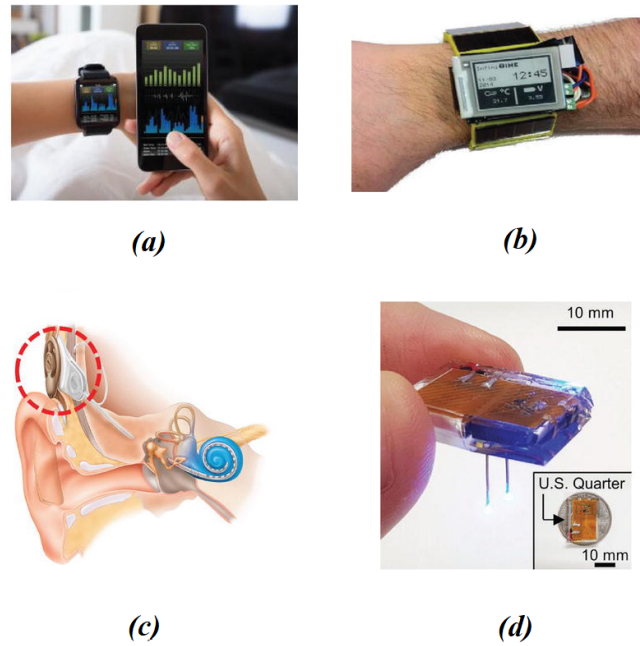


Figure 3.8: Various NFC applications in healthcare; (a) NFC enabled smart watch [174]; (b) wearable bracelet prototype [175]; (c) cochlea implant with a circle indicating the NFC communication component of the implant [163]; (d) brain optogenetic implant held with fingers, the device is smaller than a US quarter. [176].

with devices running Android, Windows, and iOS for mobile payments. Google Pay, Ali Pay, Apple Pay, Samsung Pay, PayPal, Square Wallet, and Visa payWave are some of the NFC payment apps that enable tap-and-go. Between consumers and merchants, NFC enabled mobile payment is diminishing the necessity for tangible forms of payment. Mobile point of sale (mPOS) units, for example, are wireless devices that can be used to replace traditional cash registers and sale terminals [172]. In 2019, the number of mobile payment users was close to 2.1 billion, according to data by GATE Mobile Wallet Trends (Global Acceptance Transactions Engine) [173].

Numerous NFC applications in healthcare are shown in the Figure 3.8. Secure physical access to buildings, medications, and equipment, medical information, real-time updates on patient care, medical alerts, home monitoring of patients, safer medications [177–180], storage of encrypted medical tags [180], adverse drug and allergy detection system in hospitals [153], and electronic data recording ser-

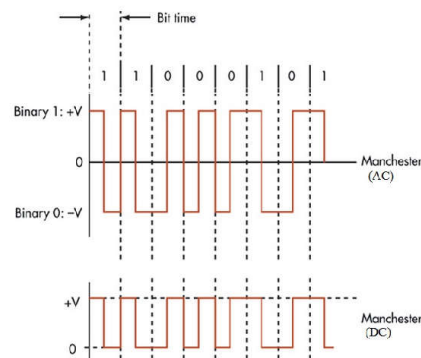
vices [181] are some of the user-friendly benefits of NFC in healthcare. Implantable health devices with more advanced NFC implementations include heart monitors [182], cochlea implants [180, 183], and optogenetics implants [184].

In the midst of the COVID-19 epidemic, Silicon Craft Technology PLC (SICT) has released an NFC-enabled wearable band to track COVID-19 patients and those in self-quarantine [185, 186]. Because of their early promising results, NFC-based access control and authentication services have gotten a lot of interest. The usage of NFC enabled contactless smart cards for access and identification badges is similar to how users obtain entry to buildings using NFC enabled mobile phones. As a result of these applications, NFC is expected to play a significant part in next-generation access control and identity management systems [180]. For instance, a two-factor access control system for building access [153] uses biometric fingerprint recognition for authentication and NFC to convey data to a computer-controlled door. The new BMW 5 Series for 2021 has an NFC enabled digital car key feature that is compatible with Apple iPhones (compatible with iPhone SE 2nd generation and iPhones running iOS 13 or higher)[185].

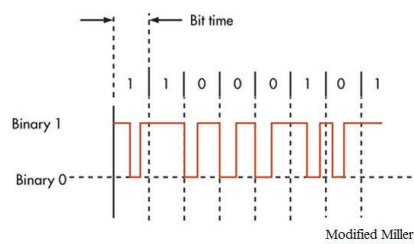
NFC-enabled mobile devices have changed the way consumers get data, make payments, and share information between devices all around the world as a result of technology advancements in the last decade. The well-known and potential applications of NFC technology are transportation and ticketing. Commuters all throughout the world have adopted mobility in all elements of their transportation, including trip planning, ticketing, and information [187]. Consumers must have NFC-capable mobile phones that are compatible with the NFC standard ISO/IEC 14443 [188] to use NFC services in transportation and ticketing. For example, a transport ticket can be quickly downloaded from an NFC-enabled kiosk using an NFC-enabled smartphone, which can then be tapped on a reader to gain access to ticketing information [188].

NFC technology Type	Polling or Listening	NFC Modulation	NFC Coding
NFC-A	Polling	ASK 100% (Read explanation below)	Modified Miller
NFC-A	Listening	Load(ASK-Amplitude Shift Keying)	Manchester
NFC-B	Polling	ASK 10% (Read explanation below)	NRZ-L
NFC-B	Listening	Load (BPSK)	NRZ-L
NFC-F	Polling	ASK 10%	Manchester
NFC-F	Listening	Load modulation (ASK), read explanation below.	Manchester

(a)



(b)



(c)

Figure 3.9: Type of NFC (a)modulations and coding table, (b)the Manchester coding and (c)Modified Miller coding.

3.3 NFC modes of communication

NFC devices can communicate in one of two modes: active or passive communication. These modes control how two NFC-enabled devices communicate with one another. Whether a gadget generates its own RF field or uses power from another device determines the mode differentiation. The initiator of a communication is the device that initiates it, and the target is the device that receives the signal from the initiator. Table 3.1 [189, 190] summarises the fundamental distinctions

	NFC	RFID	Bluetooth
Maximum Operating Range	30 cm	30cm	30 cm
Operating Frequency	13.56 MHz	Varies	2.4 GHz
Directional Communication	Two way	One way	Two way
Bit Rate	106 - 212 - 424 Kbps	Varies	22 Mbps
Set up time	< 0.1ms	< 0.1ms	22 Mbps
Selectivity	High security	Partly given	Who are you
Consumer Experience	Touch wave simply connect	Get information	Configuration needed
Potential Uses	e-Tickets, Credit card payment, Membership card	Tracking items, Toll-Pass	Communicate between phones, peripheral devices

Table 3.1: Differences between technologies: NFC vs RFID vs Bluetooth

between NFC, RFID and Bluetooth technologies.

3.3.1 Active mode

In active mode, both NFC devices (initiator and target) use an alternate RF field to send and receive data signals. Both NFC devices are self-powered, which means they do not need to send electricity to the target to complete the work, such as a smartphone or a self-powered tag. In active mode, data is transferred between two devices via amplitude shift keying (ASK), which involves modulating the base RF field signal (13.56 MHz) with data utilising coding techniques (Miller and Manchester Coding), as shown in the Figure 3.9. This mode has faster data transfer rates and can be used over longer distances [191, 192].

3.3.2 Passive mode

The initiator sends the RF field to power the target in passive mode. The target, in turn, uses the RF field to convey the stored data back via a process known as load modulation (Manchester coding) [193]. It is the most used NFC mode

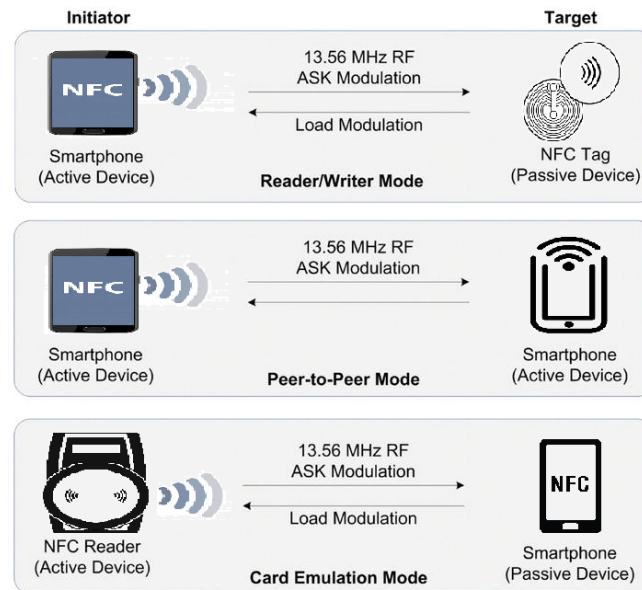


Figure 3.10: NFC three operation modes are: reader/writer, peer-to-peer, and card emulation communications.

because it does not require a battery and is less expensive [194]. When two NFC devices connect wirelessly, three potential communication combinations are possible: active-active, active-passive, and passive-active[194]. The NFC devices execute different operations during communicating in active and inactive modes. This means that NFC device 1 (initiator) must first transmit a signal to NFC device 2 (target) in order to receive a response from device 2. (target). NFC device 2 (Target) cannot deliver data to device 1 without first receiving an initial signal. Reference [153] gives a list all of the possible NFC device interaction styles. To be NFC-compliant, a device must have the capability, i.e. it must operate in reader/writer mode and peer mode, according to the NFC forum's device requirement [180].

- **Active-Active** *NFC Mobile-NFC Tag* The RF field is generated by both devices.
- **Active-Passive** *NFC Mobile-NFC Mobile* The RF field is generated by device 1 only.
- **Passive-Active** *NFC Tag-NFC Mobile* The RF field is generated by device

2 only.

During passive communication, a device must act as an initiator, and during active communication, it must act as an initiator or target. The NFC working frequency of 13.56 MHz was initially uncontrolled. The NFC Forum was founded in 2004 to standardise tags and operational standards. The NFC Forum standardised three tasks: transferring power from an NFC device to an NFC tag, sending information from an NFC device to an NFC tag via signal modulation, and sensing the modulation by the load created on the NFC tag while performing load modulation to receive information from an NFC device. The NFC forum identified these three operation modes as reader/writer, peer-to-peer, and card emulation communications, as shown in Figure 3.10. The following are the three main modes in which an NFC device can function [153]:

- **Reader/writer mode.** The device must be able to read and write different types of NFC tags in reader/writer mode. One NFC smartphone can exchange data with one NFC tag in this manner. Most NFC devices act as readers and work in active mode to read the content of tags, such as contactless smart cards and RFID tags, in reader/writer mode. The gadget must recognise the relevant tag type in order to interact with it effectively. When the NFC device comes across two tags at the same time, it uses an anti-collision algorithm to choose one of them. In the writer mode, an NFC device can write data to tags that have a writer application, such as Tag-Writer [195]. The NFC devices are compliant with ISO/IEC 14443A/B or Felica scheme tag types in reader/writer mode [153]. Smart posters, remote shopping, and remote marketing are just a few of the applications of the reader/writer mode [171].
- **Peer to peer mode.** Two NFC-specific devices can communicate data in peer-to-peer mode, such as pairing Bluetooth devices or setting up a WiFi network, exchanging business cards, or sending text messages. The ISO/IEC

18092 NFCIP-1 standards are used to standardise this mode. During communication, both devices are in active mode, and data is delivered through a bi-directional half-duplex channel, which means the second device can only transmit data when the first NFC device has finished transmitting [153].

- **Card emulation mode.** In card emulation mode, an NFC device acts as a standard contactless smart card external reader. Contactless payments can be made with credit cards, debit cards, loyalty cards, and other NFC devices without requiring any changes to the existing infrastructure. For example, an NFC-enabled mobile device can contain numerous contactless smart card applications on the same device. The ISO/IEC 14443 Type A and B, as well as the Felica standards [153] are supported by the card emulation mode.

3.4 NFC tags

In an NFC system, there is always an element that acts as a passive receptor, such as an NFC tag. The NFC tag, also known as the smart tag or information tag, is a small printed circuit containing a radio chip linked to an antenna that acts as a bit of stored memory [171]. It operates in a passive mode, in which it does not have its own power source and instead relies on the power of the NFC device with which it communicates through magnetic induction. The operating distance of NFC tags is only a few inches, therefore the NFC device must be extremely close to read the tag. NFC tags are used for a number of purposes in our daily lives, including payments, opening websites, virtual visiting cards, locking and unlocking doors, tagging pets, sharing images, videos, and other data, and so on. NFC-Forum has devised a taxonomy for NFC tags that provides critical specifications between different tag providers and device makers in order to assure compatibility. There are now five varieties of NFC tags, each with its own storage capacity, data transfer rate, and read/write capability [153]. A comparison between tags is shown in Figure 3.11.

Tag Type	Use Case	Chip Examples	User Memory (bytes)*	UID Length (bytes)	Cost
Forum Type 1	Specialized	Innovision Topaz	90 - 454	4	\$
Forum Type 2	Most common, low cost, single application like smart poster, personal label etc.	NXP MIFARE UL, MIFARE UL-C, NTAG 203, 210, 212 etc.	46 - 142	7	\$
Forum Type 3	Specialized, Asian markets	Sony FeliCa (Lite)	224 - 3984	8	\$\$\$
Forum Type 4	High memory applications, high security (in non NFC mode)	NXP MIFARE DESFire EV1 -2K, 4K, 8K, Inside Secure VaultIC 151/161, HID Trusted Tag™	1536 - 7678	7	\$\$\$
Forum Type 5 (NFC-V / ISO 15693)	If longer read range is required, industrial rugged tags – added as forum tag type June 17, 2015 .	NXP ICODE SLIx family, EM4233, Fujitsu FRAM MB89R118C, MB89R112, HID Vigo™	32 - 8192 (112 for ICODE SLIx)	8	\$ - \$\$\$
MIFARE Classic	<i>Very common, high memory</i> <i>Not compatible to all devices!</i>	NXP Mifare Classic 1K, 4K	716 - 3356	4 or 7	\$\$

Figure 3.11: Comparison between NFC tags with chip manufacturer, memory size, used ID and cost (Reference [198]).

Many factors influence the type of NFC tag used for a given application, including the application’s nature, memory and transmission rate requirements, working distance, and cost, among others as shown in Figure 3.11. To use NFC tags, an app must be installed on the NFC device, smart phone, or smart watch (e.g, Apple Pay and Google Pay for payments). In 2019, Ahold Delhaize, a European super-market behemoth, installed NFC-enabled electronics labels on its shelves, allowing customers to receive extensive product information and add items to their cart for self-checkout using their smartphones [196]. Apple recently released App Clip, a new feature in its IOS operating system that allows only clips/snippets of an App to communicate with NFC tags without having to download the entire App [197].

3.4.1 NFC tags of type 1

The NFC Type 1 tag is the simplest of the offerings. It is also the slowest chip, but because of the simplicity it offers, it is also possible to stuff more memory on this chip. Because these tags are simple, they also tend to be inexpensive, but can lack the functionality that you might need for some applications. Type 1 tags are based on ISO14443A and have a size of 96 bytes that can be expanded to 2 Kbytes. The data transfer rate is 106 Kbps, and type 1 NFC tags may read

and write data. The typical applications of these tags are: one-time provisioning, read-only applications, business cards, pairing devices with Bluetooth and reading a specific tag when more than one tag is present.

3.4.2 NFC tags of type 2

The Type 2 tag tends to be the most popular offering because it offers just enough functionality at the right price to meet a wide range of needs. The Type 2 tag is also faster than the Type 1 tag, so you can rely on it in applications in which a user expects nearly instant communication. Type 2 tags, like Type 1 tags, are based on the ISO 14443A standard. It has 48 bytes of memory that can be expanded to 2 Kbytes. The data transfer rate is 106 Kbps, and type 2 NFC tags may read and write data. The typical applications of these tags are: low-value transactions, event tickets, day transit passes and URL redirects.

3.4.3 NFC tags of type 3

The Type 3 tag relies on a different standard than the other tags in this group. This is a sophisticated tag that provides a wide range of functionality, but also comes with a relatively high price tag. The Sony FeliCa type 3 tag (JIS X 63194) is a Japanese FeliCa standard. In comparison to type 1 and 2 tags, it has larger memory and a faster data transfer speed. The memory is 2 Kbytes, expandable to 1 Mbytes, and has a 212 Kbps transfer rate. These tags are used for these types of applications and used primarily in Japan: membership cards, electronic ID, health care devices, home electronics, E-tickets, E-money and transit tickets.

3.4.4 NFC tags of type 4

The Type 4 tag offers the most flexibility and memory of all the tags. It comes with a moderate to high price tag, depending on the amount of memory you get. The most important reason to get this tag is security: It offers the functionality

needed to perform true authentication. Both ISO 14443 A and B communications are supported by Type 4 tags. These are available in read-only or read/write configurations. Unlike other tags, the mode cannot be selected by the user. The memory can be up to 32 KBytes, and the transmission speeds are considerable, ranging from 106 to 424 KBytes per second.

In addition, this is the only tag that provides support for ISO 7816 security as well as allows for self-modification of NDEF content. Given the extra capability that this tag provides, you typically see it used for transit ticket applications.

3.4.5 NFC tags of type 5

In 2015, the NFC Forum announced type 5 tags, which are the latest NFC tags. It is based on the ISO 15693 standard. It has a range of up to 1.5 metres and can communicate with RFID tags. The Type 5 tag offers support for the ISO/IEC 15693 specification. In this case, the NFC Forum chose to support Active Communication Mode, which allows overall data transfer performance similar to the RF technologies already supported by the NFC Forum. The typical applications of these tags are: healthcare (medication packaging), ticketing (such as ski passes), library books, products, and packaging.

Figure 3.11 outlines the various properties of five types of NFC tags, including standards, memory, data transmission rate, and so on, as well as their common uses [153]. In addition to these five types of tags, Type 6 NFC tags are based on ISO 15693-3 standards and are used to store NDEF messages or applications centred on identity cards [180]. It features an 8-Kbyte memory capacity and a data transfer rate of 26.48 Kbps. New types of tags have also been developed using the recently developed 3-D printing technology (e.g., Kovio's NFC Barcodes) [199]. In the field of NFC communications, new materials and printing technologies can open up a world of possibilities. In the recent decade, the number of smart phones and tablets having NFC capabilities has increased dramatically.

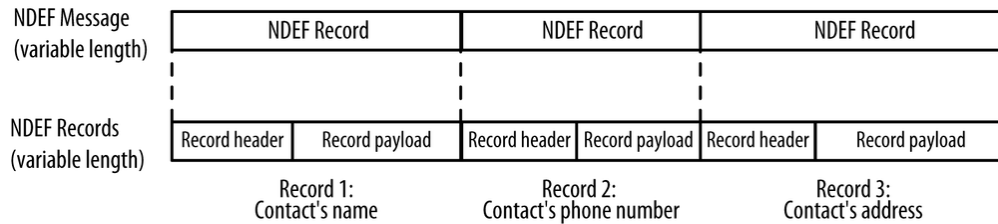


Figure 3.12: NDEF include several records, made up of a header and a payload that contains the message's content.

3.5 NFC Data Exchange Format

The NFC Forum established the NDEF ("NFC Data Exchange Format") content format for communication. NFC tags with NDEF messages are only supported by iPhones. Android not only accepts NDEF messages but also provides you with extra choices (e.g., low-level tag access). As illustrated in Figure 3.12, NDEF is a binary format structured into messages, each of which can include several records. A header, which includes metadata about the record, such as the record type, length, and so on, and a payload, which contains the message's content, make up each record. An NFC tag can store one or more NDEF messages while communicating.

Consider an NDEF message to be a paragraph, and the records within it to be the sentences. A well-structured paragraph is made up of sentences that are all about the same thing. The majority of NFC transactions are brief. In most cases, each exchange has just one message, and each tag has only one message. The NDEF message has one plus NDEF records. These last ones are where the payload is kept.

An NDEF record consists of a payload of data plus metadata indicating how to read the payload. The payload of each record can be any of many distinct data kinds. It might be standardised content, such as URLs, text, MIME types, or handover information, depending on the record type. It's also possible to create bespoke content formats. Each record's header includes metadata that describes the record and its location in the message, as well as its type and ID. The payload

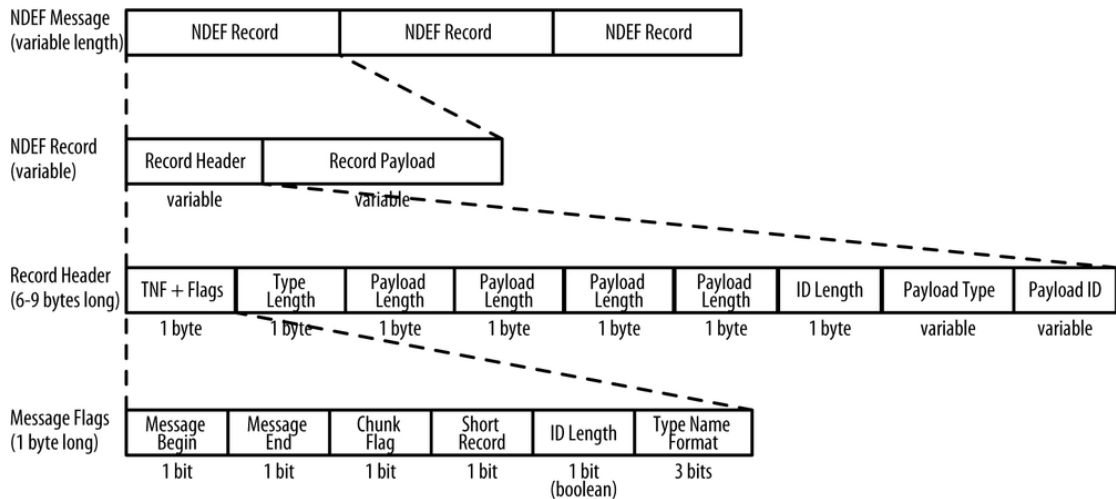


Figure 3.13: The bits and bytes of an NDEF file are shown in detail in Figure above.

comes after the header. Figure 3.13 depicts the bits and bytes of an NDEF file in detail.

An NDEF record consists of a type name format (TNF), payload type, payload identifier, and the payload, as shown in Figure 3.13. The most essential component of an NDEF record is the payload, which is the data you are sending. The TNF explains how to read the payload type. The payload type is an NFC-specific type, MIME media-type, or URI that specifies how the payload should be interpreted. Another way to look at it, is that the TNF is payload type metadata, and the payload type is payload metadata. The payload identification is optional, but it allows you to link or cross-reference several payloads. Explaining the details of the meaning of each bit goes outside of the subject of this thesis.

3.6 Security issues

Touch and go, touch and confirm, touch and connect, and touch and explore are examples of NFC uses. The use of NFC in real-world applications does not guarantee that the application is safe. As a result, NFC technology has its own set of difficulties, similar to RFID security concerns also being relevant to NFC because NFC is a counterpart to RFID and all NFC devices operate as readers

or writers, posing a variety of hazards. Another aspect contributing to the NFC security vulnerability is the lack of an NFC specification that addresses all countermeasures for x.800 security services like authentication and access control. The current specification is simply intended to serve as a reference for NFC application developers that want to protect data and communications within NFC devices. Next, there are privacy concerns posed while utilising NFC, such as the possibility of hostile attacks gaining access to personal information contained in NFC devices. For example, users that use NFC as a digital wallet to store their bank account information are vulnerable to data privacy attacks when attackers grab information from the wallet without the user's awareness at any time and from any location [200]. As NFC technology encounters difficulties, security concerns for a safe environment are growing. Many NFC applications have contactless payment applications that function in two ways: touch and confirm and touch and go. Google Wallet and Visa Paywave are two instances of contactless payment apps [196]. Google Wallet is an NFC touch-and-go application that requires a PIN code to complete the transaction [3, 201]. Visa Paywave, on the other hand, is a sort of NFC touch and go application that allows Visa cardholders to make a payment by just waving their card or NFC-enabled smartphone at a contactless payment terminal without having to confirm the payment. Previous research has found a contactless payment vulnerability in Visa contactless cards, namely that the card does not recognise foreign currencies outside of the United Kingdom, allowing fraudsters to take advantage of the contactless transaction [202]. As a result, security is a problem with NFC contactless payments, particularly in touch and go apps that perform functions without requiring approval during the transaction.

NFC apps can be classified according to their NFC communication characteristics. NFC applications fall into four categories: touch and go, touch and confirm, touch and connect, and the touch and discover [3]. The following are the features:

- Touch and go: to execute the actions that are implemented in the pro-

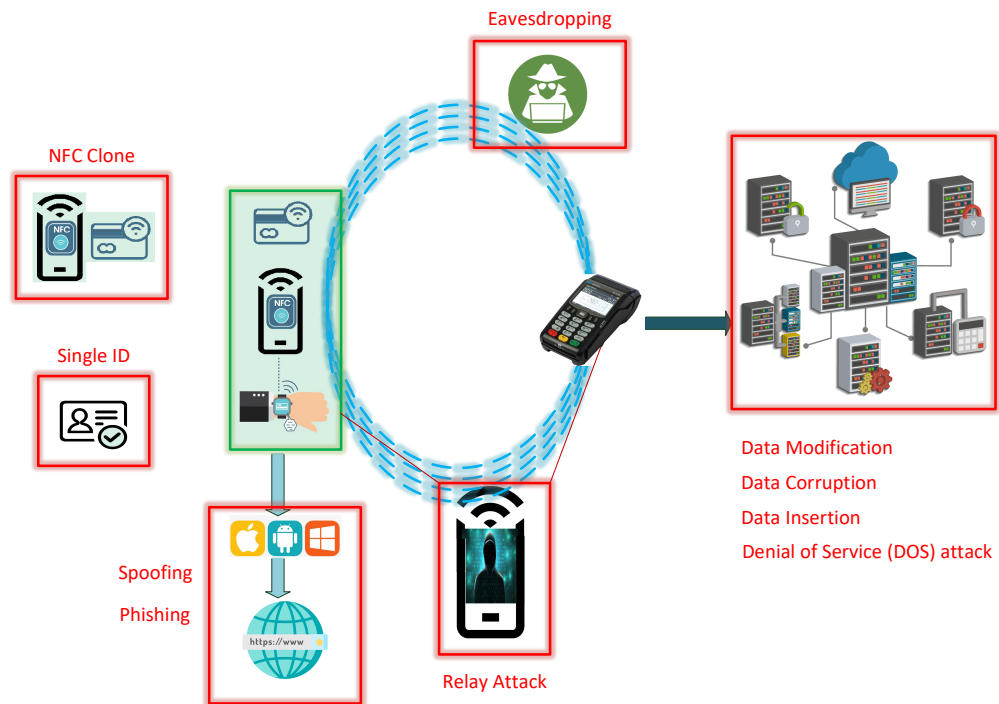


Figure 3.14: Security risks associated with NFC technology.

programme, users must bring their NFC devices close to the NFC reader or touch them. Public transit ticketing is an example of an NFC touch and go application, in which NFC users scan and touch their NFC devices to get access to the transportation system.

- Touch and confirm application: For system confirmation, the user must confirm the interaction by providing a password or accepting a payment transaction.
- The Touch and Connect programme establishes a link between two NFC devices, allowing peer-to-peer data transfer such as image exchange between two NFC-enabled smartphones.
- Touch and explore enables the user to locate and investigate applications and device features.

3.7 NFC Security Attacks

The physical nature of NFC sensors and their working mechanism, which employs an unsecured communication channel, make them vulnerable to security attacks and hazards [153]. Each contactless smart card chip has its own unique ID (ISO14443 A: UID, ISO14443 B: PUPI, Felica: IDm). They are 4, 7, or 10 bytes in length. When there is a collision during the reading process, the unique ID is required to avoid it. During the transponder selection procedure, the ID might already be obtained. The reading device is neither encrypted or authenticated throughout the reading operation. Figures 3.14 and 3.15 depict the security risks associated with NFC technology. Most of the attacks are related to the NFC working functionality and the application. However, there are two types of attacks which are related to the data stored in the devices without the need for NFC communication to be active. These type of attacks will be thoroughly explained in the following paragraph.

- **Ticket Cloning:** NFC technology may be used in ticketing services such as e-tickets and digital tickets. Ticket cloning from NFC can occur if tickets are duplicated and shared with others before they are validated [203, 204]. Everyone can use the cloned ticket as a new ticket, for example, to obtain a discount on items. The ticket can be used until it expires in case it has been validated. The cloning situation can happen in two ways, depending on how the ticketing system is designed. The purpose of ticket cloning is to share a single ticket till it expires.
- **Only use one ID:** Each contactless smart card chip has its own fixed unique ID. Because the unique ID is defined in the anti-collision standard, a simple piece of hardware like OpenPICC [203] may mimic an arbitrary ID and fake someone's identity. As a result, apps that rely on unique IDs provide not just a privacy risk to the bearer, but also a security risk to the application

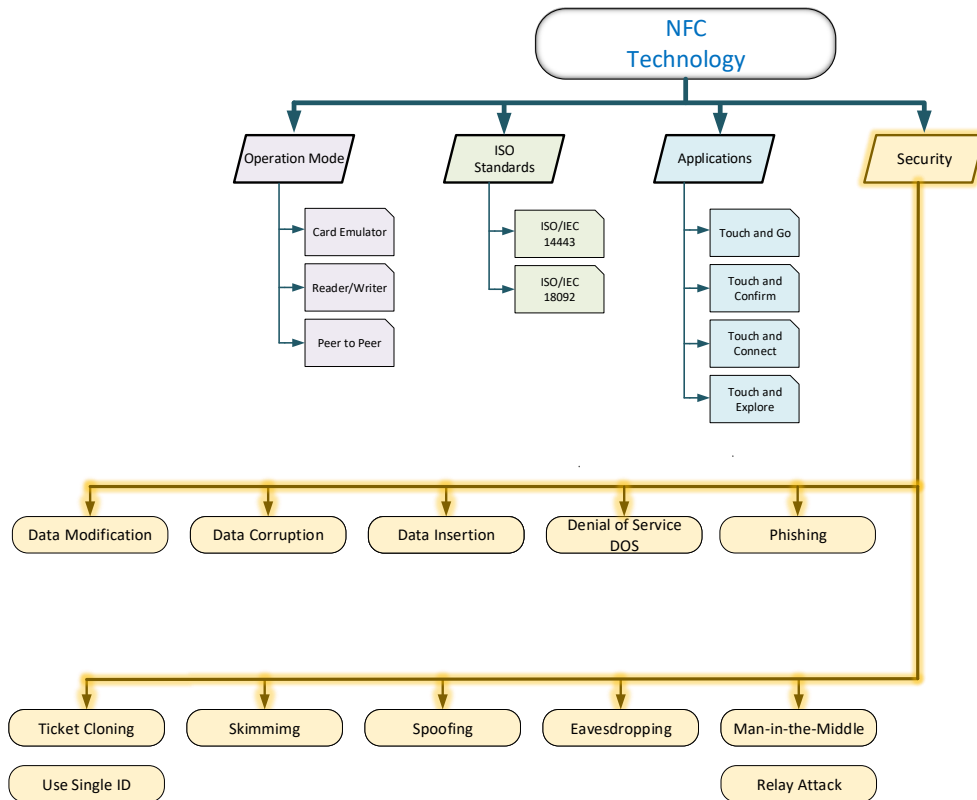


Figure 3.15: The features of NFC communication can be used to classify NFC operation modes and security.

that uses them.

Because the connection between the reader and the smart card chip is not encrypted, the ID can also be obtained by eavesdropping on it. This privacy concern might be avoided by using a random number for anti-collision, as NFC targets and e-passports currently do [204–206]. As a result, it is useless for tracking or identification. The attacker might still find out if the victim is carrying an RFID transponder, such as a smart card or an NFC device by tracing users.

3.7.1 Skimming

Another way to find and use the ID is by using software and the internet. External mode and internal mode are the two ways to secure the ID, but there are still many attacks that may be on the application.

- External Mode: In order to imitate a tag, smart card chips in NFC devices

are required. An external reader can access the secure element in external mode and cannot tell the difference between a smart card and an NFC device with a secure element. The secure element, for example, has a credit card applet that converts the NFC cellphone into a mobile payment device.

- **Internal Mode:** The host controller accesses the secure element in internal mode (reading and altering). The information in the secure element can be changed by executing apps on the handset's host controller. As a result, users may manage information in the secure element remotely via an internet connection (GPRS, Wi-Fi, and so on), commonly known as Over The Air (OTA) management. For example, when customers utilise NFC for tickets a regular smart card is a viable option. The tickets or money might be stored in a protected element that is accessible via the internet.

Memory cards (such as NXP's Mifare Application Directory) and processor cards both offer an index of applications in the secure element (JCOP e.g.). As a result, it is vulnerable to third-party players due to the exposure of other apps in secure sections. This is an issue not only in NFC technology, but also in the smart card sector.

3.7.2 Spoofing

An attacker can spoof the tag content by providing bogus information such as a fictitious domain name, URL, or email address [202]. Using SMS URIs, telephony URIs, and other URIs, smart poster URI spoofing facilitates attacks against web browsers, URLs, and mobile phone services [207]. The unique ID is defined in the standard to prevent collisions. By mimicking an ID, inexpensive hardware like OpenPICC [208, 209] may fake someone's identity. As a result, if an application utilises a fixed unique ID, the holder's privacy is easily compromised.

The authors of Reference [206] demonstrate how spoofing attacks may be used to trick the user into believing that the misleading information is real. For ex-

ample, if the user is not vigilant, the attacker will create an exact replica of a user's trusted website with a nearly identical URL, so the user will not notice the difference. Phone call and text-message spoofing utilising the NFC protocol are also applicable, in addition to uniform resource identifier (URI) and uniform/universal resource locator (URL) spoofing. Additionally, URI and URL spoofing are very helpful when used in conjunction with other attacks (i.e., cross-site request forgery).

3.7.3 Man In The Middle Attack

In a Man in the Middle Attack (MitM), an attacker deceives two parties into believing they are communicating directly with one other while, in fact, the attacker is directing the entire discussion. Let us pretend Alice and Bob are two parties that wish to communicate to each other, and Eve is the attacker who is in charge of the entire discussion. Both Alice and Bob believe they are receiving and transmitting data to one another, but the data is all originating from Eve. Assume the same basic scenario, except that the link between Alice and Bob is an NFC link, and Alice is in active mode while Bob is in passive mode. Alice creates the radio frequency field in order to convey data to Bob. Eve could eavesdrop on the data if she was close enough and deliberately disrupted the transmission to guarantee the info was not sent to Bob. In this circumstance, Alice can identify the attack by looking for any active disruption. Alice would sever the lines of contact [194]. Assume that the protocol continues without being verified by Alice. Eve would create a radio frequency field in order to communicate with Bob. However, this would result in the creation of two active radio frequency fields. Alice comes up with the first one, and Eve comes up with the second. Bob would be given data that he could not comprehend. As a result, man-in-the-middle (MitM) attacks are nearly difficult to carry out in this circumstance.

As previously stated, a MitM assault is nearly impossible on the NFC link.

However, using an active-passive communication method is strongly suggested. Furthermore, the active party should listen and examine the radio frequency field during the transmission in order to identify any disturbance caused by an assault.

3.7.3.1 Relay Attack

The relay attack is a form of MitM attack in which the attacker tries to influence communication by relaying sent/received messages between two machines. Only if at least one of the assault devices can support card emulation a relay attack can be carried out. This attack can be carried out in a variety of ways. The first case occurs when NFC is enabled in a smartphone even while it is not in use. A smart phone with a payment app can simply complete a purchase. As a result, the phone is susceptible to a relay attack. There are two attackers in this scenario, who are connected to each other over the Internet. The first assault uses a proxy device, while the second uses two NFC-enabled devices or smart phones as a relay device. In a public venue, such as a bus or metro station, a large number of people have gathered to await the arrival of the bus or metro. With a similar device, the attacker may get close to the victim's smart phone [210]. The proxy device then makes an NFC payment at the payment station. The two gadgets are used to connect the payment station and the victim's smart phone. Both ISO14443 and ISO18092 are vulnerable to relay attacks that neither the card nor the reader can detect [205, 211, 212]. Application Protocol Data Unit (APDU) instructions can be used to carry out the attack [202]. The APDU instructions can be obtained by a malicious programme through a network socket.

However, some smartphone security features, like the application sandbox, are lost. Furthermore, the security measures safeguard the sensitive parts that house the NFC payment application. As a result, the security parts on a rooted smartphone are more susceptible. In this scenario, the attacker tries to trick the user into installing a malicious programme. The victim believes he was granted access to the function by the application. The malicious programme would then get ac-

cess to the functionalities and be able to use them. Meanwhile, the programme gains access to the secure components and sends an alert to the attacker through the Internet. The attacker can now make a payment using the victim's payment information [213]. To avoid a relay attack, the user of a smart phone should make sure that NFC is turned off at all times. If the battery of an NFC device is removed, smart card functionality may be relayed. When the battery is removed, communication may not be possible unless the functioning of the device is taken into consideration. Furthermore, the owner of the smart phone should maintain the security features in order to identify any dangerous behaviour in any installed application.

3.7.4 Eavesdropping

Because NFC communication occurs via a wireless network, it is vulnerable to assault, allowing attackers to eavesdrop on NFC transmissions that are outside their reach [204, 214]. Any attacker with the right tools may listen in on a conversation between two NFC devices. The primary question is how near an attacker must be to carry out an eavesdropping assault on NFC devices. In actuality, this is dependent on the attacker's equipment, such as antennas and receivers, as well as the attack environment, such as noise and generated signal. In the card emulation mode and peer to peer mode of NFC functioning, eavesdropping is possible [204]. If the function of NFC devices is not in use, malevolent attackers can access the data content in card emulation mode. If data is transferred in peer-to-peer mode without secure security, the conversation is vulnerable to eavesdropping by an attacker. Listening to an NFC device in passive mode is more challenging since the target device may take its source power from the active device's electromagnetic field.

According to Haselsteiner et al. [194], an eavesdropping attack may be carried out up to a distance of 10 metres while an NFC device is transferring data in

active mode, but only around 1 metre when the device is in passive mode. Figure 3.14 shows how an attacker with no access to the NFC environment can listen in on a conversation between two NFC devices. An NFC transmission may be intercepted by an attacker with enough expertise and equipment, such as Proxmark. The Proxmark is a sophisticated open source gadget for investigating RFID and Near Field Communication systems that is now accessible. Proxmark costs less than USD 500 and has the ability to spy on NFC traffic between a reader and a tag. More information about Proxmark can be found here [215].

Creating a secure connection and using standard encryption algorithms between two NFC devices can protect them against eavesdropping attacks. A standard key agreement protocol such as RSA or Elliptic Curves could be used to establish a shared secret key between two NFC devices. The secret key can then be used to encrypt the communication using a symmetric key algorithm such as AES or 3DES [194]. This countermeasure will ensure the confidentiality of NFC communication and will protect against eavesdropping attacks.

3.7.5 Phishing

The act of attempting to gain sensitive information such as passwords and credit card numbers by impersonating a trustworthy entity in an electronic communication is known as phishing. Phishing attacks against the NFC environment might be simply carried out by altering or replacing NFC tags [204, 205]. The methods and diagram below show how a malicious attacker can get sensitive information such as credit card numbers by initiating a phishing attack against a parking metre that employs NFC technology to complete the payment process [216]:

- First, the attacker creates a malicious tag with misleading information, such as an URL link that leads to a phishing site. The attacker will locate a parking metre that supports NFC technology and use the malicious tag to replace the original tag.

- A victim using an NFC mobile device, such as a Samsung phone, scans the park metre tag to pay the needed charge.
- The user will be prompted to download a malicious software called com.pork-mobile, which is essentially a Web browser that leads to the phishing site.
- The user will submit sensitive information, such as credit card information, to the malicious software that has been loaded, and the attacker will gather this information.

To avoid or minimise the danger of phishing attacks, a variety of countermeasures can be undertaken. One of the most important aspects of a phishing assault is to fool users by impersonating a trustworthy institution. Nevertheless, those who are aware of the phishing attack are difficult to deceive. User education and knowledge of phishing attacks is an essential countermeasure since it reduces the frequency of successful assaults. The procedure of requiring the installation of a new programme with a dubious name will be recognised by cautious users, who will check the name and originality of the application further. Gerald et al. [205] proposed putting signatures on tags and transporters as a viable solution to this problem. Furthermore, the NFC mobile application market, such as Google's, can play a critical role in preventing rogue applications that are suspicious of phishing.

3.7.6 Data Corruption

Data corruption can occur if an attacker modifies data transferred through an NFC interface [194, 214]. When an attacker alters the data into an unknown format, it might be deemed a denial of service. Communication between the user and the receiver may be hampered. If the data on the NFC tag becomes corrupted, the tag becomes worthless, and the device must retrieve a new data. Malicious malware installed on a smartphone has the ability to damage data. To corrupt data when transferring between two NFC devices, the attacker needs a lot of power. However,

because NFC devices can examine the radio frequency field during data transfer and determine the sort of assault, this attack may be detected. Furthermore, to carry out a data corruption attack, the attacker needs more power than the NFC device can detect. As a result, NFC devices may detect this assault [217].

3.7.7 Data Manipulation

Data modification differs from data insertion, in which an attacker inserts a message into the data being transferred between two NFC devices. In data modification, an attacker can alter the data transferred between NFC devices, resulting in the recipient device getting some legitimate but modified data. During data transfer from NFC devices, the attacker can modify and convert the actual data to false data [194, 214]. During data transfer between NFC devices, the altered data might be received. The magnitude of modulation determines the viability of a data modification assault [194]. When the coding modulation is 100 percent in modified Miller coding modulation, it is impossible to conduct a data modification attack against the NFC environment, since the attacker is unable to change a bit of value 0 to a bit of value 1. Although the attacker can change a bit of value 1 to a bit of value 0 if a bit of value 1 comes before (i.e. with a probability of 0.5). In 100 percent modulation, the decoder checks two half bits for radio frequency signal on and radio frequency signal off. In order to have the decoder perceive one as zero and zero as one, the attacker must take two steps. The attacker causes a pause in the modulation that is loaded with carrier frequency in the first step, which is a viable step. The attacker creates a pause in the radio frequency signal that is received by the legitimate receiver in the second step, which is virtually impossible. Then, the attacker tries to overlap the original signal and the transmitting signal in order to give the receiver's antenna a zero signal in this phase. When the modulation is 10%, however, it is simple to carry out the data modification attack. The decoder compares and evaluates signal levels 82% and full in

10% modulation. The attacker tries to add a signal to the 82% signal in order for the 82% signal to look a full signal, and the full signal to appear as an 82% signal. As a result, the decoder would decode the valid bit of the bit's reverse value. In conclusion, the attacker is viable in all bits for a 10% modulation, but not in all bits for a 100% modulation.

There are a few techniques to protect yourself from a data alteration assault. Firstly, if 106k baud in active mode is utilised, the attacker will not be able to change all of the data transferred via the radio frequency channel. Although it is apparent that the active mode is critical, it is also subject to eavesdropping attacks. Furthermore, some bits can be changed in a 106k baud transmission. Secondly, while transferring data, the sending device continuously scans the radio frequency environment for any possible attacks. Thirdly, it appears that establishing a secure connection between two NFC devices is the best way to guard against data alteration attacks [217].

3.7.8 Data insertion

When the responding device takes longer to respond to the originating device, the objective of a data insertion attack is to inject a message into the transferred data between two NFC devices. The attack can be conducted only if the device has a latency that allows the attacker to broadcast his message before the responding device can respond. The data will be overlapped and distorted if both the attacker and the responding device transmit the data at the same time. An attacker can introduce any undesired data into messages, particularly during data transmission between NFC devices [194, 214]. The data will be sent to the reader device via the victim's mobile NFC phone. Before the original reader, the malicious reader would respond directly to the affected user. After the attacker, the initial reader will reply to the victim user, but the reply will be disregarded by the victim's mobile NFC phone.

There are three countermeasures that may be used to prevent a data insertion attack between two NFC devices. To begin, the responding device should immediately respond to the originating device. Because the attacker cannot be quicker than the responding device, the attacker will not be able to inject a message into the data transferred between the two NFC devices. Second, when transferring data, the responding device should listen to the channel to identify any possible attacks. Finally, the easiest way to avoid an attack is to create a secure connection between two NFC devices [194].

3.7.9 Denial of Service attack

The Denial of Service (DOS) in NFC occurs when a continuous stream of access requests to the NFC secure chip and malicious device block the communication [204, 205]. A malicious device might try to render an NFC device or reader inaccessible to its intended users by initiating a Denial of Service attack. The use of a jamming device that targets the NFC environment is one typical scenario of a denial of service attack [194]. The objective of jamming is to prevent two NFC devices from communicating with one other. Figure 3.14 depicts a hostile attacker using an RFID jammer to send a signal that interferes with communication between a mobile NFC phone and a service provider's reader. This interference has the potential to damage transmitted data and result in a denial of service. There is almost no method to prevent jamming. Nevertheless, there is a technique to deal with this circumstance by constantly attempting to identify jamming attacks. The application's whole installation procedure will be terminated. The secure chip could not be utilised for transactions at that time, and it was at risk of losing its functionality. Aside from that, when an NFC device is contacted with an empty tag, DOS can occur [205]. When an empty NFC card is pressed against an NFC reader, a torrent of error messages may be generated, causing NFC devices or services to be halted.

Mulliner explains another DOS assault, the objective of which is to break the trust connection between consumers and the service provider [207]. The stages below will walk you through the assault scenario description. After scanning, a malicious attacker or rival produces a tag that causes an NFC mobile phone to "crash". The malicious attacker will approach the victim or service provider in stealth mode and install the malicious tag on top of the service provider tag. After scanning, every user who visits the victim or the service provider to obtain a service using an NFC mobile phone will crash. Because the harmful tag seems to be a normal tag, it cannot be connected to a phone crash event, and this occurrence may jeopardise consumer and service provider confidence. This attack has no known solution. However, various techniques, such as fuzzing, can be used to identify it [207].

An empty NFC tag can also be used to execute a denial of service attack. According to Riyazuddin [217], simply touching an NFC device with an empty tag enables the gadget to react. The device will display an error message, which is a simple method to occupy and disable the device. Adding a control mechanism for the NFC device, such as an NFC switch, can help to avoid this type of assault. The user must turn on and off the NFC capabilities each time he needs to scan, which is a disadvantage of this approach.

3.8 Thermal issue on NFC

In addition to the security breach, there is another issue that affects NFC devices, such as the thermal issue. The Wireless Power system for smartphone charging can be schematically represented in Figure 3.16. As shown in this diagram, the device side antenna (receiver antenna) is often located near to the backcover (also known as backplate), allowing for little separation from the transmitter antenna. As a side note, the backcover must be predominantly non-conductive for wireless charging to work. Although there are ways that may allow for meaningful power transmission

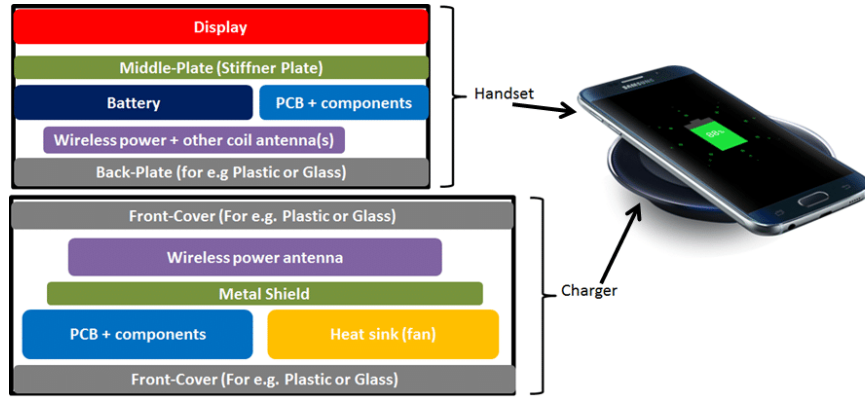


Figure 3.16: A block schematic diagram of a smartphone's and the charger. The physical equivalent of the design is shown on the right, with an image of a generic gadget put on a wireless charger.

through a mostly conductive backcover, this is not a marketed technology yet. The battery's closeness to the antenna will put additional strain on the thermal management system. In the temperature range of 0 C to 45 C, the battery, which is generally Li-ion based, is deemed to work safely (i.e. charging and discharging) [218]. As a result, the maximum temperature on the device's skin is now widely recognised to be around 45 degrees Celsius [219].

The resistive power losses (Joule heating) in the antennas, joule heating owing to eddy currents in the shielding material and any metallic components in the route of magnetic flux lines, switching losses in the power stage, and losses in passives are the main sources of heat in this system (e.g. rectifiers). Furthermore, heat is created by both the transmitter and reception systems, with a part of the heat from the transmitter side flowing to the receiver via a mix of conduction and convection.

Considering the following equations:

$$V_{R-i} = j\omega k \sqrt{L_T L_R} \cdot I_T \quad (3.1)$$

$$I_R = \frac{V_{R-i}}{R_{Coil} + Z_{Load}} \quad (3.2)$$

where V_{R-i} is the voltage induced in receiver antenna, ω is the angular fre-

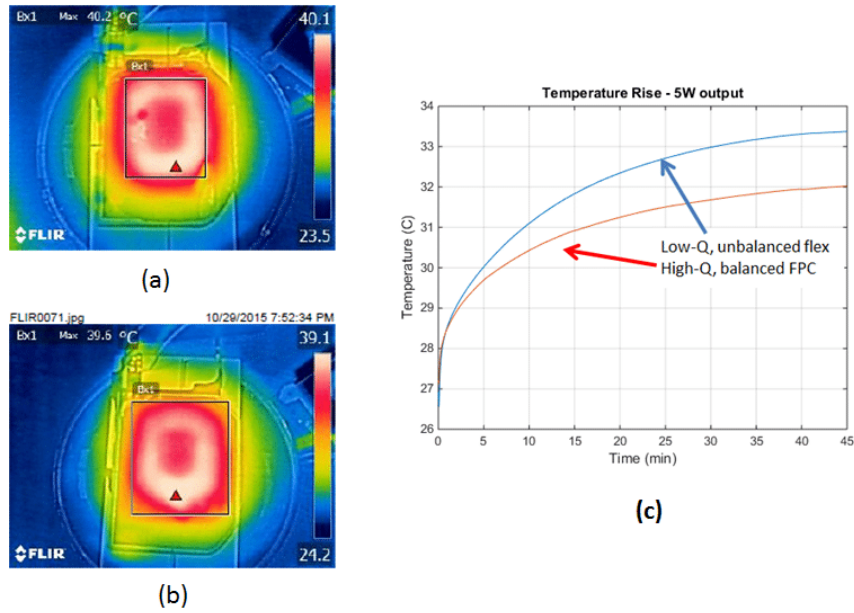


Figure 3.17: The heat map on the coil surface during the charging process. In (a) and (b) Antennas in both solutions are less than 0.3 mm thick. Figure (c) shows a 45-minute time plot at the maximum temperature location.

quency, k is the coupling coefficient, L_T is the transmitter antenna inductance, L_R is the receiver antenna inductance, I_T is the transmitter antenna current, I_R is the receiver antenna current, and $R_{AC}(\text{Coil})$ is the antenna's AC resistance at the operating frequency. Heat is generated by the $I_T^2 \cdot R$ losses in the antennas. This can be reduced by lowering the current, the I_R , and/or the R_{Coil} . To decrease the current, a higher voltage receiver Power Management IC (PMIC) architecture may be required. By utilising high-Q (quality factor) antennas with a lower ESR, the R_{Coil} can be decreased (Equivalent Series Resistance).

Apart from being high-Q, antennas for mobile devices should also have a compact form factor and a low profile (sometimes as thin as 250 μm including shielding). To decrease total cost and thickness, additional criteria such as non-standard form and integration of numerous antennas (f.e., NFC) are frequently imposed on the antenna designer. Because of the need for thinness, flexible form factors, integration, and durability, flexible circuit antennas have been the dominant technique for devices; printed antennas on a flexible substrate are present in more than 75 percent of phones delivered (200 million) in 2016, according to [220].

Thermodynamics is a problem with wireless power. The majority of wireless power systems on the market are intended to deliver a maximum of 5 watts to the load (typically battery). With the introduction of rapid charge technologies, the requirement to charge at 10W or greater is becoming increasingly urgent. In reality, the FastCharge functionality is already available on Samsung and Apple smartphones. Wireless charging in the consumer electronics arena will be increasingly seen as a thermal problem as the general electrical system design becomes quasi-commodity. The final remark implies that the thermal design of the wireless charging system will take precedence over the electrical design.

Consider the following example in terms of numbers: A 5W inductive system working at 75% efficiency dissipates around 1.67W, whereas a 10W system operating at 82% efficiency dissipates about 2.19W. Alternatively, to disperse the same amount as a 5W system, the 10W system will need to operate at roughly 86% (a 15% increase), where only a 4% efficiency reduction to 82% results in an extra 850 mW of wasted power. To consider devices in perspective, a typical WiFi modem in a smartphone uses 700 mW of power, the handset consumes around 320 mW during music playing, and 1.05 W during a 1-minute phone conversation with the display turned off [221]. In the case of a typical inductive charging system with quality factors of $Q_T = 80$, $Q_R = 15$, and coupling $k = 0.62$, the antenna to antenna efficiency is 91%. Each other block must function at 95% efficiency. In order to achieve an efficiency of 86%, the blocks in this inductive system must function at 97%.

To put it another way, we are pushing the limits of physics in terms of efficiency. First, how do we limit heat creation, and second, if heat is created, how do we distribute it fast from the major heat centres to avoid localised heating? These are the fundamental challenges that product engineers consider. The answer to the first issue is "relatively" easy, i.e. pick the best components (ICs and antennas) and assure optimum implementation for the use cases being examined, as stated in the preceding section on the quasi-commoditization of the system architecture.

Consider Figures 3.17 a, b, and c, which show the temperature data utilising two systems that are similar in every way except for the wireless power antenna design and technology. The antenna in Figure 3.17b has a higher Q (by approximately 20%), which results in a 2% increase in efficiency and operates about 1.3 degrees cooler. In contrast to the imbalanced FPC fabrication used for the coil in Figure 3.17a, the higher-Q antenna is also less expensive to make since it employs conventional flexible circuit technology.

The problem is worsened when gadgets become slimmer and batteries become larger, decreasing the amount of space available for wireless charging components. The antenna is by far the most important part of the wireless charging system. It should be emphasised that smaller devices, such as wearables, will be able to dissipate much less power before reaching the magical temperature limit of 45⁰ C [218, 219]. As a result, ultra-thin antennas that offer maximum performance are in high demand. A heat spreader material is frequently used, for example, between the antenna and the device's backcover. These heat spreaders have anisotropic thermal conductivity, which means they transfer heat better in the xy direction than in the z-direction. Heat can also be directed away from thermal sources by using Phase Change Materials (PCM) and heat pipes. This was incorporated by Samsung developers into the Galaxy 7 [222]. While the primary goal is to keep heat away from the power-hungry apps, the principle may also be applied to the wireless charging coil, particularly in higher-power systems.

Summary. The third chapter discusses the fundamentals and applications of Near Field Communication (NFC). While the NFC is still based on the WPT, and its uses go far beyond charging. While NFC is the most secure sort of WPT for the applications, it still has security concerns.

Chapter 4

Memristor and the Chua Circuit

Alongside the benefits associated with any new technology, problems and worries will be an important part of addressing them. NFC, on the other hand, has its own set of problems, including privacy and security, as shown in the previous chapter. The NFC, which is used in contactless smartcard technology, uses encryption and a specific processor to enable safe data exchange. Furthermore, wireless technology restricts communication to a small distance, lowering the chances of an attacker listening in on conversations and increasing security and privacy. While the NFC Forum claims a read range of a few millimetres (about an inch), research studies have increased it to around 80 centimetres (about 31 inches), giving attackers a considerably larger playing field.

In circuit design, both active and passive circuit components are employed, and the first circuit elements that spring to mind are passive circuit elements like resistors, capacitors, and inductors. The relationships between voltage and current, voltage and charge, and current and flux are defined by the resistor, capacitor, and inductor, respectively. In 1971 and 1976, Leon Chua of the University of California (Berkeley) demonstrated the missing connection between flux and current, as illustrated in Figure 4.1 [223, 224]. Chua termed the missing circuit element a memristor (memory + resistor) and published the new circuit element's mathematical equations at the same time. However, due of the technical challenges in

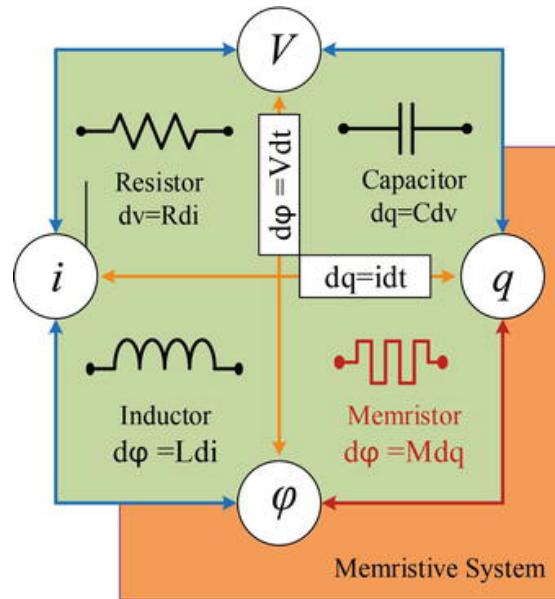


Figure 4.1: The basic passive circuit components with two terminals.

fabricating the memristor, Chua's important article failed to gain traction among scholars.

4.1 Memristor

As a result, researchers did not focus on the memristor and its applications until HP researchers fabricated the first memristor in 2008 [225]. Figure 4.2 shows the first memristor, which is composed of TiO_2 thin film and features a crossbar configuration. The mathematical model of a TiO_2 memristor was also provided by the HP research team, and the current-voltage relationship is described by

$$V = [M(x_1, x_2, \dots, x_n)] \quad (4.1)$$

where V stands for voltage, M is the memristance resistance, and it is dependent on the x_i state variables. The frequency and applied input signal affect the non-linear properties of memristance. As illustrated in Figure 4.3, the TiO_2 memristor has two major structures: a doped area and an undoped region, and the memristance varies with the ratio of the doped region and device thickness. The memristor acts as a conductor if the thickness of the doped region becomes



Figure 4.2: The memristor as seen via a scanning tunnelling microscope [225].

wide, as shown in Figure 4.3b. The undoped region becomes wide as shown in Figure 4.3c, and the memristor behaves as a high-resistance element when the input signal is applied in the opposite direction.

As illustrated in Figure 4.4, the pinched hysteresis loops serve as a fingerprint in the characterisation of memristors [226]. It means that any two-terminal device with a pinched hysteresis loop is regarded as a memristor, regardless of device material. A classic pinched hysteresis loop can be found in the first and third quadrants of the current-voltage (I-V) curves, just like in resistive switching devices [227]. To put it another way, independent of the operating mechanisms or device material, all memristors may be considered resistive switching devices [228].

Figure 4.4a shows a semiconductor-based memristor device with an active layer sandwiched between the top and bottom electrodes (TE and BE). HP laboratories used a TiO_2 metal-oxide active layer to create the first physical version of the memristor [225]. The usage of various materials and manufacturing processes was then proposed by numerous physical memristor devices. Most metal-oxide semiconductors, such as TiO_2 , ZnO , HfO_2 , VO_2 , TaO_x , and others, have memristor properties [227, 229, 230]. In semiconductors, there are two types of contacts:

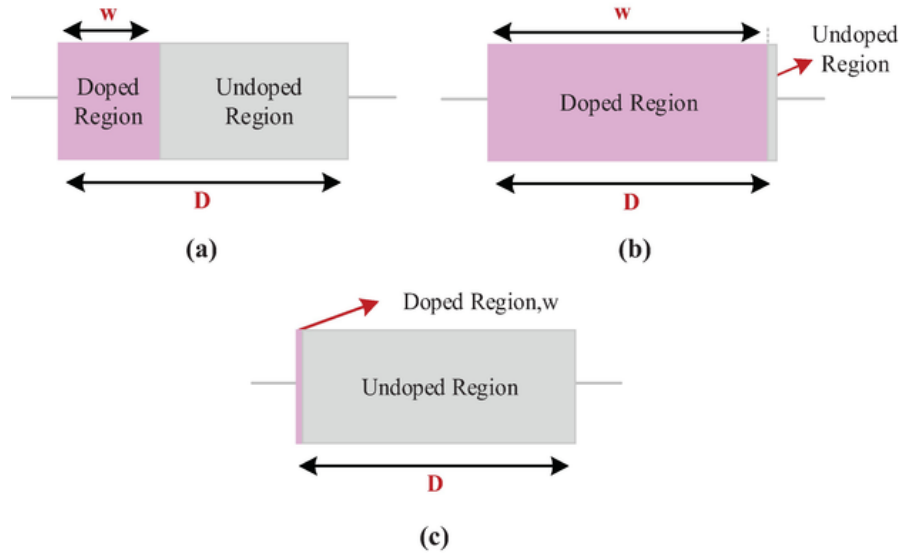


Figure 4.3: (a)Initial state, (b)low-resistance state, and (c)high-resistance state of a memristor.

Schottky (rectifying) and ohmic (non-rectifying). *Pt*, *Au*, *Ag*, *Al*, and other electrode materials can be utilised as TE or BE. One of the electrodes must be a Schottky contact in a memory cell memristor which is made of one diode and one resistor (1D1R) [231]. The memristance value depends on the w and D , which are the doped area of the memristor and the thickness of the memristor, respectively. Denoting $x = \frac{w}{D}$ the memristance results as:

$$M(x) = [R_{ON}x + R_{OFF}(1 - x)] \quad (4.2)$$

The variation of the value of x results as:

$$\frac{dx}{dt} = \frac{\mu_e R_{ON}}{D^2} i(t) \quad (4.3)$$

The electron mobility is denoted by μ_e , while the doped area and thickness of the memristor are denoted by w and D , respectively as shown in the Figure 4.3. R_{ON} and R_{OFF} represent the resistances of high and low dopant concentrations, respectively.

As illustrated in Figure 4.4, the pinched hysteresis loops serve as a finger-

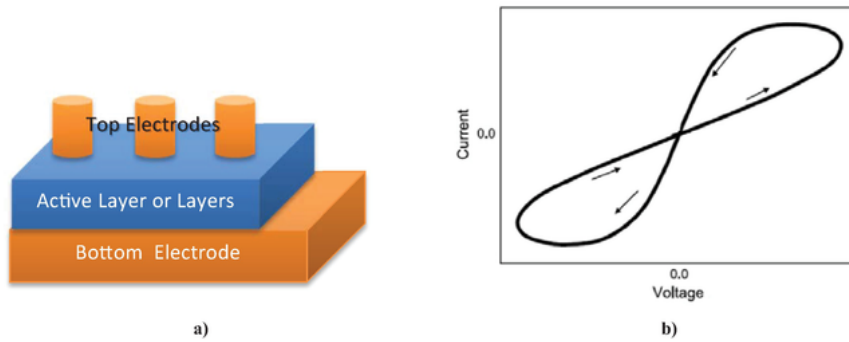


Figure 4.4: (a) Schematic depiction of a memristor device and its (b) Typical pinched hysteresis current-voltage loop.

print in the characterisation of memristors [226]. It means that any two-terminal device with a pinched hysteresis loop is regarded as a memristor, regardless of device material. By providing a certain voltage, reversible switching between a low-resistance state (LRS) or ON (SET) and a high-resistance state (HRS) or OFF (RESET) may be accomplished [232]. In both unipolar and bipolar operations, the compliance or limit current (CC) must be adjusted in order to avoid irreversible damage from overcurrent [227]. A memristor device's compliance current is also connected to its power consumption [233]. When employed as a switching device, the memristor has two states: high-resistance state (HRS) or OFF (RESET) and low-resistance state (LRS) or ON (SET) [227]. When memristors are employed as switching devices, the ON/OFF ratio, defined as the percentage between resistances in HRS and LRS, is one of the most significant factors [232]. When a resistive switching memory or ReRAM element is employed in a memristor device, the time to hold the ON/OFF state is an essential criteria [234]. Cycling endurance is one of the most important characteristics of memristor-based memory devices [232], since the memory unit must be read or written frequently by the other control units.

Figure 4.5 depicts the unipolar and bipolar functioning of memristor devices, which may be classified based on current-voltage characteristics. The amplitude of the applied voltage determines the characteristics of unipolar operations, whereas polarity and amplitude of the applied voltage are resolved in bipolar operations

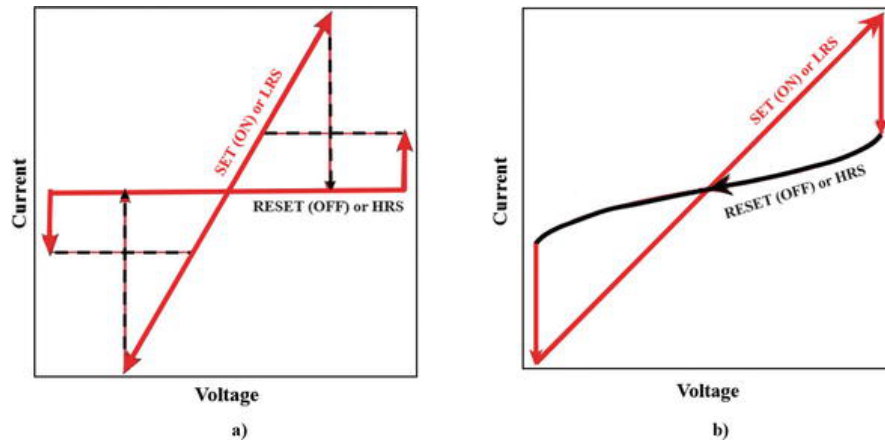


Figure 4.5: Memristor device current-voltage curves (a) unipolar and (b) bipolar.

[227]. Because it requires simple circuits, unipolar operation in memristor switching devices is more striking than bipolar operation. However, as compared to unipolar operation, bipolar operation has higher uniformity and durability [232].

4.2 Memristor Emulator

Researchers have been unable to obtain memristor devices on the market due to production issues with the memristor. As a result, researchers concentrated on developing memristor emulators for use with other circuit components.

Biolek and colleagues [235] proposed the first and most practical memristor model. The window function is used to account for boundary conditions, and the feedback-controlled integrator is used to perform the memristor's memory effect. Figure 4.6 depicts a memristor block diagram and accompanying SPICE model. All of the simulation results in Figure 4.7 were generated using the SPICE scripts listed below in Figure 4.8.

In conclusion, the memristor emulator circuits are compared based on certain key design criteria such as circuit elements utilised, electronic controllability, power supply value, and so on. Each emulator is better than the others in terms of features.

Memristor devices, models, and emulators have all been mentioned in this chapter. Because memristors exhibit non-linear properties, a mathematical model

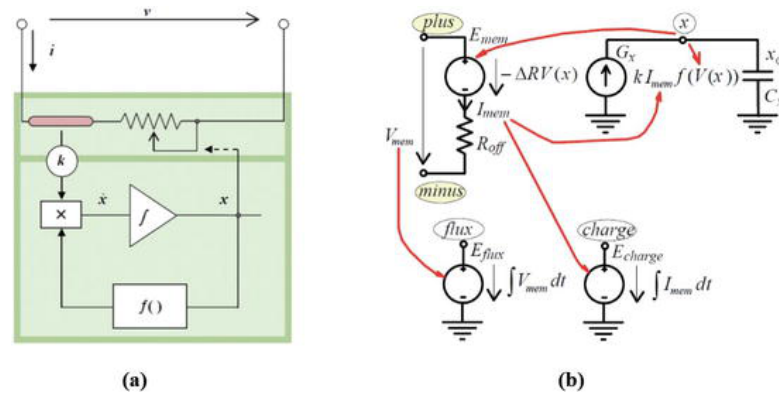


Figure 4.6: The memristor (a) is depicted as a block diagram and (b) as a SPICE model [235].

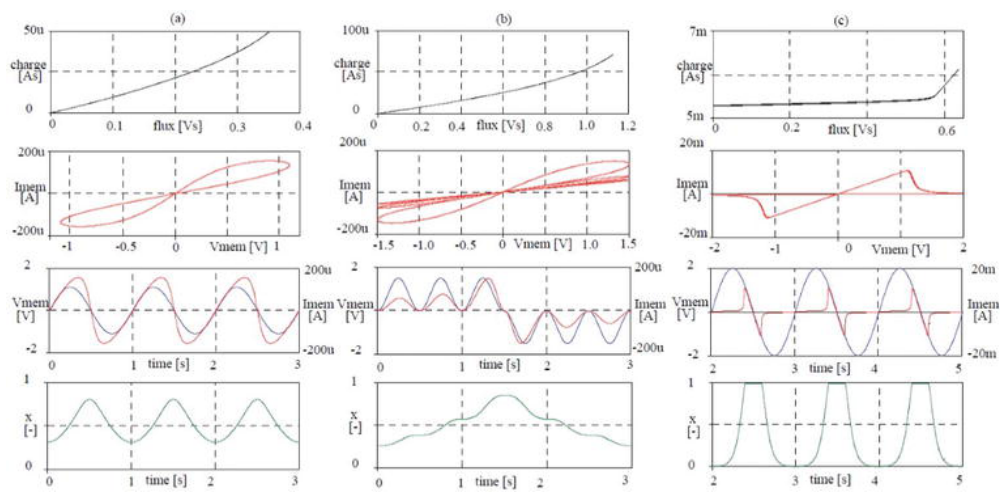


Figure 4.7: Memristor plots: charge-flux, current-voltage, current-voltage-time, and x -time curves [235].

of the memristor should be created using high-order mathematical equations. Because active circuit elements are flexible and suited for non-linear circuit element designs, they are required to construct memristor emulators. Nowadays, memristors can have a variety of properties depending on the materials used to make them. The memristor structure directly influences important features such as switching mechanism, synaptic function, and operating frequency region. As a result, multiple models and circuits must be implemented to simulate genuine memristors. Other emulator circuits have hard-switching properties, while others have smooth-switching properties, and some emulators allow for a spike-timing-dependent plasticity process. As a result, researchers are unable to easily access

```

* HP Memristor SPICE Model
* For Transient Analysis only
* created by Zdenek and Dalibor Biolek
*****
* Ron, Roff - Resistance in ON/OFF States
* Rinit - Resistance at T = 0
* D - Width of the thin film
* uv - Migration coefficient
* p - Parameter of the WINDOW-function
* for modeling nonlinear boundary conditions
* x - W/D Ratio, W is the actual width
* of the doped area (from 0 to D)
*
.SUBCKT memristor Plus Minus PARAMS:
+ Ron = 1 K Roff = 100 K Rinit = 80 K D = 10 N uv = 10F p = 1
*****
* DIFFERENTIAL EQUATION MODELING *
*****
Gx 0 x value = {I(Emem)*uv*Ron/D^2*f(V(x),p)}
Cx x 0 1 IC = {(Roff-Rinit)/(Roff-Ron)}
Raux x 0 1T * RESISTIVE PORT OF THE MEMRISTOR *
*****
Emem plus aux value = {-I(Emem)*V(x)*(Roff-Ron)}
Roff aux minus {Roff}
*****
*Flux computation*
*****
Eflux flux 0 value = {SDT(V(plus,minus))}
*****
*Charge computation*
*****
Echarge charge 0 value = {SDT(I(Emem))}
*****
* WINDOW FUNCTIONS
* FOR NONLINEAR DRIFT MODELING *
*****
*window function, according to Joglekar
.func f(x,p) = {1-(2*x-1)^(2*p)}
*proposed window function
;.func f(x,i,p) = {1-(x-stp(-i))^(2*p)}
.ENDS memristor

```

Figure 4.8: Modelled memristor SPICE coding in Reference [235].

genuine memristors, making all emulation models and circuits essential for displaying real memristors. Because memristors are ultra-dense devices that require extremely little energy, it is not just necessary to imitate a genuine emulator. Researchers also want emulator circuits with low energy consumption and a straightforward layout.

4.3 Security based on chaos

In cryptography, chaotic electrical circuits describe deterministic systems that may be utilised as random number generators. Analog chaotic circuits are the only way to create really chaotic signals. The synchronisation of the encryption and decryption sides of a cryptosystem must be ensured, which can be difficult due to the chaotic circuits' high sensitivity [236, 237]. Exclusively digital chaotic circuits, which operate only as pseudo random number generators, may accomplish total inversion of the encryption and decryption sides [238]. An appropriate mathematics model replaces the chaotic analogue circuit in a digital chaotic cryptosystem. The latter is generally represented by equations that are solved using computers and related numerical methods. As a result, the chaotic circuit's digital model is just an approximation of its analogue counterpart, acting solely as a pseudo random number generator (PRNG) rather than a really random number generator (TRNG). In a computer, the number of different values is always fixed, whereas the values are represented by a finite number of bits. Therefore, for encryption purposes, analogue circuits are the most used.

Electronic circuits can be linear or non-linear in nature. In the real world, there is no such thing as full linearity. All circuits are non-linear. Their analysis is often challenging mathematically since it involves solving non-linear differential equations. Non-linear circuits are made up of a large number of circuits with varying behaviours. Concentrating solely on autonomous non-linear circuits, we may classify them based on equation solutions, which describe their behaviour [239]. The following are some possible solutions:

- converge to a unique equilibrium point operating point (RLC-filters, amplifiers etc.);
- converge to one of several potential equilibrium points (bistable circuits, memory cells, sample-and-hold circuits, Schmitt trigger circuits etc.);

- be periodic or quasi-periodic (oscillators, periodic signal generators etc.).

The answers shown above describe what is known as "normal" circuit behaviour [239]. During the last four decades, however, circuits with even more unusual, chaotic behaviour have joined circuits with "normal" behaviour. They are non-linear circuits whose behaviour, despite a clear analytic description, cannot be predicted exactly due to their great sensitivity to beginning circumstances and particular parameters.

Simple RLC circuits, different oscillators, capacitive-trigger circuits, digital filters, flip-flops, adaptive filters, power supply and converters, and power circuits are among the items on the list.

The Chua's oscillator, shown in Figure 4.9a, is the most well-known chaotic circuit, and it has been the subject of several scientific investigations [240]. The Chua's oscillator, according to Kennedy [241, 242], is the only physical system for which the presence of chaos has been demonstrated empirically, validated numerically (with computer simulations), and mathematically proven [243].

Chaotic signals do not fit into any of the categories of nonlinear differential equation solutions listed above. Although their temporal waveforms are similar to random signals, there are significant distinctions between them since they are predictable, but only for a brief period of time. Chaotic circuits have an orderly disorderly behaviour. Experiments demonstrate that nearly all electric and electronic circuits react chaotically under certain conditions (selected parameters, beginning conditions, input signals, etc). [239]. Chaotic circuits and other chaotic systems share features such as high sensitivity to starting circumstances, bifurcations, positive Lyapunov exponents, chaotic attractors, fractals, and so on [244, 245]. These features are subsequently transmitted into cryptosystems when utilising this type of system cryptography.

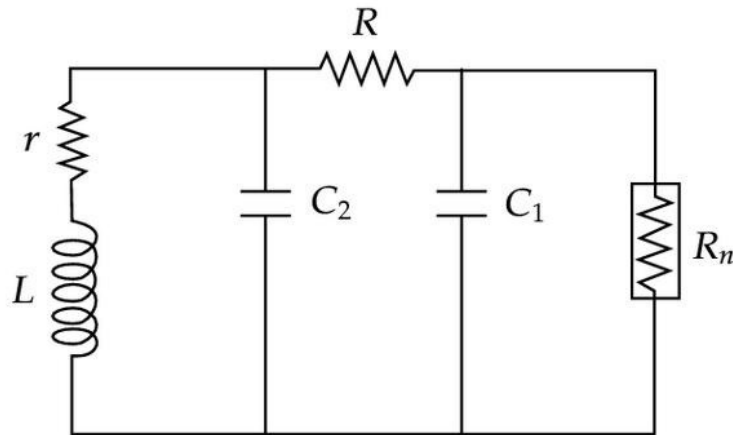


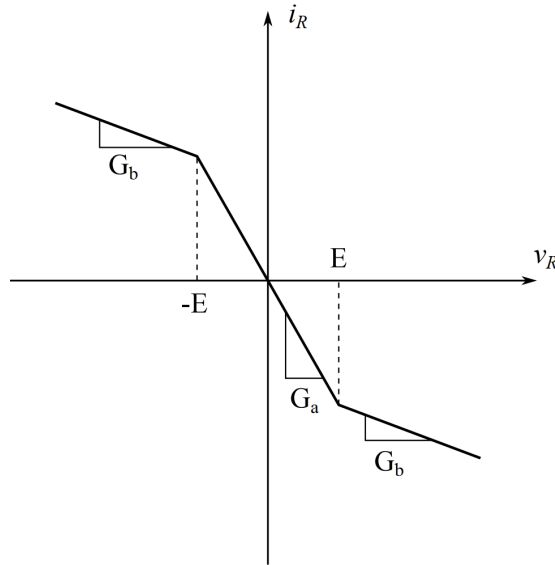
Figure 4.9: Typical Chua circuit represented with the parasitic resistance.

4.4 The Chua's Circuit

It is important to investigate the chaos generated and the Chua's Circuit's (shown in Figure 4.9) properties. The Chua's Circuit is an oscillator and a third-order non linear autonomous circuit, respectively [242]. Chua's circuit has become a global model for chaos because it is equipped with an extremely broad repertory of non-linear dynamical events. Simple electrical components such as resistors, inductors, capacitors, and a nonlinear resistor, known as Chua's diode (or memristor), make up the circuit. The fundamental oscillation frequency is determined by the values of the L inductor and C_2 capacitor, which form a resonant circuit. The $v - i$ characteristic of Chua's diode is made up of three piecewise-linear segments with two negative slopes G_0 and G_1 , as shown in Figure 4.10.

The capacitor C_1 may be thought of as a parasitic capacitor that prevents Chua's circuit from becoming chaotic. In reality, the capacitance C_1 can act in the bifurcation parameter in the same way as the resistor R can [242]. One of the first realisation of the Chua diode was like a voltage-controlled negative resistor (R_N), which is formed by the operational amplifiers U1 and U2, as well as the resistors R3 to R8 as shown in Figure 4.11.

If $R_4=R_5$ and $R_7=R_8$, the following equations give the negative slopes of the $v - i$ characteristic:

Figure 4.10: Chua diode (or memristor) $v - i$ characteristic.

$$G_a = -\frac{1}{R_3} - \frac{1}{R_6} \quad (4.4)$$

$$G_b = \frac{1}{R_5} - \frac{1}{R_6} \quad (4.5)$$

We may alter the behaviour of Chua's circuit by modifying the bifurcation parameter (such as R in the Figure 4.12), which is represented by the state differential equations:

$$\frac{di_3}{dt} = -\frac{1}{L_1}v_2 \quad (4.6)$$

$$\frac{dv_2}{dt} = \frac{1}{C_2}[G(v_1) - v_2 + i_3] \quad (4.7)$$

$$\frac{dv_1}{dt} = \frac{1}{C_1}[G(v_2) - v_1 - f(v_1)] \quad (4.8)$$

The variables v_1 , v_2 , and i_3 used here are the state variable which define the behaviour of the circuit. In order to simplify, we have defined $G = \frac{1}{R}$.

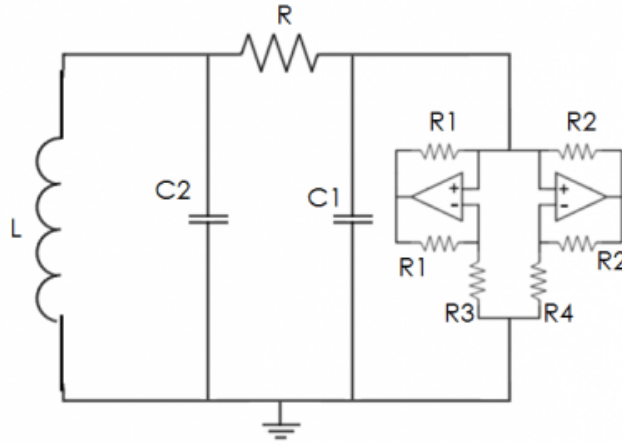


Figure 4.11: Realisation of the Chua diode with a voltage-controlled negative resistor R_N .

The so-called normalised dimensionless version of Chua's equations was employed [246]. These are obtained by adding new variables to the equation: $x = v_1/E$, $y = v_2/E$, $z = i_3/(E \cdot G)$, $\tau = tG/C_2$, $a = G_a/G$, $b = G_b/G$, $\alpha = C_2/C_1$, $\beta = C_2/(L_1 \cdot G^2)$. Typically, there are used a functions for the Chua diode, and the $f(v_1)$ function:

$$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \quad (4.9)$$

which allows to write the circuit normalised state equation as:

$$\begin{aligned} \frac{dx}{d\tau} &= \alpha[y - x - f(x)] \\ \frac{dy}{d\tau} &= x - y + z \\ \frac{dz}{d\tau} &= -\beta y \end{aligned} \quad (4.10)$$

With the answers to the differential equations presented above, we examined Chua's Circuit behaviour. The state variables time waveforms: $x(t)$, $y(t)$, and $z(t)$ are used to depict the equations' solutions (t). These are the voltage time waveforms $v_1(t)$, $v_2(t)$, and current time waveform $i_3(t)$ in figure 4.9b. We can change the overall behaviour of the circuit by altering it. It is possible to calculate: $\alpha = 9$ and $\beta = 5 \cdot 10^{-6} \cdot R^2$ based on the specified values of element parameters.

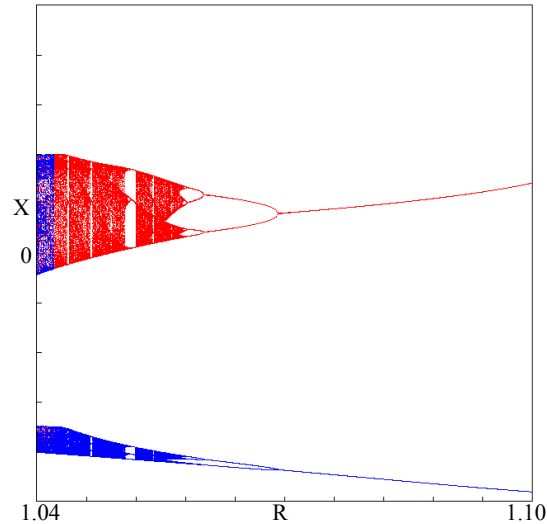


Figure 4.12: In Chua's circuit, an example of a one-parameter bifurcation diagram.

Trajectories in three-dimensional state space can be used to represent the solutions to Chua's equations. Figure 4.13 depicts several MATLAB simulations of them. When the value of $\beta > 15.4$ is used, the Chua's Circuit acts like a typical harmonic oscillator. The trajectory in this case indicates a limit cycle, as illustrated in figure 4.13. A doubling of the period occurs at the value of $\beta = 16.4$ as well as the occurrence of bifurcations, where the state variables have two distinct amplitudes. The trajectory only terminates after two rotations within the state space (figure 4.13(b)). As the parameter is reduced, the orbit splits even further, resulting in the development of 4^{th} period, 8^{th} period, 16^{th} period, and so on. Period 4 is depicted in Figure 4.13(c), with four distinct maximum values for separate state variables. The orbit splitting gets more frequent when the parameter is reduced, eventually leading to the development of an orbit with an indefinite period, which reflects the chaotic regime of the circuit functioning. At a parameter value of $\beta = 15.4$, this is possible. In this scenario, in the state space, a peculiar spiral Chua's attractor develops, as illustrated in figure 4.13(d). In such instances, the trajectory encircles one of the three virtual equilibrium circuit states and never closes [242]. The spiral Chua's attractor transforms into a double-scroll Chua's attractor as the parameter is reduced further (figure 4.13(f)). In this case, the

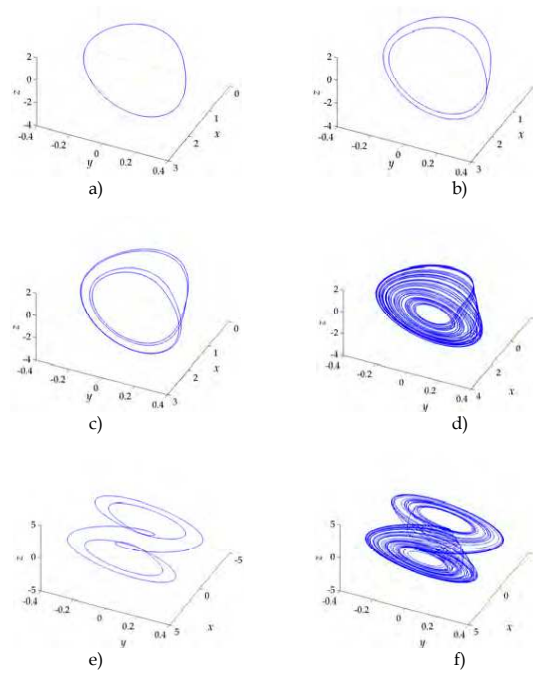


Figure 4.13: The Chua's Circuit's behaviour as a function of the β bifurcation parameter: (a) limit cycle ($\beta = 17$); (b) period 2 ($\beta = 16.2$); (c) period 4 ($\beta = 15.7$); (d) spiral Chua's attractor ($\beta = 14.9$); (e) periodic window ($\beta = 14.31$); (f) double-scroll Chua's attractor ($\beta = 14.2$).

trajectory travels and loops around two different virtual states at random. Several narrow so-called β periodic windows' within the Chua's Circuit occasionally oscillates again, interrupting the chaotic regime of the circuit functioning. Figure 4.13(e) shows an example of a periodic window, which is defined by a closed trajectory in the state space. The periodic window vanishes when the bifurcation parameter is changed slightly, and the circuit begins to fluctuate chaotically again.

4.4.1 Electric simulation Chua circuit

The study was conducted at various parameters, which in a real circuit are determined by the values of α and β and the circuit components R , C_1 , C_2 , and L_1 . The constant values of the elements were $C_1 = 10nF$, $C_2 = 90nF$, $L_1 = 18mH$, and the Chua's diode parameters were $G_a = -1/7$, $G_b = 2/7$. The variable resistance R is a bifurcation parameter to which the circuit is extremely sensitive. When the resistance R is changed in Chua's circuit, a branching route to chaos is detected,

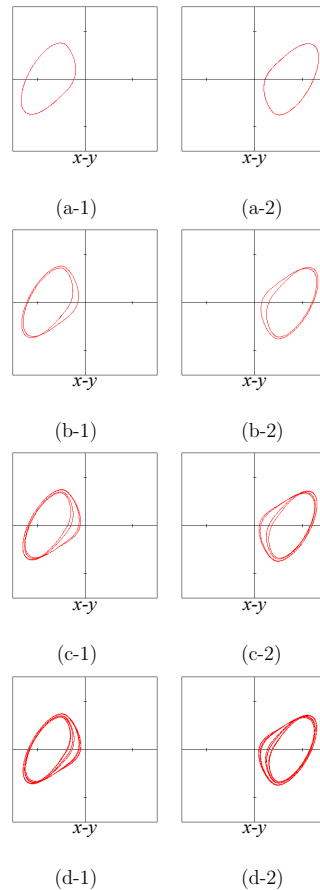


Figure 4.14: Chua's circuit attractors. Two coexisting attractors during several periods of chaos (a)-(d).

as shown below. Figure 4.14 depicts a one-parameter bifurcation diagram to chaos as resistance R decreases. When the resistance R is reduced, an equilibrium point loses stability, and a stable limit cycle arises through an Andronov-Hopf bifurcation. As the value of R is reduced further, the stable limit cycle loses stability and a period-2 limit cycle arises, which we will refer to as period-2 limit cycle. As R is reduced further, the period-2 limit cycle loses stability and is replaced by a stable period-4 limit cycle. This bifurcation happens an unlimited number of times at ever-decreasing resistance parameter intervals, converges at a geometric rate to a limit (bifurcation point), and chaos is observed. Starting with a stable limit cycle (Fig. 4.14(a)), we go on to a stable period-2 limit cycle (Fig. 4.14(b)), a stable period-4 limit cycle (Fig. 4.14(c)), a stable period-8 limit cycle (Fig. 4.14(d)), and ultimately a spiral Chua's attractor (Fig. 4.15(e)).

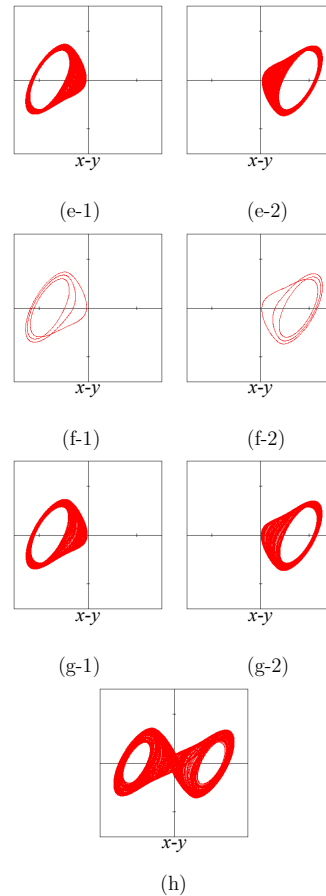


Figure 4.15: Chua's circuit attractors. Two coexisting attractors during several periods of chaos in (a)-(g). In (h) a scroll attractor with two scrolls.

With the decrease of R , chaos appears on the path, and certain parameter areas where periodic limit cycles develop appear. Between the parameter areas where chaotic attractors are found, a stable period-3 limit cycle (Fig. 4.15(f)) is observed. Two symmetric attractors focused unstable equilibrium points that are symmetrically situated at the origin coexist in the parameter areas shown above. As R is reduced further, two coexisting attractors combine to form a chaotic attractor that spans both positive and negative areas (Fig. 4.15(h)). A double-scroll attractor is a chaotic attractor with two scrolls.

4.5 A new topology of WPT circuit

The security in wireless communication is increasingly becoming important for wireless power transfer (WPT) system in order to preserve the data transmitted.

The WPT adopts inductors, due to the transmission being made by mutually coupled inductors. Increasing the security in these systems creates an opportunity for numerous new applications. An useful application of this technique is an access card or any other short range data encryption. There are many technical achievements on WPT systems, but they are mostly based on the working principles, circuit topology and transfer efficiency [123, 247].

The inductive link is able to integrate power and data together [248] and thanks to the short range functionality, it offers more security in communication. Despite the short distance, there is an inevitable risk of energy and data theft. Some solutions provide a selective WPT technology made by switching capacitors in order to achieve an oriented power transmission to a specified receiver among the unauthorised receivers [151, 249].

The Chua circuit is also known to produce chaotic behaviour. In general, the chaotic networks demonstrate unpredictable and complex dynamic behaviour. Their states oscillate around certain attractors and jump from one trajectory to the next at random intervals, with no discernible pattern. The obtained dynamical behaviours are chaotic with coexisting multiple attractors [250, 251], and hidden attractors [252–254].

In this PhD work, we are introducing a memristor which creates the oscillation of the LC resonance instead of the traditional switches. Furthermore, it is not necessary to add an external circuit to drive switches and there will be no issues related to timing. In addition, thanks to the special non-linearity and memory characteristics of the memristor, it is possible to adopt a key based mutual authentication on the last status and its subsequent encryption and decryption.

Therefore, we propose a memristor-based architecture for WPT systems. The system possesses the quality of transmitting chaos wirelessly without using any switches and driving circuitry. Furthermore, the system will not be predictable by algorithm; therefore has the possibility of achieving the highest level of encryption based on the last state of the memristor.

Summary. The conventional WPT employs switches to generate oscillations for the coil/antenna, which is inefficient and causes thermal issues. This oscillation could be accomplished through the use of alternative topologies such as self oscillating circuits. Additionally, we looked into technologies that may be used to enhance security. The Memristive Chua circuit offers chaotic self-oscillation.

Chapter 5

Memristive WPT

The security of powering systems has been a major problem over the last decade, leading to an increased interest in wireless power and data transfer. In this PhD research, a new inductive Wireless Power Transfer (WPT) circuit topology has been used. In traditional WPT circuits, the inverters are used to produce an oscillation for the transmitter coils. The classic WPT system includes intrinsic energy dissipation sources due to the use of switches, necessitating the need of an extra control circuit to ensure proper switching time. Furthermore, they have limited data encryption capabilities. As a result, an unique WPT system based on memristors has been developed, eliminating the need for switches. Additionally, because this novel topology communicates a synchronised chaotic behaviour, it becomes highly beneficial. This circuit may be used in Near Field Communication (NFC), where chaotic true random numbers (TRNG) can be generated to increase security. The results of simulations indicate the functionality of Memristor-based WPT (M-WPT) and its ability to generate random numbers. We experimentally proved the chaotic behaviour of the circuit and statistically demonstrated the development of TRNG, using an Arduino board and the Chua circuit (another representation in Figure 5.1) to build the M-WPT system.

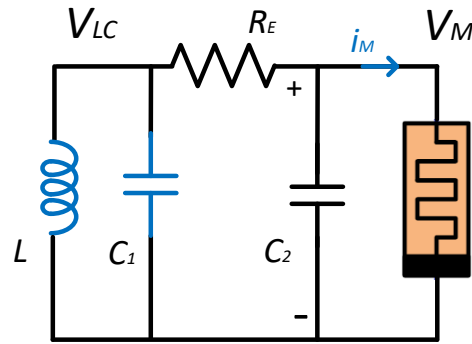


Figure 5.1: Memristive circuit developed by L. Chua[255].

5.1 Wireless Power Transfer and Memristor

Near Field Communication (NFC), which is built as a WPT system, is very sensitive to the encryption problem and it is largely used in contactless credit cards, smartphones, and digital keys (some examples are shown in Figure 5.2). NFC is a bidirectional, low-bandwidth wireless communication technology that uses electromagnetic induction to transmit information. This technology also allows data to be exchanged between devices separated by a distance of up to 10 cm [256]. The receiver harvests energy as well as transmits and receives data from the transmitter. The access cards and digital keys have internal data encrypted via software and stored in the device memory. This encryption is traditionally based on the Hash function algorithm [214, 257]. This type of algorithm is well known and it is largely available on the internet. In high-security applications, it is necessary that such important data be protected by an internal electronic device. Therefore, we introduced an NFC system built on a memristive circuit able to produce a chaotic waveform. There are three great advantages of memristors, which are used in this WPT application:

- It generates less heat than transistors or switches.
- It is capable of storing charge and remembering its last state.
- It is possible to develop chaotic behaviour.



Figure 5.2: Some security applications of NFC technology. Commercial products like a security safe lock with an NFC system opening key. A BMW door opening and NFC house handle. The image was taken from a car shop in the United Kingdom and the web source [258].

Table 5.1: Comparison between traditional WPT and a M-WPT system.

	WTP (NFC)	M-WPT
Power	Transmitted (Harvested)	Harvested
Data	Oscillation	Chaos
Distance	Over 30 cm (10 cm)	10 cm
Operating Frequency	Up to 13.5 MHz	Up to 7 KHz
Control	Timing, Switches and Data Algorithm	Data Algorithm
Receivers	Many	Only one

Table 5.1 shows a comparison between traditional WPT in NFC applications and the new topology introduced in the current article. Both systems work on harvested energy and have the same range. On the other hand, the traditional WPT allows multi-receivers and is prone to Man-in-the-Middle (MitM) attacks. Whereas the WPT system with memristors can communicate only with one receiver, being immune to MitM attacks, and does not require external circuits to drive timing for switches, and it is able to create highly encrypted protection. Moreover, it is not based on algorithms that can be software hacked. The waveform generated is chaotic and it is based on the last state of the state variables. Every time that the system reads from the memristor, it will bring the internal state of the memristor to a different point of stability, which is completely chaotic and not correlated with the previous one.

Similarly to the NFC contactless payment, the M-WPT system will have a

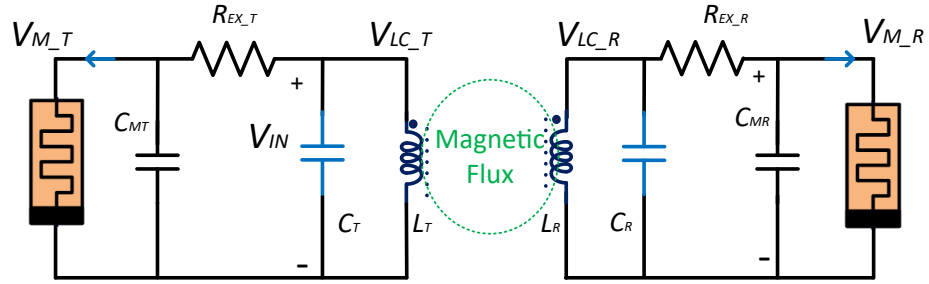


Figure 5.3: The wireless power transfer circuit and the system built with Memristors.

Table 5.2: Parameters of the system proposed.

Chua's' Parameter	Transmitter	Receiver	Value
C_1	C_{MT}	C_{MR}	6.8 nF
C_2	C_T	C_R	68 nF
R_E	R_T	R_R	2.18 k Ω
L	L_T	L_R	8 mH
M			3.8 mH

digital IC managing the data and creating the synchronisation protocol of communication. However, this is a further development for a specific application where manufacturers will apply in a successive stage.

To our knowledge, there are no records about this type of system. In the scientific literature, although a lot of security authentication schemes for NFC are presented, researchers have created protocol protections or solutions for a single electronic device. Random number generation (RNG) is the most widely adopted method for cryptography. This method can be classified into two categories, namely Pseudo Random Number Generator (PRNG) and True Random Number Generator (TRNG). The PRNG is based on the mathematical implementation of electronic devices through logic functions [259, 260]. The TRNG is a hardware component that generates numbers by relying on the intrinsic stochasticity of the physical variables as a source of randomness. For example, thermal or bust noise in electronic devices is often exploited by TRNGs methods [261, 262]. None of these solutions are based on the synchronisation of chaos between a transmitter and receiver. The most advanced security in NFC is using inter-

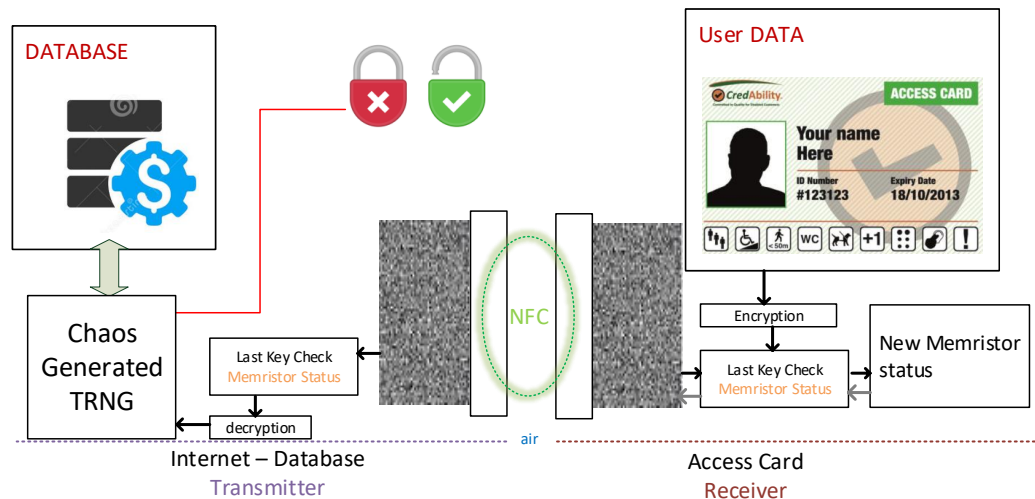


Figure 5.4: The crypto-system model is applied to high-level security: on the left, the transmitter lock and the receiver in the Card Key.

net third-party verification [263]. The memristor has also been efficiently used in imaging and communication encryption [264] providing the highest level of encryption achieved. In a memristor-based chaotic cryptosystem model, a chaotic circuit is critical to decide the chaotic encryption and decryption. For example, an user key, which is defined by initial values resulting in chaos of the memristor circuit, is given a chaotic sequence generation. Then, the encryption and decryption are developed from this sequence. Therefore, it is possible to combine the WTP technology and a memristor-based chaotic circuit by synchronising the two devices.

One of the notable advantages of the system proposed is shown in the last part of Table 5.1. The system proposed allows only one receiver during the transmission of data. If more than one receiver tries to connect, it will create an imbalance in the circuit and the communication will immediately stop.

5.1.1 Typical Functionality

The memristor-based chaotic cryptography system model consists of two parts as shown in Fig. 5.4. These are two symmetrical copies of the Chua's circuits shown in Fig. 5.1, and mutually inducted in air; hence composing the M-WPT system

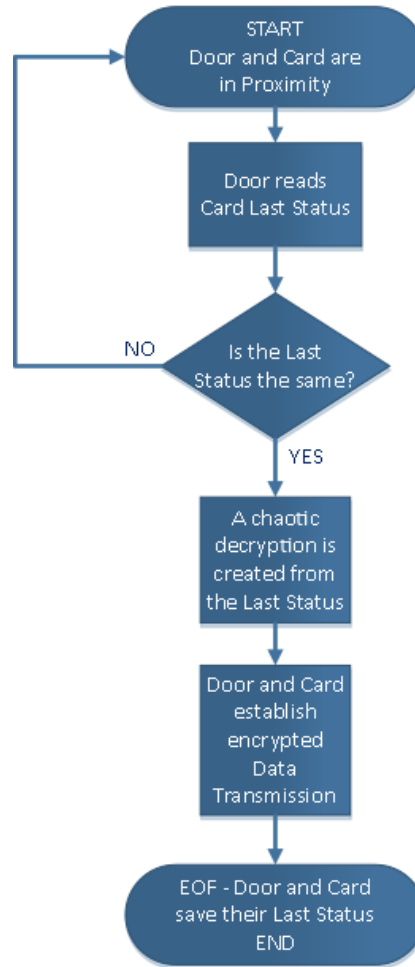


Figure 5.5: Flowchart of the door opening procedure.

shown in Fig. 5.3. In a typical Chua circuit, the initial condition is applied on the Capacitor C_T from external digital source. Therefore, in the $L_T C_T$ and $L_R C_R$ there is a connection to A/D or D/A converter. According to the cryptosystem model shown in Fig. 5.5, the process of chaotic encryption key for opening safety data is described as follows:

Step 1 - The door lock has been configured from a customer's database and has in memory the last status of the Memristor. The Access Card has an internal ID code encrypted by the last Memristor chaotic status.

Step 2 - When the transmitter and receiver are close enough, the card harvests energy from the door lock, and it is active to start a new chaotic oscillation depending on its last status. Similarly, the door lock will synchronise with the

card and its last status.

Step 3 - The last status of the card is compared with the door lock memory. If the last status coincides with the expected value, the system can decrypt and encrypt data. Otherwise, the last status of the card is modified to an unrecognisable value and any other attempt will not go over step 3. There are thousands of combinations in only one memristor, and the internal value can not be manipulated or read via software or algorithms.

Step 4 - When it is successful, the communication is established and the data keys are transmitted.

Step 5 - At the end of the payload, both digital parts will disconnect the memristor, storing their last status. The door key stores a copy of the last status of the Access Card memristor.

The cryptography model of the Memristor-based chaotic system consists of two parts, which are the two symmetrical Chua's circuits, the Transmitter and the Receiver, respectively, as shown in Figure 5.3. The initial condition is applied to the capacitor C_{1P} from an external digital source, exactly as in a typical Chua circuit. As a result, because the system is two-way, the $L_P C_{1P}$ has a connection to either an A/D or D/A converter. In the cryptosystem model, the memristor-based chaotic circuit is critical in deciding the encryption and decryption. When the user device key (UDK), which is defined as the internal state value of the memristor, is given, then a new CB is generated from the UDK. The digital sequence of the chaotic encryption (ECB) and decryption (DCB) is developed once the CB has been obtained. The information can be encoded/decoded according to the cryptosystem model.

It is important to clarify to the readers that the transmitter and receiver do not generate the same sequence of random numbers. They will, however, generate synchronised chaotic behaviour based on the last status of the receiver's memristor (internal state variable).

The system employs the symmetrical key, which uses only one secret key to

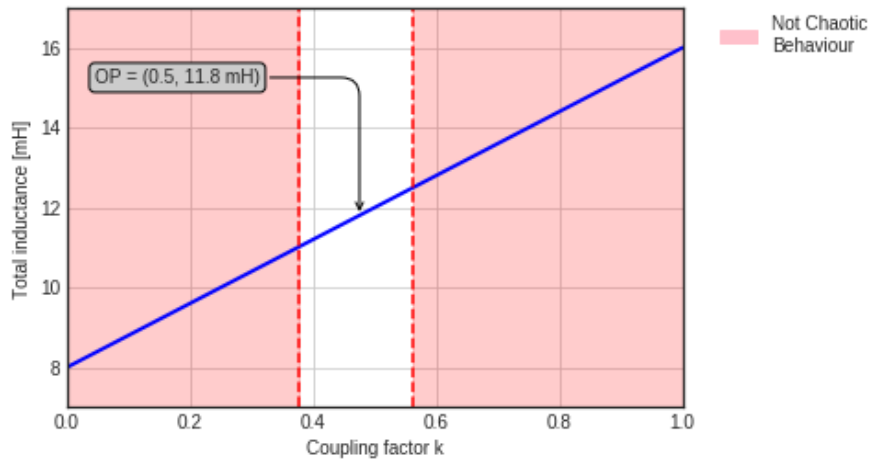


Figure 5.6: The system does not develop chaotic behaviour for all values of total inductance, but only for certain values of the coupling factor. Figure shows the operating point (OP) of the system, coupling value and the total inductance. Out of a certain range of values, the system does not develop chaos and does not oscillate.

cypher and decipher data sent to both parts. The key is the chaos generated from the circuits. The great advantage is that the key can be applied only and exclusively to the transmitter and the receiver at the same time. If a third party tries to join, the CB in the circuits will stop immediately because the inductive load will change. This type of encryption is a step over the most widely used symmetric algorithms such as AES, RC5 and DES, which support multiple receivers.

As mentioned above, any forgery attempt on the digital access card will leave an indelible mark as it will bring the memristor internal status to an unexpected value for the authentication key in a safe security lock. There is no possibility of coming back to the previous status. In spite of the fact that the electronic system could be cloned, the internal value of the memristor can never be predicted and there is no algorithm that could predict this value.

5.1.2 Wireless Power Transmission

The WPT system built with memristors is shown in Fig. 5.4. The memristive Chua's circuit shown in Figure 5.1 has been enhanced with a mutual coupled inductor, and C_R is the compensation capacitor. As depicted in Fig. 5.4, the system

is completely symmetrical as two copies of the Chua's circuit. The latter circuit creates an oscillation which can bring about equilibrium, chaos, or instability. In reference to the memristive Chua's circuit, it has been considered the parameters values shown in Table 5.2. As can be seen, the inductor values of L_T and L_R are 8 mH, which is less than the usual value in Chua memristive circuits of 11.8 mH. It is possible to use a lower value because of mutual induction. The current flowing in L_T or the transmitter coil sets up a magnetic field which passes through the receiver coil L_R ; thus, giving us mutual inductance. When the inductances of the two coils are the same and equal, L_T is equal to L_R , the mutual inductance that exists between the two coils will equal the value of one single coil (as the square root of two equal values is the same as one single value) as shown:

$$M = k\sqrt{L_T L_R} = kL \quad (5.1)$$

where k is the coupling coefficient expressed as a fractional number between 0 and 1, where 0 indicates zero or no inductive coupling, and 1 indicates full or maximum inductive coupling. In our application, the coupling coefficient is in a range between 0.4 and 0.6, as represented in Fig. 5.6. A lower or higher value of coupling is not enough to start chaotic behaviour and to change the status of the memristor. As it can be seen, if the inductance goes over a certain value, the system will not oscillate because of an over-inductive value. This makes the system robust to additional receivers and also immune to MitM attacks. As a result, the transmitter L_T causes a voltage of v_R^{in} to be induced in the receiver, and vice versa.

$$\begin{cases} v_R^{in} = L_R \frac{dL_R}{dt} + M \frac{dL_T}{dt} \\ v_T^{in} = L_T \frac{dL_T}{dt} + M \frac{dL_R}{dt} \end{cases} \quad (5.2)$$

Using these relationships, it is possible to adopt lower inductances than the Chua's circuit. Furthermore, the symmetry of the circuitry allows to transmit the chaotic

behaviour. The transmitter and receiver will resonate at the same frequency:

$$f_0 = \frac{1}{2\pi\sqrt{LC_1}} = \frac{1}{2\pi\sqrt{L_T C_T}} = \frac{1}{2\pi\sqrt{L_R C_R}} \quad (5.3)$$

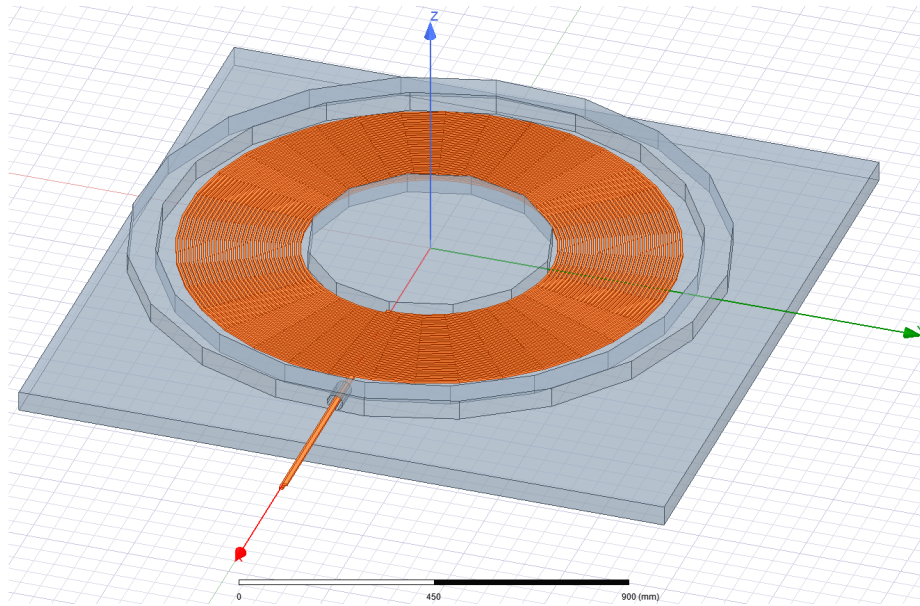
which adopts the values reported in table 5.2 gives 6.8 kHz. It is important to notice that this application is not necessary to achieve high efficiency. The receiver needs low enough power to start its own oscillation and chaotic behaviour necessary for encryption.

5.2 Simulations Results

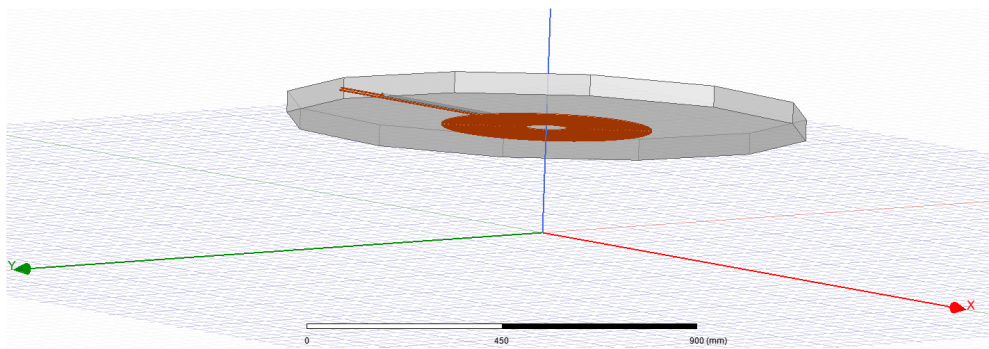
In security applications, the distance between transmitter and receiver is quite short and the power level is so low that it could be referred to in literature more as energy harvested than as power transmission. However, because the only purpose of the primary circuit is to send power and establish chaos, the overall system is a wireless power transfer. To assess the system created, different experiments have been used. Initially, the magnetic field propagation has been analysed. Secondly, the electrical circuit simulations are performed.

5.2.1 Magnetic Field

A finite element analysis (FEA) of the coil shape and the magnetic field is performed. ANSYS Maxwell v19 is one of the most accurate software in this type of analysis. This analysis is really important because it is really difficult to build a technologically high-inductance antenna. Therefore, coils of 8 mH have only been designed and not built in a lab. A core has been added to the transmitter and receiver in order to achieve higher performance. As shown in Fig. 5.7, the size of the coils is large and they can carry an even larger amount of power. Therefore, it will allow power transmission for longer distances. The main purpose of this simulation is the achievement of the necessary mutual inductance for the chaotic oscillation. Our application has low power characteristics, therefore improvements



(a)



(b)

Figure 5.7: Transmitter coil is (a) caved in the core in order to increase directionality and (b) receiver coil and flat core to enhance energy harvesting.

to the coil technology will be made in future research.

Reducing the dimension of that coil is one of the more challenging parts of this design. It is possible to design the size of the coil to be the actual size of a passport, 88 x 125 mm. As shown in the simulation design in Fig. 5.8a the spiral of the inductors has a thickness of 0.1 mm, merely visible on a larger scale as in Fig. 5.8b. In purple is the transmitter coil and the brown is the receiver one. This requires a specific manufacturer to produce and make this product available.

According to simulation results, a gap of 100 mm (air, plastic, or any material

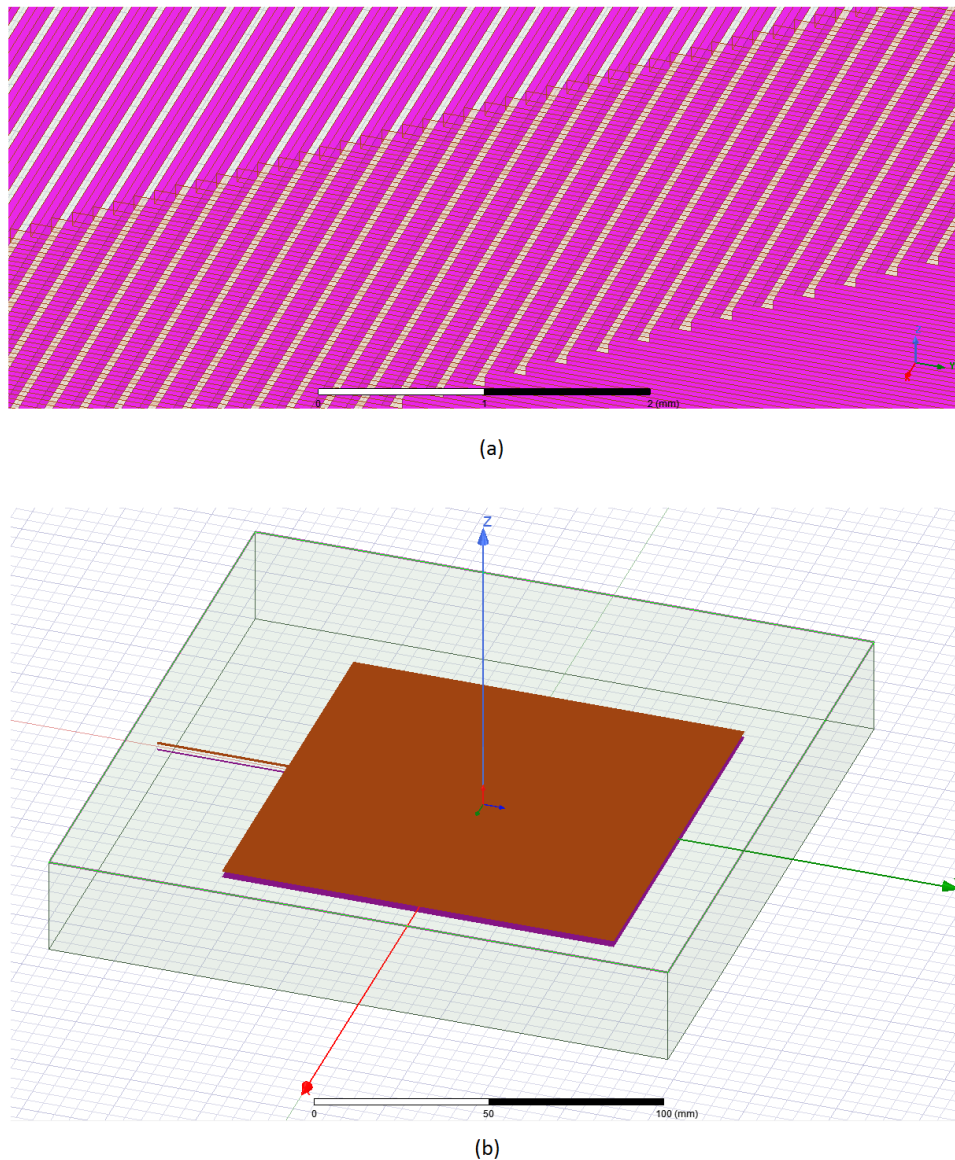


Figure 5.8: Structure of the receiver (brown) and transmitter (purple) in the ANSYS analysis. (a) Magnification of the 8 mH coils.

with a relative permeability of $\mu_{rR} = 1$) is required between coils. For security reasons, the transmitter and the receiver are equipped with a directional core. As shown in Figure 5.9, even when a large amount of power is transmitted, the magnetic field intensity reduces to zero decibels or even lower in the surrounding area.

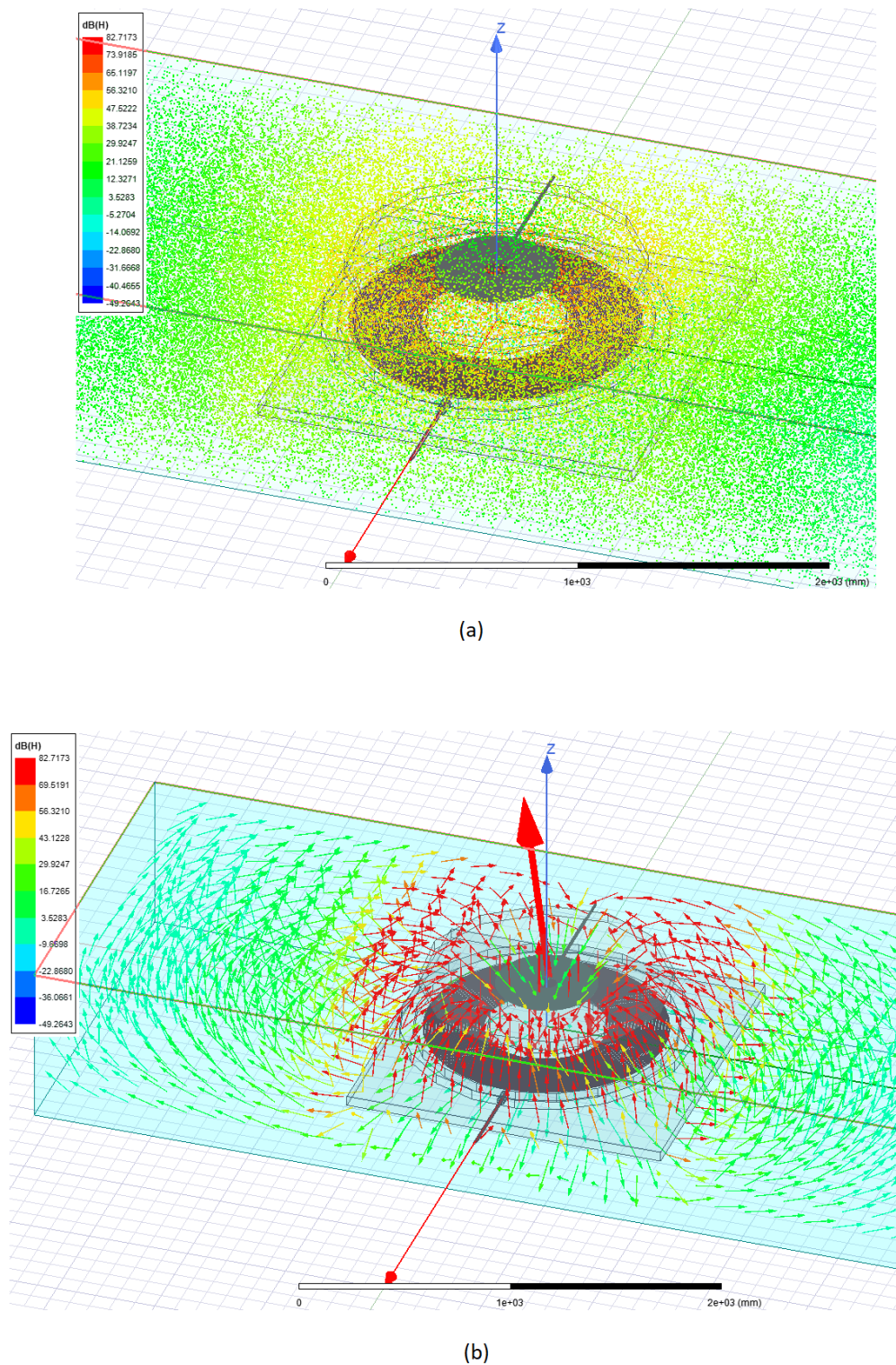


Figure 5.9: The Magnetic Field (a) Intensity H spread in the air, where it can be notice by the vast green color (0 dB) and (b) Vector B spread in the air, where it can be notice by the vast green color (0 dB).

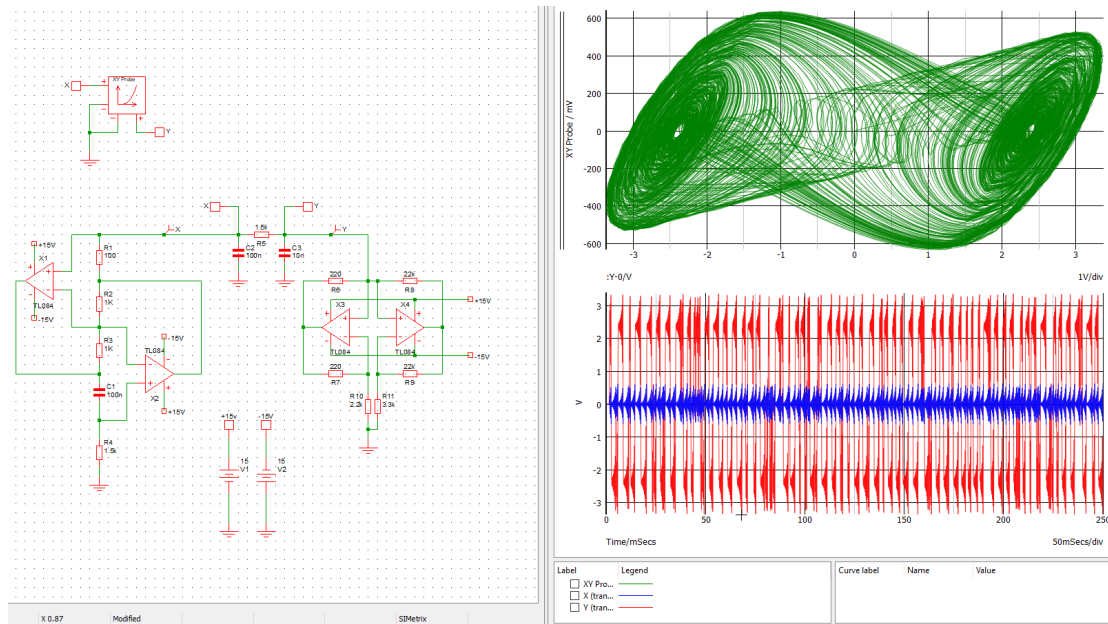


Figure 5.10: Chua circuit waveform: inductor voltage (blue) and Chua diode voltage (red); XY plot (green) on the resistor voltage.

5.2.2 Circuit Simulation

Once we have viewed the magnetic field, the directionality, and the design of the coil in reduced size, it is important to focus on the electric circuit. As usual, electronic engineers use different circuit simulators to confirm their findings before going to test a product.

In order to test the chaotic circuit, we have used a free circuit simulation software, SIMetrix, which initially built the Chua circuit as shown in figure 5.10. In the simulation, an inductor-less circuit has been used, where instead of the inductor, it has been used the Antoniu circuit (in figure 5.11) which is able to emulate an inductor. The terminal relationship between V_L and I_L is the same as an inductor. The point is that we should be able to use this circuit in place of an inductor. While it may or may not be obvious, we don't particularly care what's going on inside the Antoniou Circuit as long as it has at the terminal an expression equal to an ideal inductor. The circuit can be easily analysed by applying the virtual short-circuit method to the op-amps. By considering the Laplace transform where inductors have $V_L = Ls \cdot I_L$, we obtain:

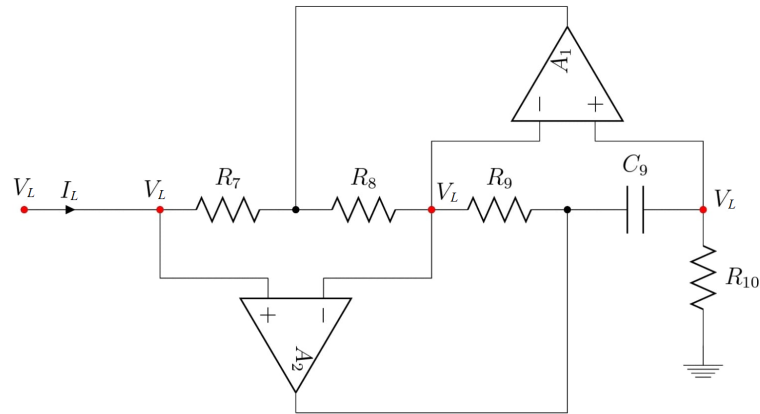


Figure 5.11: The schematic of an Antoniou Circuit.

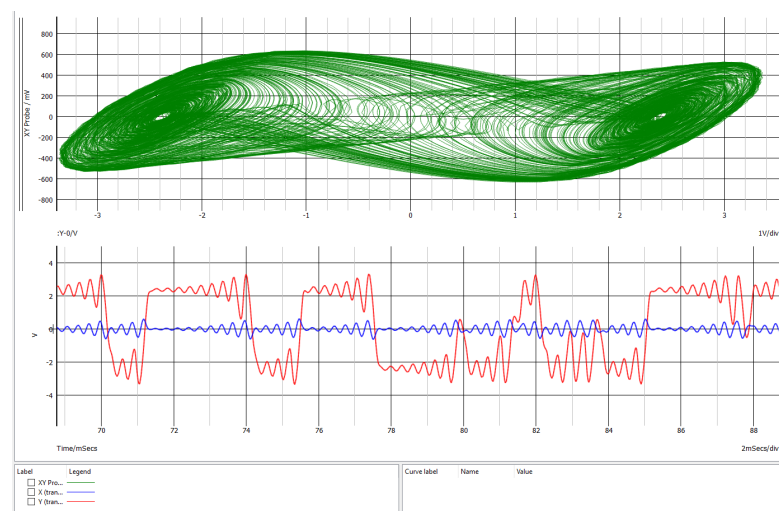


Figure 5.12: Chua circuit waveform magnified: XY plot (green) on the resistor, inductor voltage (blue) and Chua diode voltage (red).

$$V_L = \frac{C_9 R_7 R_9 R_{10}}{R_8} \cdot s \cdot I_L \quad (5.4)$$

where $L = \frac{C_9 R_7 R_9 R_{10}}{R_8}$. The inductance depends only on the resistors and capacitor ratio. This allows us to test the circuit better as we can add potentiometers to better understand how the variation of the total inductance (self-inductance and mutual) acts on the chaos generated.

The whole system has been verified to show a chaotic temporal behaviour as plotted in Fig. 5.10 and the magnified picture in Figure 5.12. The time plot can only partially give an understanding of the chaotic behaviour, such as the wave-

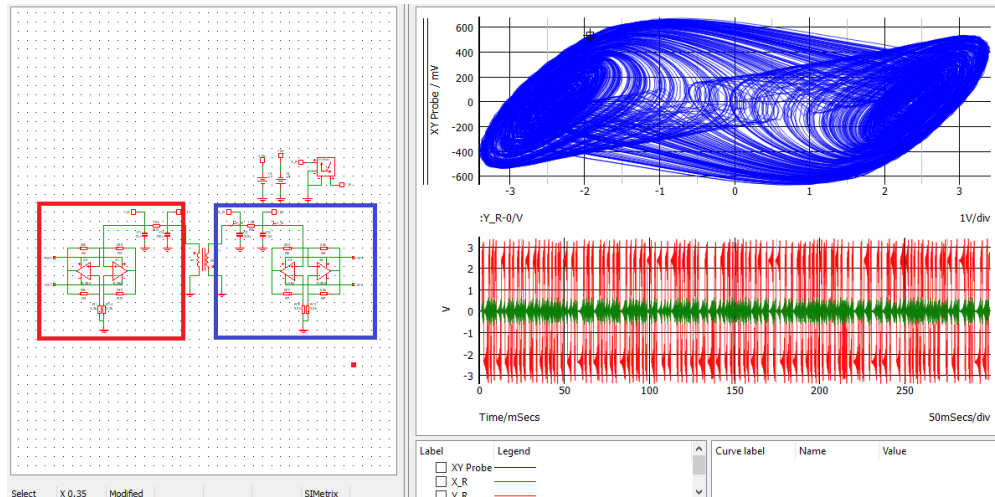


Figure 5.13: Long time step simulation for the Memristive : inductor voltage (blue) and Chua diode voltage (red); XY plot (green) on the resistor voltage.

forms in red and blue. Therefore, the system has been plotted in X-Y mode. The results are the phase portraits of the chaotic attractors in a time representation in milliseconds (50 ms/div) as shown in Fig. 5.12. This plot is also known as a phase portrait, and the circuits exhibit a typical two-attractor waveform.

5.2.3 Memristive Power Transmission

The whole system has been verified as showing chaotic behaviour. It is becoming more and more difficult to clearly display the synchronisation between the transmitter circuit (squared in red) and the receiver (squared in blue) in the figure 5.13. We have displayed only the receiver on this occasion.

The system has been simulated with the advanced software NI Multisim 14.2 to demonstrate to the reader that the circuits in the transmitter and receiver are continuously synchronising. The time plot can only partially give an understanding of the chaotic behaviour, therefore the system has been plotted with an oscilloscope in X-Y mode. We have shown the waveforms in the receiver as XY plot in 0.2 V/div and 1 V/div in Fig. 5.14 for V_{M_R} vs $V_{L_{C_R}}$, respectively. In Fig. 5.15 is shown V_{M_R} vs $i_{L_{C_R}}$ in XY mode in 1 V/div and 1 V/div, respectively. In Fig. 5.16 is shown the $v_{L_{C_R}}$ vs $i_{L_{C_R}}$ in 0.2 V/div and 1 V/div, respectively.

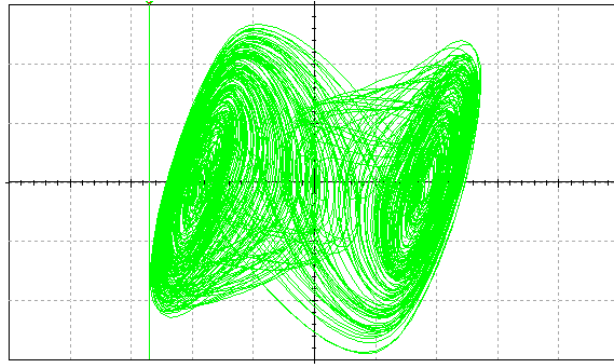


Figure 5.14: Receiver V_{MR} vs V_{LCR} shown in XY mode in 0.2 V/div and 1 V/div, respectively.

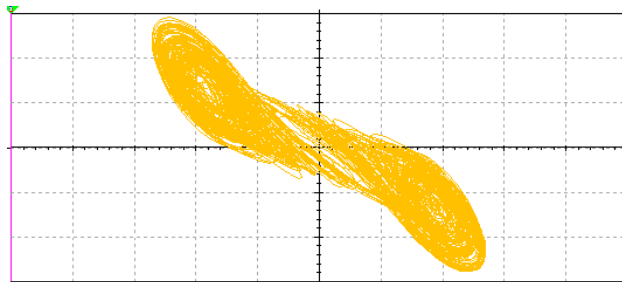


Figure 5.15: Receiver V_{MR} vs i_{LCR} shown in XY mode in 1 V/div and 1 V/div, respectively.

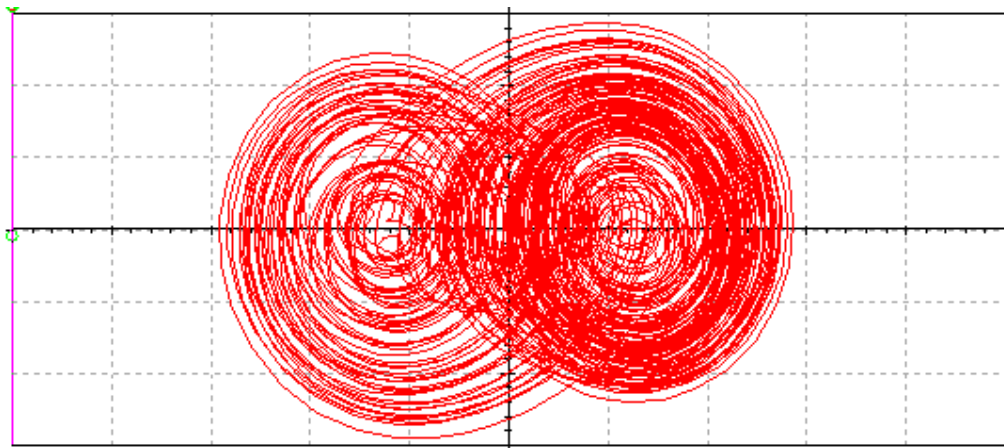


Figure 5.16: Receiver v_{LCR} vs i_{LCR} shown in XY mode in 0.2 V/div and 1 V/div, respectively.

The synchronisation of the phase portraits of the chaotic attractors is fully synchronised as shown in all the plots of the transmitter (left) and the receiver (right) in Fig. 5.17. This clearly shows the functionality of this new topology of wireless power and data transmission.

Summary. We introduced the Memristor-based (Memristive) Wireless Power

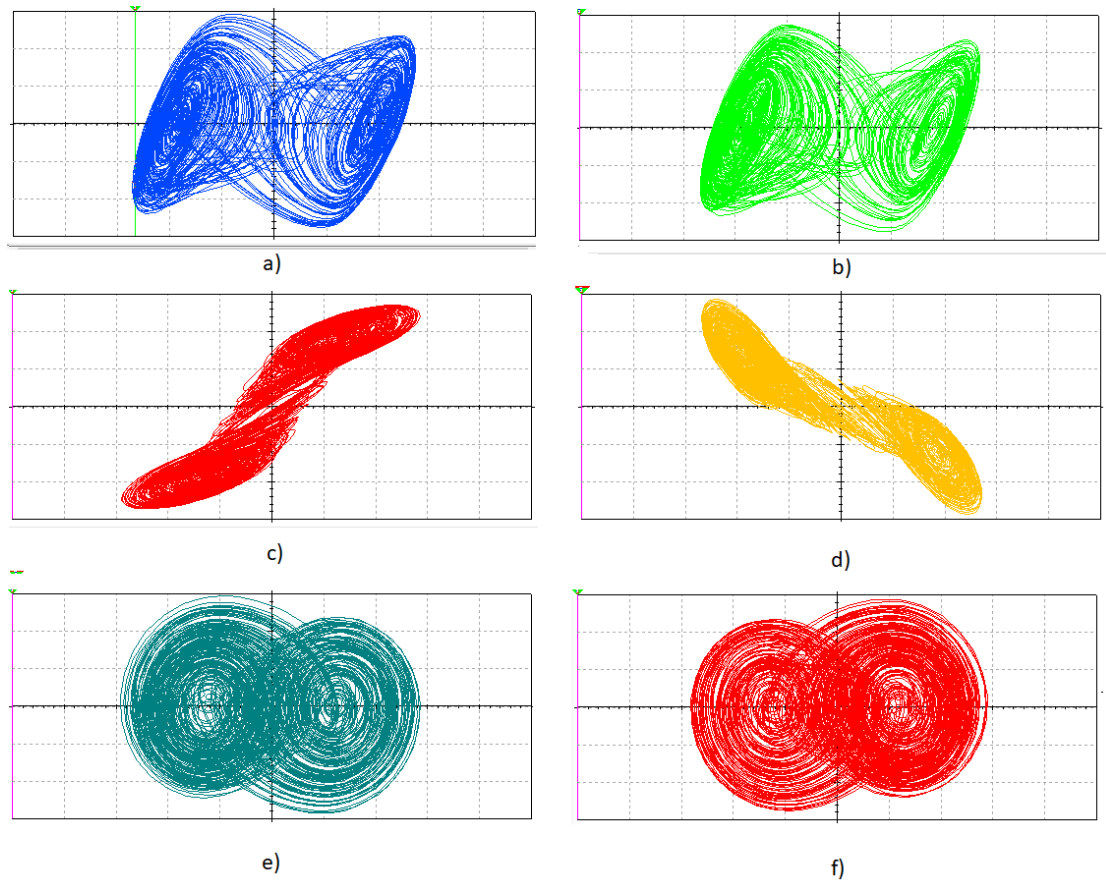


Figure 5.17: Synchronisation of the phase portraits of a chaotic attractor: voltage in the inductor V_{LC} referred to the memristor voltage V_M in the transmitter (a) and receiver (b) coil; current in the inductor i_L referred to the memristor voltage V_M in the transmitter (c) and receiver (d) coil; the memristor voltage V_M referred to its internal voltage status V_0 in the transmitter (e) and receiver (f).

Transfer in this chapter (MWPT). The system is composed of two symmetrical Chua circuits that are capable of transmitting both power and chaos by modifying the original design with mutually linked inductors. To validate the system's functionality, it was widely simulated and experimented on.

Chapter 6

Variety of Memristive WPT

The development of the Memristive WPT system will be part of a long research study which is also known as coupled chaotic systems. They have received a lot of attention as suitable models for describing complex natural events. Since the discovery of synchronisation of chaotic trajectories [265] and subsequent analysis of the synchronisation [266], the study of linked chaotic systems has grown. Studies of linked systems have been conducted in a variety of fields, including physics [267, 268], biology [269, 270], and engineering [271]. Furthermore, experts believe that coupled system synchronisation has certain connections with brain information processing. Information is processed by neurons in the brain.

Despite the simplicity of neuron activity, the neurons can have numerous states and conduct sophisticated information processing due to ion current regulation. The behaviour of neurons is modified when they are pushed by ions, allowing the neurons to assume numerous different states. However, the non-linear aspect of the memristor, which mirrors the behaviour of chemical synapses [272, 273], is highlighted, ushering in a new era for neuromorphic engineering.

We anticipate seeing future discoveries of intriguing and intricate events comparable to those seen in the brain if we investigate such a coupled system. The neurons are connected to each other through a synapse, which is a small gap at the end of a neuron that allows a signal to pass from one neuron to the next, similarly

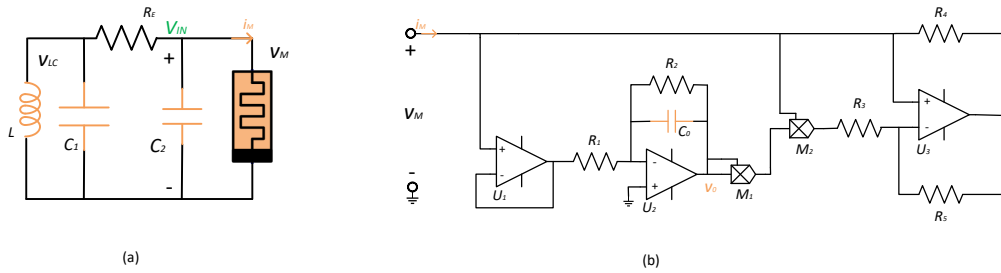


Figure 6.1: The schematic of (a) Chua's Memristive circuit. (b) Equivalent realisation of a non-ideal active voltage-controlled memristor.

to the gaps in a WPT system. We think that studying synchronisation events in chaotic coupled systems not only advances our understanding of the brain's information processing mechanism, but also aids in the development of an information processing brain computer.

However, the most simplest applications in the PhD path are the improvement of existing systems, such as NFC, considering the vast use of IOT devices nowadays.

6.1 Memristor models

The memristor's brilliance rests in its capacity to remember its history through modification of the device's internal state variable x . This memory potential is what fascinates the electronics community and is the driving force behind the memristors' circuit design revolution. Clearly, the memristor's scalability, low power consumption, and dynamic responsiveness make it an appealing candidate for a variety of applications, ranging from non-volatile memory [274] to programmable logic [275].

This device can create chaos from the well-known Chua's circuit shown in Figure 6.1a. Because the memristor is not commercially available, we use electrical circuits equivalent to the device called a memristor emulator, or model. There are many different models of memristor studied by the scientific community and used for different types of circuits. The non-ideal active voltage-controlled model, shown in Figure 6.1, has proven to generate different types and orders of chaos

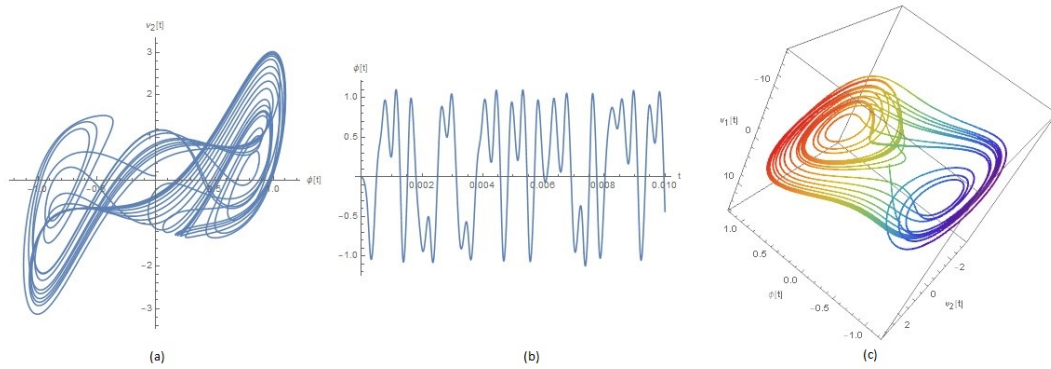


Figure 6.2: Chua's memristive circuit has the (a) Double-scroll attractor phase portrait. (b) Chaotic oscillation of the memristive Chua circuit. (c) Memristive flux characteristic with the voltage of the two capacitors.

Table 6.1: Internal values of the memristor model.

Memristor equivalent			
Parameter	Value	Parameter	Value
R_1	4 k Ω	R_5	2 k Ω
R_2	10 k Ω	C_0	1 nF
R_3	1.4 k Ω	g_1	1
R_4	2 k Ω	g_2	0.1

by small variations of parameters. For example, the variation of the resistor in the Chua circuit creates different evolutions of the chaos. Memristors, with their non-linearities, are properly integrated into existing electronic circuits to create several new chaotic circuits [276], as depicted in Figure 6.2. During the PhD research, we used different models, such as the non-ideal active voltage-controlled memristor, to generate different types of chaos.

6.1.1 Non-ideal active voltage-controlled memristor

In reference to the Chua memristive circuit, the internal relationship of the memristor mode is the same. The circuit's behaviour stems from the classic Chua circuit, substituting it with the non-ideal active controlled voltage memristor model shown in Fig. 6.1b. The values adopted are reported in table 6.1. This model is the most developed in application circuits [277], as well as the diode bridges cascaded with RC, LC or RLC filters [278]. The latter is composed of a buffer U_1 , an integrator

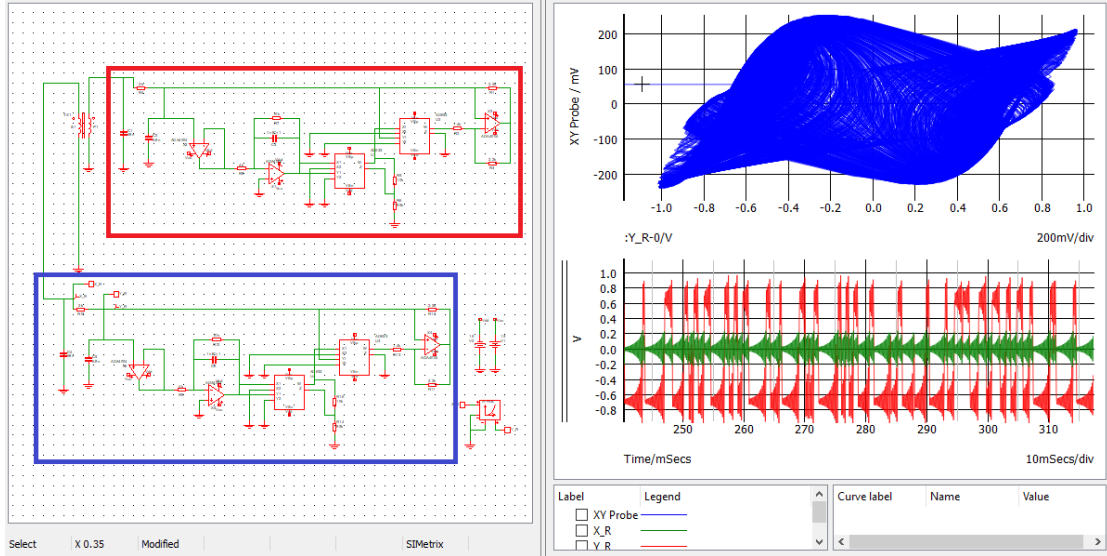


Figure 6.3: The behaviour in the transmitter (the Chua circuit) is a well-known double-attractor phase portrait. This plot shows the characteristic of the voltage in the coil and the voltage on the memristor.

U_2 connected to two resistors R_1 , R_2 , a capacitor C_0 , the multipliers M_1 and M_2 and a current inverter U_3 connected to the resistors R_3 , R_4 and R_5 . In addition, the scale factors of the multipliers M_1 and M_2 are indicated as g_1 and g_2 in order to have $G_a = \frac{1}{R_3}$ and $G_b = \frac{g_1 g_2}{R_3}$. This model is characterised by the two equations:

$$i_M = (-G_a + G_b \cdot v_0^2)v_M \quad (6.1)$$

$$\frac{dv_0}{dt} = -\frac{v_M}{R_1 C_0} - \frac{v_0}{R_2 C_0} \quad (6.2)$$

where i_M is the current flowing in the memristor, v_M is the voltage on the memristor and v_0 is the voltage on its internal capacitor, C_0 . When the two parts of the system are near each other, either side of the system will be capable of developing chaotic behaviour. The transmitter is squared in red and the receiver is squared in blue. We can notice that the receiver behaves chaotically and develops a double-scroll phase portrait, as shown in Figure 6.3.

6.1.2 Theoretical analysis

Similarly to memristive Chua's circuit, each side has four dynamic elements: the parallel LC with the mutual inductor X_R and the parallel of the non-ideal active voltage-controlled memristor W and a capacitor C_M . Thanks to the symmetry, it is possible to consider one side. It results in four state variables: v_M , v_2 , i_M , and v_0 . Therefore, a system of equations for one side can be written as:

$$\begin{cases} \frac{dv_M}{dt} = \frac{v_2 - v_M}{R_E C_1} + \frac{(G_a - G_b \cdot v_0^2)v_M}{C_1} \\ \frac{dv_2}{dt} = \frac{v_M - v_2}{R_E C_2} - \frac{i_M}{C_2} \\ \frac{di_M}{dt} = \frac{v_2}{X} \\ \frac{dv_0}{dt} = -\frac{v_M}{R_1 C_0} - \frac{v_0}{R_2 C_0} \end{cases} \quad (6.3)$$

where the voltage on the capacitor v_{C_1} coincides with the one on the memristor v_M . The system has a zero equilibrium point and two non-equilibrium points indicated as:

$$S_0 = (0, 0, 0, 0) \quad (6.4)$$

$$S_{\pm} = \left(\pm \eta \frac{R_1}{R_2}, 0, \pm \eta \frac{R_1}{R_E R_2}, \mp \eta \right) \quad (6.5)$$

where $\eta = \sqrt{\frac{G_a R_E - 1}{G_b R_E}}$ and R_E is the resistance between the coil parallel and memristor. The non-zero equilibrium points are symmetrical with respect to the origin and disappear when $R_E < R_3$ (1.4 k Ω). For the $R_E > 1.4$ k Ω and $S_0 = (0, 0, 0, 0)$ it can be demonstrated that it is always unstable.

From the equation set 6.3, a simplified equation set can be defined by using $W(u) = a - b^2$ as a non-linear function. By using the values in the table 6.1, it is possible to define new dimensionless parameters $x = v_M$, $y = v_2$, $z = R i_M$, $u = v_0$, $\tau = t/(R C_2)$, $a = R G_a$, $b = R G_b$, $\alpha = C_2/C_1$, $\beta = R_2 C_2/L$, $\gamma = R C_2/R_1 C_0$ and $\epsilon = R C_2/R_2 C_0$. This will result in $a = 1.6$, $b = 0.16$, $\alpha = 12$, $\beta = 28$,

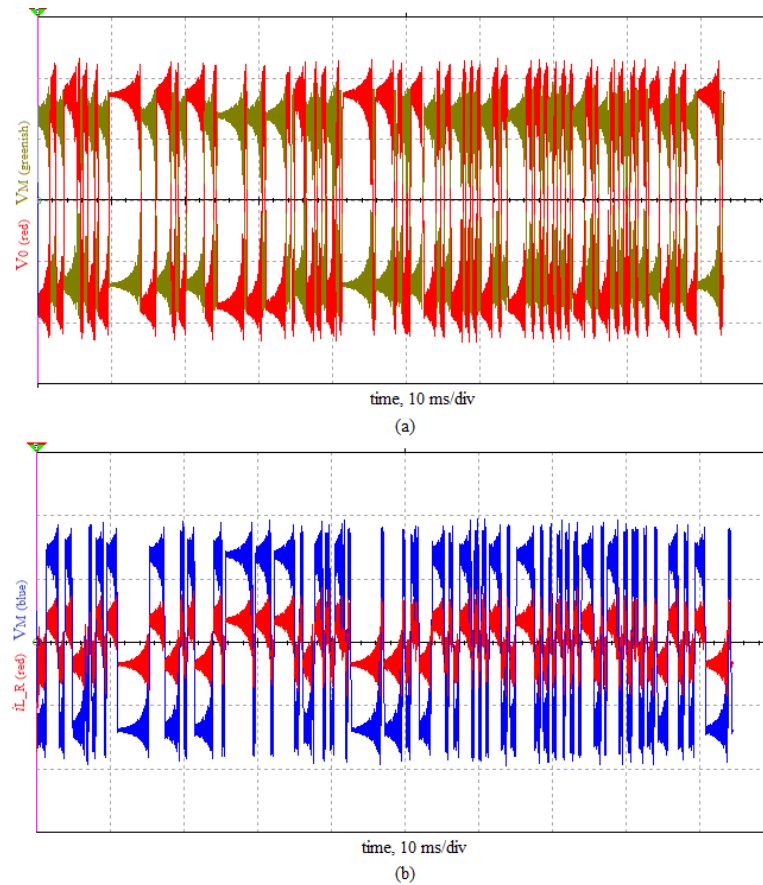


Figure 6.4: Time step of the chaotic behaviour in the receiver: the memristor voltage V_M in green and internal status V_0 in red(a) and coil current i_L in red and memristor voltage V_M in blue (b).

$\gamma = 37$ and $\epsilon = 12$ and the chaotic behaviour will develop. When the parameter α varies in the range of 8 to 15, the four Lyapunov exponents, calculated by Wolfs method [279], the bifurcation diagrams with coexisting bifurcation modes and the dynamics featured are plotted in Reference [280]. The memristive Chua's system has two stable non-zero saddle-foci and shows a remarkable dynamical behaviour of multiple attractors with multi-stability. The full complex dynamics is investigated theoretically and numerically in the Reference [280].

6.1.3 Simulation and Experimental Results

By using advanced software like NI Multisim 14.2, it is possible to investigate the performance of the memristor based WPT system. The whole system has been

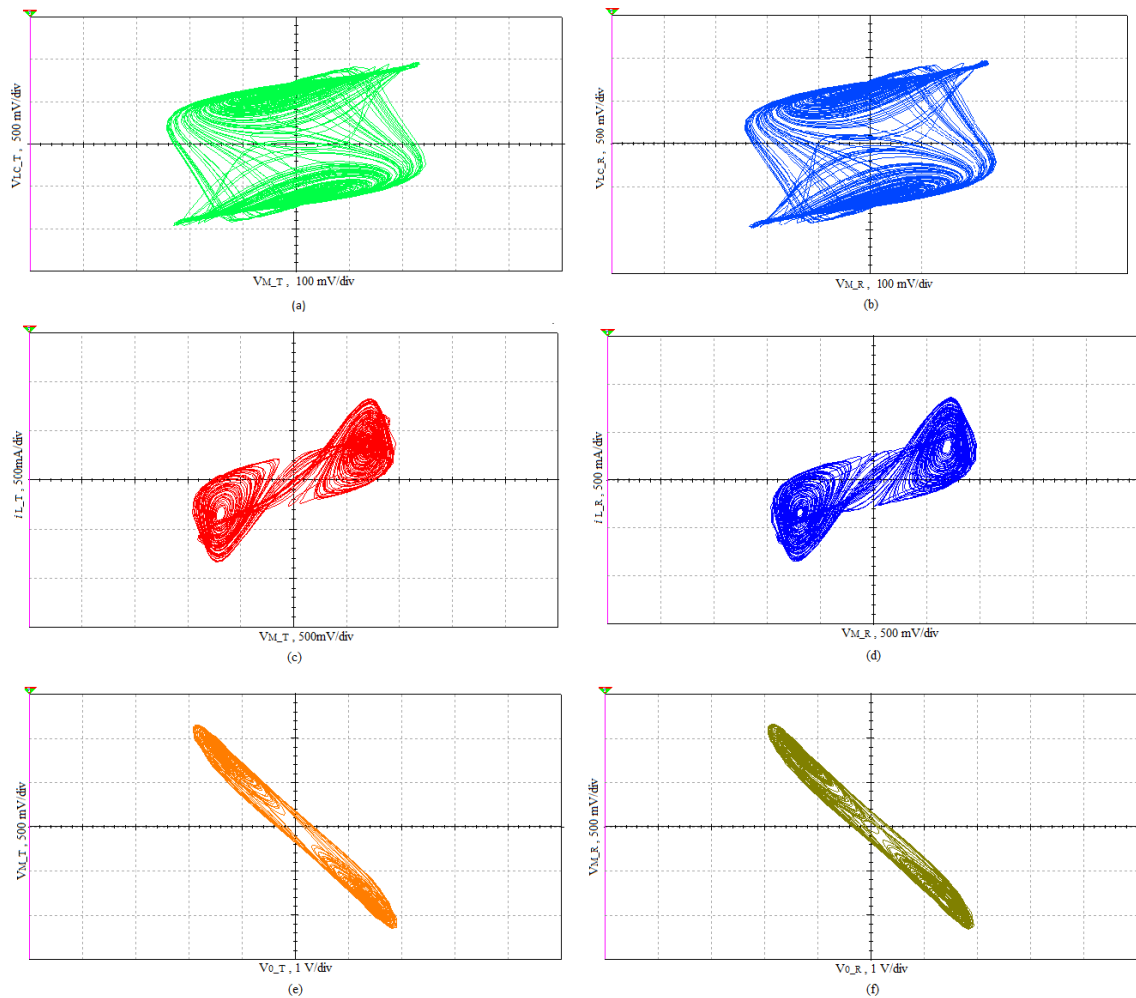


Figure 6.5: Synchronisation of the phase portraits of a chaotic attractor: voltage in the inductor V_{LC} referred to the memristor voltage V_M in the receiver (a) and transmitter (b) coil; current in the inductor i_L referred to the memristor voltage V_M in the receiver (c) and transmitter (d) coil; the memristor voltage V_M referred to its internal voltage status V_0 in the receiver (e) and transmitter (f).

verified, showing a chaotic temporal behaviour as plotted in Fig. 6.4. The time plot can only partially give an understanding of the chaotic behaviour, therefore the system has been plotted with an oscilloscope in X-Y mode. The results are the phase portraits of the chaotic attractors fully synchronised between the transmitter (left) and the receiver (right) in a time representation in milliseconds (10 ms/div) as shown in Fig. 6.5. The voltage in the transmitter coil vs the voltage on the memristor is plotted in Figures 6.5a and 6.5b. This plot is also known as a phase portrait, and the circuits exhibit a typical two-attractor waveform.

As depicted in Figure 6.6, the power levels are very low in spite of using an

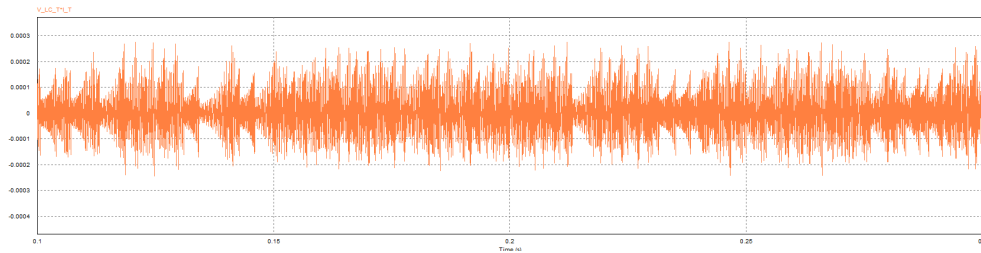


Figure 6.6: The power transmitted has a large chaotic behaviour and usually a lower value than 0.2 mW.

active memristor model. The power behaviour is also chaotic and its maximum level may reach 0.3 mW. The circuit develops a chaotic waveform following Chua's memristive circuit. The memristor actively creates the chaotic oscillation, which has been plotted in the transmitter coil in Fig 6.7. The same oscillation is induced in the receiver, creating a synchronous behaviour, as shown in figures 6.7.

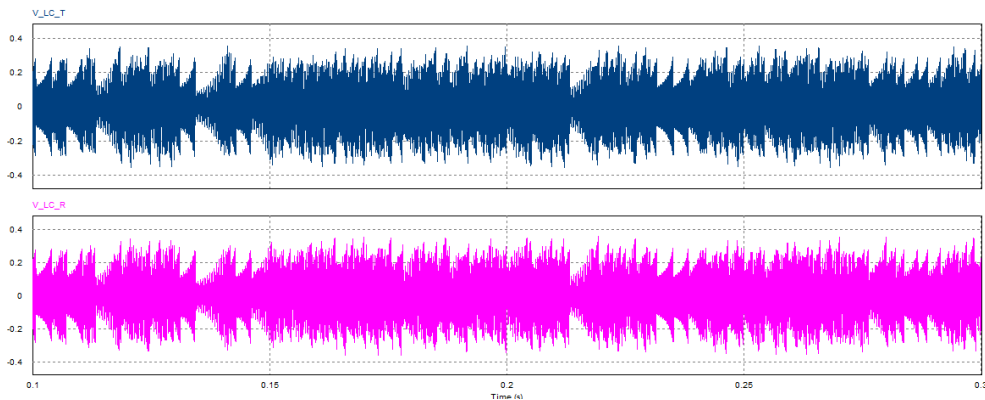


Figure 6.7: Transmitter voltage behaviour (blue) and receiver (purple) in the coil.

The graphs in figure 6.8 show the simulation of the system with two synchronisation signals. This situation is a typical encoding in which a synchronisation is sent before the payload transmission. The transmitter sends a synchronising signal through the V_{in} , which is the voltage on the capacitance C1. The first graph shows the voltage on the parallel of the capacitance and coil. As can be seen in the second graph, the voltage on the receiver coil continues to vary randomly, maintaining encryption. As it can be seen in the first graph, this is the signal transmitted on air, which is completely chaotic. The synchronisation, circled in red, is not perceptible on air and is hidden in the waveform. This does

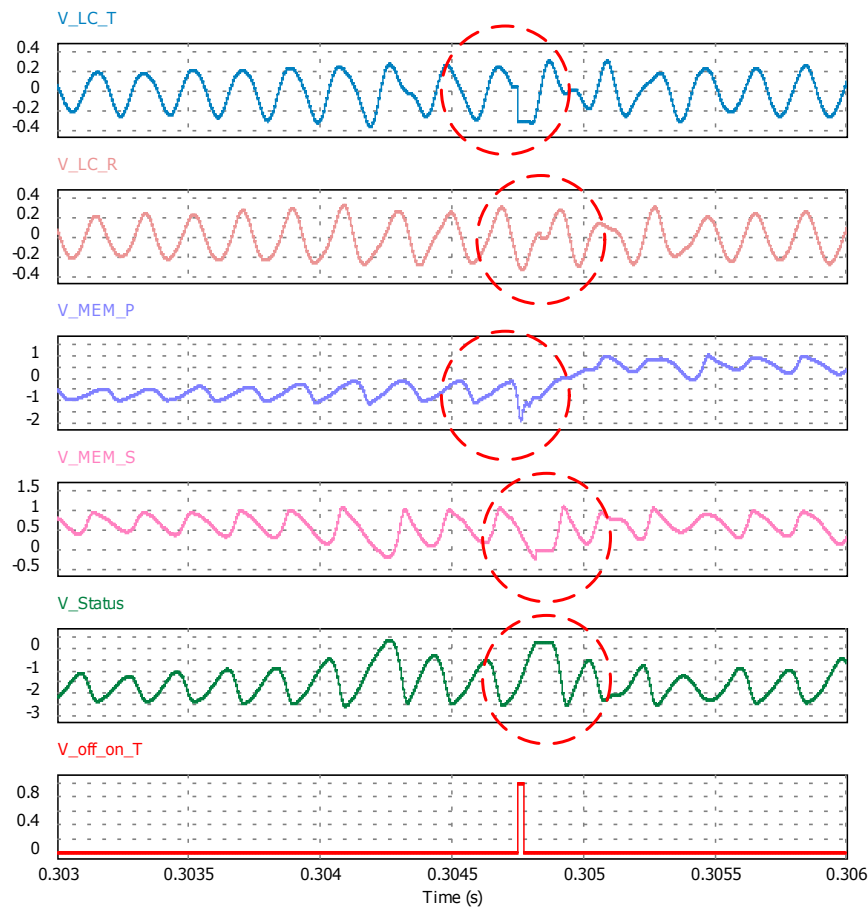


Figure 6.8: Simulation results with the synchronisation signal circled in red: LC voltage in the primary (1st plot) and the secondary (2nd plot); primary memristor voltage (3rd plot) and secondary (4th plot); the internal status of the secondary (5th plot) and the synchronisation signal (6th plot).

not happen in the memristor. In the third and fourth graphs, the synchronising signal has no effect on the status of the transmitter memristor, but on the receiver memristor instead. The latest recognises the value and keeps it constant for about the duration of the signal (in reality it lasts less for the transient "rise" and "fall" time). This internal voltage of the memristor is unique, not recognisable externally and represents an indispensable factor for coding. The fifth graph shows the synchronisation signal.

In order to test this behaviour in data transmission, we have added a switch that sends data after stopping the oscillation. The voltage on the memristor and the coil stops as highlighted in yellow in the 1st and 2nd graphs of Figure

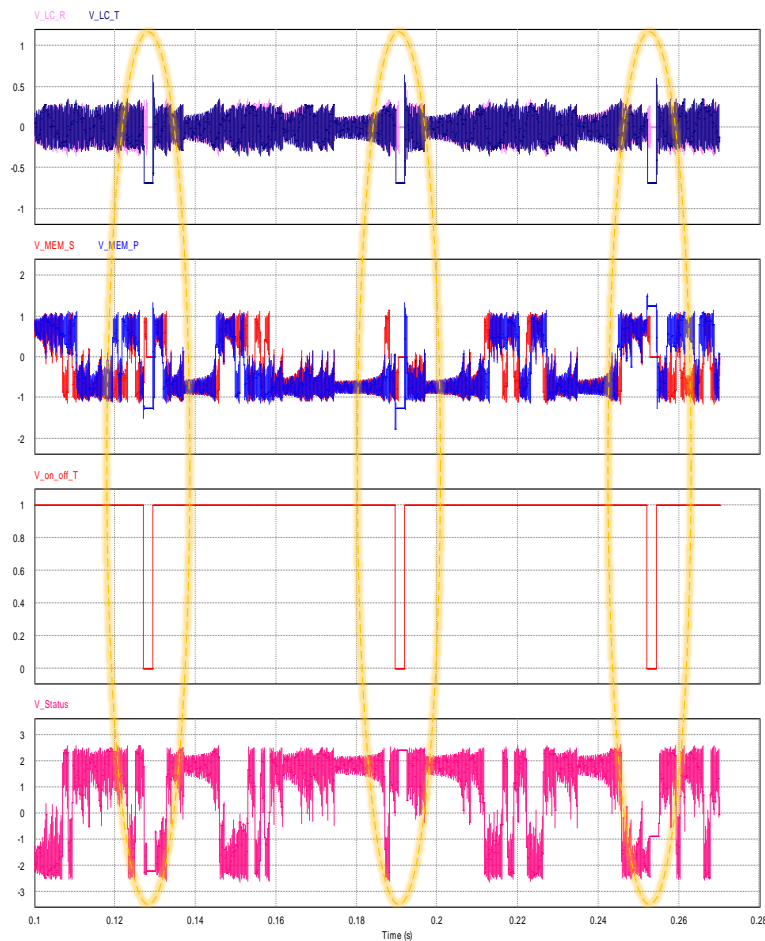


Figure 6.9: Time step of the chaotic behaviour when the receiver is disconnected (highlighted in yellow): the LC voltage V_{LC} and memristor voltage V_M in receiver and transmitter, in purple and green respectively. At the disconnection (in the 3rd graph), the receiver memristor holds its last status as shown in the 4th graph in blue.

6.9. After the circuit behaves chaotically, it stores its previous status (internal memristor voltage 4th graph) as highlighted in yellow at the time of disconnection (red 3rd graph). We have repeated the experiment three times and the internal memristor voltage value (4th graph) is totally random. For plotting reasons, the time (red 3rd graph) of disconnection is periodic as shown in the Figure 6.9.

Once we confirmed the functionality, we tested the maximum frequency of the data transmission, in which we could still have chaotic behaviour. The digital data transmitted has all "1" values (1 Volt) using the $V_{IN} = V_{LC-T}$ input voltage. We reduced the data transmission period to 0.3 ms, thereby increasing the

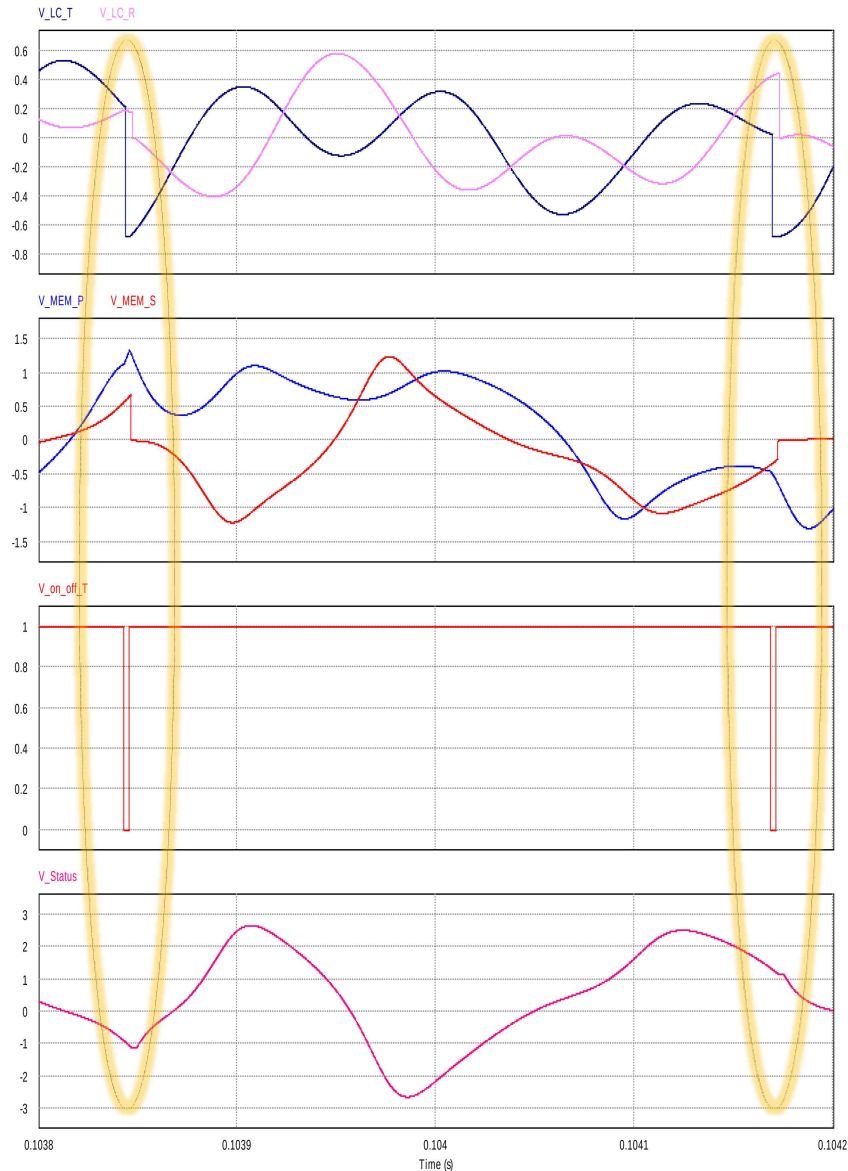


Figure 6.10: Data transmission at 3Kbps; it is possible to notice the time of switching (highlighted in yellow) the chaotic behaviour in the LC, the memristor voltage and the internal status in the 4th graph.

frequency to 3 KHz. The behaviour is still chaotic in the coils, as shown in figures 6.10. The internal memristor voltage 4th always stops at random voltage values. We have also simulated the device to a higher frequency, and it can be noticed that for frequencies over 3.4 KHz, the behaviour on the coils is not chaotic anymore. The reason is that faster variations do not give enough time for the circuit to develop chaotic oscillations. The memristor takes some time to develop its chaotic behaviour, which depends upon its internal values, the capacitor C_2 and

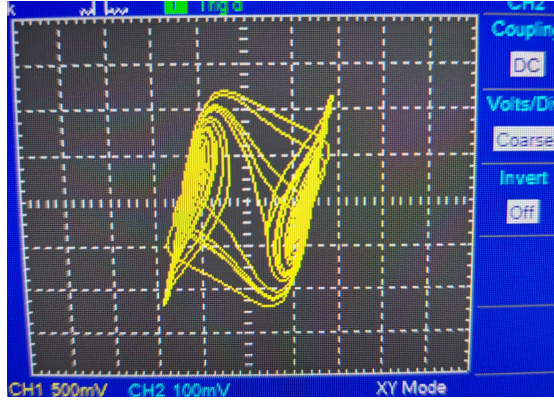


Figure 6.11: Two attractor phase portrait in the receiver side with V_{MR} vs V_{LCR} shown in XY mode in 0.5V/div and 0.5 V/div, respectively.

the oscillation frequency seen in Section 5.1.

6.1.4 Experiment

The system is comparable to the NFC system. We are also adopting an active equivalent memristor circuit rather than the real memristor. Therefore, measurements such as power transferred and distance are not significant, because the primary and secondary are both active and the system is not transferring power over distance. A PCB model of the system has been built to verify functionality. In order to build the non-ideal active voltage-controlled memristor, the AD711JRZ operational amplifier and the AD633JRZ multiplier have been used. For the physical experiment, a PCB has been built. The size of the printed circuit is very small and not clear in real pictures, because it is covered by probes and wires. Depending on the emulator, the waveform will have a different voltage range. In this way, the adaptor circuit of the WPT system can be adopted in any memristor emulator. Instead of using coils for the power transmission, the Shaffner 8 mH 2:1 transformer has been adopted. This transformer gives 4 mH mutual coupling.

The chaotic behaviour developed by the system is visualised at the receiver side using a Tektronix oscilloscope and it is in accordance with our simulations as shown in Figure 6.11.

However, the non-ideal active voltage-controlled memristor offers the possibil-

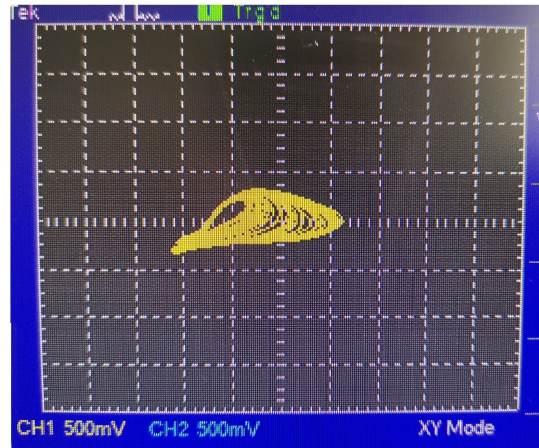


Figure 6.12: Single attractor phase portrait in the receiver side with V_{MR} vs V_{LCR} shown in XY mode in 0.5V/div and 0.5 V/div, respectively.

ity of the development of different types of chaos. For example, by varying the Chua circuit resistor, it can be a potentiometer, which variations can bring a single phase portrait as shown in Figure 6.12, differently from the simulation results obtained in Figure 6.3.

6.2 Low inductance Chua circuit

As mentioned before, the system is built on the Chua's memristive circuit, which has a large inductance that is usually difficult to build in coil windings. On the other hand, this creates a challenging technology in terms of miniaturising the inductance size. Therefore, we have proposed an array memristor-based architecture for WPT systems. This continues the new research study adopting the memristor in wireless power transfer, therefore there are no other references for this system.

6.2.1 Array of inductors

In this part of the thesis, we use the mutual inductance in the secondary coil to transmit power and data. Analogous to the NFC system, the power is harvested when the two parts of the system are in proximity. Once both parts power themselves, they synchronise chaotically. The array built for the WPT system with memristors is displayed in Figure 6.13. The modified memristive Chua's circuit is

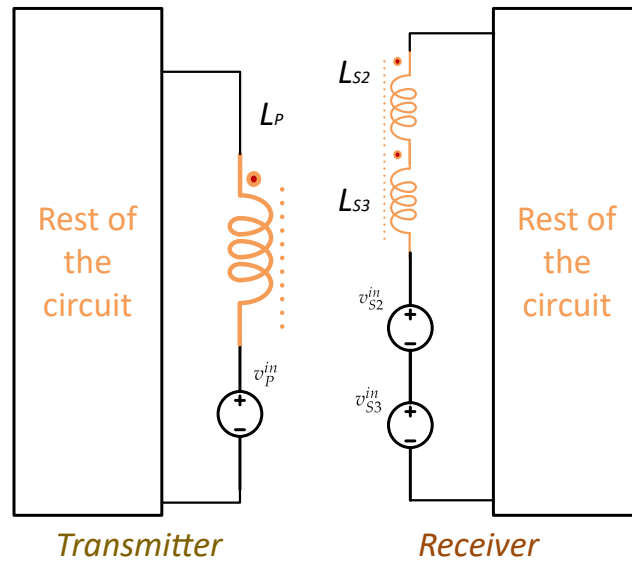


Figure 6.13: The induced voltage in each coil as shown in Equation 6.8.

adopted for both the transmitter (primary) and the receiver (secondary) circuit. The secondary has two coupled inductors in series. As shown in Figure 6.14, the system is completely symmetrical, as two copies of the Chua's circuit. An initial input voltage is applied on the capacitor C_{1P} . The latter circuit generates an oscillation that can lead to balance or chaos. Without using the array, the inductors' L_P and L_S values could be approximately 8 mH, which is much lower than the usual 12 mH values in the Chua memristive circuits. The L_{TOT} total inductance is equal to $L_P + 2 * M_{12}$, which the total is still 12 mH, but the coil design is only for a 8 mH in the primary. It is also possible to have a much lower value using the other mutual induction, as it will be shown in the next paragraph. This value is necessary to obtain the Chaotic Behaviour (CB), which will be used for the encryption. The transmitter and receiver will oscillate chaotically and resonate at the same frequency:

$$f_0 = \frac{1}{2\pi\sqrt{L_{TOT}C_1}} \quad (6.6)$$

by adopting the values reported in Table 6.2, it gives 6.8 kHz. The current

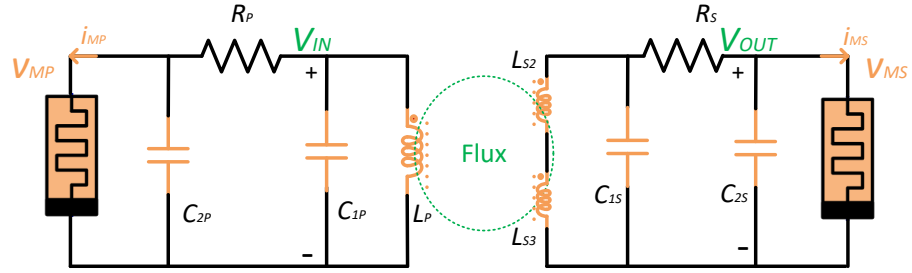


Figure 6.14: The system of Memristive Wireless Power Transfer built with two coils on the receiver side.

Table 6.2: Circuit Parameters in reference to the Chua's circuit.

Circuit Parameters			
Parameter	Transmitter	Receiver	Value
C_1	C_{1P}	C_{1S}	6.8 nF
C_2	C_{2P}	C_{2S}	68 nF
R_E	R_P	R_S	2.18 k Ω
L	L_P		5 mH
L		L_{2S}	2.5 mH
L		L_{3S}	2.5 mH

flowing in L_P , the transmitter coil, sets up a magnetic field around itself. Some of these magnetic field lines pass through the receiver coil L_S , giving mutual inductance. When the inductances of the two coils are the same and equal, L_P is equal to L_S , the mutual inductance that exists, will equal the value of one single coil, as the square root of two equal values.

$$M = k\sqrt{L_P L_S} = kL \quad (6.7)$$

M also depends on the coupling coefficient as an inductive fraction number from 0 to 1, where zero indicates no inductive coupling, and 1 indicates full or maximum inductive coupling. Values lower than 0.8 are not sufficient to initiate chaotic behaviour and, subsequently, are not able to change the memristor variable state. The transmitter coil L_P induces a voltage in the adjacent coil v_{S2}^{in} and v_{S3}^{in} , and viceversa v_P^{in} .

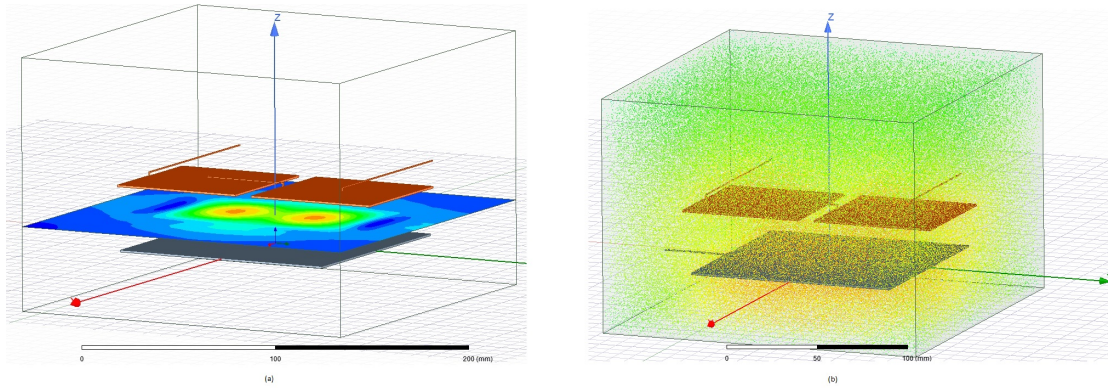


Figure 6.15: Planar intensity of the (a) Magnetic field between the coils (high in red and low in blue); (b) and in the surrounding area.

$$\begin{cases} v_P^{in} = L_P \frac{dI_P}{dt} + M_{12} \frac{dI_{S2}}{dt} + M_{13} \frac{dI_{S3}}{dt} \\ v_{S2}^{in} = L_{S2} \frac{dI_{S2}}{dt} + M_{12} \frac{dI_P}{dt} + M_{23} \frac{dI_{S3}}{dt} \\ v_{S3}^{in} = L_{S3} \frac{dI_{S3}}{dt} + M_{13} \frac{dI_P}{dt} + M_{23} \frac{dI_{S2}}{dt} \end{cases} \quad (6.8)$$

In the secondary, the two coils mutually induce themselves, as shown in the third part of the equation by the value of M_{23} . Using these relationships, it is possible to adopt lower inductances compared to the Chua's circuit, and the symmetry of the circuitry allows transmission of the chaotic behaviour. As mentioned above, the total inductance value for the circuit will be very high for each side. For this reason, we have developed the secondary coil as two mutually coupled inductors in series, which are both coupled to the primary as well. In this way, we use the mutual inductance between the two coils in the secondary to further reduce all the inductances of the coils.

6.2.2 Simulations and Experiment

In order to simulate the system created, we initially started with the design of the coils. ANSYS Maxwell v19 software has been used to test the coil design and to study the energy harvested, as well as the coupling coefficient between the coils. It is possible to design the primary coil with a 5 mH value in the dimensions of

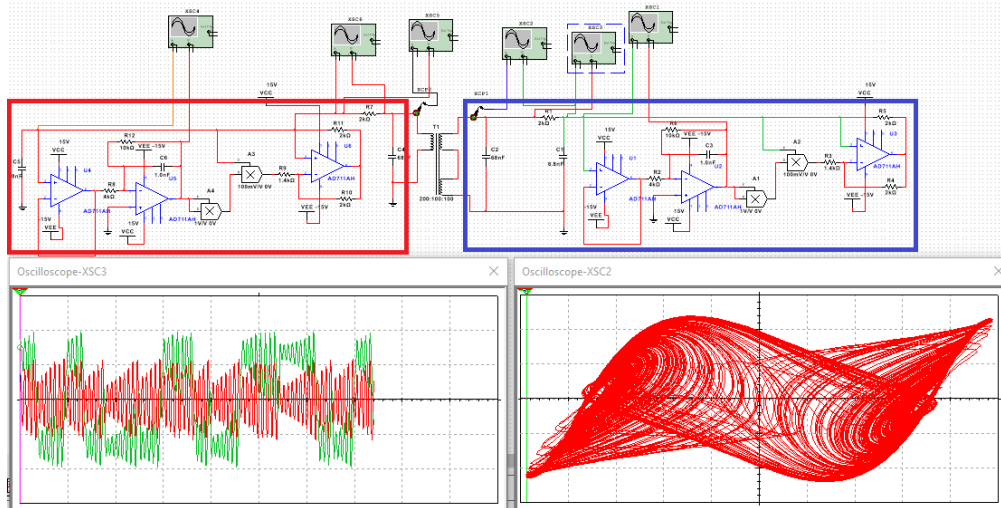


Figure 6.16: The circuit simulation of the coils array shows same chaotic behaviour such as single coil.

90 x 130 mm. For the secondary, we have fit the two coils of 2.5 mH value at the same size and achieved a small gap between the two coils. The value of 2.5 mH is one of the lowest inductive values in a Chua circuit design, which is one of the main novelties in this paper. Successively, we have started the simulation for different medium gaps (air, plastic or any material with relative permeability $\mu_R = 1$) between coils. In a close distance of 2-3 mm, the coupling reaches the value of nearly 0.9, which assures a chaotic behaviour. As shown in figure 6.15 a, the system is able to achieve energy harvesting up to 100 mm with a low coupling down to 0.4. As highlighted in the yellow cloud in figure 6.15 b, the secondary is still able to receive energy.

The coils array system has been simulated with the advanced software NI Multisim 14.2 to demonstrate that there is no variation in the result from the single coil. The time plot can only partially give an understanding of the chaotic behaviour, therefore the system has also been plotted with an oscilloscope in X-Y mode. The timestep of the chaotic behaviour in the receiver is shown in Figure 6.16: the oscilloscope on the left shows the memristor voltage V_M in red and the coil voltage i_L in greenish. We have also shown the waveforms in the receiver as XY plot in 0.2 V/div and 1 V/div in Figure 6.16 for V_{M_R} vs V_{LC_R} , respectively.

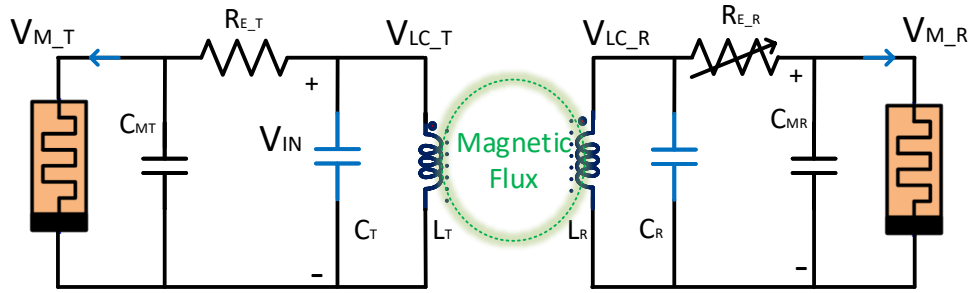


Figure 6.17: The Memristor Wireless Power Transfer Circuit built with a variable resistor which can be a LDR or thermistor.

This clearly shows the functionality of this new array topology of wireless power transmission.

The experiment's significant test is the development of chaos in the circuits using only 2.5 mH. For the physical experiment, we used all the previous circuits. Instead of using coils for the power transmission, it has been adopted by the Tamura 6 mH 2:1:1 transformer. The system developed chaotic behaviour similarly to the picture in Figure 6.11. We also tried a Tamura 5 mH 2:1:1 transformer as the simulation test, resulting in a 2.5 mH in each. Unfortunately, because of the parasitic effects (non ideal coils), the system did not oscillate.

6.3 Light dependent Chua circuit Chaos

In this part of the thesis, we are focused on variations of the typical Chua circuit. In specific, we have created a light variance of the resistor R in the Chua circuit as shown in Figure 6.17. In reality, the resistor R acts as a control for the chaotic behaviour. Therefore, we decided to study the variations of the resistance with the light in the circuit. In this way, the chaos will be controlled by the intensity of the light.

Therefore, we have used an LDR (light-dependent resistor) to detect light levels and to investigate the effects of chaos. As the intensity of the light increases, the LDR resistance decreases:

- An LDR's resistance is high in the dark and at low light levels, allowing only

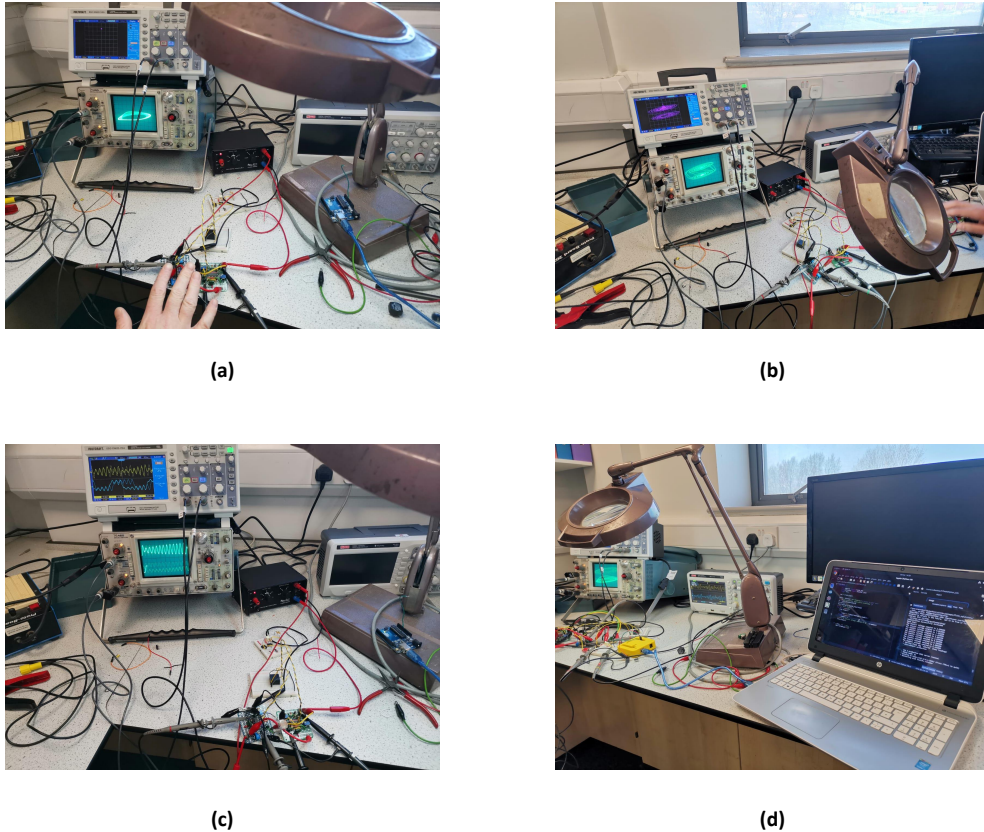


Figure 6.18: Experimental study of the symmetric chaotic circuit by using light: (a) the dark is created by covering the LDR with hands, and no chaotic behaviour is shown. (b) Light goes on the LDR, enabling the chaos to start and two phase portraits are shown on the oscilloscopes. (c) A chaotic waveform is produced. (d) Real-time waveform sampling and display on the laptop.

a small amount of current to pass through it.

- An LDR's resistance is low in bright light, allowing more current to flow through it.

In other words, the symmetrical Chua circuit now has a variable resistor which can be placed on either side, transmitter or receiver. The entire system can be used for door locking. For example, chaos can be active only during the day when there is broad daylight available. By simple circuit variation, we can make chaos when it is dark, for example, for night shifts, and it will not be available during the day shifts. In addition, by adopting mutual inductors instead of the traditional high inductance, a lower inductance can be employed, which allows the transfer of the behaviour to another symmetrical Chua circuit.

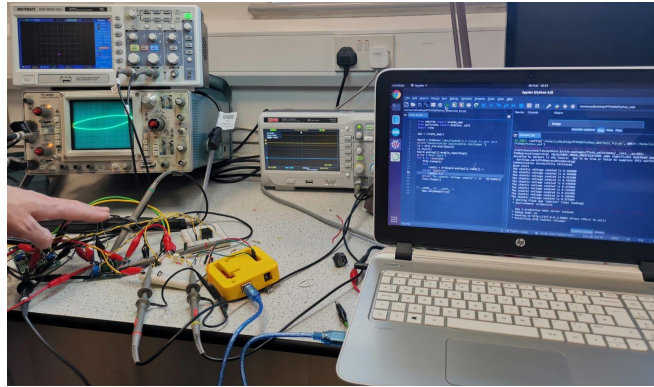
The door lock of a hotel room is an interesting application. The light in the room is set to a certain value when the room is ready to host the guest. The door-lock composed of a circuit of Chua can therefore develop into chaotic conduct. Another Chua circuit is built in the key lock. When a room is not ready, the light can be off so the resistor doesn't concede the chaotic oscillation.

Circuit simulations do not show the activation of the chaos by light. Therefore, only the experiment pictures in figure 6.18 show how the variation from chaos to non-chaos occurs when light is absent. The values of the chaotic voltages are sampled and shown on the nearby laptop. The dark is generated by covering the LDR with hands, and no chaotic behaviour is shown in figure 6.18 a. When the LDR is illuminated, allowing chaos to begin, and two phase portraits are displayed on the oscilloscopes, as shown in figure 6.18 b. In figures 6.18 c and 6.18 d, two chaotic waveforms of the voltages have been created and sampled in real time and displayed on the laptop.

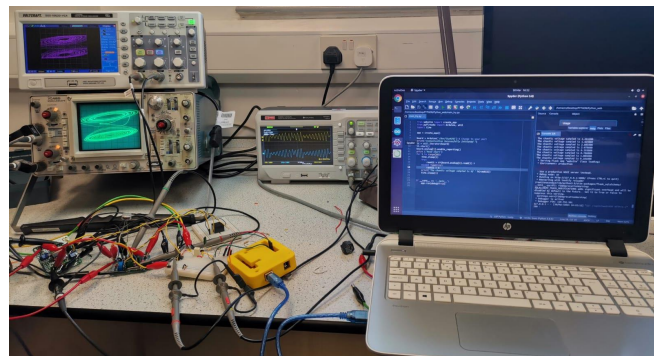
6.4 Temperature dependent Chua circuit Chaos

The temperature variation of the resistor R in the Chua circuit is the topic of the second part. In reality, the resistor R controls chaotic behavior. As a result, we decided to investigate how the resistance changes in the circuit as the temperature rises. The temperature will manage the chaos in this manner. When a room isn't ready, the temperature is regulated to a level where the resistor won't allow chaotic oscillation to occur. Thermistor or temperature sensors, such as thermocouples, are used in fire alarms. The resistance of the most popular type of thermistor falls as the temperature rises:

- A thermistor's resistance is high at low temperatures, allowing only a little amount of current to pass through it.
- A thermistor's resistance is low at high temperatures, allowing more current to pass through it.



(a)



(b)

Figure 6.19: Temperature experiment: (a) by holding with fingers we have increased the temperature resulting in no chaos behaviour; (b) after the temperature cooled down the chaotic behaviour started again.

As a result, we used a thermistor to sense the temperature and examine chaos effects. The whole system can be used to lock doors. A hotel room's door lock is an intriguing application. When the room is ready to accommodate the guest, the temperature is set to a specific value. As a result, a door lock with a Chua circuit can exhibit unpredictable behaviour. The key lock has a Chua circuit as well.

Again, the circuit simulations do not show the activation of the chaos by the temperature. Therefore, only the experiment pictures in figure 6.19 show how the variation from chaos to non chaos occurs when the temperature increases. The values of the chaotic voltages are sampled and shown on the nearby laptop. The temperature rising is created by touching the sensor. When the temperature is high enough, no chaotic behaviour is shown in figure 6.19 a. At the room temper-

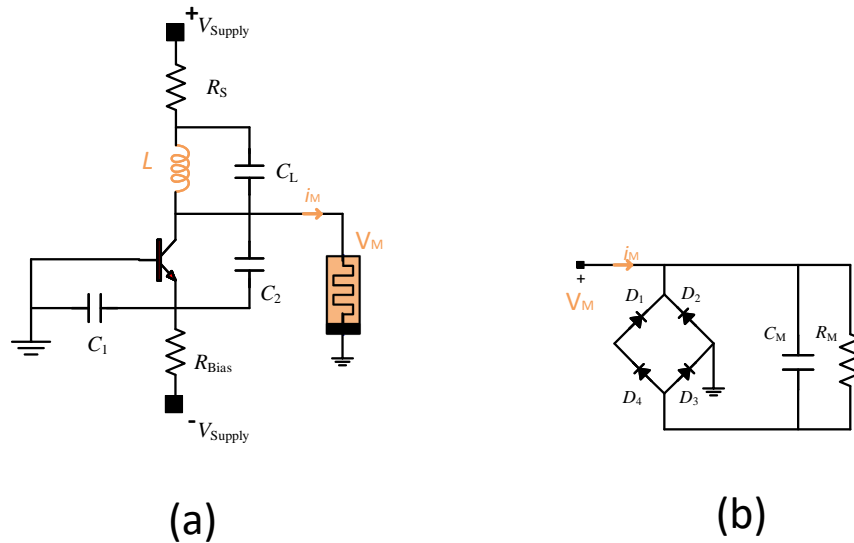


Figure 6.20: (a) Colpitts oscillator with memristor and (b) the generalised model of the memristor.

ature, the chaos begins and two phase portraits are displayed on the oscilloscopes, as shown in figure 6.19 b.

6.5 Memristive chaotic Colpitts oscillator

Memristor-based chaotic circuits, particularly memristive Chua's chaotic circuits, have Recently, in the research literature, has emerged a memristor-based Colpitts chaotic oscillator shown in Figure 6.20 a. A single-transistor implementation of a sinusoidal oscillation circuit, the third-order or fourth-order Colpitts oscillator, is widely used in electronic circuits and communication systems [281, 282]. Depending on the manufacturing process, the operation frequency might range from a few hertz to the microwave area (gigahertz). The active device's exponential [281] or piece-wise linear [282] characteristic indicates that the system is intrinsically non-linear. The Colpitts oscillator, like many other oscillator topologies studied in the literature, can display complex dynamical behaviour. There is a wealth of computational and experimental evidence of nonlinear behaviour for the Colpitts oscillator, most notably [281, 282]. As a result, by including a memristor into the fourth-order Colpitts oscillator [282], a unique memristive Colpitts oscillator can

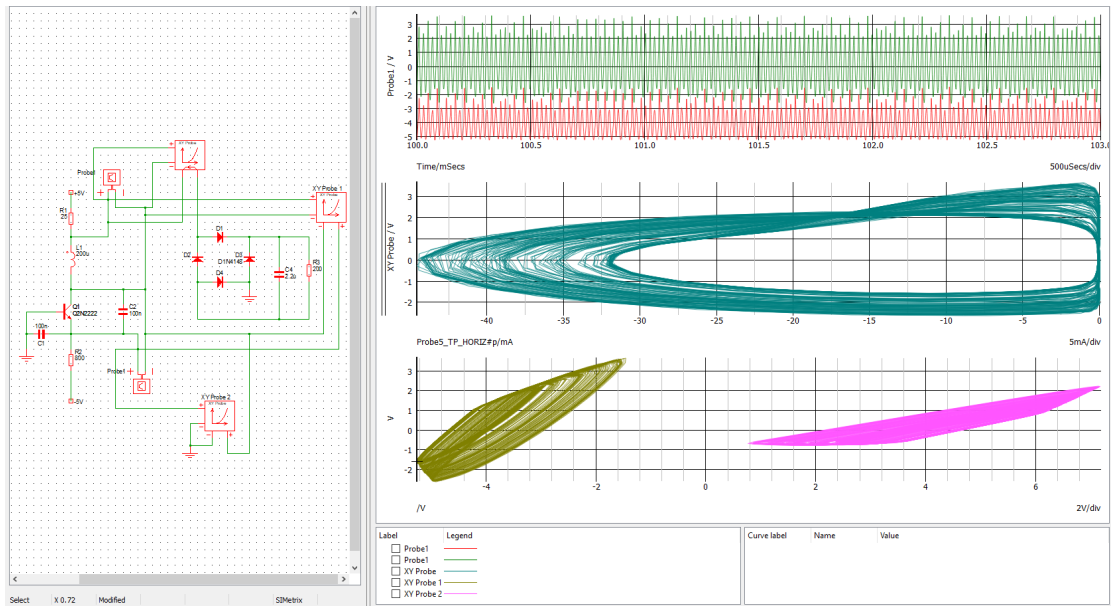


Figure 6.21: Circuit Simulations of the Memristor-based Colpitts circuit.

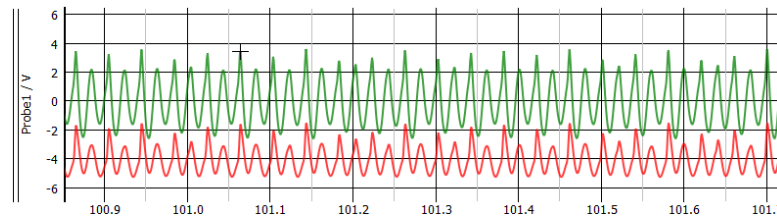


Figure 6.22: Zoom on the voltage V_L between the resistor and the inductor and the voltage V_C on the collector of the transistor.

be simply produced while retaining the original advantages.

In the References [283, 284], a diode bridge circuit can be used to create a simple analogue memristor model. The proposed memristive Colpitts oscillator is implemented using a first-order generalised memristor consisting of a diode bridge cascaded with a first-order parallel RC filter [283], which is simplified from a second-order generalised memristor realised by a memristive diode bridge with an LCR filter [284].

6.5.1 Generalised Memristor Model

In Figure 6.20 b is shown the analogous realisation circuit of the first-order generalised memristor in [283], which is a diode bridge cascaded with a first-order

parallel RC filter. The voltage limitations involving each pair of parallel diodes are the main mechanisms at the root of its memristive activity [284]. The mathematical model, with v_0 to the voltage across the capacitor C_M and i_M the current flowing through the generalised memristor's input terminal, can be written as follows:

$$i_M = G_M V_M = 2I_{S1} \cdot e^{-\rho_1 v_0} \cdot \sinh(\rho_1 V_M) \quad (6.9)$$

$$\frac{dv_0}{dt} = \frac{2I_{S1} \cdot e^{-\rho_1 v_0} \cdot \cosh(\rho_1 V_M)}{C_0} - \frac{v_0}{R_0 C_0} - \frac{2I_{S1}}{C_0} \quad (6.10)$$

The equations 6.9 and 6.10 present a mathematical model that agrees with the defining equations for the class of generalised memristors [285]. The voltage control of the generalised memristor is true, and its memductance is represented as:

$$G_M = \frac{2I_{S1} \cdot e^{-\rho_1 v_0} \cdot \sinh(\rho_1 V_M)}{V_M} \quad (6.11)$$

More details about the mathematical model are given in Reference [286]. Focusing on the circuit, the non-linear component of the Colpitts oscillator is an NPN bipolar junction transistor. In total, the fourth-order Colpitts oscillator has four state variables: voltage V_1 of capacitor C_1 , voltage V_2 of capacitor C_2 , voltage V_L of capacitor C_L , and current i_L of inductor L . In this way, the generalised memristor has just one state variable: voltage v_0 of capacitor C_M . We have tested the memristive Colpitts in SIMetrix as shown in figures 6.21 and 6.22 by analysing the voltage V_L between the resistor and the inductor and the voltage V_C on the collector of the transistor. From figure 6.22 we can notice that it behaves chaotically. The further XY plots in figure 6.21 confirm one-attractor behaviour. The fingerprint of this generalized memristor has a spiral chaotic attractor formed by the voltage on the memristor V_M and V_L mentioned above. The voltage between the inductor and the capacitor (connecting both terminals to two channels of the

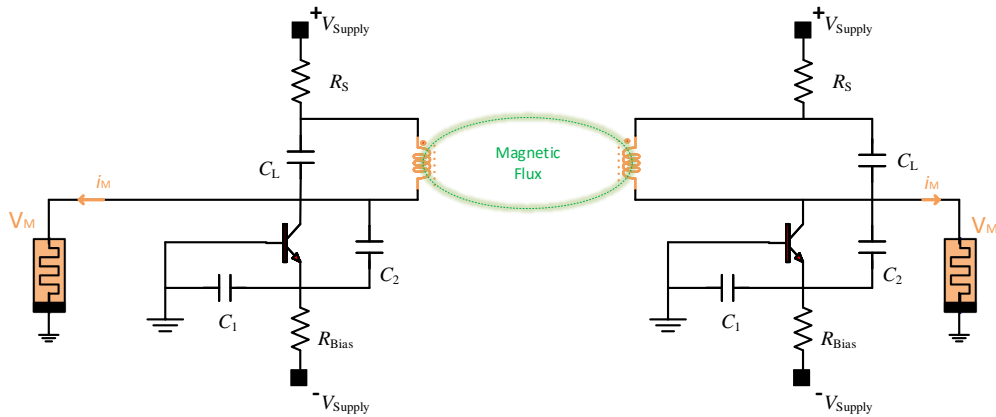


Figure 6.23: Memristive Colpitts power and chaos transmission system.

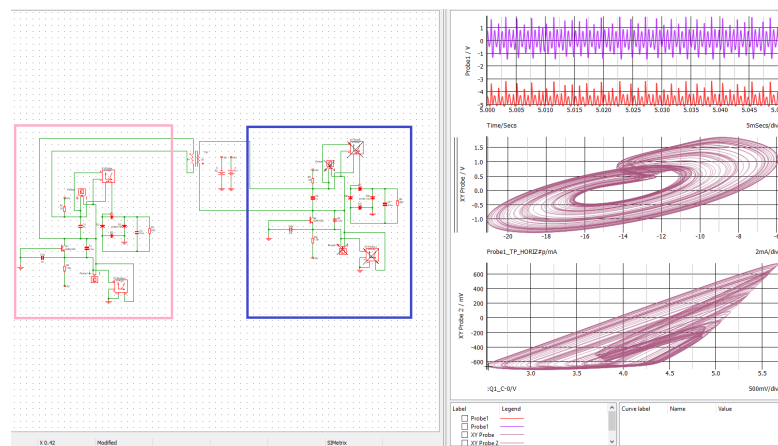


Figure 6.24: Near-Field Communication with Memristor based Colpitts oscillators: Transmitter (squared in red) waveform.

oscilloscope) is also a known triangular chaotic single attractor. These XY plots are shown in the figure 6.21.

6.5.2 NFC built with Memristive Colpitts Oscillator

Similarly to the configuration introduced before, the system model consists of two symmetrical parts of Memristive Colpitts oscillators shown in Figure 6.23. These copies of the oscillators are mutually inducted into the air through the inductor, hence composing a new topology of the M-WPT system. However, the power level in this configuration is even lower as the Colpitts circuit can be designed for very low power functionality. Similarly, the cryptosystem model, the process of chaotic encryption key for door opening, can be created.

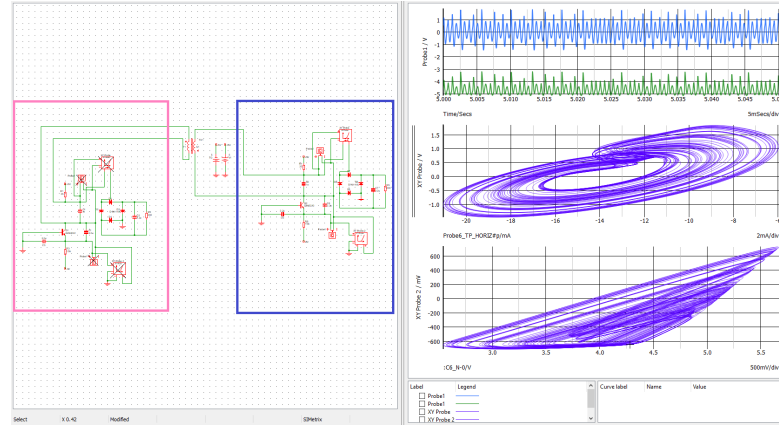


Figure 6.25: Near-Field Communication with Memristor based Colpitts oscillators: Receiver (squared in blue) waveform.

Table 6.3: Parameters of the system proposed.

M-Colpitts Parameter	Transmitter	Receiver	Value
C_1	C_{1T}	C_{1R}	6.8 nF
C_2	C_{2T}	C_{2R}	68 nF
C_L	C_{LT}	C_{LR}	6.8 nF
R_1	R_{1T}	R_{1R}	2.18 k Ω
R_2	R_{2T}	R_{2R}	2.18 k Ω
C_M	C_{MT}	C_{MR}	68 nF
R_M	R_{MT}	R_{MR}	2.18 k Ω
L	L_T	L_R	8 mH
M			3.8 mH

6.5.3 Simulations and Experiment

Firstly, we tested the circuit in simulation to compare our results to the values obtained in the Reference [286]. We see that the generalised memristor fingerprint is obtained as shown in Figures 6.24 and 6.25 of the Colpitts transmitter and receiver simulation. The aperiodic waveform of the variables can be seen at the top of Figures 6.24 and 6.25. In Figure 6.26, the synchronisation of the phase portraits (of the chaotic attractors) are fully synchronised as shown in all the XY plots of the transmitter (left) and the receiver (right) waveforms. This clearly shows the functionality of this new topology of wireless power and data transmission.

Using the same circuit parameters as in numerical simulations, an experimental setup for the memristive Colpitts oscillator will be used to examine dynamical

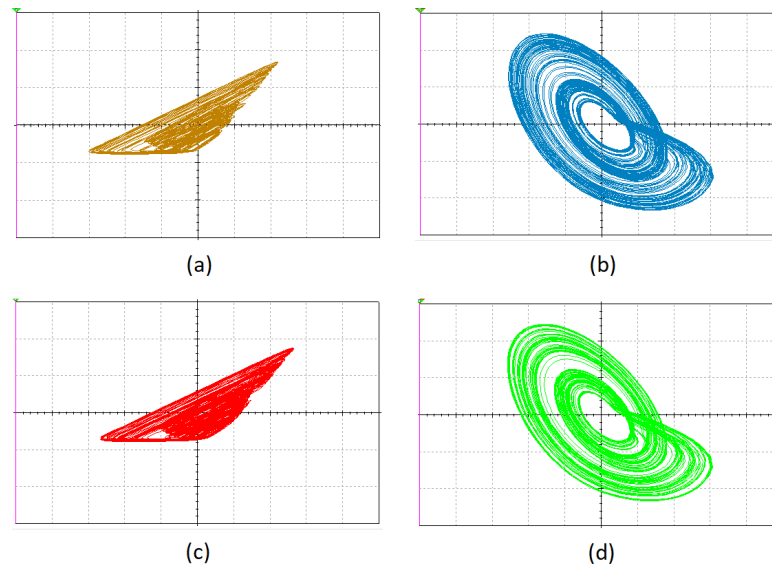
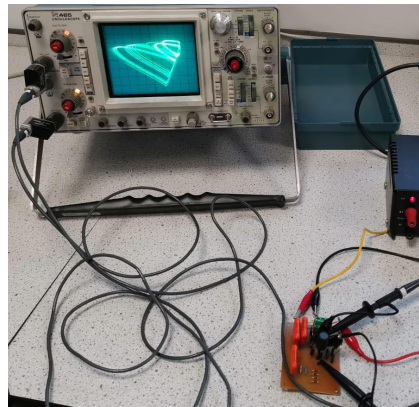


Figure 6.26: Simulation synchronisation of the phase portraits with a single chaotic attractor: the XY plots of the transmitter (a)triangular-shaped attractor and (b)the spiral chaotic attractor. The receiver is fully synchronised and shows as well a (c)triangular-shaped attractor and (d)the spiral chaotic attractor.

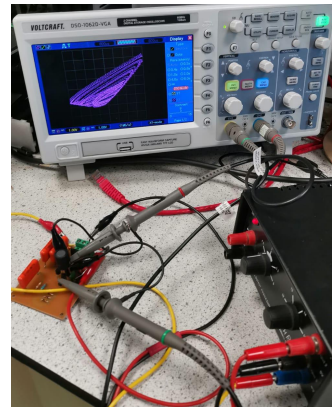
characteristics. Figure 6.27 shows experimentally the chaotic behaviour of two memristive Colpitts oscillators. Different parameters create different trajectories and different chaotic behaviour. However, it's clear from Figure 6.27 experimental results that the physical circuit may produce chaos, as predicted by the numerical calculations.

In the experiment, we have created two copies of the memristive Colpitts circuits where the inductors are replaced with a transformer the Shaffner 8 mH 2:1 which should give around 4 mH mutual coupling creating actually an over-coupling. As shown in Figure 6.28a, the circuits both show chaotic behaviour, which has been sampled from a microcontroller and the values are displayed in the computer monitor (highlighted in yellow). The waveforms are chaotic although their phase portrait are slightly different from the simulated plots shown in Figure 6.26. This is due to the higher inductance used and the parasitic effects. The microcontroller can also plot the sampled waveform in real time as shown in Figure 6.28.

Summary. We conceived, simulated, and experimented the two Chua circuits

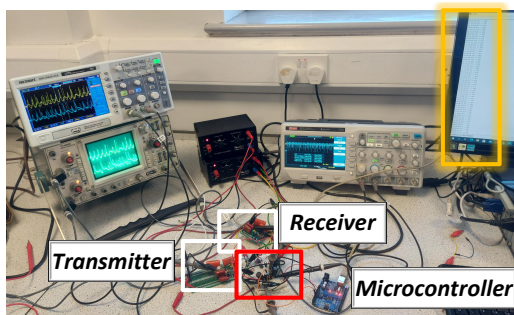


(a)

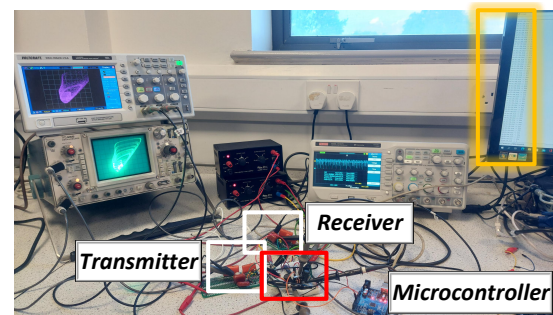


(b)

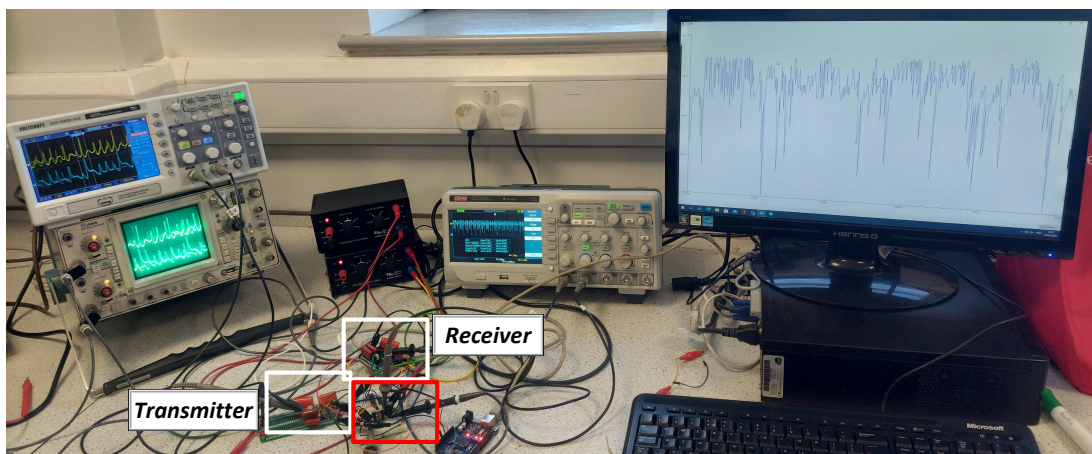
Figure 6.27: Experiment test for single Colpitts circuits with (a) some testing parameters and (b) original parameters from Reference [286].



(a)



(b)



(c)

Figure 6.28: Memristive Colpitts power and chaos transmission. The experiment also shows the sampled waveform displayed in a computer monitor.

in chaotic communication in this section of the thesis. We sampled the chaotic voltages in the receiver using a variety of memristor equivalent circuits. Additionally, we incorporated a novel technique known as the memristive Colpitts oscillator. By adding mutually linked inductors to this circuit, we witnessed the subsequent chaos. The advantages of this circuit include the possibility of low-power operation and the ability to operate at a higher frequency up to the operational limits of the memristor.

Chapter 7

NFC Security Applications

In today's world, NFC technology is employed in a variety of applications, including property protection, physical access control, system security, and cloud computing access control. NFC technology is utilised in access control to simplify the notion of access badges or keys. A smart card, like RFID, can convey data to NFC-enabled devices like tablets, phones, and laptops, as well as allow them to access cloud-based networks and system resources over the internet. Modern NFC access control systems are controlled using smartphone apps that serve as the key or information tag for an NFC-enabled reader. A communication channel is created and data exchanges take place when the mobile device is swiped or tapped over the NFC reader to validate the user's authorisation to access the secured area, resources, or applications.

7.1 The need of security in NFC devices

Therefore, it is necessary to increase the level of security in smart cards and to reduce the NFC vulnerability. In this thesis, we introduce the memristor to the NFC to improve the security of IoT devices.

An example is the NFC smartphone software applications (shown in Figure 7.1 a, where at concerts and athletic events, mobile ticketing, which involves displaying a virtual ticket with a number on the screen of your phone, is growing increasingly

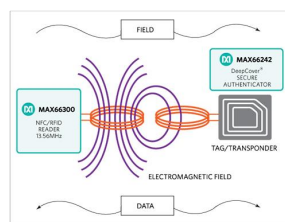


Figure 7.1: The IOT devices make a (a) Large use of NFC (b) A commercial NFC chip product collected from the manufacturer website [287].

popular. In Figure 7.1 b, there is an NFC diagram with two chip used by the manufacturer. For example, it is shown the MAX66242, which contains an I2C interface that can be used as a slave or master port for the coil antenna. For NFC purposes, the device has its own guaranteed unique 64-bit ROM ID that is factory programmed into the chip.

The NFC developments are software applications of the Internet of Things (IoT), which is based on the ability of physical objects with embedded technology to communicate with each other or with other systems, transmit data, and work in a synchronised way. An IoT security survey by Granjal et al. [288] further suggests the importance of security, privacy, and trust. NFC can assist with secure

on-demand connecting, as well as controlling and commissioning of IoT devices through proximity, in order to assure that only the two devices are communicating as shown in Figure 7.1. It can also help with secure device configuration, firmware updates, cryptographic key configuration, and log access.

Because of its proximity, NFC has an advantage. However, it uses an untrusted communication channel and does not ensure the authenticity, authorisation, and trustworthiness of the devices [289]. The standard NFC access to the IoT unit comprises of a user's device (typically a mobile device, unique cards, or maybe a key fob) to get into the IoT unit via NFC tags. These devices utilise the unreliable NFC Data Exchange Format (NDEF) communications [290] or maybe Peer-to-Peer mode [291], which is not ready to accept designers for a two way communication. Hence, it is important to develop new NFC modes that can overcome these security issues. On user devices, such as certain commercially available mobile devices, NFC uses a component called Secure Element (SE) [292]. The SE is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (for example, cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities. It can also be used for hardware card emulation of a small-sized contact-less smart card on a mobile device [153], as well as to store credentials and identities. In order to increase security, the Host Card Emulation (HCE) provides the emulation of a smart card using the ISO 7816 standard [291] at a software level. The HCE [292, 293] is the software architecture that provides accurate virtual representation of different electronic identification cards (access, transit, and banking). This technology makes it easier for retailers to deliver payment cards through mobile closed-loop contact-less payment solutions, as well as provides real-time payment card delivery, and enables a simple implementation scenario that does not require changes to the software within payment terminals. This can be accessed by a traditional card reader or a HCE reader application on another user device using the Application Protocol Data Unit (APDU) packets

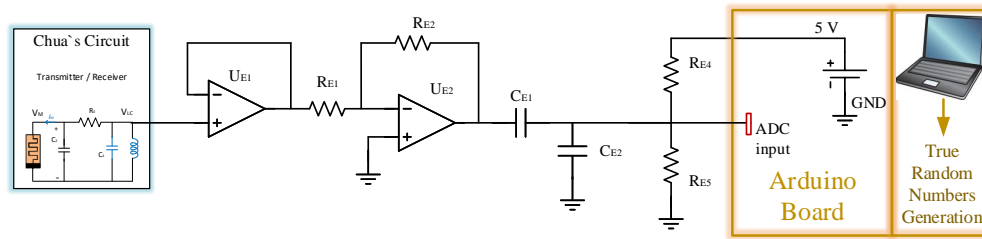


Figure 7.2: The schematic of Memristors wireless power transfer circuit with adaptive circuit for the TRNG.

[294]. However, since the HCE is totally software-based, it is vulnerable to threats and requires additional mechanisms to secure the interaction [295, 296].

7.2 Experiments for Security Applications

In this chapter, we want to use the results of the experiments done with the circuits to apply them for security purposes. Beginning with the system made up of two Chua circuits, the inductors are mutually coupled.

In order to sample the chaotic waveform, it is necessary to adapt this waveform to the dynamic of the analogue to digital converter (ADC). Thus, we have created an additional circuit (shown in Figure 7.2) which keeps the dynamic of the waveform sampled between 0 and 5 V, the Arduino ADC dynamic. As shown clearly in the simulation Figure 5.12, the Chua circuit has voltage on the receiver coil V_{LCR} (in blue) in a range between -0.5V and 0.5V. Alternatively, we can sample the memristor voltage V_{MR} (in red), which has a range of nearly -4V to 4V. However, the ADC on the Arduino board has a dynamic range of 0 to 5 V. We are using a microcontroller that has few features to minimise the cost of the production. Therefore, in the experiment we sampled the coil voltage. An important thing to notice is that negative voltages are not allowed as they can damage the electronic board; hence, it is necessary to adjust the range. For this reason, we have built an adaptor circuit, shown in the figure, which is composed of a Voltage Follower or Buffer, an Inverting Amplifier, and a Voltage Divider for the 0 to 5 volt supply.

Recalling the experiment shown previously in Chapter 6, we are using an equiv-

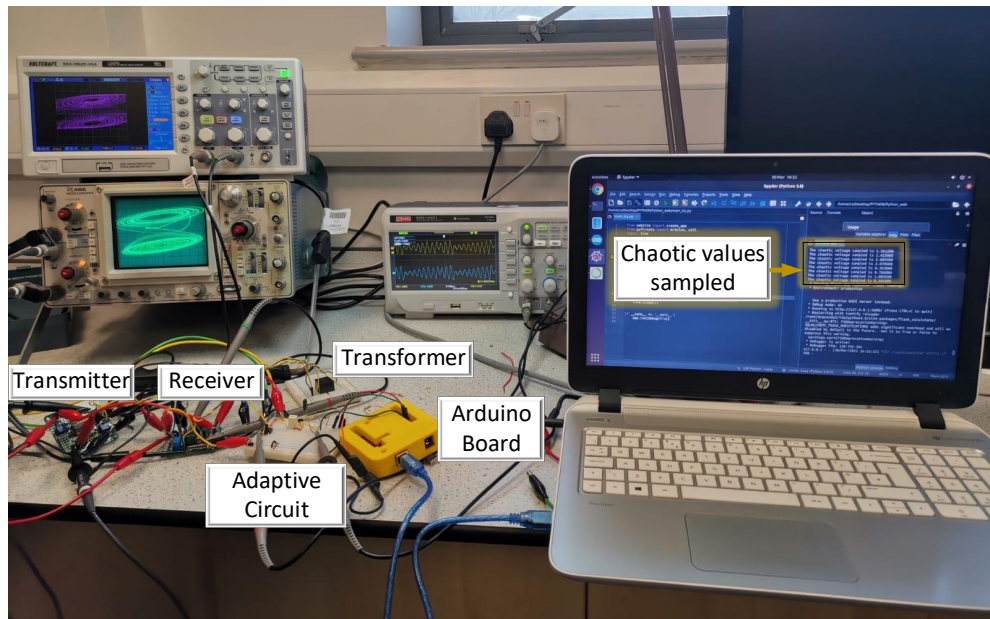


Figure 7.3: The experiment with a real time TRNG.

alent memristor circuit rather than the real memristor. In this way, the adaptor circuit of the WPT system can be adopted in any memristor emulator. Instead of using coils for the power transmission, the Shaffner 8 mH 2:1 transformer has been adopted. This transformer gives enough mutual coupling to start the chaotic behaviour. The significant test is the development of chaos in the circuits and the sampling with the Arduino board, which can create numbers.

The two circuits can generate multi-stability (two attractors phase portrait) and have the same behaviour because they have the same circuit parameters and initial conditions. The two memristor-based circuits have the same dynamical behaviour, and they also have synchronisation in their phase portrait, as shown in the oscilloscopes in Figure 7.3. The chaotic behaviour developed by the system is visualised on the transmitting side using a Tektronix 465 analogue oscilloscope and at the receiver with a Voltcraft digital storage oscilloscope and is in accordance with our simulations. Before sampling, the top oscilloscope was connected to the transmitter, the bottom one to the receiver, and the side one to the waveform generated in the adopting circuit. On the side oscilloscope, there is a plot of the waveform of the voltages of the operational amplifier U_{E2} and the input voltage of

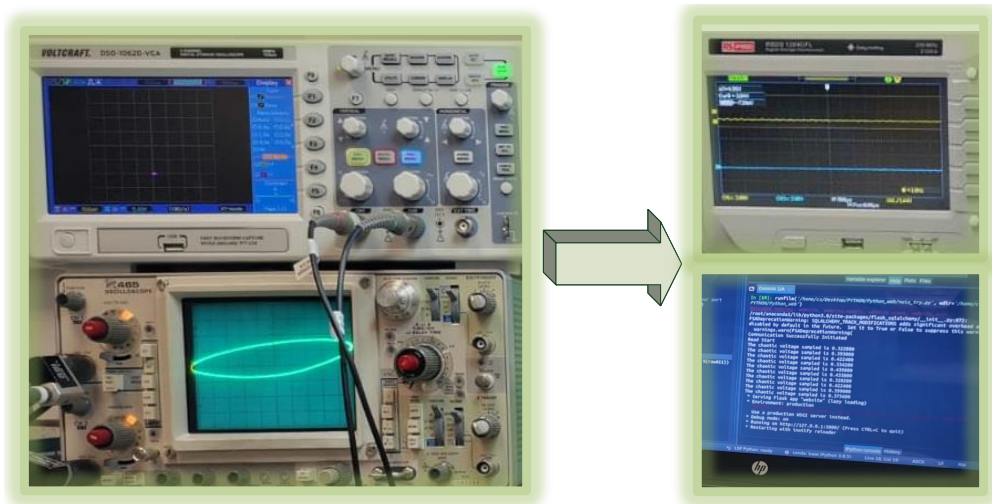


Figure 7.4: No chaotic waveform will generate near to zero random numbers. On the left, the Transmitter (bottom) and Receiver (top) are shown in a XY plot. The voltage for the microcontroller input and the execution of the Python code with number generation are shown on the right.

the ADC (the voltage on capacitor C_{E2}) before the voltage divider. The gain of the Inverting Amplifier is set to increase the input voltage to the ADC dynamic range. To protect the ADC from an over-voltage or negative voltage, the resistance R_{E1} is a potentiometer in order to promptly adjust the gain of the Inverting Amplifier as required. For safety reasons, it has been regulated to the maximum of 3.

7.2.1 Arduino True Number Generation

Once the chaos has been generated, the voltage in the coil is adjusted and sampled. Chaotic voltage behaviour is the source of entropy. Therefore, it is possible to create a true random number generator (TRNG). True random number generators create sequences that are impossible to predict. They use random physical phenomena as their source of randomness.

When the transmitter and receiver are out of range, there is no chaos and the numbers generated are near to zero. As shown in figure 7.4, the transmitter of the bottom oscillator is continuously trying to find a receiver. The waveform sampled is only noise. After 20 readings (or more), the python code concludes that there is no chaos.

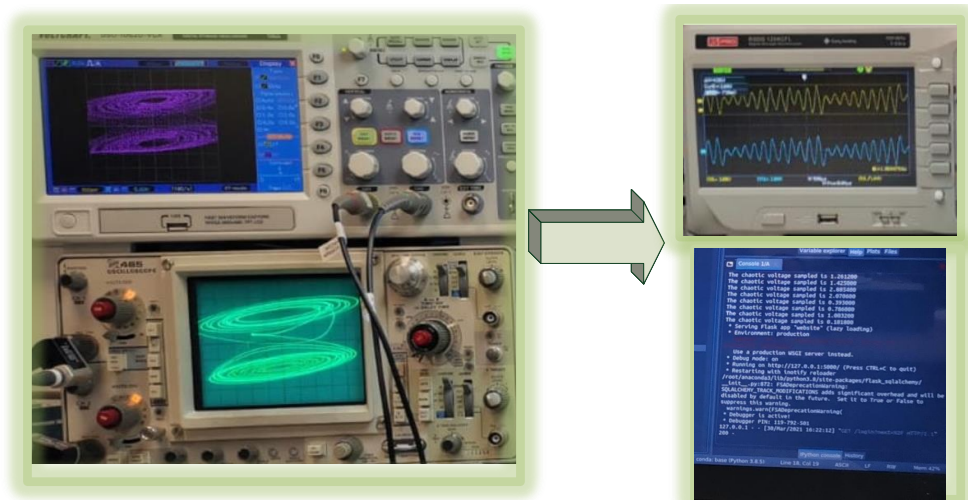


Figure 7.5: A chaotic waveform will generate true random numbers. On the left, it is shown the XYplot of the Transmitter (bottom) and Receiver (top). On the right, it is shown the ADC input voltage and the execution of the Python code with number generation.

When the transmitter and receiver are in synchronisation, there is a chaotic waveform to sample and obtain the TRNG, as shown in the figure 7.5. The values of voltage obtained are true random numbers from the entropy of a chaotic circuit.

7.2.2 Arduino Firmata Library

To connect an embedded system to a host computer, we used an intermediate protocol, Firmata, that connects via a serial port. In terms of Firmata, the Arduino platform serves as the de facto standard reference implementation. Firmata is supported by the Arduino IDE, as shown in Figure 7.6. The Firmata library communicates with the host computer using the Firmata protocol, which is implemented by the Firmata library. This eliminates the need to create your own protocol and objects for the programming environment you're using in order to write custom firmware.

Firmata is a communication protocol that allows software on a computer (or smartphone/tablet, etc.) to communicate with microcontrollers. The protocol can be implemented in both firmware and software on any microcontroller architecture (clients). Firmata is based on the midi communication format, which uses 8-bit

commands and 7-bit data bytes. The midi Channel Pressure (Command: 0xD0) message, for example, is two bytes long; in Firmata, Command 0xD0 is used to enable digital port reporting (collection of 8 pins). Although both the midi and Firmata versions are two bytes long, the meanings are clearly distinct. The number of bytes in a message in Firmata must match the corresponding midi message. Midi System Exclusive (Sysex) messages, on the other hand, can be any length and hence feature heavily in the Firmata protocol. We do not want to focus on other details of the coding.

```

#include <Firmata.h>

#define I2C_WRITE          B00000000
#define I2C_READ          B00001000
#define I2C_READ_CONTINUOUSLY B00010000
#define I2C_STOP_READING B00011000
#define I2C_READ_WRITE_MODE_MASK B00011000
#define I2C_10BIT_ADDRESS_MODE_MASK B00100000
#define I2C_END_TX_MASK B01000000
#define I2C_STOP_TX      1
#define I2C_RESTART_TX   0
#define I2C_MAX_QUERIES  8
#define I2C_REGISTER_NOT_SPECIFIED -1

// the minimum interval for sampling analog input
#define MINIMUM_SAMPLING_INTERVAL 1

/*=====
 * GLOBAL VARIABLES
 *=====

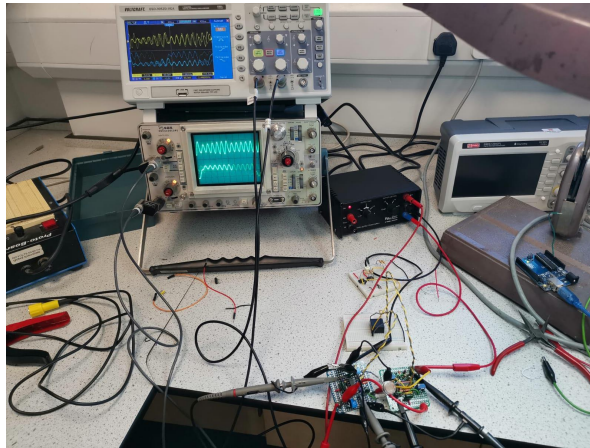
#ifdef FIRMATA_SERIAL_FEATURE
SerialFirmata serialFeature;
#endif

```

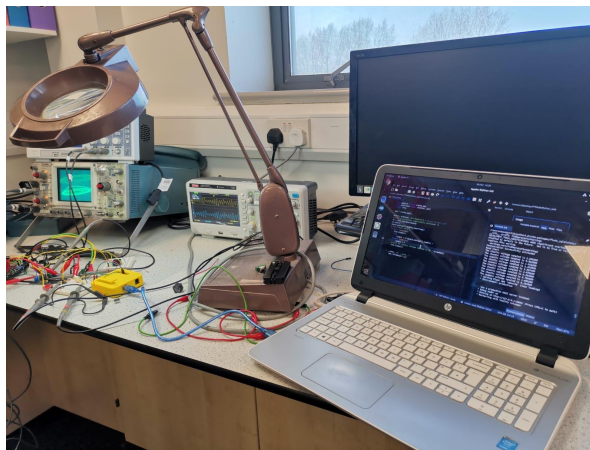
Figure 7.6: Screenshot of the Arduino IDE uploaded with Firmata coding template.

7.3 Web server application using Python

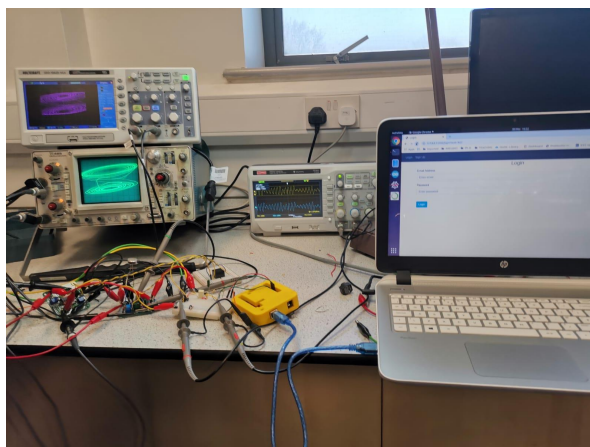
The purpose is to create a website running on a web server that will allow users to create an account and a webpage where they can write words and upload pictures. For example, it will be very similar to a social network where anyone can create a new account or log in. This web server will have the chaotic values coming from the Chua circuits sampled in real time and used for encryption in Figure 7.7. In this thesis, we will not focus on the encryption code because it will be out



(a)



(b)



(c)

Figure 7.7: The experiment set up: (a) development of the chaotic waveform; (b) sampled values of the chaos shown in Python; (c) webserver running with log in features developed with Python.

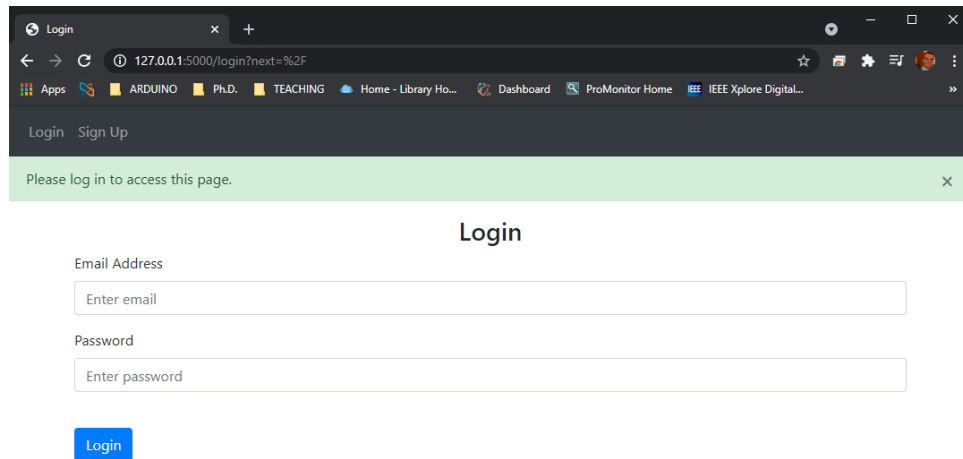


Figure 7.8: Use of Python and use chaotic encryption for web resources.

of the Electronic Engineering topic. It will be a specialist in Computer Science or Mathematics to design an algorithm for the code obtained. Therefore, let us assume that a user would like to create a new account shown in Figure 7.8. The user needs to provide an email address, e.g. colin3@gmail.com. Colin is the user name. The interface should allow you to create a user and a password. Thus, when the user has submitted a message, the account that was successfully established should appear. When logged in, a user will see a webpage labelled "notes", where they can add a new one. Later, we can log out, and any time the user logs back in, they can upload or delete a new note and observe that it has updated.

If any user attempts to return to the slash homepage, they will be denied access since they are not logged in. However, if they sign in, using the correct email and my password, we will be redirected to their notes. Naturally, if the user can create as many accounts as they want, we do not consider limited resources. Again, we are not focusing on how the application will work, but only that it has been really hard to create the application with Python libraries and use the chaotic value for any algorithm.

7.3.1 Python libraries: Flask and SQL Alchemy

As mentioned above, we have sampled the waveforms and used the Arduino Firmata library and Python to record the data on a host PC and make it available for an online service. For the web server application, the chaotic data is used in Python code in addition to the Flask libraries and SQLAlchemy. Flask is a compact and lightweight Python web framework that provides essential tools and capabilities for building online applications in Python. Because we can build a web application rapidly using only a single Python file, it allows developers more flexibility and is a more accessible framework for beginning developers. It was created with the goal of keeping the application's core simple and scalable. Instead of requiring an abstraction layer for database support, Flask allows users to build extensions to their applications. Flask is also extendable, and it doesn't require complicated boilerplate code or a certain directory structure to get started.

In other words, Flask is a web framework and a Python module that makes it simple to create web applications. The Web Application Framework, or simply a Web Framework, is a set of frameworks and modules that allow web application developers to construct apps without having to worry about low-level issues like protocol and thread management. Flask is a Python-based web application framework. The first test to use Flask is to create simple code, usually the "Hello World" code. Even though it's a micro-framework, the entire app shouldn't be contained within a single Python file. To handle complexity, we can and should use many files for larger programmes. On this occasion, only a few lines of code are required and it is possible to create and construct an online application. It then launches a "Hello World" web server that is accessible from your web device. We can simply open a web browser and type localhost on port 5000 (the url) to see "Hello World". For these reasons, Flask is one of the most widely used web frameworks, which means it's up-to-date and cutting-edge. Its functionality can be simply expanded. It may be scaled up to handle more sophisticated applications.

The popularity of SQLAlchemy stems from the fact that it is simple to use, enables the programmer to write code more quickly, and, most importantly, does not require any prior knowledge of SQL. This is a significant advantage because it allows for greater flexibility in the application of a chaotic system designed. The majority of working software engineers prefer SQLAlchemy for this reason.

For social networks, a bottom-up design is optimal because it enables us to define security and behaviour requirements precisely while allowing for updates. Additionally, this enables future upgrades to be much less likely to break things and much easier to implement and maintain. This library enables the creation of standard email/password authentication, as well as the uploading of images, setting of a profile photo, and publishing of content (with an optional image). Additionally, users can follow other users on this social network, or a company can track database variations made by employees. Additionally, the library supports strong password hashing, an auto-generated UUID as the primary key, a restricted API role/user with explicit functions for creating new entries, and strict typing via user-defined types. All of these characteristics combined with chaotic number generation may result in the creation of a unique chaotic algorithm based on memristors.

7.4 Statistical tests

In order to analyse the data collected from the Arduino board and shown from the Python code, it is necessary to have this data normalised and converted into binary numbers through symbolic dynamics. More specifically, each signal is compared to a threshold, with a value of 1 assigned to the output bit if its value at the time n exceeds the threshold's value, and 0 otherwise. The threshold for each of the two entropy sources has been set to the average of the state variable utilised, resulting in a uniform distribution of "0" and "1" symbols. There are several tests that may be used to evaluate the statistical characteristics of TRNGs.

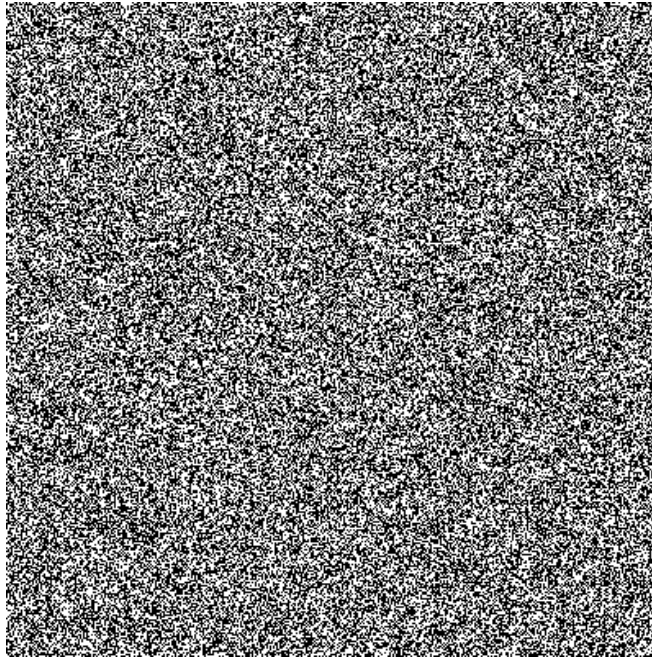


Figure 7.9: The bitmap generated from the sequence of numbers sampled which have no pattern and appear to be indistinguishable from white noise to the human eye.

```
This is free software; see the source for copying conditions. There is NO  
  
rngtest: starting FIPS tests...  
rngtest: entropy source exhausted!  
rngtest: bits received from input: 252000  
rngtest: FIPS 140-2 successes: 12  
rngtest: FIPS 140-2 failures: 0  
rngtest: FIPS 140-2(2001-10-10) Monobit: 0  
rngtest: FIPS 140-2(2001-10-10) Poker: 0  
rngtest: FIPS 140-2(2001-10-10) Runs: 0  
rngtest: FIPS 140-2(2001-10-10) Long run: 0  
rngtest: FIPS 140-2(2001-10-10) Continuous run: 0  
rngtest: input channel speed: (min=1.341; avg=4.975; max=6097.529)Mibits/s  
rngtest: FIPS tests speed: (min=47.425; avg=48.350; max=49.245)Mibits/s  
rngtest: Program run time: 45723 microseconds
```

Figure 7.10: We have used *rngtest* tests to verify the randomness of the data block. This test works on blocks of 20000 bits at a time using the FIPS 140-2. The *rngtest* is composed of five different tests: monobit, poker, runs, long run, and continuous run. The block fails the test if any of these fail.

Displaying the sequence as a bitmap graphic, with each pixel representing one bit, is the simplest and most straightforward approach to visually evaluate the randomness characteristic. This is the first test and it will be sufficient to indicate if there is anything clearly incorrect. As seen in Figure 7.9, the bitmap has no pattern and appears to be indistinguishable from white noise to the human eye,

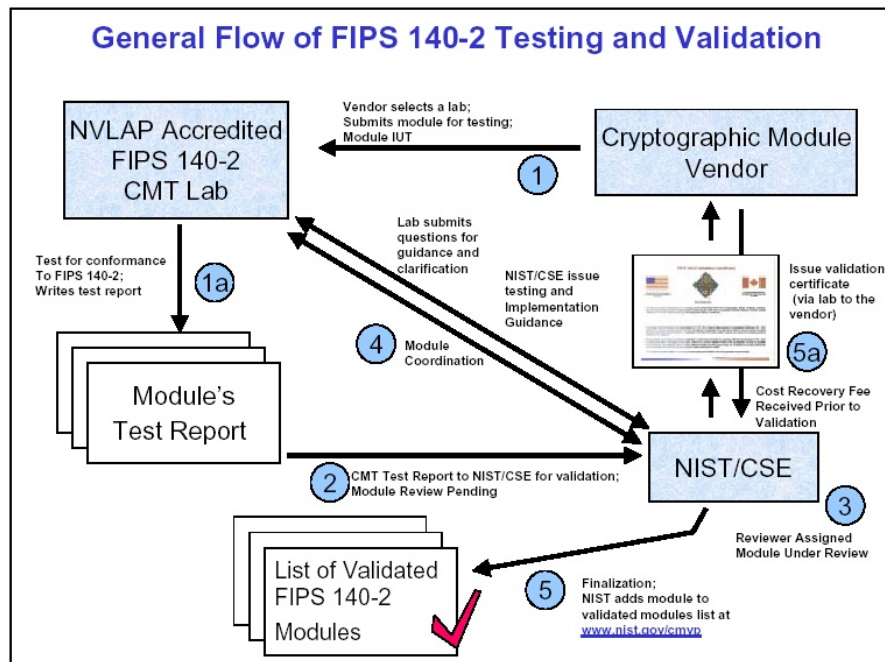


Figure 7.11: The typical Flowchart of FIPS 140-2 validation which has established the Cryptographic Module Validation Program (CMVP) as a collaborative effort between the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) for the benefit of the Government of Canada. All tests conducted under the CMVP are conducted by third-party laboratories accredited by the National Voluntary Laboratory Accreditation Program as Cryptographic Module Testing (CMT) laboratories [297].

which was anticipated above.

```

Entropy = 0.999952 bits per bit.

Optimum compression would reduce the size
of this 252000 bit file by 0 percent.

Chi square distribution for 252000 samples is 6.54, and randomly
would exceed this value 1.00 percent of the times.

Arithmetic mean value of data bits is 0.5039 (0.5 = random).
Monte Carlo value for Pi is 3.156428591 (error 0.69 percent).
Serial correlation coefficient is -0.000563 (totally uncorrelated = 0.0).
  
```

Figure 7.12: The *ent* pseudorandom number sequence test in Linux OS. The *ent* is composed of five different tests: Entropy, Monte Carlo, Chi-Square, Arithmetic mean and Serial correlation coefficient. The results confirm that our sequences are true random numbers.

In our application, we have used a package of Linux Operating System called *rngtest* (shown in Figure 7.10) which works on blocks of 20000 bits at a time (from

stdin), using the FIPS 140-2 (the U.S. government computer security standard - Federal Information Processing Standard Publication 140-2) tests to verify the randomness of the block of data [297]. The validation of FIPS 140-2 could be quite complex and can confirm the randomness of data from a dedicated laboratory after the payment of a fee, as shown in Figure 7.11. This functionality is open source in the Linux operating system and it has been widely used in the PhD research. Each of these blocks is put through five different tests: monobit, poker, runs, long run, and continuous run. If any of these fails, the block fails the test. As a direct output, a natural source of random bits may not produce unbiased bits. Many applications, particularly in cryptography, rely on unbiased bit sequences. To recover unbiased bits from a faulty generator with an unknown bias, there are several approaches known as de-skewing or whitening algorithms.

After the de-skewing algorithm, we performed a variety of checks on byte sequences stored in files by utilising *ent* pseudorandom number sequence test in the Linux OS (shown in Figures 7.12). The software may be used to test pseudorandom number generators for encryption and statistical sampling applications, compression techniques, and other applications that need to know how dense a file is. The test will be as follows:

Entropy. The number of bits per character is used to describe the information density of the file's contents. The following findings, which came from analysing a JPEG-compressed picture file, show that the file is highly packed with information basically random [298, p104-p108]. As a result, file compression is unlikely to lower the file's size. The program's C source code, on the other hand, has an entropy of around 4.9 bits per character, implying that optimum compression would reduce the file's size by 38%.

Monte Carlo. Evaluating the Monte Carlo test (shown in Figure 7.13), as stated in [299], is another easy approach to testing for randomness. Blocks of successive 48-bit numbers are used to produce (x,y) pairs, with each coordinate being a 24-bit integer. In a square (edge r) and inscribed a circle (radius r), the

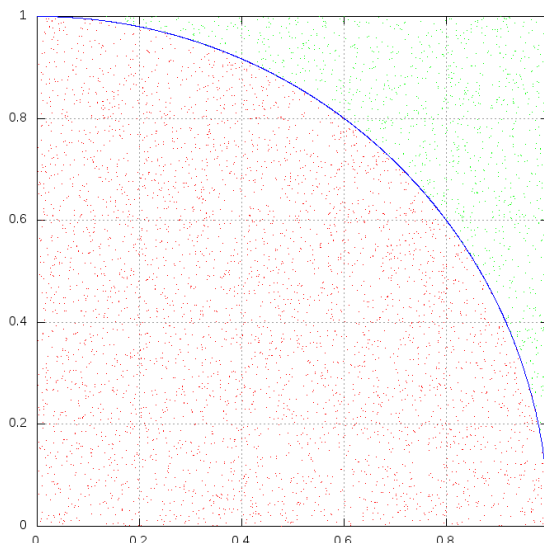


Figure 7.13: Monte Carlo test; blocks of successive 48-bit numbers are used to produce (x,y) pairs, with each coordinate being a 24-bit integer. Calculating $\pi = 4q$ with q the circle ratio in the first quadrant, where the ratio q is taken by extracting pairs of random points (x, y) from our sequence, π will approach the correct value of π confirming the randomness.

ratio, q , of the circle area in the first quadrant to the square area yields $q = \pi/4$. Calculating $\pi = 4q$, we can get the ratio q by extracting pairs of random points (x, y) from our sequence. We may estimate q by counting the number of points that fall inside the circle and dividing that number by the total number of points. If the sequence is near to random, the value calculated for π will approach the correct value of π for extremely long streams (this approximation converges very slowly).

Chi-Square. The chi-square test is the most widely used test for data unpredictability, and it is particularly sensitive to pseudorandom sequence generator mistakes. For the stream of bytes in the file, the chi-square distribution is computed and expressed as an absolute number and a percentage, indicating how often a genuinely random sequence would surpass the estimated value[300]. We interpret the % as the likelihood that the sequence being tested is not random [301, p30-p35]. The sequence is almost certainly not random if the proportion is greater than 99% or less than 1%. The sequence is suspicious if the proportion is between 99% and 95%, or between 1% and 5%. The sequence is "almost suspicious" if it

has a percentage between 90% and 95% and a percentage between 5% and 10%.

Arithmetic mean. Summing all the bytes in the file and dividing by the file length yields this result. This should be around 127.5 if the data is close to random (0.5 for -b option output). The values are consistently high or low if the mean deviates from this value.

Serial correlation coefficient. This value indicates how much each byte in the file is dependent on the previous byte. This number (which might be positive or negative) will, of course, be close to zero for random sequences. The serial correlation coefficient of a non-random byte stream, such as a C programme, will be on the order of 0.5. Serial correlation coefficients for highly predictable data, such as uncompressed bitmaps, will approach to 1, as it is further described in Reference [301, p64-p65].

The statistical characteristics are consistent with what we would expect from a really random sequence after 56 hours (nearly 3 days) of non-stop operation and 250000 bits out of the generator (after de-skewing). The results confirm that our sequences are true random numbers.

Summary. Additionally, we worked on the development of a Python-based web server application capable of utilising the sampled voltage values and encrypting them in real time. The programme may employ any encryption algorithm and may make advantage of the chaotic data obtained in real time from the circuit. We confirmed the functioning through several experiments and the unpredictability of data obtained using FIPS PUB 140-2's Security Requirements for Cryptographic Modules. The results confirm the data's real unpredictability.

Chapter 8

Future Work

Future work will be focused on improving data encryption with machine learning algorithms, because they show a great and interesting advantage in comparison with the traditional Chua's circuit. Furthermore, we have created an interesting application which, due to the COVID-19 pandemic, has not been brought forward. This application has great safety potential in road accidents.

- **Artificial Intelligence in Chaotic Encryption.** Not all of the Chua circuit chaos should be the same and equal. It is important to recognise the authorised Chua chaotic waveform. This could be the use of a supervised learning algorithm consisting of a target chaotic variable (or dependent variable) which is to be predicted from a given set of typical Chua waveform predictors (independent variables). Using these sets of variables, we generate a function that maps the inputs to desired outputs. The training process continues until the model achieves a desired level of accuracy on the training data. Examples of Supervised Learning: Regression, Decision Tree, Random Forest, KNN, Logistic Regression etc.
- **WPT for road safety.** Although the lighting in public places such as squares, streets, and other places has high safety standards, in case of accidents, these will drop instantaneously. The safety level will be very poor

until the damaged lamp post is replaced, which may take weeks. Furthermore, the lamp post will stay unlit, inducing people to believe that there is no electricity. During this time, the lighting equipment is an electric trap for any living creatures that may be in contact with it and could be electrocuted. This research introduces a unique and original lighting system which has no more cables and wires, which are replaced by a harmless magnetic flux. This new application of the Wireless Power Transfer technique is able to save lives by eliminating the electricity in the street lights. In this way, it is possible to eliminate all the deaths caused by electrocution when safety precautions fail.

- **Low power WPT for medical devices.** The power antenna plays an important role in wireless power transfer. Various kinds of power antenna techniques have been proposed in recent years in order to reduce the system size, achieve the full directionality, improve the coupling efficiency and other parameters. Accordingly, these techniques constitute many wireless power transfer structures. In medical devices, the design of the transfer structures needs to be investigated very carefully. The possible choices used in this type of WPT system are the LC-pair, the Multiple-resonators, the Quad-loops, and the Helix-derivatives. Although the transfer structures share the same physical principles, they have entirely different performance and application conditions, and further optimizations could be made. This work will continue after the PhD thesis as more equipment and longer research is required.

In preparation of the viva there will not be further progress on these projects.

Chapter 9

Conclusion

The security of the new electronic and Internet of Things devices has become a great challenge. The data protection regarding these devices is only based on the web or on well-known algorithms and software. In this work thesis, we have proposed an innovative near-field power and chaos transmission method by using the memristor and applied it for NFC security purposes. For this reason, we adopted two symmetrical Chua circuits able to transmit chaos. The circuit adopts a memristor or Chua diode, which relates the flux and current flowing in the device. Because the memristor is not commercially available, electrical circuits equivalent to the device known as the memristor emulator or model are used in literacy. There are many different models of memristors studied by the scientific community and used for different types of circuits.

Therefore, the unique behaviour of the memristor has attracted a lot of research studies and interest in developing new encryption characteristics. For this reason, we created two symmetrical Chua circuits able to transmit power and chaos by modifying the original circuit with inductors that are mutually coupled. This new technique is an interesting solution, due to the fact it can be used to implement near-field wireless communication. We have introduced an innovative implementation of the Chua circuit, which is applied to NFC. By using the chaos generated, it is possible to have a true random number generator. This new technique is an

interesting solution due to the fact that it can be used to add more security to web applications that use more NFC info. In the PhD work, we have proposed, simulated, and tested two Chua circuits in chaotic communication with each other. We have used different equivalent circuits for memristors, and sampled the chaotic voltages in the receiver. We have also used an innovative technology found in a recent article where we used a memristive Colpitts oscillator. We modified this circuit by using mutually coupled inductors and noticed the chaos generated. The advantages of this circuit are a possible low power functionality and the higher frequency achievable up to the limits of memristor.

We have also worked on the realisation of a web server application in the Python language which can use the sampled voltage values and use them in real time for encryption purposes. The web application works similarly to a social network where each user can create an account, log in with their email and password, upload notes, and log out. The application can have any algorithm of encryption and use the chaotic data received in real time from the circuit. We have tested the functionality with different experiments and verified the randomness of data obtained by using Security Requirements for Cryptographic Modules FIPS PUB 140-2. The results confirm the true randomness of the data.

Bibliography

- [1] J. Lee and B. Han. “A Bidirectional Wireless Power Transfer EV Charger Using Self-Resonant PWM”. In: *IEEE Transactions on Power Electronics* 30.4 (2015), pp. 1784–1787. ISSN: 0885-8993. DOI: [10.1109/TPEL.2014.2346255](https://doi.org/10.1109/TPEL.2014.2346255).
- [2] Johnson I Agbinya. *Principles of Inductive Near Field Communications for Internet of Things*. Vol. 18. River Publishers, 2011.
- [3] Klaus Finkenzeller. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John Wiley & Sons, 2010.
- [4] Pavel V Nikitin, KVS Rao, and Steve Lazar. “An overview of near field UHF RFID”. In: *2007 IEEE International Conference on RFID*. IEEE, 2007, pp. 167–174.
- [5] Dukju Ahn and Songcheol Hong. “Wireless power transmission with self-regulated output voltage for biomedical implant”. In: *IEEE Transactions on Industrial Electronics* 61.5 (2014), pp. 2225–2235.
- [6] Chang-Gyun Kim et al. “Design of a contactless battery charger for cellular phone”. In: *APEC 2000. Fifteenth Annual IEEE Applied Power Electronics Conference and Exposition (Cat. No. 00CH37058)*. Vol. 2. IEEE, 2000, pp. 769–773.

-
- [7] William C Brown. “The history of power transmission by radio waves”. In: *IEEE Transactions on microwave theory and techniques* 32.9 (1984), pp. 1230–1242.
- [8] Giacomo Oliveri, Lorenzo Poli, and Andrea Massa. “Maximum efficiency beam synthesis of radiating planar arrays for wireless power transmission”. In: *IEEE Transactions on Antennas and Propagation* 61.5 (2013), pp. 2490–2499.
- [9] Andrea Massa et al. “Array designs for long-distance wireless power transmission: State-of-the-art and innovative solutions”. In: *Proceedings of the IEEE* 101.6 (2013), pp. 1464–1481.
- [10] Naoki Shinohara. *Wireless power transfer via radiowaves*. John Wiley & Sons, 2014.
- [11] Jung Han Choi, Seok Hyon Kang, and Chang Won Jung. “Magnetic Resonant Wireless Power Transfer with L-Shape Arranged Resonators for Laptop Computer”. In: *Journal of electromagnetic engineering and science* 17.3 (2017), pp. 126–132.
- [12] A Reatti, F Corti, and L Pugi. “Wireless power transfer for static railway applications”. In: *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*. IEEE, 2018, pp. 1–6.
- [13] Apoorva Sharma, Eleftherios Kampianakis, and Matthew S Reynolds. “A dual-band HF and UHF antenna system for implanted neural recording and stimulation devices”. In: *IEEE Antennas and Wireless Propagation Letters* 16 (2016), pp. 493–496.
- [14] Kamal Eldin Idris Elnail et al. “Core structure and electromagnetic field evaluation in wpt systems for charging electric vehicles”. In: *Energies* 11.7 (2018), p. 1734.

- [15] Marojahan Tampubolon et al. “Dynamic wireless power transfer for logistic robots”. In: *Energies* 11.3 (2018), p. 527.
- [16] Bo H Choi et al. “7m-off-long-distance extremely loosely coupled inductive power transfer systems using dipole coils”. In: *2014 IEEE Energy Conversion Congress and Exposition (ECCE)*. IEEE. 2014, pp. 858–563.
- [17] Minghua Xia and Sonia Aissa. “On the efficiency of far-field wireless power transfer”. In: *IEEE Transactions on Signal Processing* 63.11 (2015), pp. 2835–2847.
- [18] Tianjia Sun, Xiang Xie, and Zhihua Wang. *Wireless power transfer for medical microsystems*. Springer, 2013.
- [19] Tommaso Campi et al. “Wireless power transfer charging system for AIMDs and pacemakers”. In: *IEEE transactions on microwave theory and techniques* 64.2 (2016), pp. 633–642.
- [20] CRC Press. *Transformer Design Principles: With Applications to Core-Form Power Transformers*. CRC Press, 2001. ISBN: 9781420021943. URL: <https://books.google.co.uk/books?id=Lzjs0LNHhVYC>.
- [21] Statista. *Size of the wireless charging market in the United States by application from 2012 to 2022 (in million U.S. dollars)*. 2019. URL: <https://www.statista.com/statistics/681406/us-wireless-charging-market-by-application/> (visited on 03/21/2019).
- [22] AE Umenei. “Understanding low frequency non-radiative power transfer”. In: *Bearing a date of Jun 7* (2011).
- [23] Andre Kurs et al. “Wireless power transfer via strongly coupled magnetic resonances”. In: *science* 317.5834 (2007), pp. 83–86.
- [24] Mohammed Alkahtani et al. “An Experimental Investigation on Output Power Enhancement with Offline Reconfiguration for Non-uniform Ag-

- ing Photovoltaic Array to Maximise Economic Benefit”. In: *IEEE Access* (2021), pp. 1–1. DOI: [10.1109/ACCESS.2021.3088386](https://doi.org/10.1109/ACCESS.2021.3088386).
- [25] Mohammed Alkahtani et al. “A Novel PV array reconfiguration algorithm approach to optimising power generation across non-uniformly aged PV arrays by merely repositioning”. In: *JMultidisciplinary Scientific Journal* 3.1 (2020), pp. 32–53.
- [26] Mohammed Alkahtani et al. “Investigating Fourteen Countries to Maximum the Economy Benefit by Using Offline Reconfiguration for Medium Scale PV Array Arrangements”. In: *Energies* 14.1 (2021), p. 59.
- [27] Mohammed Alkahtani et al. “Gene Evaluation Algorithm for Reconfiguration of Medium and Large Size Photovoltaic Arrays Exhibiting Non-Uniform Aging”. In: *Energies* 13.8 (2020). ISSN: 1996-1073. DOI: [10.3390/en13081921](https://doi.org/10.3390/en13081921). URL: <https://www.mdpi.com/1996-1073/13/8/1921>.
- [28] William C Brown. “Experiments involving a microwave beam to power and position a helicopter”. In: *IEEE Transactions on Aerospace and Electronic Systems* 5 (1969), pp. 692–702.
- [29] Evgeniy Donchev et al. “The rectenna device: From theory to practice (a review)”. In: *MRS Energy amp; Sustainability* 1 (2014), E1. DOI: [10.1557/mre.2014.6](https://doi.org/10.1557/mre.2014.6).
- [30] J. Cvetic. “Teslas high voltage and high frequency generators with oscillatory circuits”. In: *Serbian Journal of Electrical Engineering* 13 (2016), pp. 301–333.
- [31] Yu-Gang Su et al. “Analysis on safety issues of capacitive power transfer system”. In: *International Journal of Applied Electromagnetics and Mechanics* 53.4 (2017), pp. 673–684.

- [32] Fei Lu, Hua Zhang, and Chris Mi. “A review on the recent development of capacitive wireless power transfer technology”. In: *Energies* 10.11 (2017), p. 1752.
- [33] Aiguo Patrick Hu, Chao Liu, and Hao Leo Li. “A novel contactless battery charging system for soccer playing robot”. In: *2008 15th International Conference on Mechatronics and Machine Vision in Practice*. IEEE. 2008, pp. 646–650.
- [34] Jiejian Dai and Daniel C Ludois. “Single active switch power electronics for kilowatt scale capacitive power transfer”. In: *IEEE Journal of Emerging and Selected Topics in Power Electronics* 3.1 (2014), pp. 315–323.
- [35] Fariborz Musavi and Wilson Eberle. “Overview of wireless power transfer technologies for electric vehicle battery charging”. In: *IET Power Electronics* 7.1 (2014), pp. 60–66.
- [36] Jiejian Dai and Daniel C. Ludois. “A Survey of Wireless Power Transfer and a Critical Comparison of Inductive and Capacitive Coupling for Small Gap Applications”. In: *IEEE Transactions on Power Electronics* 30.11 (2015), pp. 6017–6029. DOI: [10.1109/TPEL.2015.2415253](https://doi.org/10.1109/TPEL.2015.2415253).
- [37] Emanuel B Tarrson. *Electric toothbrush which is rechargeable with or without a recharging stand*. US Patent 3,379,952. 1968.
- [38] Satoru Inakagata and Yoji Kawamoto. *Electric toothbrush*. US Patent 5,493,747. 1996.
- [39] Xun Liu and SY Ron Hui. “Equivalent circuit modeling of a multilayer planar winding array structure for use in a universal contactless battery charging platform”. In: *IEEE transactions on power electronics* 22.1 (2007), pp. 21–29.

- [40] Chun-Hung Hu et al. “Development of a universal contactless charger for handheld devices”. In: *2008 IEEE International Symposium on Industrial Electronics*. IEEE. 2008, pp. 99–104.
- [41] Hung-Yu Shen, Jia-You Lee, and Tsung-Wen Chang. “Study of contactless inductive charging platform with core array structure for portable products”. In: *2011 International Conference on Consumer Electronics, Communications and Networks (CECNet)*. IEEE. 2011, pp. 756–759.
- [42] Wireless Power Consortium. *Wireless Power Consortium Charter*. 2008. URL: <https://www.wirelesspowerconsortium.com/> (visited on 06/30/2021).
- [43] Powermat. *News & Events*. 2014. URL: <https://www.powermat.com> (visited on 06/30/2021).
- [44] Engadget.com. *Samsung, Qualcomm start up Alliance for Wireless Power to take on Qi*. 2012. URL: <https://www.engadget.com/2012-05-08-samsung-qualcomm-start-alliance-for-wireless-power.html> (visited on 06/30/2021).
- [45] EEPower.com. *Wireless Power War is Over, A4WP and PMA to Merge*. 2015. URL: <https://eepower.com/news/wireless-power-war-is-over-a4wp-and-pma-to-merge> (visited on 06/30/2021).
- [46] Aircharge. 2013. URL: <https://www.air-charge.com/> (visited on 06/30/2021).
- [47] Kuan-Ting Lai et al. “AnyCharge: An IoT-Based Wireless Charging Service for the Public”. In: *IEEE Internet of Things Journal* 6.6 (2019), pp. 10888–10901. DOI: [10.1109/JIOT.2019.2943030](https://doi.org/10.1109/JIOT.2019.2943030).
- [48] ChargeItSpot. 2011. URL: <http://chargeitspot.com> (visited on 06/30/2021).
- [49] InforCharge. 2014. URL: <https://www.inforcharge.com> (visited on 06/30/2021).
- [50] ChargeSpot. 2017. URL: <https://www.charge-spot.net/> (visited on 06/30/2021).

- [51] Hunter H Wu et al. “A high efficiency 5 kW inductive charger for EVs using dual side control”. In: *IEEE Transactions on Industrial Informatics* 8.3 (2012), pp. 585–595.
- [52] Omer C Onar et al. “A novel wireless power transfer for in-motion EV/PHEV charging”. In: *2013 Twenty-Eighth Annual IEEE Applied Power Electronics Conference and Exposition (APEC)*. IEEE. 2013, pp. 3073–3080.
- [53] Aqueel Ahmad et al. “A review of the electric vehicle charging techniques, standards, progression and evolution of EV technologies in Germany”. In: *Smart Science* 6.1 (2018), pp. 36–53.
- [54] Dimitrios Kosmanos et al. “Route optimization of electric vehicles based on dynamic wireless charging”. In: *IEEE Access* 6 (2018), pp. 42551–42565.
- [55] Songyan Niu et al. “The state-of-the-arts of wireless electric vehicle charging via magnetic resonance: principles, standards and core technologies”. In: *Renewable and Sustainable Energy Reviews* 114 (2019), p. 109302.
- [56] Alireza Khaligh and Serkan Dusmez. “Comprehensive topological analysis of conductive and inductive charging solutions for plug-in electric vehicles”. In: *IEEE Transactions on Vehicular Technology* 61.8 (2012), pp. 3475–3489.
- [57] Mohammed Al-Saadi et al. “Capacitive Power Transfer for Wireless Batteries Charging.” In: *Electrotehnica, Electronica, Automatica* 66.4 (2018).
- [58] Deepa Vincent et al. “Evolution of hybrid inductive and capacitive ac links for wireless EV charginga comparative overview”. In: *IEEE Transactions on Transportation Electrification* 5.4 (2019), pp. 1060–1077.
- [59] Brandon Regensburger et al. “High-performance 13.56-MHz large air-gap capacitive wireless power transfer system for electric vehicle charging”. In: *2018 IEEE 19th Workshop on Control and Modeling for Power Electronics (COMPEL)*. IEEE. 2018, pp. 1–4.

- [60] Deepak Rozario et al. “Modified resonant converters for contactless capacitive power transfer systems used in EV charging applications”. In: *IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society*. IEEE. 2016, pp. 4510–4517.
- [61] Sreyam Sinha et al. “A new design approach to mitigating the effect of parasitics in capacitive wireless power transfer systems for electric vehicle charging”. In: *IEEE Transactions on Transportation Electrification* 5.4 (2019), pp. 1040–1059.
- [62] EE—Times. *Qualcomm Sells Off Halo Wireless EV Charging Technology*. 2019. URL: <https://www.eetimes.com/qualcomm-sells-off-halo-wireless-ev-charging-technology/#> (visited on 06/30/2021).
- [63] The Guardian. *Britains electric car charging network boosted by €300m funding*. 2021. URL: <https://www.theguardian.com/environment/2021/may/24/britain-electric-car-charging-network-ofgem-points> (visited on 06/30/2021).
- [64] Department of Energys Oak Ridge National Laboratory. *Successful delivery: ORNL demonstrates bi-directional wireless charging on hybrid UPS truck*. 2020. URL: <https://www.ornl.gov/news/ornl-demonstrates-120-kilowatt-wireless-charging-vehicles> (visited on 06/30/2021).
- [65] Deepa Vincent et al. “Evolution of hybrid inductive and capacitive ac links for wireless EV charginga comparative overview”. In: *IEEE Transactions on Transportation Electrification* 5.4 (2019), pp. 1060–1077.
- [66] Shu Yuen Ron Hui, Wenxing Zhong, and Chi Kwan Lee. “A critical review of recent progress in mid-range wireless power transfer”. In: *IEEE Transactions on Power Electronics* 29.9 (2013), pp. 4500–4511.
- [67] Sokol Kuka, Kai Ni, and Mohammed Alkahtani. “A review of methods and challenges for improvement in efficiency and distance for wireless power

- transfer applications”. In: *Power Electronics and Drives* 5.1 (2020), pp. 1–25.
- [68] Poonam Lathiya, Marcel Kreuzer, and Jing Wang. “RF complex permeability spectra of Ni-Cu-Zn ferrites prepared under different applied hydraulic pressures and durations for wireless power transfer (WPT) applications”. In: *Journal of Magnetism and Magnetic Materials* 499 (2020), p. 166273.
- [69] Surender Kumar, Tukaram Shinde, and Pramod Vasambekar. “Engineering High Permeability: Mn-Zn and Ni-Zn Ferrites”. In: *International Journal of Applied Ceramic Technology* 12.4 (2015), pp. 851–859.
- [70] Poonam Lathiya and Jing Wang. “Near-Field Communications (NFC) for Wireless Power Transfer (WPT): An Overview”. In: *Wireless Power Transfer—Recent Development, Applications and New Perspectives* (2021).
- [71] Woncheol Lee et al. “A simple wireless power charging antenna system: Evaluation of ferrite sheet”. In: *IEEE Transactions on magnetics* 53.7 (2017), pp. 1–5.
- [72] Poonam Lathiya and Jing Wang. “Effects of the sintering temperature on RF complex permeability of NiCuCoZn ferrites for near-field communication applications”. In: *IEEE Transactions on Magnetics* 55.2 (2018), pp. 1–4.
- [73] Seung-Hwan Lee and Robert D Lorenz. “Surface spiral coil design methodologies for high efficiency, high power, low flux density, large air-gap wireless power transfer systems”. In: *2013 Twenty-Eighth Annual IEEE Applied Power Electronics Conference and Exposition (APEC)*. IEEE. 2013, pp. 1783–1790.
- [74] Charles R Sullivan. “Layered foil as an alternative to litz wire: Multiple methods for equal current sharing among layers”. In: *2014 IEEE 15th Work-*

- shop on Control and Modeling for Power Electronics (COMPEL)*. IEEE. 2014, pp. 1–7.
- [75] Mohammad Etemadrezaei and Srdjan M Lukic. “Coated-strand litz wire for multi-megahertz frequency applications”. In: *IEEE Transactions on Magnetics* 52.8 (2016), pp. 1–11.
- [76] Jaegue Shin et al. “Design and implementation of shaped magnetic-resonance-based wireless power transfer system for roadway-powered moving electric vehicles”. In: *IEEE Transactions on Industrial electronics* 61.3 (2013), pp. 1179–1192.
- [77] Weiyang Zhou and Ke Jin. “Optimal photovoltaic array configuration under Gaussian laser beam condition for wireless power transmission”. In: *IEEE Transactions on Power Electronics* 32.5 (2016), pp. 3662–3672.
- [78] A Alphones and JPK Sampath. “Metamaterial assisted wireless power transfer system”. In: *2015 Asia-Pacific Microwave Conference (APMC)*. Vol. 2. IEEE. 2015, pp. 1–3.
- [79] Filiberto Bilotti and Levent Sevgi. “Metamaterials: Definitions, properties, applications, and FDTD-based modeling and simulation”. In: *International Journal of RF and Microwave Computer-Aided Engineering* 22.4 (2012), pp. 422–438.
- [80] Ki Young Kim. “Comparative Analysis of Guided Modal Properties of Double-Positive and Double-Negative Metamaterial Slab Waveguides.” In: *Radioengineering* 18.2 (2009).
- [81] Bingnan Wang and Koon Hoo Teo. “Metamaterials for wireless power transfer”. In: *2012 IEEE International Workshop on Antenna Technology (iWAT)*. IEEE. 2012, pp. 161–164.

- [82] ALAK Ranaweera et al. “Experimental investigation of 3D metamaterial for mid-range wireless power transfer”. In: *2014 IEEE Wireless Power Transfer Conference*. IEEE. 2014, pp. 92–95.
- [83] Jaewon Choi and Chulhun H Seo. “High-efficiency wireless energy transmission using magnetic resonance based on negative refractive index metamaterial”. In: *Progress In Electromagnetics Research* 106 (2010), pp. 33–47.
- [84] Jing Wu et al. “Wireless power transfer with artificial magnetic conductors”. In: *2013 IEEE Wireless Power Transfer (WPT)*. IEEE. 2013, pp. 155–158.
- [85] Tianze Kan et al. “A new integration method for an electric vehicle wireless charging system using LCC compensation topology: Analysis and design”. In: *IEEE Transactions on power electronics* 32.2 (2016), pp. 1638–1650.
- [86] Siqi Li et al. “A double-sided LCC compensation network and its tuning method for wireless power transfer”. In: *IEEE transactions on Vehicular Technology* 64.6 (2014), pp. 2261–2273.
- [87] Junjun Deng et al. “Compact and efficient bipolar coupler for wireless power chargers: Design and analysis”. In: *IEEE Transactions on Power Electronics* 30.11 (2015), pp. 6130–6140.
- [88] Kanako Wake et al. “Derivation of coupling factors for different wireless power transfer systems: Inter-and intralaboratory comparison”. In: *IEEE Transactions on Electromagnetic Compatibility* 59.2 (2016), pp. 677–685.
- [89] Changbyung Park et al. “Innovative 5-m-off-distance inductive power transfer systems with optimally shaped dipole coils”. In: *IEEE transactions on power electronics* 30.2 (2014), pp. 817–827.
- [90] Fei Lu et al. “A dynamic charging system with reduced output power pulsation for electric vehicles”. In: *IEEE Transactions on Industrial Electronics* 63.10 (2016), pp. 6580–6590.

- [91] Adeel Zaheer et al. “A dynamic EV charging system for slow moving traffic applications”. In: *IEEE transactions on transportation electrification* 3.2 (2016), pp. 354–369.
- [92] Takehiro Imura and Yoichi Hori. “Maximizing air gap and efficiency of magnetic resonant coupling for wireless power transfer using equivalent circuit and Neumann formula”. In: *IEEE Transactions on industrial electronics* 58.10 (2011), pp. 4746–4752.
- [93] Vincenzo Cirimele, Lionel Pichon, and Fabio Freschi. “Electromagnetic modeling and performance comparison of different pad-to-pad length ratio for dynamic inductive power transfer”. In: *IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society*. IEEE. 2016, pp. 4499–4503.
- [94] Vincenzo Cirimele, Fabio Freschi, and Paolo Guglielmi. “Wireless power transfer structure design for electric vehicle in charge while driving”. In: *2014 International Conference on Electrical Machines (ICEM)*. IEEE. 2014, pp. 2461–2467.
- [95] Chenglin Liao, Junfeng Li, and Shufan Li. “Design of LCC impedance matching circuit for wireless power transfer system under rectifier load”. In: *cpss transactions on power electronics and applications* 2.3 (2017), pp. 237–245.
- [96] Mukesh Kumar Khandelwal, Binod Kumar Kanaujia, and Sachin Kumar. “Defected ground structure: fundamentals, analysis, and applications in modern wireless trends”. In: *International Journal of Antennas and Propagation* 2017 (2017).
- [97] Sherif Hekal et al. *Compact Size Wireless Power Transfer Using Defected Ground Structures*. Springer, 2019.

- [98] Jian Zhang et al. “Comparative analysis of two-coil and three-coil structures for wireless power transfer”. In: *IEEE Transactions on Power Electronics* 32.1 (2016), pp. 341–352.
- [99] Sherif Hekal et al. “Asymmetric wireless power transfer systems using coupled DGS resonators”. In: *IEICE Electronics Express* 13.21 (2016), pp. 20160591–20160591.
- [100] Alanson P Sample, David T Meyer, and Joshua R Smith. “Analysis, experimental results, and range adaptation of magnetically coupled resonators for wireless power transfer”. In: *IEEE Transactions on industrial electronics* 58.2 (2010), pp. 544–554.
- [101] Chunting Chris Mi et al. “Modern advances in wireless power transfer systems for roadway powered electric vehicles”. In: *IEEE Transactions on Industrial Electronics* 63.10 (2016), pp. 6533–6545.
- [102] Fabian L Cabrera and Fernando Rangel de Sousa. “Achieving optimal efficiency in energy transfer to a CMOS fully integrated wireless power receiver”. In: *IEEE Transactions on Microwave Theory and Techniques* 64.11 (2016), pp. 3703–3713.
- [103] Kim Ean Koh et al. “Impedance matching and power division using impedance inverter for wireless power transfer via magnetic resonant coupling”. In: *IEEE Transactions on Industry Applications* 50.3 (2013), pp. 2061–2070.
- [104] Kyriaki Niotaki et al. “Dual-band resistance compression networks for improved rectifier performance”. In: *IEEE Transactions on Microwave Theory and Techniques* 62.12 (2014), pp. 3512–3521.
- [105] Jia Hou et al. “Analysis and control of series/series-parallel compensated resonant converter for contactless power transfer”. In: *IEEE Journal of Emerging and selected topics in Power Electronics* 3.1 (2014), pp. 124–136.

- [106] SangCheol Moon and Gun-Woo Moon. “Wireless power transfer system with an asymmetric four-coil resonator for electric vehicle battery chargers”. In: *IEEE Transactions on Power Electronics* 31.10 (2015), pp. 6844–6854.
- [107] Mohsen Koohestani, Maxim Zhadobov, and Mauro Ettore. “Design methodology of a printed WPT system for HF-band mid-range applications considering human safety regulations”. In: *IEEE Transactions on Microwave theory and Techniques* 65.1 (2016), pp. 270–279.
- [108] Med Nariman et al. “A compact 60-GHz wireless power transfer system”. In: *IEEE Transactions on Microwave Theory and Techniques* 64.8 (2016), pp. 2664–2677.
- [109] Kainan Chen and Zhengming Zhao. “Analysis of the double-layer printed spiral coil for wireless power transfer”. In: *IEEE Journal of Emerging and Selected Topics in Power Electronics* 1.2 (2013), pp. 114–121.
- [110] Farid Jolani, Yiqiang Yu, and Zhizhang Chen. “A planar magnetically coupled resonant wireless power transfer system using printed spiral coils”. In: *IEEE Antennas and Wireless Propagation Letters* 13 (2014), pp. 1648–1651.
- [111] Wang-Sang Lee et al. “Contactless energy transfer systems using antiparallel resonant loops”. In: *IEEE Transactions on Industrial Electronics* 60.1 (2011), pp. 350–359.
- [112] Würth Elektronik. *REDEXPERT*. 2021. URL: <https://redexpert.wurth-electronic.com/redexpert/#> (visited on 06/30/2021).
- [113] Marian P Kazmierkowski and Artur J Moradewicz. “Unplugged but connected: Review of contactless energy transfer systems”. In: *IEEE Industrial Electronics Magazine* 6.4 (2012), pp. 47–55.

-
- [114] Weihan Li et al. “Integrated *LCC* compensation topology for wireless charger in electric and plug-in electric vehicles”. In: *IEEE Transactions on Industrial Electronics* 62.7 (2014), pp. 4215–4225.
- [115] Linhui Chen et al. “An optimizable circuit structure for high-efficiency wireless power transfer”. In: *IEEE Transactions on Industrial Electronics* 60.1 (2011), pp. 339–349.
- [116] Manuel Pinuela et al. “Maximizing DC-to-load efficiency for inductive power transfer”. In: *IEEE transactions on power electronics* 28.5 (2012), pp. 2437–2447.
- [117] Yi-Feng Wang et al. “High step-up 3-phase rectifier with fly-back cells and switched capacitors for small-scaled wind generation systems”. In: *Energies* 8.4 (2015), pp. 2742–2768.
- [118] Seung-Duck Yu, Seong-Woo Yim, Kijun Park, et al. “Optimizing compensation topologies for inductive power transfer at different mutual inductances”. In: *2017 IEEE PELS Workshop on Emerging Technologies: Wireless Power Transfer (WoW)*. IEEE. 2017, pp. 153–156.
- [119] Hunter H Wu et al. “A 90 percent efficient 5kW inductive charger for EVs”. In: *2012 IEEE Energy Conversion Congress and Exposition (ECCE)*. IEEE. 2012, pp. 275–282.
- [120] Udaya K Madawala and Duleepa J Thrimawithana. “A bidirectional inductive power interface for electric vehicles in V2G systems”. In: *IEEE Transactions on Industrial Electronics* 58.10 (2011), pp. 4789–4796.
- [121] Xiaohui Qu et al. “Higher order compensation for inductive-power-transfer converters with constant-voltage or constant-current output combating transformer parameter constraints”. In: *IEEE Transactions on Power Electronics* 32.1 (2016), pp. 394–405.

- [122] Hao Feng et al. “An LCC-compensated resonant converter optimized for robust reaction to large coupling variation in dynamic wireless power transfer”. In: *IEEE Transactions on Industrial Electronics* 63.10 (2016), pp. 6591–6601.
- [123] Mohamad Abou Houran, Xu Yang, and Wenjie Chen. “Magnetically coupled resonance WPT: Review of compensation topologies, resonator structures with misalignment, and EMI diagnostics”. In: *Electronics* 7.11 (2018), p. 296.
- [124] Chaoqiang Jiang et al. “An overview of resonant circuits for wireless power transfer”. In: *Energies* 10.7 (2017), p. 894.
- [125] Fang Liu et al. “A comparative study of load characteristics of resonance types in wireless transmission systems”. In: *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*. Vol. 1. IEEE. 2016, pp. 203–206.
- [126] Suwendu Samanta and Akshay Kumar Rathore. “A new current-fed CLC transmitter and LC receiver topology for inductive wireless power transfer application: Analysis, design, and experimental results”. In: *IEEE Transactions on Transportation Electrification* 1.4 (2015), pp. 357–368.
- [127] Mingyu Park et al. “A study of wireless power transfer topologies for 3.3 kW and 6.6 kW electric vehicle charging infrastructure”. In: *2016 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific)*. IEEE. 2016, pp. 689–692.
- [128] Weihan Li et al. “Comparison study on SS and double-sided LCC compensation topologies for EV/PHEV wireless chargers”. In: *IEEE Transactions on Vehicular Technology* 65.6 (2015), pp. 4429–4439.

- [129] Yijie Wang et al. “S/CLC compensation topology analysis and circular coil design for wireless power transfer”. In: *IEEE Transactions on Transportation Electrification* 3.2 (2017), pp. 496–507.
- [130] Jin Huh et al. “Narrow-width inductive power transfer system for on-line electrical vehicles”. In: *IEEE Transactions on Power Electronics* 26.12 (2011), pp. 3666–3679.
- [131] John M Miller, Omer C Onar, and Madhu Chinthavali. “Primary-side power flow control of wireless power transfer for electric vehicle charging”. In: *IEEE journal of Emerging and selected topics in power electronics* 3.1 (2014), pp. 147–162.
- [132] Chwei-Sen Wang, Oskar H Stielau, and Grant A Covic. “Design considerations for a contactless electric vehicle battery charger”. In: *IEEE Transactions on industrial electronics* 52.5 (2005), pp. 1308–1314.
- [133] Tobias Diekhans and Rik W De Doncker. “A dual-side controlled inductive power transfer system optimized for large coupling factor variations and partial load”. In: *IEEE Transactions on Power Electronics* 30.11 (2015), pp. 6320–6328.
- [134] Nathan O Sokal and Alan D Sokal. “Class EA new class of high-efficiency tuned single-ended switching power amplifiers”. In: *IEEE Journal of solid-state circuits* 10.3 (1975), pp. 168–176.
- [135] Nguyen Kien Trung et al. “PCB design for 13.56 MHz half-bridge class D inverter for wireless power transfer system”. In: *2015 9th International Conference on Power Electronics and ECCE Asia (ICPE-ECCE Asia)*. IEEE, 2015, pp. 1692–1699.
- [136] Frederick H Raab. “Effects of circuit variations on the class E tuned power amplifier”. In: *IEEE Journal of Solid-State Circuits* 13.2 (1978), pp. 239–247.

- [137] Nathan O Sokal. “Class E high-efficiency power amplifiers, from HF to microwave”. In: *1998 IEEE MTT-S International Microwave Symposium Digest (Cat. No. 98CH36192)*. Vol. 2. IEEE. 1998, pp. 1109–1112.
- [138] Joaquin J Casanova, Zhen Ning Low, and Jenshan Lin. “Design and optimization of a class-E amplifier for a loosely coupled planar wireless power system”. In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 56.11 (2009), pp. 830–834.
- [139] Jungwon Choi et al. “High-frequency, high-power resonant inverter with eGaN FET for wireless power transfer”. In: *IEEE Transactions on Power Electronics* 33.3 (2017), pp. 1890–1896.
- [140] Kan Peng, Xian Tang, and Zhihua Wang. “A Simultaneous Wireless Power and Uplink Data Transfer System with Ultra-Low Crosstalk between the Power and Data Link”. In: *2020 IEEE International Conference on Integrated Circuits, Technologies and Applications (ICTA)*. IEEE. 2020, pp. 49–50.
- [141] Li Ji et al. “Crosstalk study of simultaneous wireless power/information transmission based on an LCC compensation network”. In: *Energies* 10.10 (2017), p. 1606.
- [142] Zhe Zhou et al. “A High-Efficiency GaN-based Transmitter for Wireless Power Transfer System”. In: *2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA)*. IEEE. 2019, pp. 1699–1702.
- [143] Junsheng Sun and D. Tsang. “Performance Analysis of Dynamic Wireless Charging System for Electric Vehicles: A Queueing Approach”. In: *Proceedings of the Eighth International Conference on Future Energy Systems* (2017).

- [144] K. Hwang et al. “An Autonomous Coil Alignment System for the Dynamic Wireless Charging of Electric Vehicles to Minimize Lateral Misalignment”. In: *Energies* 10 (2017), p. 315.
- [145] DB Geselowtiz, Quynh TN Hoang, and Roger P Gaumond. “The effects of metals on a transcutaneous energy transmission system”. In: *IEEE transactions on biomedical engineering* 39.9 (1992), pp. 928–934.
- [146] S Abdollah Mirbozorgi, Pyungwoo Yeon, and Maysam Ghovanloo. “Robust wireless power transmission to mm-sized free-floating distributed implants”. In: *IEEE transactions on biomedical circuits and systems* 11.3 (2017), pp. 692–702.
- [147] Douglas C Galbraith, Mani Soma, and Robert L White. “A wide-band efficient inductive transdennal power and data link with coupling insensitive gain”. In: *IEEE Transactions on Biomedical Engineering* 4 (1987), pp. 265–275.
- [148] John S Ho, Sanghoek Kim, and Ada SY Poon. “Midfield wireless powering for implantable systems”. In: *Proceedings of the IEEE* 101.6 (2013), pp. 1369–1378.
- [149] International Commission on Non-Ionizing Radiation Protection et al. “Guidelines for limiting exposure to time-varying electric and magnetic fields (1 Hz to 100 kHz)”. In: *Health physics* 99.6 (2010), pp. 818–836.
- [150] Zhen Zhang et al. “Energy encryption for wireless power transfer”. In: *IEEE Transactions on Power Electronics* 30.9 (2014), pp. 5237–5246.
- [151] Zhen Zhang et al. “An efficient wireless power transfer system with security considerations for electric vehicle applications”. In: *Journal of Applied Physics* 115.17 (2014), 17A328.
- [152] Stephen F Bush. *Nanoscale communication networks*. Artech House, 2010.

- [153] Vedat Coskun, Busra Ozdenizci, and Kerem Ok. “A survey on near field communication (NFC) technology”. In: *Wireless personal communications* 71.3 (2013), pp. 2259–2294.
- [154] L. Francis et al. “Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms”. In: *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)* (2009), pp. 1–8.
- [155] TechPats Blog. *The Evolution of Near Field Communication (NFC)*. 2013. URL: www.techpats.com/evolution-near-field-communication-nfc/ (visited on 06/30/2021).
- [156] Kyung-Jae Bae et al. “The ubiquitous library for the blind and physically handicappedA case study of the LG Sangnam Library, Korea”. In: *IFLA journal* 33.3 (2007), pp. 210–219.
- [157] Mark Cathey’s Tech Site. *RIM’s secure element manager solution to power nfc mobile payments in Canada*. 2021. URL: <https://markcathey.com/tag/rim/> (visited on 06/30/2021).
- [158] TelstraExchange. *6 innovative examples of NFC technology*. 2013. URL: <https://exchange.telstra.com.au/6-innovative-examples-of-nfc-technology/> (visited on 06/30/2021).
- [159] BlueBite. *The State of NFC in 2021*. 2021. URL: <https://www.bluebite.com/%20nfc/the-state-of-nfc-in-2020> (visited on 06/30/2021).
- [160] Matt Hamblen. *A short history of NFC*. 2012. URL: <https://www.computerworld.com/article/2493888/a-short-history-of-nfc.html> (visited on 06/30/2021).
- [161] Felix Köbler et al. “Using NFriendConnector to Extend Facebook to the Real World”. In: *Wirtschaftsinformatik*. 2011.

- [162] Roy Want. “An introduction to RFID technology”. In: *IEEE pervasive computing* 5.1 (2006), pp. 25–33.
- [163] Han-Joon Kim et al. “Review of near-field wireless power and communication for biomedical applications”. In: *IEEE Access* 5 (2017), pp. 21264–21285.
- [164] Identiv. *RFID vs. NFC: Whats the Difference?* 2013. URL: <https://www.identiv.com/community/2019/06/14/rfid-vs-nfc-whats-the-difference/> (visited on 06/30/2021).
- [165] Jeremy Landt. “The history of RFID”. In: *IEEE potentials* 24.4 (2005), pp. 8–11.
- [166] Luigi Atzori, Antonio Iera, and Giacomo Morabito. “The internet of things: A survey”. In: *Computer networks* 54.15 (2010), pp. 2787–2805.
- [167] MEHRJERDI YAHIA ZARE. “RFID: a bibliographical literature review with future research directions”. In: (2014).
- [168] Gabriella Arcese et al. “Near field communication: Technology and market trends”. In: *Technologies* 2.3 (2014), pp. 143–163.
- [169] YVES I GONZALES. “Application of near field communication technology for mobile airline ticketing”. In: *Journal of Computer Science* 8.8 (2012), pp. 1235–1243.
- [170] Woo Young Moon and Soo Dong Kim. “A payment mediation platform for heterogeneous fintech schemes”. In: *2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*. IEEE. 2016, pp. 511–516.
- [171] Kevin Curran, Amanda Millar, and Conor Mc Garvey. “Near field communication”. In: *International Journal of Electrical and Computer Engineering* 2.3 (2012), p. 371.

- [172] Alliedwallet. *The Future of Mobile Payment Technology*. 2020. URL: <https://www.alliedwallet.com/blog/blog-posts/future-mobile-payment-technology/> (visited on 06/30/2021).
- [173] Technavio. *The Future Trends of Mobile Payment: NFC Payments to Expand its Majority Market Share*. 2019. URL: <https://blog.technavio.com/blog/mobile-payment-trends-nfc-payments-leads-growth> (visited on 06/30/2021).
- [174] Lorenzo Gutierrez. *Using Smartphones as a Medical Device for Point-of-Care Applications*. 2020. URL: <https://starfishmedical.com/blog/smartphones-as-a-medical-device/> (visited on 06/30/2021).
- [175] Michele Magno et al. “Infinitime: A multi-sensor energy neutral wearable bracelet”. In: *International Green Computing Conference*. IEEE. 2014, pp. 1–8.
- [176] Choong Yeon Kim et al. “Soft subdermal implant capable of wireless battery charging and programmable controls for applications in optogenetics”. In: *Nature communications* 12.1 (2021), pp. 1–13.
- [177] Jesus Fontecha et al. “An NFC approach for nursing care training”. In: *2011 Third International Workshop on Near Field Communication*. IEEE. 2011, pp. 38–43.
- [178] Adam Marcus et al. “Using NFC-enabled mobile phones for public health in developing countries”. In: *2009 first international workshop on near field communication*. IEEE. 2009, pp. 30–35.
- [179] Rosa Iglesias et al. “Experiencing NFC-based touch for home healthcare”. In: *Proceedings of the 2nd international conference on pervasive technologies related to assistive environments*. 2009, pp. 1–4.

- [180] J Bravo et al. “Touch-based interaction: An approach through NFC”. In: *2007 3rd IET International Conference on Intelligent Environments*. IET. 2007, pp. 440–446.
- [181] J Morak et al. “Near field communication technology as the key for data acquisition in clinical research”. In: *2009 First International Workshop on Near Field Communication*. IEEE. 2009, pp. 15–19.
- [182] Antonio J Jara et al. “Heart monitoring system based on NFC for continuous analysis and pre-processing of wireless vital signs”. In: *Proc. Int. Conf. Health Informatics (HEALTHINF)*. 2012.
- [183] Guillem Erràez Castelltort. “Design of an electrical nerve stimulator using wireless power transmission through NFC”. MA thesis. Universitat Politècnica de Catalunya, 2018.
- [184] Dipon K Biswas et al. “An NFC (near-field communication) based wireless power transfer system design with miniaturized receiver coil for optogenetic implants”. In: *2018 Texas Symposium on Wireless and Microwave Circuits and Systems (WMCS)*. IEEE. 2018, pp. 1–5.
- [185] Apoorva Hegde. *NFC Latest Trends 2021: 7 NFC Technology Trends to Watch Out for!* 2020. URL: <https://blog.beaconstac.com/2020/10/nfc-latest-trends/> (visited on 06/30/2021).
- [186] BangkokPost. *SICT Brings the World-Class RFID and NFC Technology*. 2020. URL: <https://www.bangkokpost.com/thailand/pr/1985815/sict-brings-the-world-class-rfid-and-nfc-technology> (visited on 06/30/2021).
- [187] Niranjana Rao. *The Increasing Adoption of NFC in Public Transportation*. 2018. URL: <https://blog.sasken.com/the-increasing-adoption-of-nfc-in-public-transportation> (visited on 06/30/2021).

- [188] Eva Brumerickova, Bibiana Bukova, and Leszek Krzywonos. “NFC technology in public transport”. In: *Communications-Scientific letters of the University of Zilina* 18.2 (2016), pp. 20–25.
- [189] Antonio Lazaro et al. “NFC Sensors based on energy harvesting for IoT applications”. In: *Recent Wireless Power Transfer Technologies* (2019).
- [190] Zhonglin Cao et al. “Near-field communication sensors”. In: *Sensors* 19.18 (2019), p. 3947.
- [191] M Mareli et al. “Experimental evaluation of NFC reliability between an RFID tag and a smartphone”. In: *2013 Africon*. IEEE. 2013, pp. 1–5.
- [192] Annika Paus. “Near field communication in cell phones”. In: *Chair for Communication Security* 24.8 (2007).
- [193] SERIALIO.COM. *The NFC Forum Standard*. 1996. URL: <https://www.serialio.com/support/learn-rfid/what-near-field-communication-nfc#:~:text=The%20NFC%20device%20in%20Reader,magnetic%20field%20from%20the%20reader>. (visited on 06/30/2021).
- [194] Ernst Haselsteiner and Klemens BreitfuSS. “Security in near field communication (NFC)”. In: *Workshop on RFID security*. Vol. 517. 517. sn. 2006, p. 517.
- [195] NFCforum. 2013. URL: <https://nfc-forum.org/resources/what-are-the-operating-modes-of-nfc-devices/> (visited on 06/30/2021).
- [196] Mike Clark. *Ahold Delhaize to roll out NFC shelf edge labels in supermarkets across Europe*. 2019. URL: <https://www.nfcw.com/2019/09/16/364378/ahold-delhaize-to-roll-out-nfc-shelf-edge-labels-in-supermarkets-across-europe/> (visited on 06/30/2021).

- [197] Britta O’Boyle. *What are App Clips on iPhone and how do they work?* 2020. URL: <https://www.pocket-lint.com/phones/news/apple/152664-what-are-app-clips-on-iphone-and-how-do-they-work> (visited on 06/30/2021).
- [198] The RFIP Blog. *NFC for Beginners A short introduction*. 2016. URL: <https://rfipblog.wordpress.com/2016/10/20/nfc-for-beginners-a-short-introduction/> (visited on 01/22/2022).
- [199] verimatrix. *Inside Secure*. 2020. URL: <https://www.insideseure.com/Company/Press-releases/Inside-Secure-NFC-SOLUTIONS-NOW-KOVIO-RF-BARCODE-READY-REVOLUTIONARY-PRINTED-SILICON-TAGS-ENABLE-ITEM-LEVEL-INTERACTION-BETWEEN-CONSUMERS-AND-BRANDS> (visited on 06/30/2021).
- [200] Jaap-Henk Hoepman and Johanneke Siljee. *Beyond RFID: the NFC Security Landscape*. Delft: TNO, 2007.
- [201] VISA. *Contactless*. 1996. URL: <https://www.visa.co.uk/run-your-business/small-business-tools/payment-technology/visa-paywave.html> (visited on 06/30/2021).
- [202] B Arief, M Emms, N Little, et al. “Risks of Offline Verify PIN on Contactless Cards”. In: *Financial Cryptography and Data Security* (2013).
- [203] U Biader Ceipidor et al. “Mobile ticketing with NFC management for transport companies. Problems and solutions”. In: *2013 5th International Workshop on Near Field Communication (NFC)*. IEEE. 2013, pp. 1–6.
- [204] Cheng Hao Chen, Iuon Chang Lin, and Chou Chen Yang. “NFC attacks analysis and survey”. In: *2014 eighth international conference on innovative mobile and internet services in ubiquitous computing*. IEEE. 2014, pp. 458–462.

- [205] G. Madlmayr et al. “NFC Devices: Security and Privacy”. In: *2008 Third International Conference on Availability, Reliability and Security* (2008), pp. 642–647.
- [206] Antonio J Jara, Miguel A Zamora, and Antonio FG Skarmeta. “Secure use of NFC in medical environments”. In: *5th european Workshop on RFID Systems and Technologies*. VDE. 2009, pp. 1–8.
- [207] Collin Mulliner. “Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones”. In: *2009 International Conference on Availability, Reliability and Security* (2009), pp. 695–700.
- [208] Synopsysn. *OpenPCD*. 2007. URL: <https://www.openhub.net/p/openpcd> (visited on 06/30/2021).
- [209] Milosch Meriac and Harald Welte. *OpenPCD*. 2007. URL: https://media.ccc.de/v/23C3-1566-en-openpcd_openpicc/related (visited on 06/30/2021).
- [210] Ziv Kfir and Avishai Wool. “Picking virtual pockets using relay attacks on contactless smartcard”. In: *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM’05)*. IEEE. 2005, pp. 47–58.
- [211] International Organization for Standardization/International Electrotechnical Commission et al. “Identification CardsContactless Integrated Circuit CardsProximity CardsPart 4: Transmission Protocol”. In: *ISO/IEC* (2008), pp. 14443–4.
- [212] International Organization for Standardization/International Electrotechnical Commission et al. “Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)”. In: *ISO/IEC* (2013), 18092:2013, 2, 1–44.

- [213] Lishoy Francis et al. “Practical NFC peer-to-peer relay attack using mobile phones”. In: *International Workshop on Radio Frequency Identification: Security and Privacy Issues*. Springer. 2010, pp. 35–49.
- [214] Naveed Ashraf Chattha. “NFC Vulnerabilities and defense”. In: *2014 Conference on Information Assurance and Cyber Security (CIACS)*. IEEE. 2014, pp. 35–38.
- [215] *Proxmark3*. 2007. URL: <https://code.google.com/p/proxmark3/wiki/HomePage?tm=6> (visited on 06/30/2021).
- [216] Square. *Security risks of near field communication*. 2017. URL: <http://www.nearfieldcommunication.org/nfc-security-risks.html> (visited on 06/30/2021).
- [217] M. Riyazuddin. “1 NFC : A review of the technology , applications and security”. In: 2011.
- [218] Wireless Power Consortium. *The Thermal Efficiency Behind Smartphone Trends*. 2015. URL: <https://www.wirelesspowerconsortium.com/blog/97/wireless-charging-in-automotive-that-is-here-and-now> (visited on 03/21/2019).
- [219] Qualcomm. *The Thermal Efficiency Behind Smartphone Trends*. 2013. URL: <https://www.qualcomm.com/news/onq/2013/10/09/thermal-efficiency-snapdragon-processors-under-screen-and-behind-trends> (visited on 03/21/2019).
- [220] Cnet Tech. *Dell laptops coming soon with WiTricity wireless charging*. 2016. URL: <https://www.cnet.com/tech/computing/dell-laptops-coming-soon-with-witricity-wireless-charging/> (visited on 03/21/2019).
- [221] Christopher Helman. *How Much Electricity Do Your Gadgets Really Use?* 2013. URL: <https://www.wirelesspowerconsortium.com/blog/97/>

- [wireless-charging-in-automotive-that-is-here-and-now](#) (visited on 03/21/2019).
- [222] Aaron Carroll, Gernot Heiser, et al. “An analysis of power consumption in a smartphone.” In: *USENIX annual technical conference*. Vol. 14. Boston, MA. 2010, pp. 21–21.
- [223] L O Memristor Chua. “The missing circuit element. circuit theory”. In: *IEEE Trans* 18 (1971), pp. 507–519.
- [224] Chua LO and Kang SM. “Memristive Devices And Systems”. In: *Proceedings of The IEEE* (1976), pp. 209–223.
- [225] Dmitri B Strukov et al. “The missing memristor found”. In: *Nature* 459.7250 (2009), p. 1154.
- [226] Shyam Prasad Adhikari et al. “Three fingerprints of memristor”. In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 60.11 (2013), pp. 3008–3021.
- [227] Akihito Sawa. “Resistive switching in transition metal oxides”. In: *Materials today* 11.6 (2008), pp. 28–36.
- [228] Leon Chua. “Resistance switching memories are memristors”. In: *Handbook of memristor networks*. Springer, 2019, pp. 197–230.
- [229] Ee Wah Lim and Razali Ismail. “Conduction mechanism of valence change resistive switching memory: a survey”. In: *Electronics* 4.3 (2015), pp. 586–613.
- [230] DB Strukov and H Kohlstedt. “Resistive switching phenomena in thin films: Materials, devices, and applications”. In: *MRS bulletin* 37.2 (2012), pp. 108–114.
- [231] Chi-Hsin Huang et al. “ZnO_{1-x} nanorod arrays/ZnO thin film bilayer structure: from homojunction diode and high-performance memristor to complementary 1D1R application”. In: *Acs Nano* 6.9 (2012), pp. 8407–8414.

- [232] Daniele Ielmini. “Resistive switching memories based on metal oxides: mechanisms, reliability and scaling”. In: *Semiconductor Science and Technology* 31.6 (2016), p. 063002.
- [233] Fatih Gul and Hasan Efeoglu. “ZnO and ZnO_{1-x} based thin film memristors: The effects of oxygen deficiency and thickness in resistive switching behavior”. In: *Ceramics International* 43.14 (2017), pp. 10770–10775.
- [234] Hiroyuki Akinaga and Hisashi Shima. “Resistive random access memory (ReRAM) based on metal oxides”. In: *Proceedings of the IEEE* 98.12 (2010), pp. 2237–2251.
- [235] Zdenk Biolek, Dalibor Biolek, and Viera Biolkova. “SPICE Model of Memristor with Nonlinear Dopant Drift.” In: *Radioengineering* 18.2 (2009).
- [236] Chuan Lian Koh and TOSHIMITISU Ushio. “Digital communication method based on M-synchronized chaotic systems”. In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 44.5 (1997), pp. 383–390.
- [237] Maciej J Ogorzalek. “Taming chaos. i. synchronization”. In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 40.10 (1993), pp. 693–699.
- [238] Ljupco Kocarev and Shiguo Lian. *Chaos-based cryptography: Theory, algorithms and applications*. Vol. 354. Springer Science & Business Media, 2011.
- [239] Maciej J Ogorzalek. *Chaos and complexity in nonlinear electronic circuits*. Vol. 22. World Scientific, 1997.
- [240] Leon O Chua et al. “A universal circuit for studying and generating chaos. I. Routes to chaos”. In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 40.10 (1993), pp. 732–744.

- [241] Michael Peter Kennedy. “Three steps to chaos. I. Evolution”. In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 40.10 (1993), pp. 640–656.
- [242] Michael Peter Kennedy. “Three steps to chaos. II. A Chua’s circuit primer”. In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 40.10 (1993), pp. 657–674.
- [243] LEONO Chua, Motomasa Komuro, and Takashi Matsumoto. “The double scroll family”. In: *IEEE transactions on circuits and systems* 33.11 (1986), pp. 1072–1118.
- [244] Robert C Hilborn et al. *Chaos and nonlinear dynamics: an introduction for scientists and engineers*. Oxford University Press on Demand, 2000.
- [245] Julien Clinton Sprott. *Chaos and time-series analysis*. Vol. 69. Citeseer, 2003.
- [246] Luigi Fortuna, Mattia Frasca, and Maria Gabriella Xibilia. *Chua’s Circuit Implementations: Yesterday, Today and Tomorrow*. Vol. 65. World Scientific, 2009.
- [247] Xuezhe Wei, Zhenshi Wang, and Haifeng Dai. “A critical review of wireless power transfer via strongly coupled magnetic resonances”. In: *Energies* 7.7 (2014), pp. 4316–4341.
- [248] J. Wu et al. “Wireless Power and Data Transfer via a Common Inductive Link Using Frequency Division Multiplexing”. In: *IEEE Transactions on Industrial Electronics* 62.12 (Dec. 2015), pp. 7810–7820. ISSN: 0278-0046. DOI: [10.1109/TIE.2015.2453934](https://doi.org/10.1109/TIE.2015.2453934).
- [249] Y. Zhang et al. “Selective Wireless Power Transfer to Multiple Loads Using Receivers of Different Resonant Frequencies”. In: *IEEE Transactions on Power Electronics* 30.11 (Nov. 2015), pp. 6001–6005. ISSN: 0885-8993. DOI: [10.1109/TPEL.2014.2347966](https://doi.org/10.1109/TPEL.2014.2347966).

- [250] Quan Xu et al. “Multiple attractors in a non-ideal active voltage-controlled memristor based Chua’s circuit”. In: *Chaos, Solitons & Fractals* 83 (2016), pp. 186–200.
- [251] Han Bao et al. “Bi-stability in an improved memristor-based third-order Wien-bridge oscillator”. In: *IETE Technical Review* 36.2 (2019), pp. 109–116.
- [252] BC Bao et al. “Hidden extreme multistability in memristive hyperchaotic system”. In: *Chaos, Solitons & Fractals* 94 (2017), pp. 102–111.
- [253] Han Bao et al. “Initial condition-dependent dynamics and transient period in memristor-based hypogenetic jerk system with four line equilibria”. In: *Communications in Nonlinear Science and Numerical Simulation* 57 (2018), pp. 264–275.
- [254] M. Chen, J. Yu, and B. Bao. “Finding hidden attractors in improved memristor-based Chua’s circuit”. In: *Electronics Letters* 51.6 (2015), pp. 462–464. ISSN: 0013-5194. DOI: [10.1049/e1.2014.4341](https://doi.org/10.1049/e1.2014.4341).
- [255] Leon O Chua and Sung Mo Kang. “Memristive devices and systems”. In: *Proceedings of the IEEE* 64.2 (1976), pp. 209–223.
- [256] S. Hameed et al. “Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters”. In: *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. Sept. 2014, pp. 900–905. DOI: [10.1109/TrustCom.2014.118](https://doi.org/10.1109/TrustCom.2014.118).
- [257] Z. Zhuang, J. Zhang, and W. Geng. “Analysis and Optimization to an NFC Security Authentication Algorithm Based on Hash Functions”. In: *2014 International Conference on Wireless Communication and Sensor Network*. Dec. 2014, pp. 240–245. DOI: [10.1109/WCSN.2014.56](https://doi.org/10.1109/WCSN.2014.56).
- [258] Aliexpress. *NFC Door Lock*. 2013. URL: <http://aliexpress.com> (visited on 06/30/2021).

- [259] Wei Li and Xuan Yang. “A Parallel and Reconfigurable United Architecture for Fibonacci and Galois LFSR”. In: *2015 7th International Conference on Intelligent Human-Machine Systems and Cybernetics*. Vol. 1. 2015, pp. 203–206. DOI: [10.1109/IHMSC.2015.265](https://doi.org/10.1109/IHMSC.2015.265).
- [260] M. Essaid et al. “A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map”. In: *Procedia Computer Science* 127 (2018), pp. 539–548. ISSN: 1877-0509. DOI: <https://doi.org/10.1016/j.procs.2018.01.153>.
- [261] Vittorio Bagini and Marco Bucci. “A Design of Reliable True Random Number Generator for Cryptographic Applications”. In: *Cryptographic Hardware and Embedded Systems*. Ed. by Çetin K. Koç and Christof Paar. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 204–218.
- [262] Wei Chen et al. “Ultra-low power truly random number generator for RFID tag”. In: *Wireless Personal Communications* 59.1 (2011), pp. 85–94.
- [263] H. Abunahla et al. “Novel microscale memristor with uniqueness property for securing communications”. In: *2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*. Oct. 2016, pp. 1–4. DOI: [10.1109/MWSCAS.2016.7870134](https://doi.org/10.1109/MWSCAS.2016.7870134).
- [264] F. Yang et al. “Color Image Compression-Encryption Algorithm Based on Fractional-Order Memristor Chaotic Circuit”. In: *IEEE Access* 7 (2019), pp. 58751–58763. ISSN: 2169-3536. DOI: [10.1109/ACCESS.2019.2914722](https://doi.org/10.1109/ACCESS.2019.2914722).
- [265] Hirokazu Fujisaka and Tomoji Yamada. “Stability Theory of Synchronized Motion in Coupled-Oscillator Systems: ” in: *Progress of Theoretical Physics* 69.1 (Jan. 1983), pp. 32–47. ISSN: 0033-068X. DOI: [10.1143/PTP.69.32](https://doi.org/10.1143/PTP.69.32). eprint: <https://academic.oup.com/ptp/article-pdf/69/1/32/5195059/69-1-32.pdf>. URL: <https://doi.org/10.1143/PTP.69.32>.

- [266] Louis M Pecora and Thomas L Carroll. “Synchronization in chaotic systems”. In: *Physical review letters* 64.8 (1990), p. 821.
- [267] G Abramson, VM Kenkre, and AR Bishop. “Analytic solutions for nonlinear waves in coupled reacting systems”. In: *Physica A: Statistical Mechanics and its Applications* 305.3-4 (2002), pp. 427–436.
- [268] Pedro G Lind et al. “Coupled bistable maps: a tool to study convection parameterization in ocean models”. In: *International Journal of Bifurcation and Chaos* 14.03 (2004), pp. 999–1015.
- [269] Walter J Freeman. “A neurobiological theory of meaning in perception Part I: Information and meaning in nonconvergent and nonlocal brain dynamics”. In: *International Journal of Bifurcation and Chaos* 13.09 (2003), pp. 2493–2511.
- [270] Jordi Cosp et al. “Synchronization of nonlinear electronic oscillators for neural computation”. In: *IEEE transactions on neural networks* 15.5 (2004), pp. 1315–1327.
- [271] Gouhei Tanaka and Kazuyuki Aihara. “Multistate associative memory with parametrically coupled map networks”. In: *International Journal of Bifurcation and Chaos* 15.04 (2005), pp. 1395–1410.
- [272] Bernabé Linares-Barranco and Teresa Serrano-Gotarredona. “Memristance can explain spike-time-dependent-plasticity in neural synapses”. In: *Nature precedings* (2009), pp. 1–1.
- [273] Sung Hyun Jo et al. “Nanoscale memristor device as synapse in neuromorphic systems”. In: *Nano letters* 10.4 (2010), pp. 1297–1301.
- [274] MJ Rozenberg, IH Inoue, and MJ Sanchez. “Nonvolatile memory with multilevel switching: a basic model”. In: *Physical review letters* 92.17 (2004), p. 178302.

- [275] Julien Borghetti et al. “Memristiveswitches enable statefullogic operations via material implication”. In: *Nature* 464.7290 (2010), pp. 873–876.
- [276] Bocheng Bao et al. “Coexisting infinitely many attractors in active band-pass filter-based memristive circuit”. In: *Nonlinear Dynamics* 86.3 (2016), pp. 1711–1723.
- [277] D. Yu et al. “A New Circuit for Emulating Memristors Using Inductive Coupling”. In: *IEEE Access* 5 (2017), pp. 1284–1295.
- [278] Huagan Wu et al. “Chaotic and periodic bursting phenomena in a memristive Wien-bridge oscillator”. In: *Nonlinear Dynamics* 83.1-2 (2016), pp. 893–903.
- [279] Alan Wolf et al. “Determining Lyapunov exponents from a time series”. In: *Physica D: nonlinear phenomena* 16.3 (1985), pp. 285–317.
- [280] Leon Chua. “Memristor-the missing circuit element”. In: *IEEE Transactions on circuit theory* 18.5 (1971), pp. 507–519.
- [281] Gian Mario Maggio, Oscar De Feo, and Michael Peter Kennedy. “Nonlinear analysis of the Colpitts oscillator and applications to design”. In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 46.9 (1999), pp. 1118–1130.
- [282] Yu Si-Min. “Fourth-order Colpitts chaotic oscillator”. In: *Acta Physica Sinica* 57.6 (2008), pp. 3374–3379.
- [283] Bocheng Bao et al. “Generalized memristor consisting of diode bridge with first order parallel RC filter”. In: *International Journal of Bifurcation and Chaos* 24.11 (2014), p. 1450143.
- [284] Fernando Corinto and Alon Ascoli. “Memristive diode bridge with LCR filter”. In: *Electronics letters* 48.14 (2012), pp. 824–825.
- [285] Leon O Chua. “The fourth element”. In: *Proceedings of the IEEE* 100.6 (2012), pp. 1920–1927.

- [286] Ling Lu et al. “Colpitts chaotic oscillator coupling with a generalized memristor”. In: *Mathematical Problems in Engineering* 2015 (2015).
- [287] Maxim Integrated. *MAX66242*. May 2020. URL: <https://www.maximintegrated.com/en/products/embedded-security/secure-authenticators/MAX66242.html>.
- [288] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. “Security for the internet of things: a survey of existing protocols and open research issues”. In: *IEEE Communications Surveys & Tutorials* 17.3 (2015), pp. 1294–1312.
- [289] D. Sethia, D. Gupta, and H. Saran. “NFC Secure Element-Based Mutual Authentication and Attestation for IoT Access”. In: *IEEE Transactions on Consumer Electronics* 64.4 (2018), pp. 470–479.
- [290] V. Odelu, A. K. Das, and A. Goswami. “SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms”. In: *IEEE Transactions on Consumer Electronics* 62.1 (2016), pp. 30–38.
- [291] Michael Roland and Josef Langer. “Comparison of the usability and security of NFCs different operating modes in mobile devices”. In: *e & i Elektrotechnik und Informationstechnik* 130.7 (2013), pp. 201–206.
- [292] Ronald Toegl and Michael Hutter. “An approach to introducing locality in remote attestation using near field communications”. In: *The Journal of Supercomputing* 55.2 (2011), pp. 207–227.
- [293] F. Dang et al. “Pricing Data Tampering in Automated Fare Collection with NFC-Equipped Smartphones”. In: *IEEE Transactions on Mobile Computing* 18.5 (2019), pp. 1159–1173.
- [294] Divyashikha Sethia et al. *Technical report for implementation of secure NFC-based IoT prototype using mobile devices*. Ed. by Google Sites. URL: <https://sites.google.com/site/divyashikhasethia/home/securenfc-based-iot-access/IoTPrototypeTechReport.pdf>.

- [295] Mohamed Amine Bouazzouni, Emmanuel Conchon, and Fabrice Peyrard. “Trusted mobile computing: An overview of existing solutions”. In: *Future Generation Computer Systems* 80 (2018), pp. 596–612.
- [296] Shirsha Ghosh et al. “Swing-pay: One card meets all user payment and identity needs: A digital card module using NFC and biometric authentication for peer-to-peer payment”. In: *IEEE Consumer Electronics Magazine* 6.1 (2016), pp. 82–93.
- [297] Federal Information Processing Standard Publication. *SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES*. 2001. URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf> (visited on 06/30/2021).
- [298] Richard W Hamming. *Coding and information theory*. Prentice-Hall, Inc., 1986, pp. 104–108.
- [299] Lee Howes and David Thomas. *Chapter 37. Efficient Random Number Generation and Application Using CUDA*. 2001. URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf> (visited on 06/30/2021).
- [300] John Walker. *Chi-Square Calculator*. URL: <http://www.fourmilab.ch/rpkp/experiments/analysis/chiCalc.html> (visited on 06/30/2021).
- [301] Donald E Knuth. *Art of computer programming, volume 2: Seminumerical algorithms*. Addison-Wesley Professional, 2014, pp. 35–65.