University of Sheffield

Thesis submitted for the degree of Doctor of Philosophy

in the Faculty of Science

School of Mathematical and Physical Sciences

Quantum Dot Spin Dynamics and Quantum Randomness for Secure Optical Communication

---

Author:

Marius Čižauskas

2026-07-02

Abstract

This thesis investigates two complementary quantum technologies for secure optical communication: spin dynamics in telecom C-band quantum dots and a high-bandwidth source-device-independent quantum random number generator. Together, they address two central requirements of quantum networks: long-lived spin memories for quantum repeaters and secure, high-rate entropy generation for quantum key distribution.

The first part studies the spin dynamics of InAs/InGaAs/InP quantum dots grown by strain-free droplet epitaxy using time-resolved Faraday ellipticity. Compared to Stranski-Krastanov grown telecom dots, droplet epitaxy shows improved spin properties, including an electron spin relaxation time of 3.0 μs and reduced in-plane electron g-factor anisotropy, indicating enhanced structural symmetry. Polarization recovery and Hanle measurements reveal nuclear spin lifetimes comparable to electron spin lifetimes, attributed to quadrupolar interactions arising from Ga-In interdiffusion. These results demonstrate the advantages of droplet epitaxy over strain-based growth and indicate further potential through optimized material compositions.

The second part investigates one-, two-, and four-layer InAs/InAlGaAs Stranski-Krastanov quantum dots to assess layer-dependent carrier type and spin coherence. Increasing layer number induces a transition from electron to hole resident carriers due to interlayer tunnelling into lower-energy dots, the emergence of spin-mode locking for four or more layers, and the appearance of a non-oscillating spin component likely associated with reduced heavy-hole/light-hole mixing. Although droplet epitaxy samples exhibit superior spin parameters overall, no spin-mode locking is observed, potentially due to shorter transverse coherence or electron-dominated charging.

The final part presents a source-device-independent quantum random number generator based on heterodyne detection of vacuum fluctuations. Using a 90° optical hybrid, balanced photodetectors, a dual-channel 12-bit ADC operating at 3.2 GS/s per channel, and FPGA-implemented Toeplitz hashing with PCIe transfer, a total extracted bandwidth of 33.91 Gbit/s is achieved. The system assumes no trust in the optical source and performs all extraction in hardware, maintaining

security even under adversarial state preparation.

Publications

The results presented in this thesis appear in the following publications:

1. **M. Cizauskas**, E. M. Sala, J. Heffernan, A. M. Fox, M. Bayer, and A. Greilich, "Spin properties in droplet epitaxy-grown telecom quantum dots," *Phys. Rev. B*, vol. 112, p. 165412, Oct. 2025 [1].

2. **M. Cizauskas**, A. Kors, J. P. Reithmaier, A. M. Fox, M. Benyoucef, M. Bayer, A. Greilich, "Layer-dependent spin properties of charge carriers in vertically coupled telecom quantum dots," *arXiv*, 2509.15051, Sep. 2025 [2].

3. **M. Cizauskas**, H. Tebyanian, A. M. Fox, M. Bayer, M. Assmann, A. Greilich, "33 Gbit/s source-device-independent quantum random number generator based on heterodyne detection with real-time FPGA-integrated extraction," *arXiv*, 2512.07319, Dec. 2025 [3].

Acknowledgements

Firstly, I would like to thank my supervisor Professor Mark Fox for providing extensive guidance necessary to navigate PhD studies and for understanding whenever any unexpected issues arose. I am thankful to EPSRC, Bundesministerium für Forschung, Technologie und Raumfahrt, EIN Quantum NRW program for providing the funding for the projects completed in this thesis and University of Sheffield for funding the PhD. I am grateful to Professors Manfred Bayer and Marc Aßmann for giving me the chance to work in the Technical University of Dortmund Experimentelle Physik 2 group and for support during my time in TU Dortmund. I am especially thankful to my supervisor at TU Dortmund apl. Prof. Alex Greilich, whose seemingly endless patience, knowledge and optimism helped me immensely during experiments, research and writing. Sincere thanks to Igor Itskevich, who introduced me to the LDSD group and always helped me no matter the circumstances. Thanks also go to Elisa Sala, Jon Heffernan, Andrei Kors, Johann Peter Reithmaier, Mohamed Benyoucef for the sample growth, Hamid Tebyanian for help developing the theory for the quantum random number generator and Lars Wieschollek for providing helium and help with the cryostat systems.

I would also like to thank my present and past colleagues at LDSD, especially: Luke Brunswick, Alistair Brash, Andrew Foster and Catherine Philips for sharing their wisdom in how to survive a PhD. In TU Dortmund I would like to thank Vladimir Kats for helping me get familiar with lab work, encouragement and for always making me laugh, and Simon Siegeroth for the tangential chats during our breakfasts. Without doubt thanks go to my friends and family who always encouraged and supported me both before and during my studies.

Lastly, I want to express my sincere gratitude to my fiancée Giedrė who made this work possible with her love, compassion, joy and support during every step of this long journey.

Contents

1
Introduction

1.1 Motivation

Quantum technologies have become a central focus of modern physics and engineering, offering new approaches to communication, computation, and metrology. These technologies exploit the intrinsic properties of quantum systems, such as superposition, entanglement, and quantum measurement uncertainty, which helps realize functionalities that are not attainable by any classical means. Advances in materials science, nanofabrication, and optical measurement have particularly enabled experimental access to different quantum phenomena in quantum optics. These developments have established the foundation for applications such as secure key distribution, photonic quantum computation and quantum-enhanced metrology, where the ability to manipulate and measure individual quantum systems plays a central role [4].

Particularly important is the development of secure communications using quantum technology. As quantum technologies become increasingly advanced, particularly quantum computing, classical communication channels become at risk to decryption using quantum computation algorithms which exponentially reduce the amount of time required to break the key-exchange algorithms of asymmetric encryption, which uses factorization and discrete logarithms [5]. However, this only applies to currently used encryption algorithms and there already exists post-quantum classical cryptography, which currently has no realistic method to be broken even by quantum computing [6]. Nonetheless, as technology further develops, new attack vectors may present which could still break the post-quantum cryptography algorithms. Quantum key distribution (QKD) resolves this intrinsic issue by relying on quantum phenomena to prevent any man in the middle attacks on transferred keys, which then allows the use of secure symmetric encryption algorithms with the exchanged keys [7].

The focus of this thesis is to experimentally investigate photonic quantum technologies (specifically quantum dots (QDs) and heterodyne measured vacuum fluctuations) for the potential use of establishing secure communication networks. In particular, two different aspects are covered: spin dynamics of telecom C-band QDs for the potential use as quantum repeaters for long range QKD [8] and high bandwidth source-device-independent (DI) quantum random number generator (QRNG) for the practical generation of secure keys in QKD systems. Although these two topics differ in implementation, they share a common objective of enabling scalable and verifiable quantum communication. The first part addresses the challenge of realizing QD-based quantum memories that operate at wavelengths compatible with existing fiber infrastructure, while maintaining long spin coherence. The second part focuses on the realization of quantum entropy sources capable of producing high-rate random numbers with quantifiable security models, which are essential for implementing fast and trustworthy QKD schemes.

The first part is further split into two separate chapters with differing potential uses regarding quantum repeaters. For the first chapter, simple, effectively single-layer QD ensemble structure is covered, with the idea that a different, strain-free method could result in improved coherence times, improving the potential in being used as quantum memory for quantum repeater applications. The second chapter examines QDs grown by the standard strain method. The difference here is that a multi-layer structure is investigated. Firstly, the goal was to investigate how the spin properties change and whether improvement can be seen in terms of coherence. This was indeed the case since from all the investigated QD structures, coherence time T_2 was only possible to be measured with an increased layer count. Moreover, not only resident carriers can be used as quantum memory. It has been theoretically demonstrated that QD molecules can be used as repeaters and that they also have potential for significantly longer coherence times [9]. While conclusive evidence was not seen for the existence of QD molecules, a stacked QD structure is necessary to form them and a telecom C-band stacked QD structure was successfully measured and investigated, paving the way for future QD molecule research.

Overall, a quantum communications network ties QDs and QRNGs together by addressing complementary requirements of the same underlying goal: distributing secure keys over distances beyond what direct transmission allows. In a QKD link, photons carrying entangled states are attenuated as they travel through fiber [10], and because quantum states cannot be copied, the classical method of reading and re-broadcasting a weakening signal is not possible. The solution is the quantum repeater, which divides a long link into shorter segments, generates entanglement within each segment, and then joins these segments through entanglement swapping at intermediate nodes, extending entanglement across the full distance without ever measuring the transmitted key [11]. This process depends on a stationary system that can hold a quantum state long enough for the neighbouring segments to be ready, which is precisely the role of a quantum memory. QD spins are well suited to this task, since a resident electron or hole spin can store quantum information while the QD itself couples efficiently to single-mode fiber and emits in the telecom C-band, which is advantageous due to already existing extensive C-band fiber infrastructure.

In order to achieve actual transmission of entanglement over long distances, two nodes swapping entanglement is not enough. Intermediate nodes are necessary where entangled pairs have to be stored and then entangled between each other to actually transfer the entanglement between the start and end nodes. One proposed way to do it is by dipole-dipole interactions between excitons in two or more quantum dots as the local coupling mechanism [12]. In the multi-layer structure investigated thesis excitons are not considered as potential quantum memory, rather resident carriers are. Quantum repeater protocols have been developed where potentially stacked QDs could be used for entangling the two electron spin stored states in the intermediate node, allowing for long-distance transmission [13]. This is another potential application of the investigated multi-layer structure. While spin coupling between QDs was not investigated in this thesis, the multi-layer QD structure was shown to be optically active and that it has measurable spin coherence, which makes it a potential platform for quantum repeaters not only as quantum memory.

The same network places equally strict demands on the generation of the keys themselves. Many of the most secure QKD schemes are entanglement-based: rather than one party preparing and sending states, both parties share entangled pairs and measure them independently, deriving a key from their correlated outcomes [14]. Such protocols are attractive because their security can be made device-independent, meaning it rests on the observed quantum correlations, which are not affected by classical imperfection in source and measurement devices, so that even imperfect or partially adversarial devices cannot compromise the key without being detected. Distributing entanglement in this way over long distances is exactly the problem that quantum repeaters, and hence QD spin memories, are intended to solve. Underpinning all of these protocols is the need for genuinely unpredictable random numbers, used to choose measurement bases, seed privacy amplification, and form the keys themselves. Any predictability in these choices opens an attack channel, and because deterministic classical generators cannot provide true unpredictability, a QRNG drawing its randomness from the intrinsic indeterminacy of quantum measurement is required. To keep pace with QKD systems operating at GHz rates, this entropy source must also be fast and carry a quantifiable security model, which motivates the high-bandwidth source-device-independent QRNG developed in the final part of this thesis. Together, the QD spin memories of the first chapters and the QRNG of the later chapters form an effective secure quantum communication network based on entangled state measurement QKD.

1.2 Thesis Outline

Chapter 2 focuses on providing the necessary background required for the main chapters of the thesis. The chapter starts with covering the fundamental principles of QDs and their growth methods. Afterwards, the most attention is given to the spin dynamics of QDs, specifically for ensemble samples. Spin polarization, precession, coherence and longitudinal spin lifetimes are covered, how relaxation mechanisms impact the lifetimes and lastly spin mode locking, which is relevant for spin coherence. The other part of the background is the quantum cryptography, which is necessary for the QRNG part of the thesis. The section starts out with providing context on QKD, which is necessary for the understanding for what QRNG is used. Then it covers how quantum mechanics are utilized to generate true randomicity. Lastly, theory is provided how vacuum fluctuations are measured by light field quadratures, which is used in this thesis for QRNG, and then measurement imperfections are covered, what are the potential insecurities of QRNG and how they are taken into account.

Chapter 3 covers the experimental methods that were used to obtain the results detailed in the main chapters. This chapter only covers the methods of QD samples, since the QRNG measurements are relatively simpler and covered in Chapter 6. The first few sections cover the theoretical background of the measurements. In particular, Faraday effect, Hanle Effect and spin inertia are described. Then the actual set-up is covered in detail and how each part of the set-up is utilized in measurements. Again, the set-up is only covered for the QD samples, since for the QRNG it is fully covered in Chapter 6.

The thesis is written in publication format, which means that the results chapters are taken from published articles [1, 2, 3] and reformatted to fit the style of the thesis. The main chapters cover the two parts mentioned in the introduction. The first two content chapters investigate two different QD samples which were grown by different methods and are structurally different. The last results chapter covers the source-DI heterodyne QRNG.

Chapter 4 presents the results of a metalorganic vapour-phase epitaxy (MOVPE) droplet epitaxy (DE) grown QDs. The chapter discusses the details of the sample, particularly its composition and growth method. The main results presented are the calculated carrier g-factors, their anisotropy, dephasing, longitudinal spin relaxation times, and polarization recovery curve (PRC)/Hanle effect curves plotted in combination. The discussion investigates resident carrier determination in the sample, nuclear spin effects on carrier spins and the observed spin lifetime values.

Chapter 5 investigates three different QD samples grown by molecular beam epitaxy (MBE) using the Stranski-Krastanov (SK) method. The three samples are one-, two-, and four-layer with barriers thin enough to allow tunneling of electrons. Similar experiments were done to Chapter 4 and results presented as in the previous chapter. However, additional results were shown for effects of interest, such as change of resident carriers with more layers and an appearing non-oscillating component. The discussion primarily focuses on interpreting the previously not seen effects.

Chapter 6 presents the developed source-DI QRNG based on heterodyne measurement of vacuum fluctuations. The chapter is split into effectively three parts. First part covers the source-DI security model and how different measurement electronic imperfections are taken into account. The second part covers the field programmable gate array (FPGA) implementation in detail and how it manages real-time randomness extraction. Lastly, the results are presented, which are in the form of what parameters for the security model were calculated, the achieved bandwidth and statistical tests that certify that no non-random patterns are found (important to clarify that these tests do not show whether true randomicity is achieved).

Chapter 7 provides a summary of all the results, presents a comparison of results between Chapters 4 and 5 and relates the main text chapters to potential QKD applications. Lastly, potential future work is provided. Both short-term improvements and ideas and long-term extension to the projects are provided.

2

Background

This chapter provides an overview of QDs, their optical and electronic properties, their spin dynamics and growth using different epitaxial methods. It also briefly covers quantum cryptography topics such as QRNGs and QKD. While a part of the theory is covered in the main content chapters themselves, they do not provide enough required context as they are written for journal publications. Therefore, the required background for the publications is covered more extensively in this chapter.

2.1 Quantum Dots

2.1.1 Fundamental Physics of Quantum Dots

Quantum Confinement in Semiconductors

Quantum dots are semiconductor devices that use semiconductor materials with different band gap values to create a three-dimensional region for confining charge carriers [15]. The de Broglie wavelength for the electron can be approximated as follows:

$$\lambda_D \sim \frac{h}{\sqrt{m_e^* k_B T}} \tag{2.1}$$

where λ_D is the de Broglie wavelength, h is the Planck constant, m_e^* is the effective electron mass, k_B is the Boltzmann constant and T is the temperature. If all the dimensions in a bulk semiconductor are longer than the electron wavelength, the electron is free to travel in any direction. However, if one of the dimensions is reduced to be smaller than the wavelength, the electron's motion becomes quantized in that direction, causing confinement.

If the confinement is within a single dimension, it is considered a quantum well, in two, quantum wire and in three, quantum dot. As the number of confined dimensions change, so does the density of states. When all three dimensions are confined, the density of states become discrete. In this case, a quantum dot can be approximated to a two-level system, similar to an atom, which is why QDs are sometimes called artificial atoms. Fig. 2.1 shows how the density of states change with confinement.

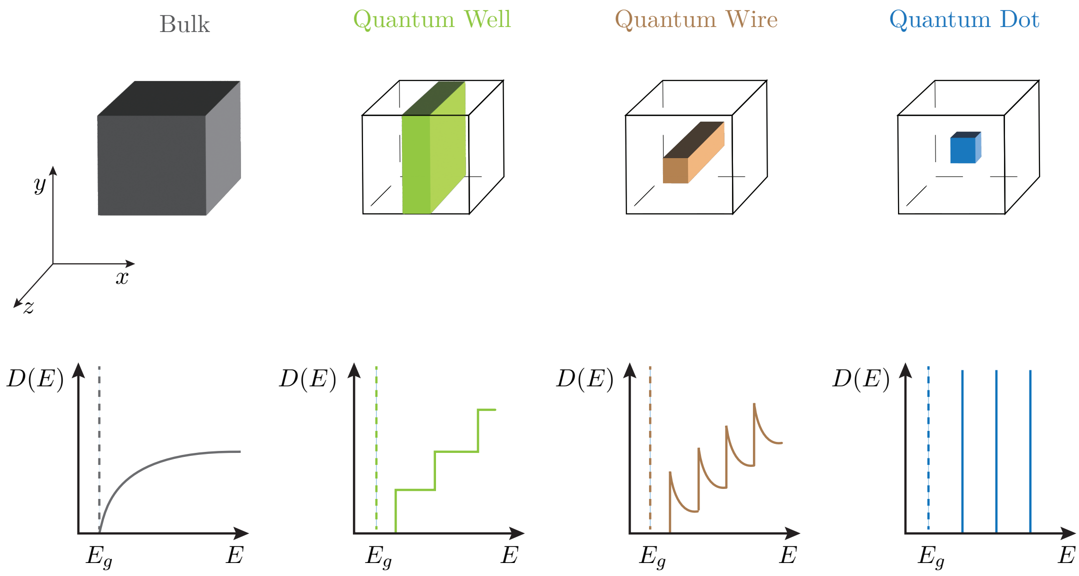

Figure 2.1: Illustration of quantum confinement effects across different dimensional structures. The figure demonstrates the structural geometries and corresponding density of states for bulk semiconductors, quantum wells, quantum wires, and quantum dots. In bulk materials, carriers experience unrestricted motion and a continuous density of states. Quantum wells exhibit one-dimensional confinement resulting in step-like density functions. Quantum wires show two-dimensional confinement with increasingly discrete energy states. Quantum dots represent three-dimensional confinement where the density of states becomes completely discrete, resembling atomic energy levels.

Effective Mass Approximation

The understanding of effective mass in semiconductors emerges from examining the energy-momentum dispersion relation for electrons in crystalline solids. In free space, electrons follow the parabolic dispersion [16]:

$$E = \frac{\hbar^2 k^2}{2m_0} \tag{2.2}$$

where $\hbar$ is the reduced Planck's constant, k is the wavevector and m_0 is the mass. In this case, the curvature of the relationship is determined by $1/m_0$. In crystalline semiconductors, the periodic potential creates band structures that deviate from the free electron case. Particularly, near band gaps, there are regions of high curvature. Therefore, this can result in the mass to be reduced by a factor of 10 to 100 [16]. This results in the effective mass quantity, which does not actually mean that the mass of the carrier changes; rather it quantifies how much a carrier in a periodic potential is accelerated relative to the lattice when an electric or a magnetic field is applied. The effective mass can be defined as [16]:

$$\frac{1}{m^*} = \frac{1}{\hbar^2}\frac{d^2\epsilon}{dk^2} \tag{2.3}$$

where ϵ is the energy.

This is of relevance since usually QDs are made with III-V semiconductor materials. Effective mass impacts several qualities, such as tunneling, assuming the barrier thickness is small enough [17] or various spin properties of the carriers [18]. It has been shown that in indium arsenide (InAs) systems, the electron effective mass is $m_e^* = 0.04m_0$ and hole $m_h^* = 0.34m_0$ [19].

2.1.2 Optoelectronic Properties

Electronic Structure

QDs have an atomic like behavior due to their electronic structure which can be approximated to a two-level system. It has been demonstrated that the energy levels in QDs can be modeled using a parabolic confinement potential along the growth axis [20]. Moreover, the shape of grown QDs tend to be broader in the lateral dimension than in height (more on QD growth in Section 2.2), resulting in the in-plane orbital wavefunction exhibiting circular symmetry and harmonic oscillator behavior [21]. This electronic structure is similar to atomic systems, allowing the energy levels to be classified using familiar atomic notation (*s*, *p*, *d*...).

Fig. 2.2 shows a typical III-V semiconductor band structure. At the top is the conduction band (black), and at the bottom are the three valence bands (red).

When an electron is excited, it jumps from the valence band to the conduction band, leaving behind a hole. The electron and hole attract each other via Coulomb interaction and form a bound state quasi-particle called an exciton. Both electron and hole are fermionic particles with spins $\pm\frac{1}{2}$, therefore, in a QD, the *s*-shell can only be occupied by two carriers of opposing spin and the *p*-shell four carriers (assuming no degeneracy between HH and LH bands) due to Pauli exclusion

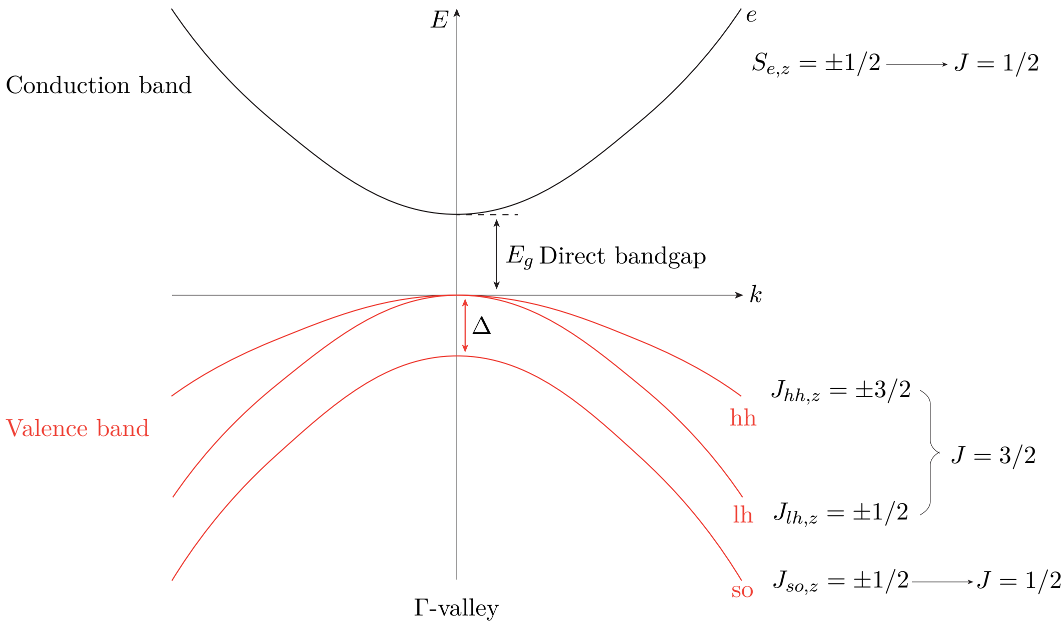

Figure 2.2: The electronic band structure of a typical direct bandgap III-V semiconductor consists of distinct conduction and valence band regions. The conduction band (shown in color black) comprises a single band where electrons reside, positioned above the valence band and separated from it by the fundamental band gap energy (E_g). The valence band structure is more complex, containing holes and divided into three distinct subbands (shown in color red): the heavy-hole (HH) band, light-hole (LH) band, and split-off band. The spin-orbit coupling creates an energy separation Δ between the split-off band and the heavy/light hole bands. At the Γ-point (k = 0), the heavy hole and light hole bands are energetically degenerate (in unstrained materials), but this degeneracy is lifted as the wave vector k increases away from the zone center, causing the bands to separate in energy.

principle.

The electronic band structure of bulk III-V semiconductors shows distinct orbital contributions: s orbitals from the constituent atoms form the conduction band [22], while the valence band displays mainly p-orbital character with some d-orbital involvement [23]. Therefore, electron wavefunctions take on s-type atomic characteristics, resulting in zero orbital angular momentum ($\mathbf{L} = 0$). The total angular momentum of a carrier is:

$$\mathbf{J} = \mathbf{L} + \mathbf{S} \tag{2.4}$$

where $\mathbf{S}$ is the spin angular momentum. The eigenvalues of angular momentum are $|l - s| \leq J \leq |l + s|$ [24]. This results in an electron having only two projections along the z-axis, spin up $(+\frac{1}{2}, \uparrow)$ and spin down $(-\frac{1}{2}, \downarrow)$.

For the hole, it is not as simple as for electron due to holes having *p*-type wavefunctions. This means the angular momentum for holes is $|\mathbf{L}| = 1$, therefore, the eigenvalues in this case are $J = 3/2$ and $J = 1/2$. In terms of z-axis projection, the eigenvalue $J = 3/2$ can have projections $J_z = \pm 1/2, \pm 3/2$, where the $J_z = \pm 3/2$ is considered HH and $J_z = \pm 1/2$ is considered the LH bands. The eigenvalue $J = 1/2$ can have $J_z = \pm 1/2$, where this is considered the spin-orbit band. These three bands are shown in Fig. 2.2. Between the HH, LH and spin-orbit bands there is the spin-orbit splitting, which is usually in the range of 0.1 to 0.5 eV for III-V semiconductors [25]. Moreover, the HH and LH bands are degenerate if the structure is symmetric. However, the aspect ratio of quantum dots is usually more than unity, which results in broken symmetry and so lifting the HH-LH degeneracy [26]. Usually, the LH band is found at higher energies, so in most cases, the two-level approximation is applied between the HH band and the conduction band.

Excitons

As mentioned before, when an electron and a hole are excited in a QD, an exciton is created. There is the neutral exciton (X^0), where there is only a single bound hole and electron. Neutral excitons can also be classified into bright and dark excitons. Assuming HH and electron exciton, bright excitons have holes and electron with antiparallel spins, resulting in angular momentum of $J = \pm 1$ and dark excitons have parallel spins, resulting in angular momentum of $J = \pm 2$. Dark excitons are optically forbidden because a single photon does not carry enough angular momentum to generate an exciton with the required spin [27]. As discussed previously in Section 2.1.2, normally it is considered that the excitons are formed between an electron and HH. However, it has been demonstrated that there is significant HH-LH mixing in asymmetric QDs [28].

The electrons in the conduction band eventually relax back to the valence band, in other words, the exciton recombines. Generally, bright exciton recombination times are in the range of several nanoseconds in III-V self-assembled QDs [29, 30]. If it is a bright exciton, the exciton radiatively recombines. The emitted photon energy depends on the band gap of the QD. The band gap in a QD is determined by two main factors, the first one being the material that the QD is composed from. Different III-V semiconductor materials can be used to form QDs, which have different band gap energies [31] and so results in different photon emission energies. The second factor is the QD size. The smaller the QDs, the stronger the confinement, which results in higher energy separation between conduction and valence bands [32]. An illustration of this effect can be seen in Fig. 2.3. This is of importance as QD size can be regulated during growth process to some extent, which allows for tuning their energy for their required application.

There are additional types of excitations or charge carrier complexes, one being trions, which have an additional carrier. There are either positive trions (X^+), which have an additional hole or negative trions (X^-), which have an additional electron. They are of interest when investigating the carrier spin dynamics of a QD (see Section 2.3.1). They can be created in several ways, one such way is by applying suitable voltage to QDs with electrical contacting, specifically to the gate electrodes to allow for electrons to tunnel from the reservoir to the QDs [33]. Another method, and which is more relevant for this thesis, is by having resident carriers in the QDs, which then go to form a trion when an exciton is optically created [34]. One of the most reliable ways to achieve this is by either p or n-doping the QD sample, which ensures that each quantum dot contains one carrier on average under equilibrium conditions [34, 35]. Lastly, there are biexcitons, since, as seen in Fig. 2.2, both in the valence and conduction bands, there can exist two particles with opposite spins, resulting in two excitons forming simultaneously.

2.2 QD Growth

In this thesis, we investigate two different QD samples. One sample contains InAs/InGaAs/InP QDs grown by the MOVPE DE method and the other one contains InAs/InAlGaAs QDs grown by the MBE SK method. The different deposition and growth methods are therefore covered in this section.

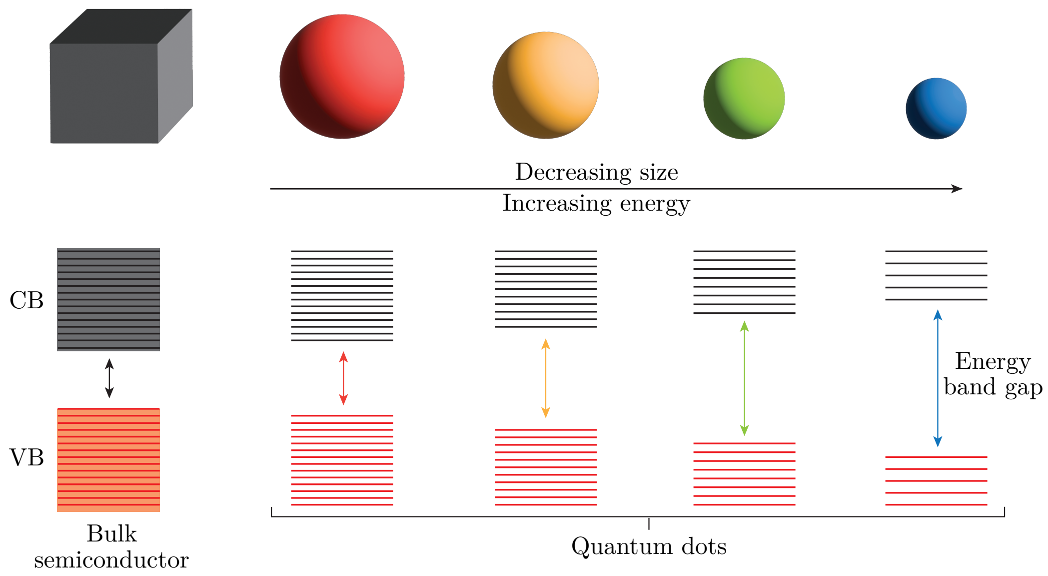

Figure 2.3: Size-dependent quantum confinement effects in semiconductor quantum dots. The figure illustrates how reducing quantum dot dimensions from bulk semiconductor to nanoscale particles leads to progressive energy level discretization and bandgap expansion.

2.2.1 Deposition Methods

There are two main deposition methods used in the growth of QDs: MBE and MOVPE. MBE is a highly controlled thin-film deposition technique [36], where element sources (such as gallium, indium, arsenide, or phosphide) are evaporated in ultra-high vacuum from effusion cells, forming collimated beams of atoms or molecules that travel without collisions until they reach the heated substrate. There, they condense epitaxially in accordance with the crystalline lattice of the substrate. A key feature of MBE is the extremely slow growth rate (on the order of one monolayer per second), which enables atomic-scale control of layer thickness and composition. This precision allows for the fabrication of nanostructures where quantum confinement emerges, such as quantum wells and QDs.

MOVPE, otherwise known as metalorganic chemical vapour deposition (MOCVD), is a chemical vapor thin-film deposition method that relies on chemical vapor reactions of volatile metal-organic precursors and hydrides at the heated substrate surface [37]. Unlike MBE which requires ultra-high vacuum, MOVPE is performed at elevated pressures, typically in the range of a few mbar up to atmospheric, and at higher substrate temperatures, which enhances reaction kinetics and growth rates. Precursors such as trimethylgallium, trimethylindium, arsine, and phosphine are transported into the reactor by a carrier gas (commonly hydrogen or nitrogen), and decompose upon reaching the hot substrate, releasing the group III and V atoms that incorporate into the crystalline lattice. MOVPE offers uniformity across large wafer areas, scalability to industrial volumes, and compatibility with complex heterostructure growth, which has made it the dominant commercial technology for III-V semiconductor devices such as lasers, LEDs, and solar cells.

Generally, MBE is the preferred method for creating confined semiconductor nanostructures. MBE shows better purity due to the ultra-high vacuum environment [38] and sub-monolayer precision, allowing for more precise structures to be formed [39]. However, MOVPE has not only better industrial potential, as mentioned before, but it also has access to the DE growth method for InAs/InP which is advantageous to QDs growth, discussed in subsequent sections.

2.2.2 QD Self Assembly

The SK growth mode is one of the most common mechanisms for strain-driven self-assembly of QDs in lattice-mismatched epitaxial systems. In SK growth, during the initial 2D (wetting) stage, material arriving on the surface diffuses and incorporates into a film with no dislocations, despite lattice mismatch. Elastic energy builds up in the wetting layer (WL) as each additional monolayer is deposited. At a certain thickness (the critical thickness), the elastic energy penalty of continued layer growth outweighs the cost associated with creation of new surface and interface area. At that point, islands nucleate to lower the total free energy: the transition to 3D islands reduces strain at the expense of vertical growth. The balance of strain energy, surface energy, and edge energy dictates the onset of islanding [40]. A diagram of SK growth for InAs/InAlGaAs QDs can be seen in Fig. 2.4.

The island density, size, and uniformity are strongly dependent on growth parameters. Higher substrate temperature increases material diffusivity, favoring the formation of fewer but larger islands [41, 42], whereas higher deposition rate (or supersaturation) tends to increase nucleation density and produce smaller dots [42]. After an initial nucleation phase, processes such as Ostwald ripening or coarsening can further modify the dot size distribution over time (as treated in theoretical models) [43].

Once islands are nucleated, their morphology and composition can evolve further during capping (overgrowth) or annealing. Capping layers can drive intermixing between dot and barrier materials, alter strain fields, and reshape the dots (height reduction, lateral spreading), which can change the emission properties of the QDs [44, 45]. Annealing induces significant structural modifications in quantum dots through temperature-driven atomic processes. Annealing at

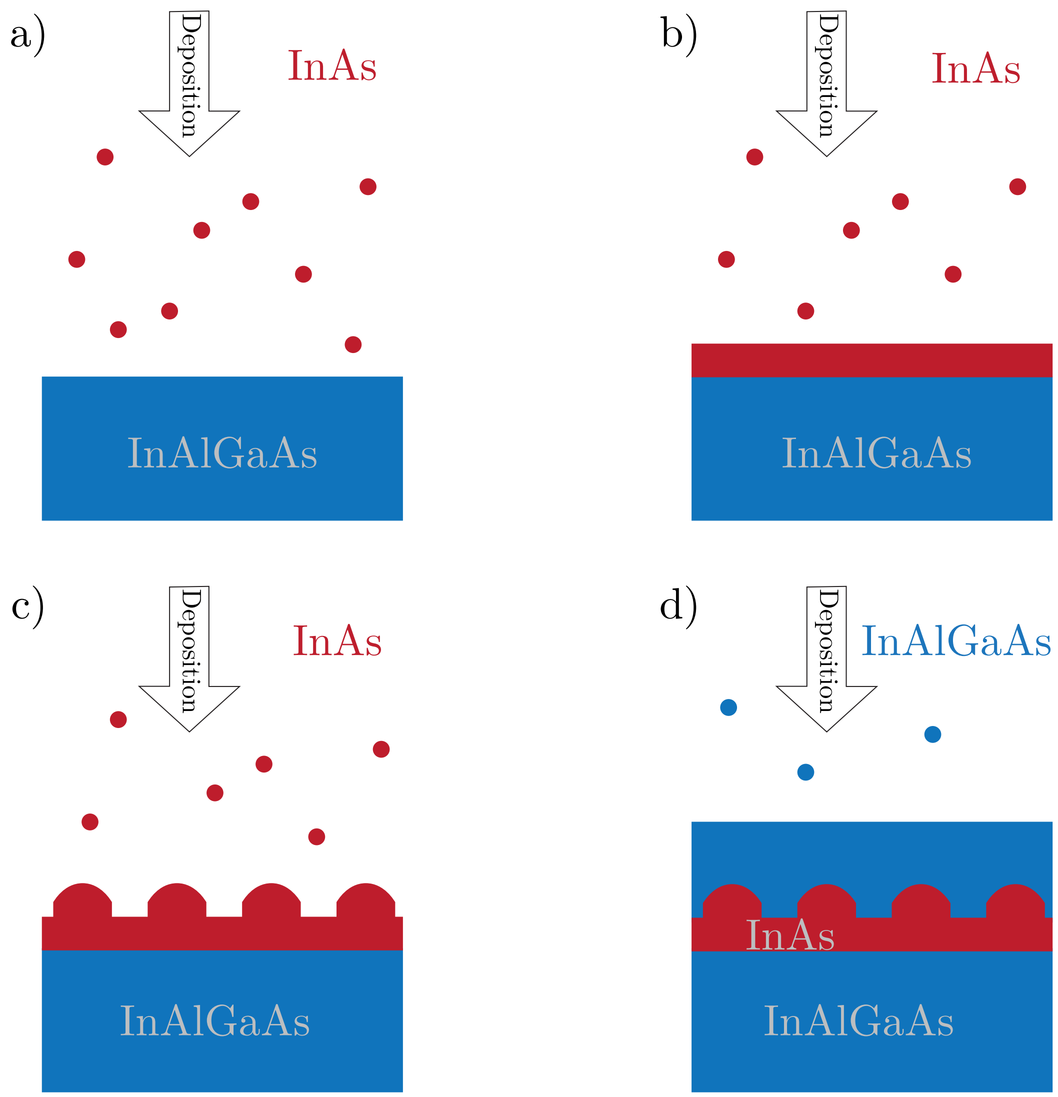

Figure 2.4: Schematic representation of the SK self-assembly process for InAs quantum dots on an InAlGaAs substrate. (a) InAs deposited on top of InAlGaAs substrate. (b) WL forms on top of the substrate and deposition of InAs continues. (c) Critical layer thickness is reached, islands nucleate to reduce the built-up strain. (d) The QDs are covered by a InAlGaAs barrier.

higher temperatures can cause strain-driven self-assembly, which is followed by Ostwald ripening, causing larger dots to grow at the expense of smaller ones, improving QD size distribution uniformity [46, 47].

Despite its advantages, SK self-assembly has some intrinsic challenges. The presence of the wetting layer remains inevitable; it forms a quasi-continuum of states that can couple to dot states, potentially degrading carrier confinement and coherence [48]. Achieving narrow size dispersion across the ensemble is difficult, particularly when dots nucleate over a range of times and diffusion conditions [8]. Moreover, the SK mechanism inherently yields random lateral dot positions (unless modified by patterning or template methods) [8]. Most importantly, due to SK being a strain-based growth method, it can result in asymmetric QD shapes, especially relevant to InAs dots grown on InP, which then causes the QDs to develop elongated shapes [49]. This can significantly impact both the emission and spin properties of QDs, which is discussed in further text.

2.2.3 QD Droplet Epitaxy

In contrast to strain-driven SK growth, DE provides a different approach to self-assembled QD formation, one that is not limited by lattice mismatch strain and the wetting layer mechanisms [50, 51]. DE typically proceeds in two steps: first, group-III metal droplets (e.g. Ga, In) are deposited under reduced group-V flux to form nanoscale liquid droplets on the substrate surface; second, the droplets are crystallized into compound semiconductor dots (e.g. GaAs, InAs) by exposing them to a group-V source (e.g. As, P). Because the dot formation is not strain-driven, DE can yield epitaxial QDs even on lattice-matched or low-mismatch substrates, and is flexible with regard to substrate orientation and material combinations. The DE process is shown in Fig. 2.5.

One major appeal of DE is the possibility of avoiding a WL altogether. Because the islands do not nucleate via strain relaxation, there is no prerequisite two-dimensional film that acts as a continuum. This reduces or even eliminates coupling of dot states to WL states, which allows for achieving higher confinement [52]. DE-grown QDs have shown excellent coherence properties: in an InAs/InP implementation, the DE growth mode enabled 96 % of exciton transitions to have coherence times exceeding typical detector resolution, outperforming SK in two-photon interference visibility (98.6 %) under non-resonant excitation conditions [53].

DE also shows better shape and symmetry characteristic compared to SK. For example, high-temperature DE of GaAs/AlGaAs achieved highly symmetric QDs with reduced defect densities, capitalizing on controlled arsenization dynamics of nanoscale Ga droplets [54]. Similarly, it has

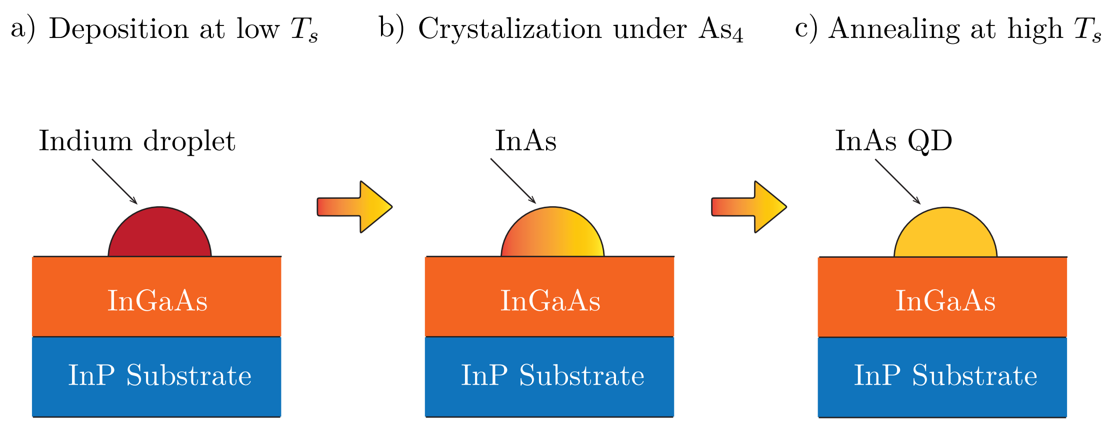

Figure 2.5: Formation of InAs QD by DE on InP. (a) At low substrate temperature, indium is deposited under group-V deficient conditions, leading to the nucleation of nanoscale indium droplets on an InGaAs buffer layer. (b) Subsequent exposure to an As_4 flux crystallizes the droplets into InAs islands. (c) A subsequent annealing step at elevated substrate temperature refines the dot shape and improves crystal quality, yielding strain-free, symmetric InAs QDs embedded in the InGaAs/InP matrix.

been demonstrated that InAs/InP grown by DE show improved structural symmetry [55, 56]. Because strain is not the driving force, DE is less predisposed to produce elongated or anisotropic dot shapes arising from lattice misfit, which is a known drawback in SK-grown InAs dots on InP where strain leads to elongation [57]. As such, DE is particularly interesting for applications requiring high symmetry and coherence, e.g., entangled photon generation.

However, DE also faces certain challenges. One of the fundamental problems in DE is the position and size distribution of QDs. Just as SK grown QDs, DE dots also display unordered spatial positioning [58]. Moreover, DE growth can display bimodal QD size distribution, which happens as the smaller QDs appear first and later merge together into larger ones [59, 60], which can also be observed in Section 4.

2.3 Spin Properties of QDs

Two of the chapters in this thesis focus on investigating spin properties of carriers in the QD samples. Therefore, this section covers the necessary theory for carrier spins in semiconductors and, in particular, QDs.

2.3.1 Optically Polarized Carrier Spin

As mentioned in Section 2.1.2, optical excitation has to follow angular momentum conservation, where the transition of the electron from the valence band (angular momentum eigenvalue $J =$

$3/2$) to the conduction band (angular momentum eigenvalue $J = 1/2$) must correspond to the angular momentum of the photon $J = \pm 1$, which correspond to positive circular polarization (σ^+, $J = 1$) and negative circular polarization (σ^-, $J = -1$). Additionally, energy must also be conserved, where the energy of the photon must exceed the band gap energy in order to excite an electron.

The angular momentum conservation results in optical selection rules which allow only for the electron spin initialized parallel to the propagation direction of the exciting photon, which essentially reflects the projection of the photon's momentum onto its propagation axis. Fig. 2.6 shows a diagram of the selection rules [61].

It should be noted that these selection rules only apply for QDs that are not symmetric, i.e., grown by strain methods. When a QD is perfectly symmetric, there is no longer splitting between the HH-LH bands. In terms of optical selection rules, there are no changes for trion states. Due to the presence of a resident carrier, which results in the two identical carriers forming a singlet spin state due to their opposing spins, their exchange with the remaining trion carrier is cancelled, in which case there is no effect from changes in symmetry [62]. Is is more relevant for neutral excitons, which has exchange interaction between electron and hole, resulting in either circular polarization emission as shown in 2.6 when there is perfect symmetry, or in linearly polarized emission when symmetry is broken, resulting from superposition of the circular polarization states. Therefore, this diagram still holds for DE grown QDs, which exhibit improved symmetry as will be discussed in 4, since only trion states were investigated in this thesis.

While symmetry does not directly affect the optical selection rules, it can be affected by LH-HH mixing. If there is LH-HH admixture, the assumption that an exciton is formed only between HH and electron breaks down, weak extra transitions appear and polarization deviates from the perfect circular polarization due to the impure optical selection rules [28]. There are two factors that cause mixing to increase: increased splitting between LH and HH bands [63], and increase in the QD asymmetry [28]. However, as previously mentioned before, increase in asymmetry also increases the LH-HH band splitting. Therefore, there is no simple relationship that defines that with improvement in QD symmetry there is a clear increase or decrease in mixing and so significant deviations regarding optical selection rules for DE grown QDs are not expected.

The selection rules described above enable spin initialization in a QD. In a doped sample containing resident carriers, absorption of a circularly polarized photon leads to the formation of either a positive or negative trion, with the carrier spin orientation determined by the photon's helicity.

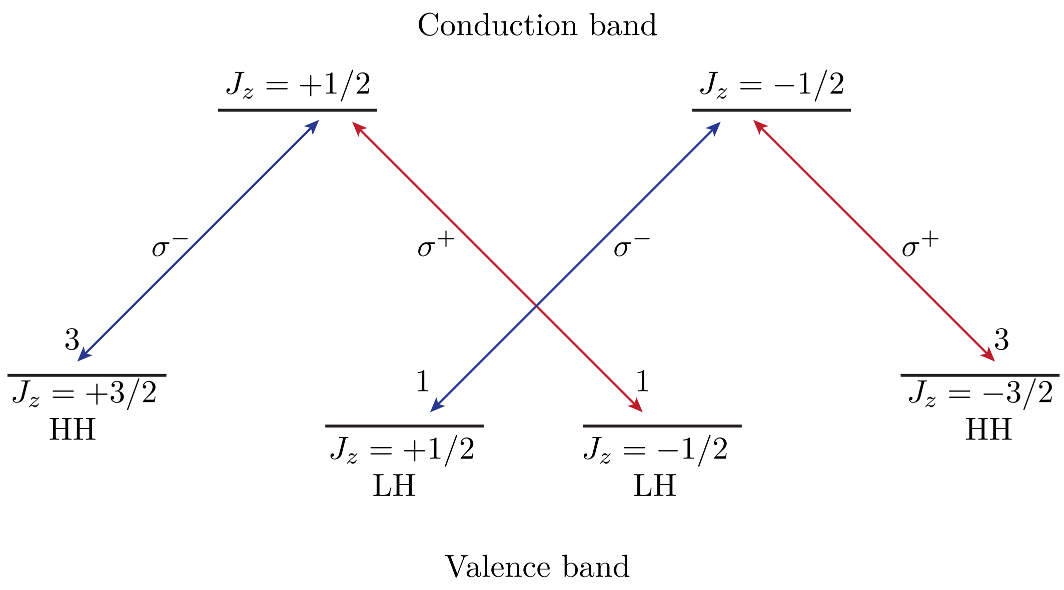

Figure 2.6: Optical selection rules for interband transitions in semiconductors. Shown are the conduction band states with $J_z = \pm 1/2$ and the valence band HH and LH states with $J_z = \pm 3/2, \pm 1/2$. Circularly polarized light couples these states according to angular momentum conservation: σ^- (blue arrows) excites transitions decreasing J_z by one unit, while σ^+ (red arrows) excites transitions increasing J_z by one unit. The transition probability ratio between heavy-hole and light-hole states is 3:1, reflecting their relative oscillator strengths.

Owing to the Pauli exclusion principle, the spin of the resident carrier that completes the trion is also initialized. Since resident carrier spin lifetimes tend to exceed trion or neutral exciton lifetimes, the electron-hole pair recombines and a spin initialized carrier is left behind.

Based on this, spin polarization of the sample can be achieved. A circularly polarized laser pulse resonantly drives Rabi oscillations between the ground state and the trion state. The quantum state of the system during the pulse can be expressed as [64]:

$$|\psi\rangle_{\sigma^-} = \alpha\,|\Uparrow\rangle + \beta\cos\left(\tfrac{\Theta}{2}\right)|\Downarrow\rangle + i\beta\sin\left(\tfrac{\Theta}{2}\right)|\Downarrow\Uparrow\Downarrow\rangle. \tag{2.5}$$

where α and β are the initial probability amplitudes of the carrier spin states, $|\Uparrow\rangle$ and $|\Downarrow\rangle$ are the spin states of the resident carrier, $|\Uparrow\Downarrow\Uparrow\rangle$ is the optically excited trion state and Θ is the pulse area.

Θ controls how the laser pulse redistributes population between the ground and trion states. For example, a π-pulse ($\Theta = \pi$) transfers population from $|\Downarrow\rangle$ to the trion state, while a 2π-pulse returns the system back to its initial state. In this way, the pulse acts as a controllable rotation in the Hilbert space of the two-level system where in this case, since trions are excited, the pulses effectively control the polarization of resident carriers in the sample. This concept is important for spin mode locking, which is discussed in Section 2.4.4.

2.3.2 QDs in Magnetic Fields

When an external magnetic field B is applied to a QD, the carrier spin states undergo Zeeman splitting due to their spin projections. For the lowest-energy (s-shell) carriers, this splitting arises from the different signs of the magnetic quantum number m_j for electrons and heavy holes. The energy shift of a given carrier or excitonic complex i is described by [61]:

$$E_i^Z = g_0 \mu_B B \tag{2.6}$$

where g_0 is the effective Landé g-factor of a free exciton, and μ_B is the Bohr magneton. While the Landé g-factor applies to free electrons, this also applies to both electrons and holes in QDs by replacing it with the effective g-factor of the QD. Because g_i is defined with respect to the spin projection $J_z = m_j$, the heavy-hole g-factor includes an implicit factor of three relative to electrons. However, even with this factor of 3, the hole g-factors are usually lower than electrons in QDs [65, 66, 17]. Along with the reduced magnitude, hole g-factors are more anisotropic (changes as the magnetic field angle is changed) compared to electrons in QDs; this is due to orbital angular momentum quenching. While electrons are only weakly affected by changes in the confining potential, holes derive a larger contribution to their Zeeman response from orbital motion in the valence band [67, 68]. It should also be mentioned that both electron and hole g-factor depends on factors such as QD shape, size, strain (which also means growth mode) and material [69, 70, 71].

The samples investigated in this thesis are not single QDs; rather the samples contain ensembles of QDs. Fig. 2.7 shows the photoluminescence (PL) of the two-layer InAs/InAlGaAs sample that is investigated in Section 5. The inhomogeneous distribution means that the g-factor not only depends on the physical parameters of the sample, but also on the excitation energy. As different excitation energy is used, different QD ensembles are excited and therefore different size QDs (energy is directly related to size as shown in Fig. 2.3) contribute to the measured g-factor.

Both hole and electron g-factors show different behavior with changing energy, where the electron g-factor magnitude decreases with increasing energy, and the hole increases with increasing energy in telecom C-band QD samples [65, 72, 17]. However, in this case, it is the absolute g-factor shown (due to measurement method limitations), whereas when looking at the non-absolute values, the opposite behavior is observed, since the values are negative [73, 68]. For the electron this is due to orbital angular momentum quenching, where with increasing band gap size, which corresponds to decreasing QD size, the confinement increases and the electron g-factor tends towards the free electron value [73]. This is further demonstrated by the Roth-Lax-Zwerdling relation [74]. For holes the analysis is less straightforward, since the hole state mixes many envelope angular momentum components [73]. It has been demonstrated that for smaller QDs at higher energies, rather than the HH-LH mixing being the main contributor to the g-factor values, envelope orbital angular momentum starts to dominate, which is why an increase in the g-factor magnitude is seen for holes with increasing energy [71].

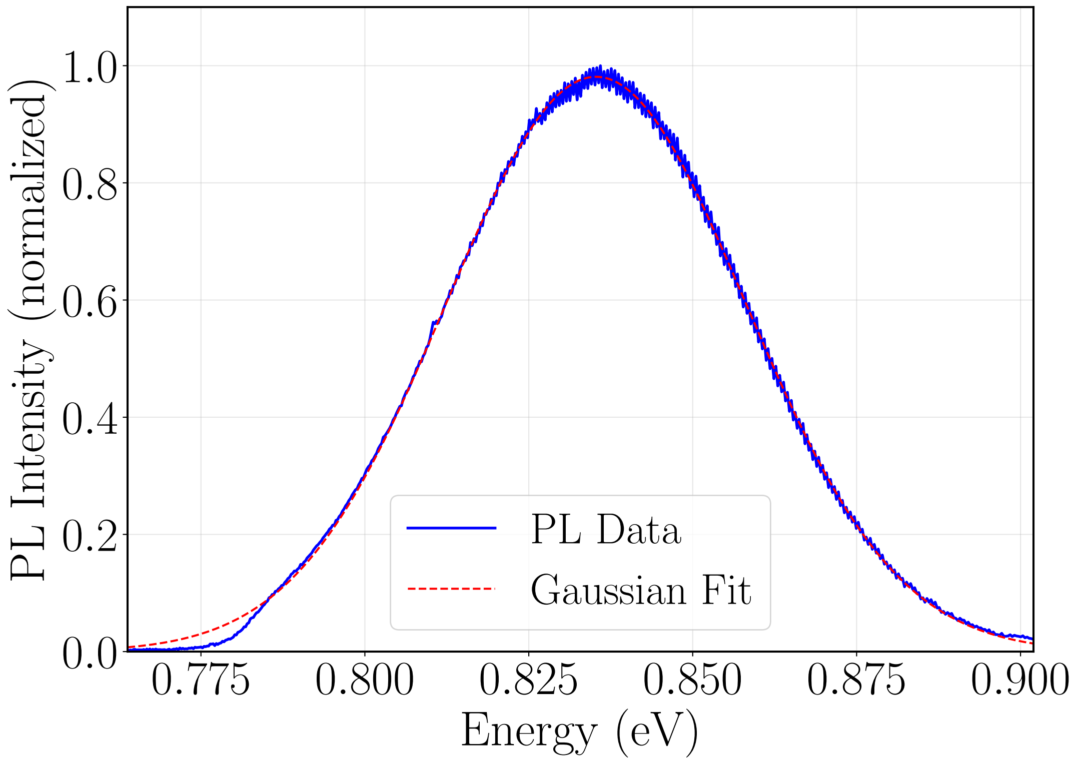

Figure 2.7: PL spectrum of the InAs/InAlGaAs two-layer quantum dot sample, which is discussed in Section 5. The measurement illustrates the ensemble emission from the quantum dots in the structure in the form of a Gaussian PL.

The behavior of the carrier spins differs depending on the direction of the applied magnetic field. There are two main cases to consider: Voigt (in-plane) geometry, where the magnetic field is oriented within the sample plane, and Faraday (out-of-plane) geometry, where the field is oriented along the QD growth direction. This is more clearly illustrated in Fig. 2.8.

Voigt Geometry

When a magnetic field is applied in Voigt geometry and the resident carriers have spin polarization, the spins start to precess. It can be understood from the perspective of magnetic moment, where it

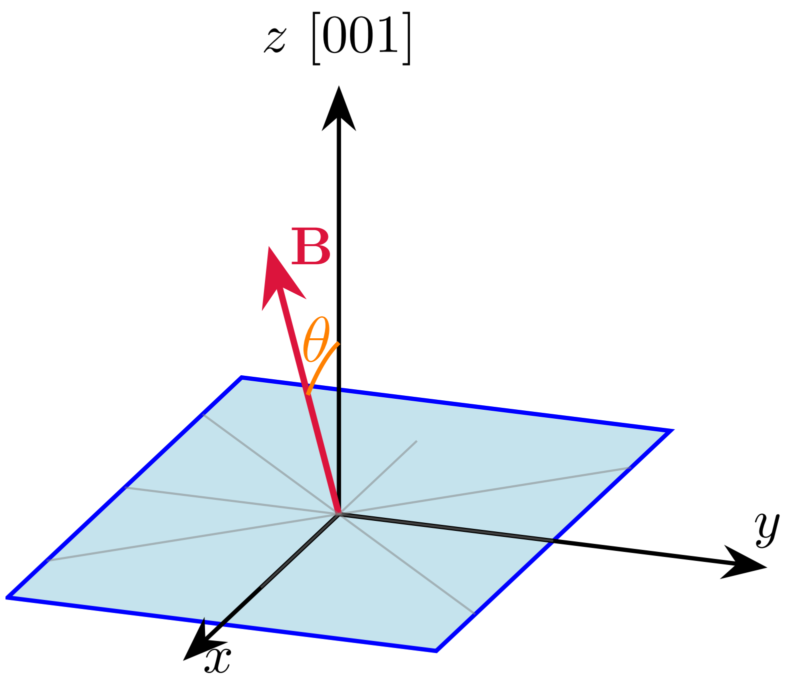

Figure 2.8: Schematic of the magnetic field orientation relative to the quantum dot growth axis [001]. The external magnetic field **B** is applied at an angle θ with respect to the growth axis. For $\theta = 0°$, the field is parallel to the optical axis (Faraday geometry), while for $\theta = 90°$, the field lies in the sample plane (Voigt geometry).

is known that there is torque applied on a dipole if there is an external magnetic field:

$$\boldsymbol{\tau} = \boldsymbol{m} \times \boldsymbol{B} \tag{2.7}$$

where $\boldsymbol{\tau}$ is the torque applied to the dipole or spin of the carrier, $\boldsymbol{B}$ is the magnetic field and $\boldsymbol{m}$ is the magnetic moment or spin of the carrier. If the magnetic field is perpendicular to the spin direction, which it is in Voigt geometry, then there is torque applied on the carrier's spin, which results in precession of spin. However, the spin of a carrier cannot rotate, as there is only a spin up or a spin down state. A more accurate representation is to consider the quantum behavior, where a spin prepared along the optical axis becomes a coherent superposition of the magnetic field eigenstates when a transverse field is applied. Then, the relative phase of the two states oscillates, leading to precession of the resident carrier spin polarization.

The spin polarization precession frequency can be obtained from the Zeeman splitting energy, defined in Eq. 2.6:

$$\omega_L = \frac{g_i \mu_B B}{\hbar} \tag{2.8}$$

where ω_L is the Larmor frequency, g_i is the effective g-factor of the carrier in the QD and $\hbar$ is the reduced Planck's constant. Care has to be taken with the g-factors in this equation since both carrier g-factors are anisotropic (with holes being more so); therefore, this means that as the angle of the magnetic field changes, so does the precession frequency.

If the frequency of the precession can be measured, the g-factor can be calculated, and by knowing g-factors, electron and hole carriers can be identified. Moreover, if the precession can be measured, spin dephasing of the carriers and the Hanle effect can be measured [17, 1], which is further discussed in Chapters 3 and 4.

Faraday Geometry

A key distinction from the Voigt geometry is that in Faraday geometry no coherent Larmor precession of the spin occurs because the spin direction is aligned with the magnetic field. Under these conditions, the Zeeman splitting manifests directly as a shift in the optical transition energies, and the optical selection rules remain preserved: circularly polarized photons couple to spin states with well-defined angular momentum projections. In this geometry, the spin physics is governed by longitudinal relaxation processes (T_1 times), which describe how the spin populations equilibrate with the lattice [75]. Therefore, Faraday geometry measurements allow for extracting the T_1 time of the QDs, which is further addressed in Chapters 3 and 4.

As mentioned previously, the carrier g-factors are anisotropic, especially for holes. For example, a telecom C-band InAs/InAlGaAs QD sample shows in-plane absolute g-factor value $|g_{h,x}| = 0.64$ and out of plane value $|g_{h,z}| = 2.29$ [66]. It is important to know that unlike in Voigt geometry, the g-factor cannot be directly measured in Faraday geometry, since there is no precession. However, the g-factor anisotropy has an oscillatory dependence [66]:

$$|g_i| = \sqrt{(g_x \cos\theta)^2 + (g_z \sin\theta)^2} \tag{2.9}$$

where g_x is the in-plane g-factor value, g_z is the out of plane g-factor value and θ is the rotation of the magnetic field in degrees. If the g-factor value is known at several points of rotation, it can be fit with this equation to obtain the effective g-factor values in both Voigt and Faraday geometry.

2.4 Spin Dynamics in QDs

In the previous section we have covered the properties and behaviors of carrier spins in QDs. In this section, the dynamics of spins in carriers will be covered.

2.4.1 Longitudinal and Transverse Spin Lifetimes

The temporal evolution of a spin system is commonly characterized by two timescales: the longitudinal relaxation time T_1 and the transverse relaxation time T_2 (often referred to as the decoherence time). In a longitudinal (Faraday geometry) magnetic field, the Zeeman splitting defines two spin levels. The quantity T_1 denotes the characteristic time over which a non-equilibrium spin population relaxes back to the ground state, typically through energy exchange with the surrounding lattice. Examples of T_1 process is tunneling of carriers out of QDs [76], radiative recombination (assuming no resident carriers) [77] and spin flips. When the applied magnetic field is transverse (Voigt geometry) to the spin direction, the spin undergoes Larmor precession around the field axis. In this situation, T_2 quantifies the time over which the relative phase coherence between the spin eigenstates is lost. Unlike T_1, this process does not require an energy transfer or a change in the populations of the spin levels, but instead reflects the gradual decay of phase coherence.

When working with an ensemble of spins, an additional dephasing T_2^* time constant must be considered. It reflects the apparent loss of coherence caused by variations in the local environment across the ensemble. For example, slight differences in ensemble g-factors, applied magnetic field strengths, or hyperfine interactions lead to a spread of Larmor precession frequencies [17]. Due to this, the ensemble spin polarization decays faster than the intrinsic T_2. Importantly, T_2^* does not represent an irreversible loss of coherence.

When a sample is excited, there is an ensemble of QDs with prepared spins which precess in Voigt geometry, causing effective precession of the total spin polarization. Due to this, there are two main types of spin dephasing: homogeneous and inhomogeneous [75]. The inhomogeneous decay is related to inhomogeneities of the sample (g-factor variations between QDs, nuclear magnetic field variations) and the experimental set-up (non-homogeneous applied magnetic field, excitation intensity/energy variations). Whereas homogeneous dephasing is related to physical effects occuring within the QDs. Homogeneous dephasing is addressed further in Section 2.4.2.

Since inhomogeneous dephasing is related to sample inhomogeneities, it can be assumed that the precession frequencies are distributed in a Gaussian, which is further confirmed by looking at the sample PL shown in Fig. 2.7, which shows a Gaussian distribution. Therefore, the frequency spread is [75]:

$$f(\omega_e) = Ce^{-(\omega_e-\omega_0)^2/2(\Delta\omega_e)^2} \tag{2.10}$$

where ω_0 is the center frequency and $\Delta\omega_e$ is frequency distribution width. With this, the spin polarization signal is:

$$S = A_0 e^{-t^2/2T_2^{*2}} \cos(\omega_0 t) \tag{2.11}$$

where A_0 is the amplitude of the spin polarization signal and T_2^* in this case denotes relaxation in terms of frequency distribution width $T_2^* = 1/\Delta\omega_e$ [75]. However, usually in QD ensemble samples both hole and electron spin precessions can be observed, therefore, the full spin polarization signal is [17]:

$$S = \sum_i A_i \cos(\omega_i t) e^{-\frac{t^2}{2T_{2,i}^{*2}}} \tag{2.12}$$

where A_i is the amplitude of carrier spin polarization signal, ω_i is the Larmor precession frequency of the respective carrier and $T_{2,i}^*$ is the dephasing time of the respective carrier. With homogeneous dephasing, the equation remains mostly the same, with the exception that the decay is exponential e^{-t/T_2^*} rather than Gaussian [75].

2.4.2 Spin Relaxation Mechanisms

Homogeneous Dephasing

In contrast to inhomogeneous broadening, which originates from variations across the ensemble, homogeneous dephasing reflects the intrinsic loss of coherence of individual spins. Here, the decay is driven by scattering processes in which a carrier spin exchanges angular momentum with its environment, for example via phonons or other carriers [75].

There are several mechanisms that drive homogeneous dephasing. However, some of them contribute minimally in systems with strong confinement, such as QDs, therefore in those cases, they will not be covered in depth.

Elliot-Yafet mechanism describes spin relaxation through spin-orbit coupling embedded in the Bloch wavefunctions. In bulk semiconductors, electronic states are not pure spin eigenstates but contain a small admixture of the opposite spin. During a momentum scattering event (e.g. with a phonon or impurity), the spin admixture allows for a finite probability of a spin flip [78, 79]. In QDs, the Elliot-Yafet mechanism is significantly suppressed compared to bulk semiconductors, since due to the strong confinement in QDs, the carriers are completely stationary, which prevents carriers undergoing collisions with impurities, phonons or surfaces [80].

The Dyakonov-Perel mechanism dominates in bulk and two-dimensional semiconductor systems lacking inversion symmetry. Spin-orbit interaction generates an effective, momentum dependent internal magnetic field that causes spins to precess. Frequent scattering events randomize the carrier momentum, and thus the direction of the effective field, causing variation of spin precessions and leading to dephasing of the spin ensemble [81, 82]. This mechanism is again suppressed in QDs due to their confinement, more specifically, carriers lack the defined momentum states which are required for this mechanism [83, 80].

The Bir-Aronov-Pikus mechanism arises from the exchange interaction between electrons and holes. When both carrier species are present, e.g. in optically excited systems or in p-doped semiconductors, the electron spin can flip through scattering processes mediated by the hole spin [84, 85]. In this thesis, this mechanism is also not entirely relevant, since even though there are samples with resident carriers being holes, in a QD the hole and electron are only present while a trion is excited, which has a much shorter lifetime than the spin lifetimes of a resident carrier.

A more prevalent mechanism in QDs is the spin-phonon coupling. It can be divided into two different groups: spin admixture mechanism resulting from spin-orbit coupling and direct spin-phonon coupling. The latter causes reduced symmetry due to phonons displacement field and so causing spin relaxation when spin-orbit coupling is present [86]. This direct coupling mechanism is usually not as significant in QDs systems [87]. However, spin admixture mechanism resulting from spin-orbit coupling contributes strongly to dephasing, especially at higher temperatures. In this mechanism, the spin couples indirectly to acoustic or optical phonons via spin-orbit admixture of orbital states. Thermally excited phonons couple to the orbital part of the carrier wavefunction. Because spin-orbit interaction mixes opposite-spin components into these orbital states, phonon-driven orbital transitions can simultaneously flip the spin [88]. Therefore, as temperature increases, the dephasing becomes faster. It should be noted that this mechanism behaves differently for electrons and holes. For electrons, phonon-induced spin relaxation is often weak at cryogenic temperatures, where hyperfine interactions dominate, but becomes relevant when temperature is above 10-20 K [89]. In contrast, holes, which couple more strongly to spin-orbit interactions in the valence band [90], exhibit noticeable phonon-driven dephasing already at lower temperatures [91].

Nuclear Spin Effects

In addition to phonons and carrier-carrier scattering, the surrounding lattice nuclei and the nuclear spins within each QD provide another environment that interacts with localized spins in quantum dots. Each carrier spin couples to the nuclear spin ensemble of the host crystal or/and to the nuclear spin of the QD through the hyperfine interaction. This coupling is bidirectional: not only does the fluctuating configuration of nuclear spins act back on the carrier as an effective magnetic field (the

Overhauser field [92]), but carrier spins can also transfer angular momentum to the nuclei, altering their polarization [61]. While details of nuclear spin dynamics and polarization lies outside the scope of this thesis, hyperfine interaction is an important mechanism that limits spin coherence in QDs, especially for electrons.

Hyperfine interaction can be considered as both homogeneous and inhomogeneous relaxation mechanisms. In the inhomogeneous case, the spin interacts with the surrounding nuclei through the Fermi contact interaction. The interaction with the nuclei in the lattice Hamiltonian is [93, 94]:

$$H_{\text{HF}} = \sum_n A_n \left(\mathbf{I}_n \cdot \mathbf{S}\right) \tag{2.13}$$

where A_n is the hyperfine coupling constant for nucleus n, $\mathbf{I}_n$ is the spin operator (vector) of the n-th nucleus and $\mathbf{S}$ is the electron spin operator. This equation only includes the electron spin operator, not the hole. This is due to the fact that the hole hyperfine interaction coupling constant is an order of magnitude lower for holes compared to electrons [95], because the hole Bloch wavefunctions vanish at the nuclear sites [93]. That is why in a lot of QD samples, the hole dephasing times are longer than electrons, sometimes by an order of magnitude [17, 89, 95].

Hyperfine interaction can also be expressed as an effective magnetic field acting on electron spins [93, 94]:

$$\mathbf{B}_N = \frac{1}{g_e \mu_B} \left\langle \sum_n A_n \, \mathbf{I}_n \right\rangle_N \tag{2.14}$$

In most cases, this magnetic field is quasi-static, meaning it does fluctuate due to nuclear spins not being static, but the nuclear spin timescales are significantly longer than carrier spin times at cryogenic temperatures [93]. Therefore, the main dephasing contributor in this case is the inhomogeneous distribution of nuclear spins, which creates a non-uniformly distributed magnetic field, causing inhomogeneous electron spin dephasing. It is important to mention that this is relevant only to Voigt geometry. In Faraday geometry the electron spins are essentially uncoupled from the nuclear spins due to the magnetic field being aligned with the electron spin axis.

As mentioned before, the hyperfine interaction can also act as a homogeneous dephasing mechanism. In such a case, either the nuclear spins fluctuate on timescales similar to electron spins, or the electron's position changes, which causes it to couple to different nuclei spins, which is effectively the same as the nuclear spin fluctuating. However, in QDs, only the inhomogeneous hyperfine interaction is relevant, since measurements are done in cryogenic temperatures and, due to QD confinement, the electrons are stationary.

There is one case where homogeneous hyperfine interactions becomes relevant for QDs. Nuclei with spin $I > 1/2$ carry not only a magnetic dipole moment but also an electric quadrupole moment. While the dipole moment describes the interaction of a nucleus with magnetic fields, the quadrupole moment characterizes the deviation of the nuclear charge distribution from perfect spherical symmetry [96]. In other words, the nucleus has an elongated or flattened charge distribution, which makes it sensitive to gradients of the surrounding electric field rather than to uniform fields.

In QDs, strain and material fluctuations can disort the local crystal symmetry, which generates an electric field gradient (EFG) [97]. The quadrupole moment couples to these gradients, leading to additional splitting and mixing of nuclear spin states. This modifies the nuclear spin dynamics by enabling faster relaxation, which then results in reduced temporal stability of the Overhauser field. Consequently, this causes accelerated spin dephasing in electrons, although quadrupole only acts on nuclear spins. This has been demonstrated in InGaAs/GaAs QDs [98] and it is theorized that this is what contributes to the dephasing of the InAs/InGaAs/InP samples measured in this thesis, discussed in Section 4.

2.4.3 Relation of T_1, T_2, and T_2^* to Relaxation Mechanisms

All the previous covered relaxation mechanisms apply to the T_2^* time. This is because spin ensemble dephasing is formed from both the homogeneous and inhomogeneous dephasing components [99]:

$$\frac{1}{T_2^*} = \frac{1}{T_2} + \frac{1}{T_{\text{inhom}}} \tag{2.15}$$

where T_2 is the spin coherence, which is determined by homogeneous dephasing and T_{inhom} is the inhomogeneous dephasing.

For carriers in QDs, the longitudinal relaxation time T_1 is not constrained by the same mechanisms that dominate transverse dephasing. Hyperfine interactions with the nuclear spin bath, quadrupole-driven nuclear dynamics, or static g-factor inhomogeneities dephase the transverse spins and therefore limit T_2 and T_2^*, but they do not provide the energy exchange required for longitudinal relaxation. As a result, T_1 in quantum dots is predominantly determined by phonon-assisted spin flips enabled by spin-orbit coupling. Due to this, carriers in QDs show significantly longer T_1 times compared to T_2 and T_2^* times. At temperatures below 100 mK longitudinal spin lifetimes up to a second have been measured [100] whereas in telecom C-band QDs samples at higher temperatures of 5-10 K T_1 times are usually in microsecond range as seen in Ref. [89] and in Chapter 4.

2.4.4 Spin Mode Locking

In ensembles of QDs subject to periodic pulsed excitation, the carriers spin can undergo a synchronization effect known as spin mode locking (SML). Normally, the previous listed inhomogeneous relaxation mechanisms lead to rapid dephasing. However, when the laser repetition period matches an integer multiple of the spin precession period for a subset of spins and the T_2 exceeds the laser repetition period T_R, those spins remain phase-synchronized with the pump pulse train [101]. More precisely, the pump pulse polarizes the spins every T_R and normally, it clears the old residual spin polarization if the period does not match the spin precession period. If it does, it results in the pump pulse polarization phase matching with the spin precession, which causes constructive interference, which effectively builds up the spin. Several spin precession frequencies end up synchronized, where finally their superposition results in a decaying polarization signal which revives before the next excitation pulse. This is illustrated in Fig. 2.9.

The precise condition that has to be satisfied in order for SML to occur is the following[101]:

$$\omega_L = \frac{2\pi N}{T_R}, \qquad T_2 > T_R, \tag{2.16}$$

where N is an integer denoting the number of Larmor cycles between successive pump pulses. Spin mode locking is inherently an ensemble phenomenon. It relies on the presence of a continuous distribution of Larmor precession frequencies, so that a subset of spins naturally satisfies the phase synchronization condition.

The spin polarization peaks shown in Fig. 2.9 can be calculated by the following [101]:

$$S_z(\omega_e) = -\frac{1}{2} \frac{\left(\frac{W}{2T_R}\right)\left(\frac{W}{2T_R} + \frac{1}{T_2}\right)}{\left(\frac{W}{2T_R} + \frac{1}{T_2}\right)^2 + (\omega_e - N\Omega)^2}, \tag{2.17}$$

where $W = \sin^2(\Theta/2)$ is the excitation power, which is dependent on the excitation pulse area Θ, and $\Omega = 2\pi/T_R$ is the repetition angular frequency. From this equation it is seen that if SML is observed, it can be used to calculate the QD coherence time T_2. The procedure to calculate T_2 from SML is detailed in Ref. [101].

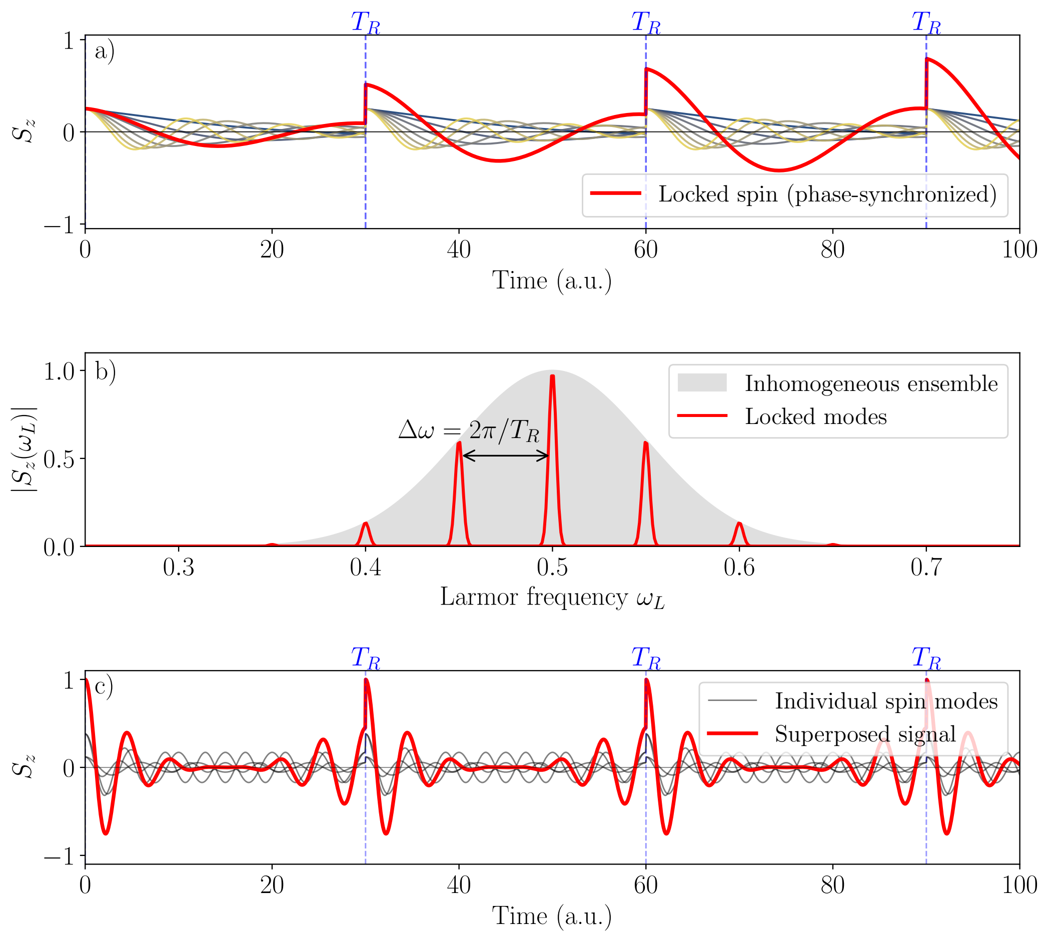

Figure 2.9: Schematic illustration of spin-mode locking in an ensemble of quantum dots. (a) Time-domain representation of ensemble spin dynamics under periodic optical excitation. Each pump pulse (blue dashed lines, separated by T_R) reinitializes all spins. Spins with different Larmor frequencies dephase between pulses and decay, while those satisfying the phase-synchronization condition (red trace) remain in phase and gradually build amplitude through constructive interference of successive excitations. (b) Frequency-domain view showing how periodic pumping selects discrete phase-synchronized modes (red peaks) within the inhomogeneous distribution of Larmor frequencies (gray envelope) $\Delta\omega = 2\pi/T_R$ corresponds to the pulse-repetition frequency, defining the set of locked spin modes that contribute to the long-lived ensemble coherence. (c) Superposition of the individual locked spin modes, illustrating how their overlap produces an ensemble polarization that decays, but revives before the next pulse arrives. All units in the figure are arbitrary.

SML can be observed for both electrons and holes; it depends primarily on the resident carriers of the sample. Initially, SML was observed in electrons in an n-doped (In,Ga)As/GaAs ensembles [101]. Later, it has been demonstrated in holes in an InAs/GaAs QD ensemble sample [102]. Lastly, it has been observed in multi-layer telecom C-band InAs/InAlGaAs QD samples [17], which are also further investigated in this thesis.

2.5 Quantum Cryptography

In the previous sections QDs, their properties, growth and spin dynamics were covered. This section covers how quantum optics can be utilized for secure communications, which is relevant for the potential applications of the telecom QDs that are studied in this thesis and also for the heterodyne QRNG that was developed for this thesis.

2.5.1 Quantum Key Distribution

QKD is a cryptographic protocol that enables two distant parties (commonly named Alice and Bob) to establish a shared secret key with information-theoretic security, relying on the laws of quantum mechanics rather than computational assumptions. It has been theoretically shown that Shor's algorithm in quantum computing presents a significant issue to public-key cryptography, as it can factor large integers and solve discrete logarithm problems in polynomial time [5], which poses a threat to commonly used symmetric key based encryption. QKD is not an encryption protocol, instead it provides a secure way of exchanging keys based on the fact that any attempt by an eavesdropper (Eve) to intercept or measure the quantum states necessarily introduces disturbances that can be detected by the legitimate parties. The transferred keys can then be used for secure classical symmetric encryption. One example of such encryption being one-time pad (OTP), otherwise known as Vernam cryptographic system. OTP relies on using keys, which are the same length as the data being encrypted, to encrypt the data by using exclusive-or (XOR) logical operation [103]. OTP is considered perfectly secure as the encrypted data does not provide information about the original data, besides the length, making it theoretically unbreakable by both classical and quantum computing [103].

The first QKD protocol developed was BB84 [104]. The protocol follows a four stage procedure for secure transfer. Firstly, Alice generates a random sequence of bits where each bit is encoded with a quantum state in either rectilinear or diagonal basis. In a real system, the rectilinear basis usually corresponds to horizontally or vertically ($\langle H|$, $\langle V|$) polarized photons and the diagonal basis corresponds to $45°$ and $-45°$ ($\frac{\langle H|+\langle V|}{\sqrt{2}}$, $\frac{\langle H|-\langle V|}{\sqrt{2}}$) polarized photons.

The bits are encoded using a randomly selected basis and then are sent to Bob. Upon receiving the photons, Bob then independently and randomly chooses which basis to measure the polarization of the received photon. If the measured basis is the same as the one used to encode the bit, Bob will obtain the correct bit; if not, then there is a 50 % chance of measuring either one or the other state. Afterwards, Alice and Bob use a classical information transfer channel to exchange in which basis each bit was measured. Then, Bob knows which bits were measured in the correct basis and can be kept, whereas the other ones are left unused; the same applies to Alice. This process is called bit sifting. Lastly, part of the key is announced by Alice and Bob to check for error rates. If the error rate is too high, it indicates that either the measurement/source devices are too noisy or that Eve was eavesdropping, which corrupted the key [105], in which case the bits are discarded; otherwise, they perform error correction to reconcile any residual differences and use privacy amplification in the form of hashing algorithms (for example, Toeplitz hashing) to eliminate any partial information Eve might have gained.

There are numerous other protocols which are out of scope for this thesis. However, there are several important classifications of protocols. Firstly, there is the classification on the type of encoding that is used: discrete-variable (DV) QKD and continuous-variable (CV) QKD [106]. An example of DV-QKD is BB84, which uses discretely prepared quantum states such as photon polarization, whereas CV-QKD exploits light beam amplitudes or phase for transmitting keys [106]. DV-QKD is further characterized into three more subgroups [107]: prepare-send-measure protocols, which BB84 corresponds to, measure-only protocols, where both Alice and Bob randomly measure shared entangled states that are generated by an untrusted source (E91 protocol) [14] and prepare-send-only protocol where both Alice and Bob prepare quantum states and send them to an untrusted third party, who measures and returns classical results [108].

This section shows the importance of two concepts which are explored in this thesis: QRNGs and quantum repeaters. QRNGs are essential not only for generating true random keys which are essential to ensure OTP encryption is fully secure [103], but also for generating truly random encoding/measurement basis choices as detailed in the BB84 protocol, seed generation for privacy amplification and randomly choosing which bits are shared for quantum error correction purposes. The use of random data is essential, since insecure RNGs such as pseudorandom number generator (PRNG) or cryptographically secure pseudorandom number generator (CSPRNG), which rely on deterministic classical algorithms, introduce potential vulnerabilities. Any predictability in the random sequence, arising from algorithmic generation or partial knowledge of the seed state, constitutes an additional attack channel that can compromise the fundamental security assumptions of the protocol. Moreover, as is seen from the BB84 protocol, the efficiency is less than 50 % accounting all factors; therefore high-bandwidth QRNG is needed to transfer a reasonable amount of keys.

The other key factor of QKD is the ability to use it for long-range communication. If an entanglement based QKD protocol is used over long distances, the entangled states might experience decoherence over long distances of fiber travel [10]. For this reason, quantum repeaters are needed, which require quantum memories and quantum processors to perform entanglement swapping and distillation [109]. QDs can be used as a quantum memory; however, they require long spin coherence times in order to store the states long enough for the required quantum operations [34]. As QD spin properties have already been covered in the previous section, the following sections will focus on QRNG theory, which also applies to QKD to a certain extent.

2.5.2 Quantum Random Number Generation

As mentioned briefly in the previous section, if a photon in the diagonal polarization basis is measured in the rectilinear basis, it results in a 50 % chance of measuring either a vertically or horizontally polarized photon. More accurately, the measurement non-deterministically breaks down the superposition into one of the states, governed by Born rule [110]. The non-deterministic nature of quantum measurements make it a perfect RNG, since it avoids the problem of predictability that PRNG and CSPRNG have.

It is important to clarify that random numbers generated by either classical sources such as PRNGs, CSPRNGs or by QRNGs are indistinguishable. The principle of true randomicity is that in an infinite sequence of numbers there would be no apparent pattern. Therefore, in order to determine whether a source is truly random, an infinite amount of numbers would be required, which is not feasible. Practically, it can only be determined whether the RNG source is not random. Different statistical tests exist to determine whether the numbers present any apparent patterns, such as autocorrelation, discrete Fourier transform, pi value determination using Monte Carlo method, Chi-square distribution, various pattern matching tests like checking repetition frequency, longest run of ones, cumulative sums and etc [111]. These statistical methods are used to test the random numbers, and then whether the test passes or fails is determined by applying the null hypothesis, which is what the outcome of the test is assuming the test was applied to a perfectly random, uniform distribution. The test outcomes are compared to the null hypothesis and p-values are produced, which quantify the probability of that a random source would produce a test statistic at least as extreme as the one observed. A low p-value therefore means that if the sequence was truly random, the observed result would be highly improbable, which is evidence against the null hypothesis, indicating that the sequence under test is not random [112].

However, just because a sequence has a low p-value, it does not indicate that the source is not random. Same applies to the opposite, if a p-value is high, it also does not indicate that the source is truly random. This is because if a truly random source is taken and a finite sequence is tested, there is a finite probability that either a sequence with significant patterns or no patterns will be produced. These probabilities are, low, therefore, with these tests, rather than using the individual p-values as an indicator on whether the source is not random, the distribution is what indicates whether a source is not random. If p-values are distributed normally, it indicates that the source does not have any apparent issues. If the values skew towards lower or higher end of p-values, it indicates that the source is imperfect and cannot be used for any cryptographic applications.

Again, it should be made clear that just because a source passes statistical tests, that it is truly secure. It has been shown that classic PRNG sources pass randomness statistical tests [112]. However, they lack security because PRNGs are intrinsically deterministic, they take a short seed number and extend it into a long sequence of random numbers [113], therefore, if the adversary obtains the seed, the random numbers can be completely reproduced. CSPRNGs are more secure because they utilize entropy sources to generate seeds from which then the random numbers are generated. One such example is the */dev/urandom* implementation on Linux, which uses data from the different drivers and peripherals connected to the computer for the seed data [114]. Nonetheless, classical entropy sources are used and while CSPRNGs are enough for most classical encryption algorithms, they still can be controlled by an adversary, making the RNG source unsafe.

Since the principle of QKD relies on the fact that adversarial control or interception is impossible due to using quantum states for key transfer, using an RNG with a classical entropy source defeats the purpose of the QKD, since then the unsafe RNG becomes a potential attack vector. That is why it is necessary to use a QRNG source, since the same concept to it applies as for QKD where the entropy source is non-classic and it cannot be intercepted or controlled (assuming semi- or device-independent security model, which is covered further below).

Like in QKD, there is DV-QRNG and CV-QRNG. Some examples of DV-QRNG include single photons going through 50:50 beamsplitter [115], where either one of the single photon detectors correspond to a 0 or 1 bit, a beam of photons going through a polarizing beamsplitter [116], which effectively obtains random data from polarization, and randomness generation based on photon arrival time [117]. There are more DV systems, however, in most cases they rely on single-photon effects, which become a limiting factor on the maximum achievable bandwidth, where usual single photon generation rates in QDs are in the MHz range [118, 119].

CV-QRNG rely on continuous measurement outcomes, which then are mostly limited by the bandwidth of measurement devices; therefore CV-QRNG with bandwidths higher than 100 Gbps have been demonstrated [120, 121]. Some examples include measurement of vacuum fluctuations using homodyne detection [122], laser phase fluctuations [123] and fiber amplified spontaneous emission [124]. Covering all these methods is out of scope of this thesis. Since in this thesis the QRNG was implemented using vacuum fluctuation measurements, that will be the focus of the rest of the chapter text.

Vacuum Fluctuation QRNG

To elaborate on vacuum fluctuation measurements, first, light field quadratures have to be considered. A monochromatic solution to the wave equation can be written as [125]:

$$\boldsymbol{E}(\boldsymbol{r},t) = (\alpha(\boldsymbol{r})e^{-i\omega t} + \alpha^*(\boldsymbol{r})e^{i\omega t})\mathbf{p}(\boldsymbol{r}), \tag{2.18}$$

where ω is the wave frequency, t is the time, $\boldsymbol{r}$ is the position vector, $\mathbf{p}(\boldsymbol{r})$ is the polarization vector and $\alpha(\boldsymbol{r})$ is the amplitude, which can also be written as[125]:

$$\alpha(\boldsymbol{r}) = a_0(\boldsymbol{r})e^{i\phi(\boldsymbol{r})}, \tag{2.19}$$

where $a_0(\boldsymbol{r})$ is the field magnitude and $\phi(\boldsymbol{r})$ is the phase. If a plane wave is considered which travels along the positive z-axis and that the wavevector is $k = \omega/c$, the solution to the wave equation becomes [125]:

$$\boldsymbol{E}(\boldsymbol{r},t) = 2\alpha_0\cos(kz-\omega t)\mathbf{p}(\boldsymbol{r}). \tag{2.20}$$

Based on this equation, the following quadratures can be used [125]:

$$q(\boldsymbol{r}) = \alpha_0(\boldsymbol{r}) + a_0^*(\boldsymbol{r}), \tag{2.21}$$

$$p(\boldsymbol{r}) = -i(\alpha_0(\boldsymbol{r}) - a_0^*(\boldsymbol{r})). \tag{2.22}$$

Then, if the phase is defined as follows:

$$\phi_0(\boldsymbol{r}) = \tan^{-1}\left(\frac{p(\boldsymbol{r})}{x(\boldsymbol{r})}\right), \tag{2.23}$$

the monochromatic wave equation solution can be defined as [125]:

$$\boldsymbol{E}(\boldsymbol{r}, t) = E_0(x(\boldsymbol{r})\cos(\omega t) + p(\boldsymbol{r})\sin(\omega t))\mathbf{p}(\boldsymbol{r}), \tag{2.24}$$

where in this case x quadrature denotes the amplitude and p quadrature denotes the phase of the light field.

If the quantum mechanical picture is considered and light is quantized and considered as a quantum harmonic oscillator, the Hamiltonian is [125]:

$$\hat{H} = \sum_l \hbar\omega_l \left(\hat{a}_l^\dagger \hat{a}_l + \frac{1}{2}\right), \tag{2.25}$$

where ℓ is a positive integer denoting mode number, ω_l is the mode frequency, $\hat{a}$ is the annihilation operator and $\hat{a}^\dagger$ is the creation operator. From this and from the classical light field quadrature definitions in Eqs. 2.21 and 2.22, the position and momentum quadrature operators can be defined [125]:

$$\hat{x}_l = \sqrt{\frac{\hbar}{2\omega_l}}\left(\hat{a}_l + \hat{a}_l^\dagger\right), \tag{2.26}$$

$$\hat{p}_l = -i\sqrt{\frac{\hbar}{2\omega_l}}\left(\hat{a}_l - \hat{a}_l^\dagger\right),. \tag{2.27}$$

They can also be defined as /dimensioneless variables:

$$\hat{X} = \frac{1}{\sqrt{2}}\left(\hat{a} + \hat{a}^\dagger\right), \tag{2.28}$$

$$\hat{P} = -i\frac{i}{\sqrt{2}}\left(\hat{a} - \hat{a}^\dagger\right). \tag{2.29}$$

These quadrature operators are the analog to the harmonic oscillator position and momentum operators. Therefore, these operators are defined as position and momentum quadratures respectively.

Finally, if Fock states are considered and the same position and momentum quadrature definitions are used, it can be shown that even with the Fock state $|0\rangle$, corresponding to no light, the uncertainty is [126]:

$$\Delta X \Delta P \geq \frac{1}{2}, \tag{2.30}$$

which also results in the variances being non-zero $(\Delta X)^2 = (\Delta P)^2 = 1/2$. Therefore, even without photons present, the vacuum field fluctuates, which is expected, since otherwise the uncertainty principle would be broken [126].

2.5.3 Vacuum Fluctuation Measurement

Based on the previous section, if the quadratures of the vacuum field fluctuations can be measured, they can be utilized for CV-QRNG. This can be done by either homodyne or heterodyne measurement schemes. Balanced homodyne detection is fundamentally based on the interference between a weak optical signal and a strong phase-stable local oscillator (LO) field. When these two fields are combined on a 50:50 beam splitter, their optical amplitudes interfere at the two output ports. The intensities of these two output fields are measured with photodiodes, and the corresponding photocurrents are subtracted, resulting in an effectively amplified signal measurement [127]. An example balanced homodyne detection set-up can be seen in Fig. 2.10. In the case of vacuum fluctuations, signal input is left blocked, which effectively measures the amplified vacuum signal.

The simplified interference process of the homodyne detection can be described in terms of field operators as follows [128]. Let the annihilation operators of the signal and local oscillator modes incident on the beam splitter be $\hat{a}_{\text{sig}}$ and $\hat{a}_{\text{LO}}$. For a 50:50 beamsplitter, the outputs $\hat{b}_1$ and $\hat{b}_2$ are:

$$\hat{b}_1 = \frac{1}{\sqrt{2}} \left(\hat{a}_{\text{sig}} + \hat{a}_{\text{LO}} \right), \qquad \hat{b}_2 = \frac{1}{\sqrt{2}} \left(\hat{a}_{\text{sig}} - \hat{a}_{\text{LO}} \right). \tag{2.31}$$

Each output is detected by a photodiode, and the measured photocurrents are proportional to the respective photon number operators,

$$\hat{i}_1 \propto \hat{b}_1^\dagger \hat{b}_1, \qquad \hat{i}_2 \propto \hat{b}_2^\dagger \hat{b}_2, \tag{2.32}$$

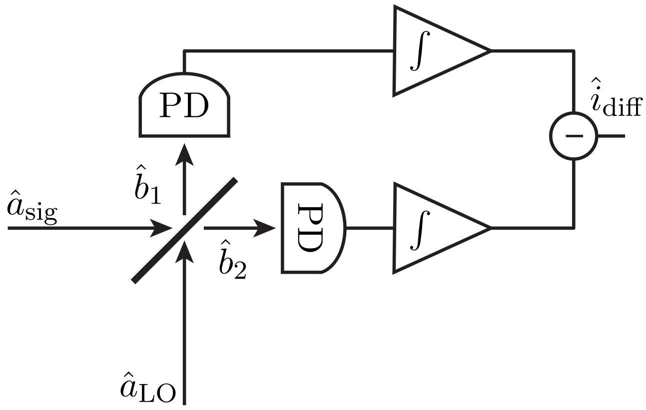

Figure 2.10: Schematic of a balanced homodyne detection setup. The weak signal field $\hat{a}_{\mathrm{sig}}$ and a strong local oscillator $\hat{a}_{\mathrm{LO}}$ interfere on a 50:50 beam splitter, producing output fields $\hat{b}_1$ and $\hat{b}_2$. Each output is detected by a photodiode (PD), integrated, and the corresponding photocurrents are subtracted to yield the difference current $\hat{i}_{\mathrm{diff}}$.

The difference photocurrent is then

$$\hat{i}_{\mathrm{diff}} \propto \hat{b}_1^\dagger \hat{b}_1 - \hat{b}_2^\dagger \hat{b}_2 = \hat{a}_{\mathrm{sig}}^\dagger \hat{a}_{\mathrm{LO}} + \hat{a}_{\mathrm{LO}}^\dagger \hat{a}_{\mathrm{sig}}. \tag{2.33}$$

If the local oscillator is much stronger than the signal, its quantum fluctuations are negligible and it can be approximated as a classical coherent field $\hat{a}_{\mathrm{LO}} \approx \alpha_{\mathrm{LO}} e^{i\theta}$, where α_{LO} is amplification and θ denotes the LO phase relative to the signal. Substituting into Eq. 2.33 gives:

$$\hat{i}_{\mathrm{diff}} \approx \alpha_{\mathrm{LO}} \left(\hat{a}_{\mathrm{sig}} e^{-i\theta} + \hat{a}_{\mathrm{sig}}^\dagger e^{i\theta} \right) = \sqrt{2}\, \alpha_{\mathrm{LO}}\, \hat{X}_\theta, \tag{2.34}$$

where the substitution in the parentheses is done by using the generic quadrature definition [125]:

$$\hat{X}_\theta = \frac{1}{\sqrt{2}} \left(\hat{Q} \cos(\theta) + \hat{P} \sin(\theta) \right) = \frac{1}{\sqrt{2}} \left(\hat{a} e^{-i\theta} + \hat{a}^\dagger e^{i\theta} \right). \tag{2.35}$$

Heterodyne measurement, which is used to implement the QRNG covered in this thesis, works in a similar principle, except it allows for measuring both quadratures at the same time by implementing another beamsplitter with a 90° phase shift between the two paths. This then effectively measures the other quadrature since the definition of the general momentum quadrature is the position quadrate phase shifted by 90° [129]:

$$\hat{P}_\theta = -\frac{i}{\sqrt{2}}\left(\hat{a}e^{-i\theta} - \hat{a}^\dagger e^{i\theta}\right). \tag{2.36}$$

An example of heterodyne set up and a more in depth discussion can be found in Chapter 6.

2.5.4 QRNG Security and Extraction

Even though measuring quantum states provides non-deterministic, random outcomes, the actually measured results are not fully secure due to the devices that are used for measurement. In terms of vacuum fluctuation measurement using either homodyne or heterodyne measurement schemes, the insecurities arise primarily from source (laser) and measurement (photodiodes) device imperfections. Lasers can have classical intensity fluctuations and photodiodes have intrinsic, classical, electrical noise, which is theoretically predictable. Moreover, if an attacker has access to the system, it could be potentially manipulated in producing deterministic random numbers.

For this reason, an essential component of QRNGs is the underlying security model, which accounts for practical imperfections and assumptions to varying degrees. First, there is the device dependent model, in which case it is assumed that both the source and the device are not manipulated in any way and only classical noise limits the QRNG quality [130]. One such example is the homodyne measurement of vacuum fluctuations [122]. A more secure model is semi-DI, where either the source, measurement, or both devices are characterized and their impact on the QRNG security is considered, either by self-testing or calibration procedures [130, 131]. One example of semi-DI is the QRNG investigated in this thesis, in which the measurement device is characterized and considered to be safe. Lastly, there is the full DI model, where both the source and measurement devices are fully-untrusted and QRNG quality is ensured by continuous self-testing, providing guarantees that outside parties cannot predict the output. The DI security model relies on realizing the Bell test; specifically two entangled photon states are measured independently in independently chosen measurement basis. Local hidden variable theories indicate that there is a bound for correlation between the two entangled state measurements. If this bound is broken, it shows that the correlation cannot be explained by classical deterministic mechanisms, indicating true randomness [132]. Therefore, by using this condition, usually in the form of Clauser-Horne-Shimony-Holt game [132], continuous self-testing guarantees that true randomness is being output.

While full DI provides guaranteed security, due to requiring entangled photon pairs and continuos self-testing, the implementation is both complicated and has low bandwidth, up to tens of kbps [132, 133]. On the other hand, trusted device protocols provide bandwidths up to Gbps/s [120, 121]. However, the QRNG is insecure and cannot be used to safety sensitive applications. Semi-DI, in particular source-DI provides a middle ground, where bandwidths of Gbps can be achieved while being more resistant to tampering [131].

The measured random data also needs to be conditioned, especially in the cases of CV-QRNG. The raw random data has a Gaussian probability distribution, which, while theoretically random, makes it significantly easier to guess the values compared to a uniform distribution. Therefore, hashing algorithms have to be applied in order to extract the random data from the raw measurement values. The parameters of extraction depend on the previously discussed security models, which determine how much random data can be extracted without affecting the security of the random numbers [130]. This is quantified by minimum entropy H_{min}, which determines how many bits per sample can be extracted. Further discussion and calculations can be found in Chapter 6.

3

Methodology

In this chapter, the concepts and procedures for the experiments are covered, aiming to explain the experimental techniques and the set-ups used for performing the experiments. This chapter will mostly cover the experimental procedures of QD samples, since for the QRNG the set-up and the measurement methods are explained in the publication seen in Chapter 6. The first few sections cover the concepts behind the measurements and the rest covers the actual experimental set-up and how it is used.

3.1 Time-Resolved Faraday Rotation

When linearly polarized light propagates through a magneto-optic medium in the presence of a magnetic field aligned along the direction of propagation, the plane of polarization is rotated. This phenomenon, known as the Faraday effect (or Faraday rotation), arises because the magnetic field induces circular birefringence: the medium acquires different refractive indices for right- and left-circularly polarized components, causing a relative phase shift between them [134]. The recombination of these two components at the exit yields a rotated linear polarization, since linearly polarized light can be formed from a superposition of σ^+ and σ^- polarization. The rotation angle Δ_F is proportional to the magnetic field B and to the path length d through a medium:

$$\Delta_F = \frac{VBd}{\mu_0} \tag{3.1}$$

where V is the Verdet constant which denotes how strong is the Faraday effect in a medium and μ_0 is the vacuum permeability.

The Faraday effect also applies to QD spin polarization. A particle with non-zero spin has a magnetic moment. If in an ensemble the spins are aligned randomly, with an effectively equal amount of spin up and spin down orientations, the net magnetic moment is zero. However, if the spins are aligned in a single direction, the effective magnetic moment is increased, which means that there is an effective magnetic field [135]. Therefore, if a QD ensemble sample is placed in a Voigt geometry magnetic field and the spins are polarized using circularly polarized light, there is an effective magnetic field in the sample that rotates. Therefore, if another light pulse were to travel through the sample after excitation, it would change the polarization of the light depending on the state of the spin polarization of the sample.

A more complete description arises when considering optical selection rules. When a population of resident carriers with aligned spins is already present, optical transitions that would create an exciton with a parallel spin orientation to the resident carrier become forbidden due to the Pauli exclusion principle. Consequently, only one of the two circular polarization components (σ^+ or σ^-) can couple to the allowed transition. When a linearly polarized probe pulse containing equal σ^+ and σ^- components is incident on a spin polarized ensemble, the two components experience different refractive indices. This induces a spin-dependent phase shift between them, which manifests as an effective rotation of the linear polarization plane of the transmitted light [136].

This is called time-resolved Faraday rotation and it is the basis of pump-probe measurement. In the case of this thesis, for measuring the QD samples, a variable wavelength (in the telecom C band range) pulsed laser (repeition rate of 76 MHz) is used to first pump the sample by initializing spins of resident carriers with circularly polarized light and then probe with a delayed linearly polarized pulse. This is achieved by using a 90:10 beamsplitter (90 % for pump to ensure maximum spin polarization) to split the beam into two paths, where the pump path then goes into a mechanized delay line with micrometer positional accuracy to vary the delay between the pump and probe pulses. If the delay line is scanned, the result shows the change of spin polarization in time due to the probe pulse polarization being rotated in different points of time by Faraday rotation. This allows to fit Eq. 2.12 with either the Gaussian or exponential dephasing, depending on the system, which in turn enables examination of the spin properties of the QDs.

In the case of this thesis, Faraday ellipticity rather than rotation is used for measuring the QD samples. The main difference lies in that the imaginary parts of the refractive indices are different for left and right circularly polarized light, which results in different absorption coefficients. The outcoming light then becomes elliptically polarized, with varying degrees of ellipticity depending on the magnetic field strength (or spin polarization), which is then measured to obtain the sample spin dynamics.

3.2 Hanle Effect Measurement

The Hanle effect was regarded first as a semi-classical effect which shows how scattered light changes polarization when a magnetic field in Voigt geometry is applied, and was explained by using damped spatial oscillator models [137]. The quantum mechanical explanation of the Hanle effect is the same as of spin precession in Section 2.3.2, except in this case it applies to an ensemble of spins which have an increasing precession frequency as the magnetic field strength increases, where the frequency increase causes dephasing between the spins, resulting in the reduction of polarization. The spin polarization dependency on magnetic field has a Lorentzian shape that depends on the spin dephasing time [24]:

$$S_z(B) = \frac{S_z(0)}{1 + (\omega_L T_2^*)^2}. \tag{3.2}$$

The Hanle effect allows the measurement of the intrinsic spin dephasing times of QDs in samples. Firstly, the Hanle effect itself can be measured by measuring the spin polarization while scanning the magnetic field just before the sample is excited again by a pump pulse. The reason for measuring just before the pump pulse is to avoid any transient effects, such as exciton recombination and to only measure the resident carriers. Then, the dephasing time can be extracted by [138]:

$$T_s = \frac{\hbar}{g_e \mu_B B_{\text{HWHM}}}, \tag{3.3}$$

where B_{HWHM} is the half width at half maximum (HWHM) of the Hanle curve and in this case the dephasing is denoted as T_s since it is not the intrinsic dephasing that is being measured, as the sample is excited by a pump pulse. To extract the intrinsic dephasing, the measurements have to be repeated at different pump powers, the dephasing times extracted and then a linear fit with an exptrapolation to zero pump power is done to obtain the intrinsic dephasing value. While this can also be done using pump-probe Faraday rotation measurements, this allows more accurate measurement of the dephasing values at zero magnetic field, since with pump-probe, the delay line is usually not long enough to fully observe the dephasing.

3.3 Polarization Recovery Curve (PRC)

PRC is similar to the Hanle effect measurements in the sense that it is also measures spin polarization just before the excitation pump pulse while sweeping the magnetic field. The main difference is that in this case the magnetic field is in Faraday geometry. In this case, the opposite effect is observed, where the spin polarization increases as the magnetic field increases due to the fact that the spins become increasingly decoupled from the different dephasing mechanisms, since the Faraday geometry aligns and stabilizes the spin along the external field direction.

PRC is useful for two primary purposes: determining the type of the resident carriers in the QD sample and investigating the nuclear spin interaction strength with the charge carriers. In terms of resident carriers, since electrons have a strong hyperfine coupling constant, as the magnetic field tends towards zero, hyperfine interactions start to affect electrons at larger magnetic field compared to holes, resulting in a V-like Lorentzian dip in the spin polarization when the resident carriers are electrons [139]. If it is holes, firstly, the dip HWHM becomes much more narrow compared to the electron because of weaker hyperfine coupling. Moreover, if a sample is p-doped, it means that positive trions are created upon excitation. Therefore, there is an additional component in this case because the unpaired carrier is an electron, which has stronger hyperfine coupling, which means that initially the spin polarization rises as the magnetic field increases, but then starts to decrease due suppresed trion spin relaxation causing decreasing spin generation rate, resulting in an effective M-shape of the PRC [140]. An illustrated example can be seen in Fig. 3.1. The simulated PRCs in Fig. 3.1 are generated from two components: one for the resident carrier and one for trion-mediated spin generation, each written as a baseline plus a Lorentzian field response:

$$L(|B|, B_0) = \frac{|B|^2}{|B|^2 + B_0^2}, \qquad |B| = \sqrt{B^2}, \tag{3.4}$$

and write every component as:

$$S(B) = S_0 + A\,L(|B|, B_0), \tag{3.5}$$

where S_0 is the zero-field baseline, A is the Lorentzian amplitude, and B_0 controls the width. The total PRC is

$$S_d^{(\mathrm{tot})}(B) = S_d^{(\mathrm{res})}(B) + S_d^{(\mathrm{trion})}(B), \tag{3.6}$$

with $d \in \{n, p\}$. The parameter sets directly match the code:

Table 3.1: Model parameters used to generate the simulated polarization recovery curves. Baselines S_0 and amplitudes A are dimensionless; B_0 is in mT.

Dopant	$S_0^{(\mathrm{res})}$	A_{res}	$B_{0,\mathrm{res}}$	$S_0^{(\mathrm{trion})}$	A_{trion}	$B_{0,\mathrm{trion}}$
n	0.33	0.67	35	0.0	−0.05	110
p	0.33	0.67	20	0.0	−0.30	110

Evaluating Eqs. (3.5)–(3.6) with the parameters above for $B \in [-300, 300]$ mT yields the dashed resident/trion curves and the solid total PRCs plotted in Fig. 3.1.

PRC in conjunction with Hanle curve can be used to investigate how nuclear spin dynamics affect the carriers in a semiconductor sample, in this case being QDs. By normalizing both the PRC and Hanle curves using the maximum value of the PRC and then plotting them together, the curve widths and where they meet can determine the hyperfine interaction mechanism [141]. Since both curves show how the hyperfine interaction governs spin dephasing in complementary magnetic field geometries, their properties can be used to interpet the timescales of nuclear spin precessions and hyperfine interaction anisotropy [141]. More details on the different cases and interepretations is provided in Chapters 4 and 5.

3.4 Spin Inertia

When measuring spin polarization in Faraday geometry, the normal pump-probe measurement technique is not enough, since, as mentioned in Section 2.4.3, the T_1 times are in the microsecond range, whereas with a 1-meter delay line, only a several nanosecond timescale can be measured (more details in Section 3.5). Spin inertia is a measurement technique that uses pump pulse modulation between σ^+ and σ^-.

When the T_1 time is in the range of microseconds and the pump is modulated at, for example, 10 kHz between σ^+ and σ^-, the spins are first initialized by σ^+ and then the spins still have enough time to relax to equilibrium before the σ^- pump initializes them to the opposite spin. However, as the modulation frequency gets closer to the T_1 time, not all spins are relaxed back to equilibrium and therefore at σ^- polarization not all the spins are reinitialized due to Pauli exclusion principle and so the spin polarization signal ends up being reduced. This behavior is similar to a low-pass filter which has a dependency on the T_1 time and can be described by [139]:

$$S(f_m) = \frac{S_0}{\sqrt{1 + (2\pi f_m T_s)^2}}, \tag{3.7}$$

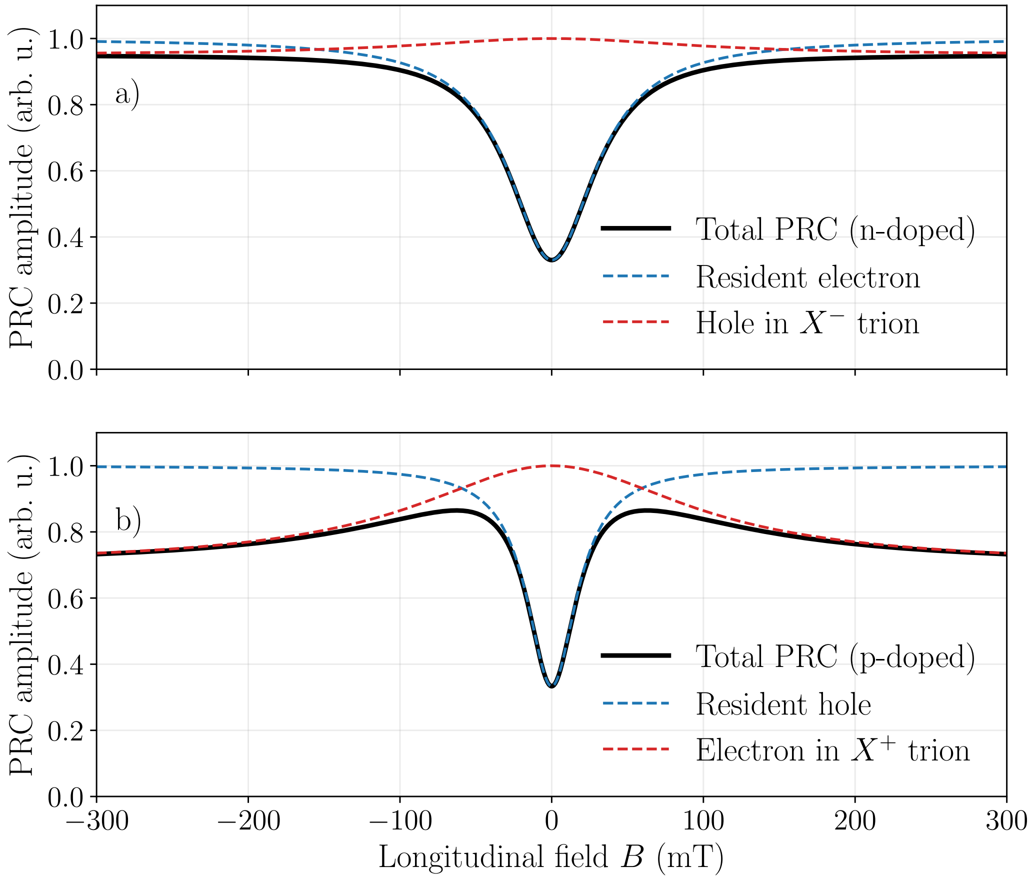

Figure 3.1: Illustrative polarization recovery curves (PRCs) for n- and p-doped quantum dots.(a) For n-doped dots, excitation via the negative trion (X^-) yields a V-shaped PRC. The resident electron spin (blue, dashed) undergoes hyperfine-induced dephasing that is suppressed by the longitudinal magnetic field, while the unpaired hole in the trion (red, dashed, corresponds to spin generation rate) shows only weak field dependence. Their superposition (black, solid) gives the recovery of spin polarization characteristic of resident electrons. (b) For p-doped dots, excitation via the positive trion (X^+) produces an M-shaped PRC. The resident hole (blue, dashed) exhibits a narrow dip due to weak hyperfine coupling, whereas the unpaired electron in the trion (red, dashed, corresponds to spin generation rate) experiences strong, hyperfine coupling that suppresses the spin generation rate with increasing field. The resulting total signal (black, solid) shows a dip at intermediate fields, characteristic of hole resident carriers [139]. The data shown here is simulated using Eqs. 3.4 - 3.6 with parameters taken from Table 3.1.

where f_m is the modulation frequency and T_s corresponds to the T_1 time, but not the intrinsic value. To extract the intrinsic T_1 time, a pump power sweep has to be done and then the T_1 time can be obtained by extrapolating to zero pump power, which then gives the real T_1 time of the QDs. Higher pump powers cause lattice heating and transient population of excitons and trions, which affect the resident carrier spin.

3.5 Set-up

The full set-up for measuring the QD samples can be seen in Fig. 3.2. The following subsections will cover the set-up shown in this figure.

3.5.1 Excitation Lasers

One of the lasers used was the Coherent Verdi V18 which is a diode, frequency-doubled Nd:Vanadate laser. The maximum output power of the laser is 18 W and the output wavelength is 532 nm. The pump laser was set to 14 W during measurements. The laser pumps the Coherent Mira-HP, which is a Ti:Sapphire oscillator which was used to convert the continuos wave (CW) pump laser into pulsed light. The Mira-HP was used in picosecond pulse regime, in which case the pulse width is approximately 2 ps and the maximum achievable power is 3.5 W. The picosecond regime was used since we are measuring QD ensembles; therefore a more narrow width in frequency domain is preferred to limit the distribution of QDs excited. The oscillator wavelength can be tuned in the range of 700-1000 nm and it was set to 835 nm. The repetition rate of the Mira-HP is 76 MHz, which corresponds to 13.2 ns separation in time between pulses.

Since telecom C-band QD samples were measured, the pulsed laser light from the Mira-HP is directed to the APE optical parametric oscillator (OPO) PP Automatic. The oscillator operation is based on converting modelocked Ti:Sapphire pulsed light to telecom range wavelengths by using a periodically poled nonlinear crystal. The OPO can either be used in a linear or ring cavity configurations. In the case of the measurements in this thesis, the OPO was used in the linear cavity configuration. In this configuration, the Ti:sapphire pump pulses drive a folded five-mirror linear OPO cavity containing a periodically poled nonlinear crystal, Brewster windows, and dispersion plates. Inside the crystal, the $\chi^{(2)}$ interaction converts pump photons into lower-energy signal and idler photons through optical parametric down-conversion.

With the 835 nm Mira-HP pump laser, the tuneable wavelength range of the OPO was 1400-

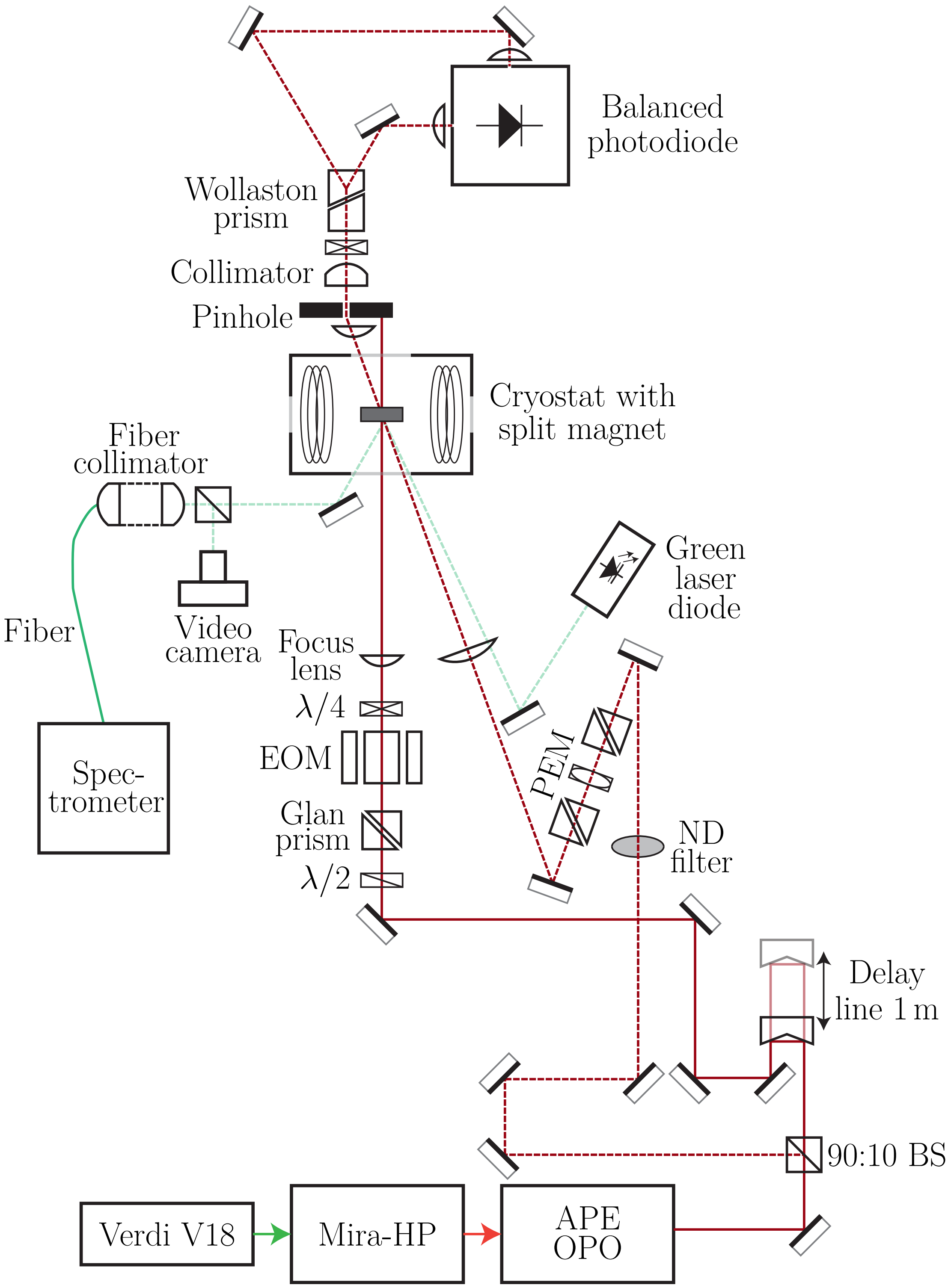

Figure 3.2: Schematic of the pump-probe Faraday ellipticity setup.

1600 nm, with an output power of 0.5 W. The spectral width of the OPO was 2 nm, which corresponds to approximately 1.66 ps pulse duration with a wavelength of 1500 nm. It should be noted that while even though the threshold power for the OPO is only 0.5 W, high power pump laser and oscillator are used to ensure that there is enough power for the full optical set-up.

3.5.2 Pump-Probe Path

As already mentioned in Section 3.1, the measurements were done using the pump-probe method based on time-resolved Faraday rotation. The laser beam from the OPO first goes into a 90:10 beamsplitters, where the 10 % beam is considered the probe path (dark red dashed line in Fig. 3.2) and the 90 % beam is considered the pump path (dark red solid line in Fig. 3.2). The pump path needs more power since it is both useful for power sweep measurements and also to ensure that there is enough power for measurements such as SML. Probe path needs less power since it only measures the polarization of the spins and also higher probe powers can also cause excitation of the QDs, which can have unintended effects on the measurements.

Pump Path

The pump path (dark red solid line in Fig. 3.2) first goes into the mechanized delay line (OWIS, LIMES 170, 1000 mm), which has micrometer movement resolution, corresponding to $2l/c \approx$ 6.7fs time resolution and the total duration covered by the delay line is 6.7 ns, where the factor of two is added because the delay line uses retroreflection, which doubles the effective length. However, with the way the full path is set-up, at the 0.503 m point the pump and probe delays overlap, so it results that in total the length that the duration that the delay line covers is 3.35 ns into the positive or negative delay directions.

After the delay line, first the pump pulse goes to a $\lambda/2$ waveplate and then into a Glan prism. The $\lambda/2$ waveplate is attached to a rotation stage so that the pump pulse could be adjusted between s and p-polarization linear polarization axes where then the Glan prism only lets through s-polarized light. This combination serves a dual purpose: first to adjust the pump power for power sweep measurements, second to have only s-polarized light.

From the Glan prism the linearly polarized light then goes through a electro-optic modulator (EOM) (Linos LM0202 IR P, with a wavelength range of 950-1100 nm, works also at higher wavelengths, but with reduced transmission) after which a $\lambda/4$ waveplate follows. The EOM uses an electro-optical crystal with controlled birefringence, which change the linear polarization of the transmitted light as the voltage is applied to the crystal. For measuring, the EOM was connected to a pulse amplifier (Linos DIV 20) which was set to produce a square wave output corresponding to orthogonal linear polarizations. The modulation frequency can be tuned between 1 kHz and 2.2 MHz. Then the $\lambda/4$ waveplate was rotated to match the orthogonal polarizations of the EOM, which then produces σ^+ and σ^- light pulses at the set modulation frequency. Modulation is necessary for some of the measurement methods, as detailed in Section 3.4, and it also helps with removing noise and background light from the signal. The pulse amplifier reference frequency signal was connected to the lock-in amplifier (Zurich Instruments HF2LI) for demodulation. Demodulation is explained in more detail in following text.

Lastly, the modulated light goes through a focusing lens which produces an approximately 150 μm beam spot on the sample. The focusing lens is placed on a three-dimensional translation stage to adjust the overlap with the probe spot and to adjust the focus on the sample. The overlap is crucial to obtain Faraday rotation, since the probe pulses have to pass through the same pump excited QD ensembles.

Probe Path

In the probe path (dark red dashed line in Fig. 3.2), the pulses first go through an neutral density (ND) filter to adjust the appropriate probe power without causing additional excitation. Then, the attenuated light goes through a Glan prism to have only linearly polarized light. It then passes through the photoelastic modulator (PEM) (Hinds Instruments PEM 100), which oscillates between linear, elliptical and circular polarizations by electrically oscillating a piezoelectric transducer which creates stress in a crystal, creating oscillating birefringence. The modulation was set to 84 kHz and the reference frequency was connected to the lock-in amplifier. Then, from the PEM, the light goes through another Glan prism, which is aligned to the same axis as the linear polarization of the light coming out of the PEM, which results in intensity modulated light. Lastly, the beam goes through a focusing lens, which focuses it on the sample to a 100 μm diameter. The probe beam diameter is smaller to ensure that even with vibrations of the system, there would still be overlap between pump and probe.

3.5.3 PL and Imaging Path

Next to the PEM, there is a green laser diode placed, which first goes through a mirror (green dashed path in Fig. 3.2) that was adjusted to make sure that the beam uses the same focusing lens as for the probe path. The green laser is used to obtain the PL of the sample, which is collected by placing a mirror right by the cryostat window, which then directs the PL into a beamsplitter where one of the paths is to a monochromator (Princeton Instruments Acton SP2300) with a grating size of 600 l/mm. The beamsplitter is also directed at a video camera, which was used for imaging by illuminating the sample by an external halogen lamp. Imaging was primarily used for overlapping the pump and probe beams and also for seeing which sample was being measured. The pump-probe overlap was done on a special sample which has second harmonic generation, allowing for the telecom beams to be observed on the camera.

3.5.4 Cryostat

To cool down the QD samples, an Oxford Instruments SM4000-8 liquid helium bath cryostat was used. Inside the magnet, there is superconducting split magnet from two of the cryostat sides that applies a magnetic field along a single direction. The split magnet configuration allows for ensuring a homogeneous magnetic field while also leaving a free optical pathway for transmission measurements. The cryostat can be cooled down to 2.2 K with additional pumping, however, that was not necessary for these measurements since 6 K is enough to avoid significant thermal phonon coupling to the carriers. The magnetic field can be raised up to 8 T, but fields up to 4 T were used, since dephasing times at that point already become short. The magnetic field was controlled by a dedicated superconducting magnet power supply (Oxford Instruments 120-10).

The cryostat consists of the outer vacuum layer which is usually in the 10^{-6} mbar range, the middle layer with a liquid nitrogen bath, an inner layer with the liquid helium bath and finally a chamber for the experimental insert. A variable temperature insert (VTI) is placed into the insert, which is separated from the rest of the cryostat with a vacuum. A VTI allows temperature control by regulating the liquid helium flow to the sample with a needle valve and by a dedicated heater. Both the heater and the helium flow were controlled by a digital temperature controller (Oxford Instruments ITC 503S). On the end of the VTI, a sample holder is attached. The holder can house 4 samples in total, with one of the samples attached always being the second harmonic generation sample for pump-probe alignment use.

3.5.5 Detection

Once the pump and probe beams pass through the sample, the probe beam (dark red dashed line in Fig. 3.2) goes through a focusing lens and then through a micrcometer diameter pinhole. This ensures that the pump beam (dark red solid line in Fig. 3.2) does not make it into the detection path. Then, a collimator lens is used to minimize the beam divergence after the pinhole focusing lens. Finally, the beam goes through a $\lambda/4$ waveplate mounted on a rotation stage and then through a Wollaston prism, which separates σ^+ and σ^- polarization paths, where then the $\lambda/4$ waveplate is used to balance the paths before being measured by a high speed, telecom wavelength range balanced photodiode (Femto HBPR-450M-10K-IN). A Wollaston prism and $\lambda/4$ waveplate is used since Faraday ellipticity was measured. A change in the spin polarization results in a difference between the σ^+ and σ^- polarizations when they are balanced.

Since the probe modulation is done at 84 kHz, the demodulation is done at 168 kHz. This is because if the $\lambda/4$ waveplate is rotated to 45° (determined by the balancing of sigma σ^+ and σ^-, where the photodiode output is monitored with an oscilloscope and balance is found by finding minimum output current), the Faraday ellipticity is measured from the second harmonic. Since the pump is also modulated at 10 kHz (except for spin inertia measurements), the signal is detected at the difference frequency 158 kHz or the sum 178 kHz.

4

Spin properties in droplet epitaxy-grown telecom quantum dots

4.1 Preamble

This chapter reproduces the published manuscript on spin dynamics in droplet-epitaxy telecom-band InAs/InGaAs/InP quantum dots. The text, figures, and results are unchanged from the original paper. Only formatting, notation consistency, and layout adjustments have been applied so that the chapter fits the overall thesis style. Experimental measurements, data analysis and manuscript writing was done by me. Project conceptualization and initial setup was done by A. Greilich. Sample growth was done by E. M. Sala and J. Heffernan. Supervision, project management and manuscript editing was done by A. M. Fox, M. Bayer and A. Greilich. The corresponding publication is:

M. Cizauskas, E. M. Sala, J. Heffernan, A. M. Fox, M. Bayer, and A. Greilich, "Spin properties in droplet epitaxy-grown telecom quantum dots," *Phys. Rev. B*, vol. 112, p. 165412, Oct. 2025 [1].

4.2 Abstract

We investigate the spin properties of InAs/InGaAs/InP quantum dots grown by MOVPE deposition using droplet epitaxy, which emits in the telecom C-band. Using pump-probe Faraday ellipticity measurements, we determine electron and hole g factors of $|g_e| = 0.93$ and $|g_h| = 0.47$, with the electron g-factor being nearly twice as low as typical MBE SK grown samples. Most significantly, we measure a longitudinal spin relaxation time $T_1 = 3.0\,\mu s$, representing an order of magnitude improvement over comparable MBE SK grown samples. Despite significant electron g-factor anisotropy, we observed that it is reduced relative to similar material composition samples grown with MBE or MOVPE SK methods. We attribute this g-factor anisotropy and spin lifetime improvements to the enhanced structural symmetry achieved via MOVPE droplet epitaxy, which mitigates the inherent structural asymmetry in strain-driven growth approaches for InAs/InP quantum dots. These results demonstrate that MOVPE droplet epitaxy-grown InAs/InGaAcompresss/InP quantum dots exhibit favorable spin properties for potential implementation in quantum information applications.

4.3 Introduction

With the rapidly growing field of quantum computing, there is an increasing need of effective quantum network solutions. Currently, one of the significant problems in quantum networking is the decoherence of entangled states. When traveling a longer distance through a fiber, entangled states can get entangled with the environment, causing decoherence of the initial states [10]. One solution is satellite-based communication, which would allow for transmission distances of over 800 km [142, 143] across a wide range of wavelengths, spanning from visible light to telecom C band [144].

However, the preferred option is to use the already established telecommunication fiber network. In this case, quantum repeaters are needed to mitigate against loss. Unlike classic repeaters, quantum repeaters do not amplify the signal; rather they perform entanglement swapping at dedicated nodes [11]. To implement quantum repeaters effectively, quantum storage devices that can maintain coherence for an extended period are required to allow the stored quantum state to become entangled with a photon [145]. Telecom QDs are a good contender due to their efficient coupling to single-mode fibers (with additional nanostructures designed to couple to fibers) [146, 147]. It has been demonstrated that MBE-grown InAs/InAlGaAs quantum dots can have hole carrier coherence times of up to 0.4 μs [17].

Better coherence times can also be achieved by exploring different methods besides strain-driven QD growth modes, most often SK growth in the context of QDs. Using SK poses a challenge growing InAs dots on InP, since anisotropic indium diffusion causes these quantum dots to develop highly elongated shapes [49]. In contrast, quantum dots grown via MOVPE DE exhibit enhanced structural symmetry [148], resulting in longer optical coherence times [149]. Consequently, MOVPE droplet epitaxy grown InP quantum dots present more favorable characteristics for implementation in quantum repeater applications.

Telecom quantum dots have been successfully grown via MOVPE using both self-assembly techniques [150, 151] and DE [152, 53, 153] methodologies. InAs/InP QDs demonstrate exceptional single-photon purity [150, 151] at operational temperatures reaching 80 K [151], making them promising candidates for quantum optical applications. Comparative analyses indicate that MOVPE DE-fabricated InAs/InP quantum dots exhibit significantly enhanced coherence times relative to strain-based growth methods [53]. Additionally, experiments have shown the feasibility of quantum entanglement generation using MOVPE DE-grown structures [152], thereby expanding their potential use in quantum communication protocols. This paper aims to characterize the spin properties of InAs/InGaAs/InP quantum dots produced through MOVPE droplet epitaxy using a pump-probe measurement scheme to evaluate their potential applications and conduct comparative analyses with samples grown by other techniques.

4.4 Experimental details

The QD sample under study is grown by MOVPE on a (100)-oriented InP substrate in an Aixtron CCS 3x2" reactor. The sample's layer structure is presented in Fig. 4.2. None of the layers are intentionally doped. The QD density is approximately 10^{10} cm^{-2}. Measurements are performed on the central part of the wafer. The signal quality exhibits strong spatial dependence within the sample, possibly due to inhomogeneous QD distribution. For more details on the growth process, see Ref. [59].

The sample is placed in a helium bath cryostat with an electronic heater to control the temperature. A superconducting magnet inside the cryostat is used to apply magnetic fields. The magnetic field can be applied either longitudinally to the **k**-wavevector of light (Faraday geometry)

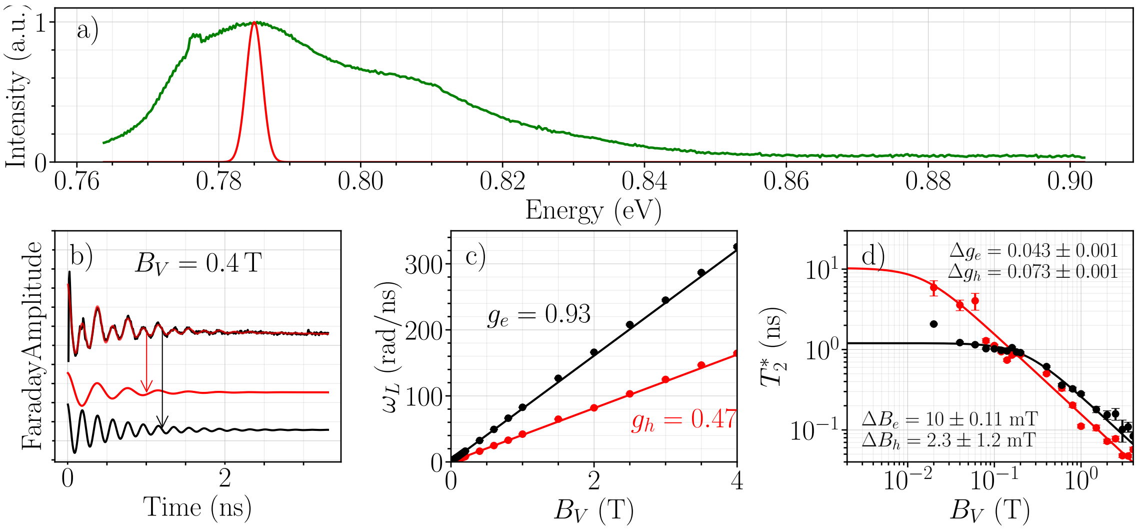

Figure 4.1: MOVPE droplet epitaxy grown InAs/InGaAs QD spin properties of carriers in transverse magnetic field. Excitation energy for all measurements is 0.785 eV. Measurements are done at 6K temperature, 20 mW pump power and 2 mW probe power. (a) Photoluminescence of the sample (green) and the excitation laser spectrum (red). (b) QD oscillatory behavior is displayed when a transverse magnetic $B_V = 0.4\,\mathrm{T}$ is applied and the Faraday ellipticity signal is measured. The black curve is the raw data, and the red curve is the fit. The red and black curves correspond to hole and electron contributions, respectively. (c) Larmor precession frequencies depending on the transverse magnetic field for electron (black) and hole (red). The g-factor calculated for both carriers is displayed in the plot. (d) Spin dephasing times as a function of transverse magnetic field. The calculated g-factor and B field spreads for each component are displayed in the top right.

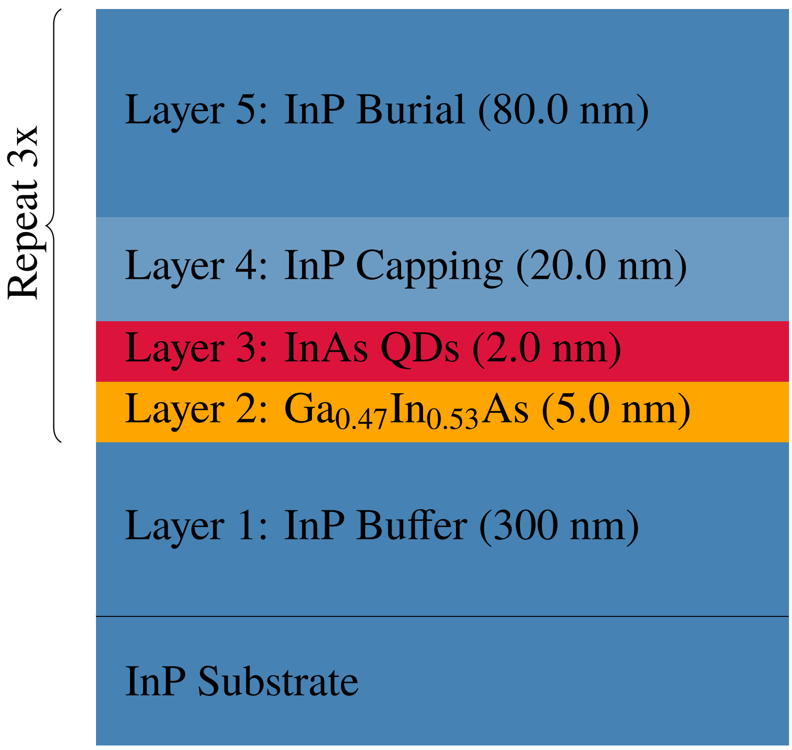

Figure 4.2: Layer structure of MOVPE droplet epitaxy grown InAs/InGaAs/InP quantum dots showing the substrate, buffer layer, and three repetitions of the quantum dot active region consisting of InGaAs interlayer, InAs QDs, InP capping, and InP burial layers.

or transverse (Voigt geometry) by rotating the sample relative to the magnet.

The sample spin dynamics are measured using a pump-probe method. The laser source is a Ti:Sapphire pulsed laser at 76.7 MHz repetition rate, pumping an optical parametric oscillator, which produces 2 nm wide 1.8 ps duration pulses with variable wavelength in the telecom C or L band. The pulses are split into two paths, pump and probe, where the probe path goes through a mechanized delay line for scanning delay. The beams are then focused to a diameter of 100 µm for the probe and 150 µm for the pump and overlapped at the sample.

The pump pulses are modulated between σ^+ and σ^- using an electro-optic modulator with a frequency range of 1 kHz to 2 MHz (10 kHz for all Voigt geometry measurements), while the probe pulses are modulated in intensity using a photoelastic modulator at 86 kHz followed by a Glan-Thompson polarizer. The circularly polarized pump pulses create the spin-polarized charge carriers in the sample, while the linearly polarized probe pulses are used to measure the spin polarization by the Faraday effect [135]. To reduce the possible amount of scattered pump light in the probe detection channel, a 10 µm pinhole was used to let through only the probe pulses. It is followed by a quarter-wave plate converting the circular components of the induced ellipticity into linear ones, a Wollaston polarizer separating the linearly polarized probe into two orthogonal linearly polarized components, which are then directed to the balanced photodiodes. The probe signal is demodulated at the difference modulation frequency and amplified by a lock-in amplifier.

4.5 Experimental results

Figure 4.1(a) shows PL of the sample at 6 K, which was obtained by exciting the sample with a laser diode at 2.33 eV photon energy. The pump excitation is done at the peak of the PL 0.785 eV [shown in Fig. 4.1(a) by a red Lorentzian] for two reason: to ensure that the smallest possible distribution of QD sizes is excited and because signal amplitude was highest, shown in Fig. 4.3(c). There is a larger amplitude peak at higher energies, however, at that point a larger distribution of dots would be excited, which would degrade the measured optical properties of the sample.

Figure 4.1(b) displays pump-probe QD spin polarization signal, measured by Faraday ellipticity, with an applied transverse magnetic field of 0.4 T. Measurements are done at 0.4 T since at this magnetic field strength the signal provides optimal signal clarity.

In the studied quantum dot ensemble, the oscillatory pump-probe signal originates from the coherent precession of resident carrier spins. When the pump pulse is resonant (or nearly resonant) with the trion transition, a circularly polarized excitation prepares a spin-polarized trion complex. After its rapid radiative recombination, one resident carrier (electron or hole, depending on the charge state of the dot) remains behind in a spin-polarized state. This trion-mediated initialization mechanism is well established in time-resolved Kerr and Faraday rotation studies of singly charged dots [154, 155, 135, 156]. Because the resident carrier lifetime exceeds both the trion and neutral-exciton lifetimes by orders of magnitude (see later in the text), the corresponding spin polarization survives on the nanosecond scale and dominates the long-delay oscillatory response. Thus, the signals we observe are the coherent dynamics of resident spins initialized via trion recombination [157, 158].

In this regime, the oscillatory response observed for an inhomogeneous QD ensemble can be decomposed into contributions from electron and hole spin precession with distinct Larmor frequencies. This additive description has been successfully employed in many ensemble experiments [159, 160, 65, 161]. Since the two spin species are initialized independently in different QDs by the trion mechanism and retain coherence over times much longer than the excitonic lifetime, fitting the data as a superposition of electron and hole oscillations provides a direct and reliable way to extract their g factors. We note that within the short sub-nanosecond lifetime of the neutral exciton, the electron-hole exchange interaction and fine-structure splitting require a pseudospin description [162]. However, because in our measurements the oscillations persist well beyond this time window, the observed signals can be unambiguously assigned to resident electron and hole spins.

Additionally, the observed decay is related to the spin dephasing, which is influenced by the inhomogeneity of the excited QD ensemble [135]. The Faraday ellipticity signal can therefore be fitted with the following equation:

$$S = \sum_i A_i \cos(\omega_i t) \exp\left(-\frac{t}{T^*_{2,i}}\right), \tag{4.1}$$

where i is the index for component, A_i is the amplitude of component, ω_i is the component Larmor precession frequency, and $T^{*2}_{2,i}$ is the component spin dephasing time. We can deduce that in Fig. 4.1, the red component corresponds to the hole and the black to the electron by the extracted values of the g factors. The g-factor of both can be calculated by following a linear relationship of Larmor precession frequency on the strength of the applied transverse magnetic field:

$$\omega_L = \frac{g\mu_B B_V}{\hbar}, \tag{4.2}$$

where ω_L is the Larmor precession frequency, μ_B is the Bohr magneton constant, B_V is the transverse magnetic field strength, and $\hbar$ is the reduced Planck constant. Figure 4.1(c) shows the frequency dependence on the transverse magnetic field strength. A linear equation is observed for both hole and electron, from which the g factors can be extracted using Eq. (4.2). We obtain $|g_e| = 0.93$ and $|g_h| = 0.47$. From these results, we attribute the respective electron and hole components [163, 65, 164]. This assignment can also be approached through the corresponding spin dephasing times. Since holes are less affected by the hyperfine interaction, they exhibit longer spin dephasing times [95], as further discussed in the following paragraph. At low magnetic fields, the component with the longer spin dephasing corresponds to $|g_h| = 0.47$ [see Fig. 4.1(d)]. Therefore the hole component can be attributed to the lower g-factor, while the electron component corresponds to the higher g-factor, consistent with its shorter spin dephasing times at low fields. It should be noted that the pump–probe measurement method employed here provides only absolute g-factor values. Consequently, the g factors obtained in this study, as well as all subsequent ones, are absolute.

Figure 4.1(d) displays the extracted spin dephasing times depending on the transverse magnetic field. Spin dephasing is affected mostly by the g-factor spread due to QD size and content inhomogeneity and by hyperfine coupling to the nuclear spins. The relationship between T_2^* and B_V is described by [17]

$$T_{2,i}^* = \hbar / \sqrt{(\Delta g_i \mu_B B_V)^2 + (g_i \mu_B \Delta B_i)^2}, \tag{4.3}$$

where Δg_i is the g-factor spread and ΔB_i is the magnetic field fluctuation spread, which quantifies the fluctuation of the nuclear spins. Figure 4.1(d) shows data that are fitted by Eq. (4.3). At magnetic fields below 0.1 T, the dephasing times are limited by the hyperfine interaction to nuclear spins. The data show that spin dephasing at low magnetic field is saturated at $T_{2,e}^* = 1.2$ ns for electrons and at $T_{2,h}^* = 10$ ns for holes. This is expected due to the nuclear interaction hyperfine constant of a hole being a magnitude smaller than for the electron [95]. This is further supported by the magnetic field spread values seen from the fit, which are $\Delta B_e = 10 \pm 0.11$ mT and $\Delta B_h = 2.3 \pm 1.2$ mT. At higher magnetic fields, contributions from g-factor spread become significant, causing the spin dephasing time to reduce. The g-factor spread values are $\Delta g_e = 0.043 \pm 0.001$ and $\Delta g_h = 0.073 \pm 0.001$.

It is seen that the electron g-factor spread is lower than that of the hole, which is expected, due to the smaller effective mass for the electron and the correspondingly broader wavefunction, leading to the spatial averaging of the inhomogeneities. For comparison, in the case of a coupled multi-layer MBE SK grown InAs QDs, despite the electron having a broader wavefunction, the g-factor spread of electrons was higher than that of holes. This is attributed to a higher probability of electron tunneling between the layers in the structure, due to its lower effective mass, providing a bigger variation of environment, causing increased g-factor spread [17]. In our sample, tunneling probability is greatly reduced due to barrier thickness of 100 nm, as opposed to 15 nm in Ref. [17].

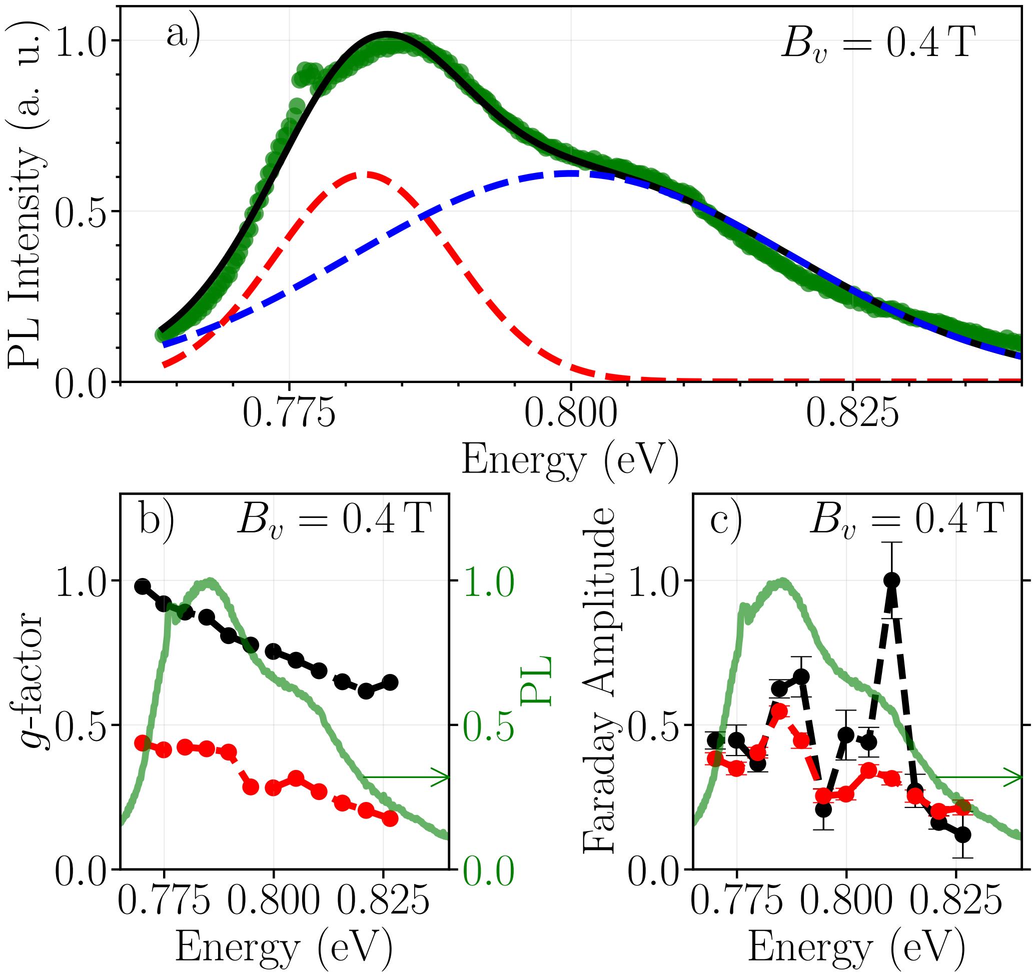

Figure 4.3: PL spectra, spectral dependence of g factors and Faraday ellipticity amplitudes at $B_V = 0.4\,\mathrm{T}$ of electron and hole components in MOVPE droplet epitaxy grown InAs/InGaAs QDs. Measurements are done at 6 K temperature, 20 mW pump power and 2 mW probe power. (a) PL spectrum of the sample (green markers) fitted with a bimodal distribution (black curve, with red and blue dashed curves showing components of the bimodal). (b) Absolute values of g-factor as a function of excitation energy for electron (black) and hole (red) components. The normalized PL spectrum is shown as a green line (plotted on the right axis). (c) Normalized Faraday ellipticity amplitudes for electrons (black) and holes (red) as a function of excitation energy.

The g-factor spread values are also lower for both components compared to the MBE SK sample, which is possibly caused by MOVPE DE grown samples having reduced QD size inhomogeneity. Figure 4.3 shows the PL of the measured sample with a bimodal distribution fit. Compared to the previously mentioned MBE SK samples, the spectrum appears to be similar [17, 65, 165]. It has been previously demonstrated that MOVPE for deposition results in a bimodal distribution of QD sizes [59, 60]. This is due to the fact that the smaller QDs grow first and then merge together to form larger ones [59, 60]. It may also be a consequence of stacking multiple layers of QDs, where a different layer may have a different distribution of QD sizes. Two different QD distributions can be further confirmed by looking at Fig. 4.3(c), which shows Faraday amplitude of carrier components measured at different excitation energies. It can be seen that there are two peak values for both electron and hole components.

Referring back to results in Fig. 4.1(c), if one compares our results to the grown InAs/InAlGaAs monolayer QD sample in Ref. [65], it shows more similar g-factor spread values of $\Delta g_e = 0.02$ and $\Delta g_h = 0.05$. Our sample exhibits a PL spectral width of approximately 19 meV for the narrower size distribution seen in Fig. 4.3(a) red curve and approximately 46 meV for the wider size distribution shown by the blue curve. The sample in Ref. [65] shows PL width of 60 meV, which is similar to our case if we combine the widths of both components, resulting in a width of 65 meV. Since the width of our PL is larger, it is expected that our g-factor spread values are also marginally larger.

The emission energy of a QD is dependent on its size, meaning that the g factors of components change due to different size QDs being excited at different energies [166, 167]. In similar QD samples, the electron g-factor decreases and the hole g-factor increases as the excitation energy increases [17, 65, 72]. In Fig. 4.3(b), it can be seen that the electron g-factor values follow what is seen in other QD samples, but for the hole, it differs. The explanation for that is that the magnetic field was not exactly along [001] direction [$\theta = 90°$ in Fig. 4.4(d)]. It has been theoretically shown that the hole g-factor demonstrates the same behavior as in our case when the magnetic field is applied along [011] direction [68]. S. A. Crooker demonstrates this experimentally with InGaAs/GaAs QDs [168], where by applying a magnetic field along the $[0\bar{1}1]$ instead of [011], the hole g-factor gradient inverts, which is in good agreement with our observed hole behavior.

Fig. 4.4(a) shows how the spin dephasing of electron and hole carriers changes as temperature changes. These results further confirm that we observe both an electron and a hole component in the previous measurements. It can be seen from the data that the dephasing time starts decaying for one of the components at 10 K (holes) and for the other at 20 K (electrons). The data were fitted

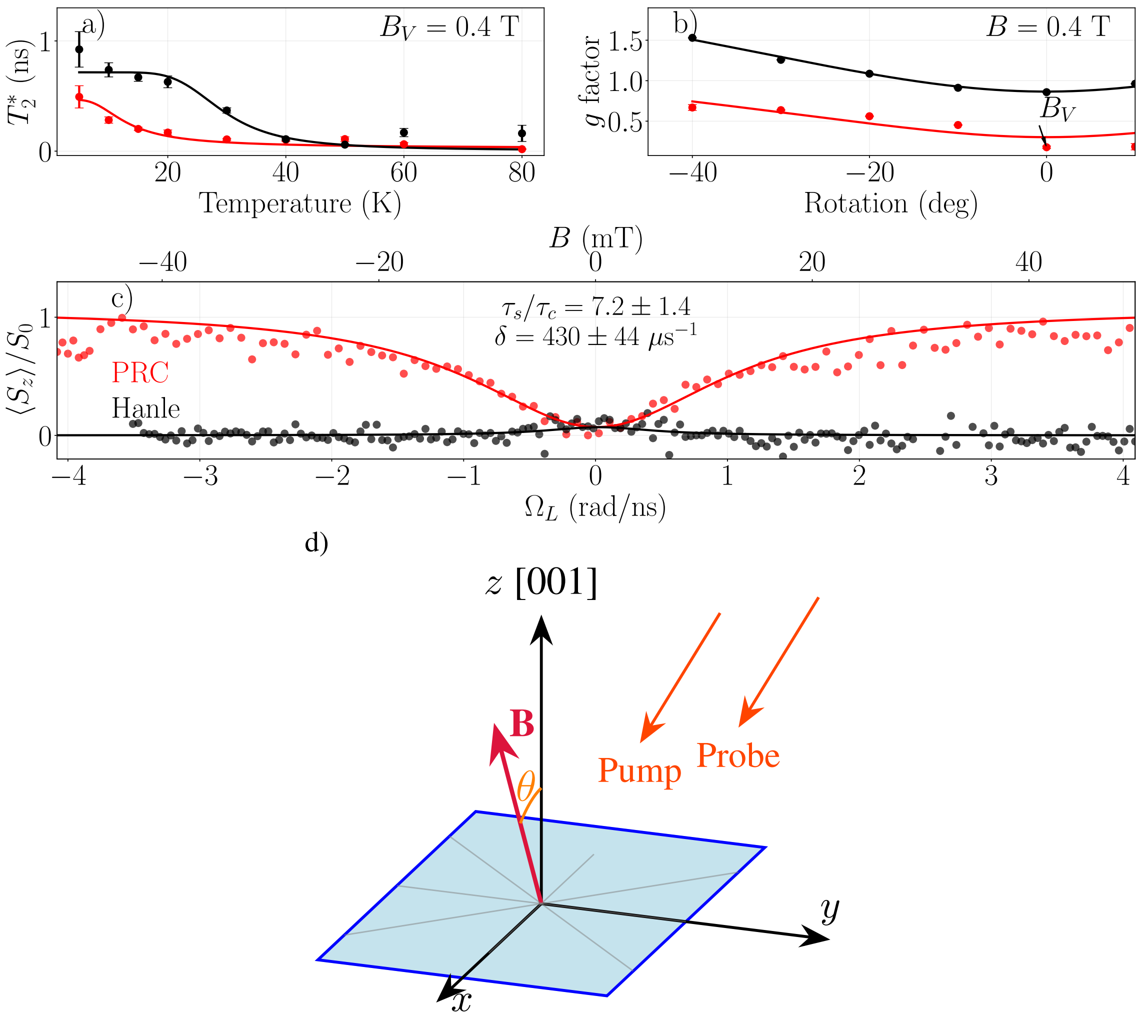

Figure 4.4: (a) Temperature dependence of spin dephasing times at a transverse magnetic field of 0.4 T for electrons (black) and holes (red), fitted with Arrhenius equation. (b) Anisotropy of g factors measured at $B = 0.4$ T as a function of magnetic field rotation angle. (c) Magnetic field dependence of electron spin polarization showing the polarization recovery curve (red) and Hanle effect (black). Measurements are done at 6 K temperature, 2 mW probe power, 17 mW pump power for PRC, and 15 mW for Hanle. The top axis shows the original measurement units. (d) Sample rotation geometry showing magnetic field B at angle θ relative to the [001] growth axis, enabling measurement of g-factor anisotropy between transverse and parallel orientations.

with Arrhenius equation [169]:

$$\frac{1}{T_2^*} = \frac{1}{T_g} + \frac{1}{T_e} \exp\left[-\frac{E_a}{k_B T}\right], \tag{4.4}$$

where T_g is the ground state relaxation time, T_e is the excited state relaxation time and E_a is the activation energy. The fit gives activation energies of 15 meV for electrons and 3.6 meV for holes.

It has been demonstrated in 900 nm (In,Ga)As/GaAs QDs that spin coherence for holes starts decaying at 10 and 20 K for electrons, since as temperature rises, elastic scattering processes that leverage the broad phonon sidebands are expected to significantly accelerate the deterioration of hole spin coherence [170]. However, while there is good agreement between our sample and the example in Ref. [170] in terms of when dephasing starts decaying, spin dephasing is only bounded by coherence times. Coherence does not have a direct influence on dephasing, and in the previously shown example, the coherence times are significantly larger than the dephasing times displayed in Fig. 4.4. A more relevant reference [89] shows spin dephasing times for both electrons and holes in InAs/InAlGaAs/InP QDs. It is demonstrated that electron dephasing time starts decaying at higher temperatures compared to hole, which is the same behavior we see in our sample. This behavior is due to the inherently stronger spin-orbit interactions in the valence band, which enhance hole coupling to phonons [90]. The biggest difference is the activation energy, which is significantly larger in Ref. [89]. This is likely due to the Ref. [89] QDs having greater confinement, where it has been shown that the presence an AlGaAs barrier increases activation energy [171].

Figure 4.4(b) shows how the g-factor of electron and hole change as the magnetic field is rotated; in this case, the magnetic field direction was kept constant, and the sample was rotated. The data are fitted with the following equation [66]:

$$|g| = \sqrt{(g_\perp \cos\theta)^2 + (g_\parallel \sin\theta)^2}, \tag{4.5}$$

where θ is the magnetic field at angle relative to the [001] growth axis, $g_\perp$ is the transverse magnetic field g-factor, and $g_\parallel$ is the parallel magnetic field g-factor. The transverse g factors were $g_{\perp,e} = 0.87 \pm 0.017$, $g_{\perp,h} = 0.30 \pm 0.087$ and parallel $g_{\parallel,e} = 2.1 \pm 0.043$, $g_{\parallel,h} = 1.1 \pm 0.16$. Compared to another InAs/InAlGaAs sample [66], the results are not as expected, where in our case the electron anisotropy is larger than the hole anisotropy. However, in another InAs/InP sample, it is shown that a decrease in excitation energy (from 0.91 eV to 0.86 eV) causes a significant increase in electron g-factor anisotropy [72]. Measurements for the electron g-factor anisotropy are also done in Ref. [66]. However, they show barely any change. This indicates that the presence of InP impacts the electron g-factor anisotropy. The possible cause of this is the increasing asymmetry of the QDs as the size increases [72]. It is also known that due to the low lattice mismatch between InAs and InP (3%), both MBE and MOVPE strain-based growth methods for such QDs have an asymmetric growth profile [57], which could be further exacerbated by the larger size of the QDs. This would explain the increasing anisotropy for the mentioned InAs/InP sample, which was grown by MOVPE SK method. Based on this trend, our sample should exhibit even greater anisotropy since our excitation energy is 0.075 eV lower than the highest value in Ref. [72], where they already demonstrated significant anisotropy increases with a decrease of excitation energy. However, our measured electron g-factor anisotropy is comparable, rather than larger for both MOVPE and MBE SK grown InAs/InP QDs. It has been demonstrated that the same QDs can be produced with improved symmetry properties by utilizing MOVPE droplet epitaxy [55], which mitigates the expected increase in anisotropy in our sample, despite the lower excitation energy compared to Ref. [72].

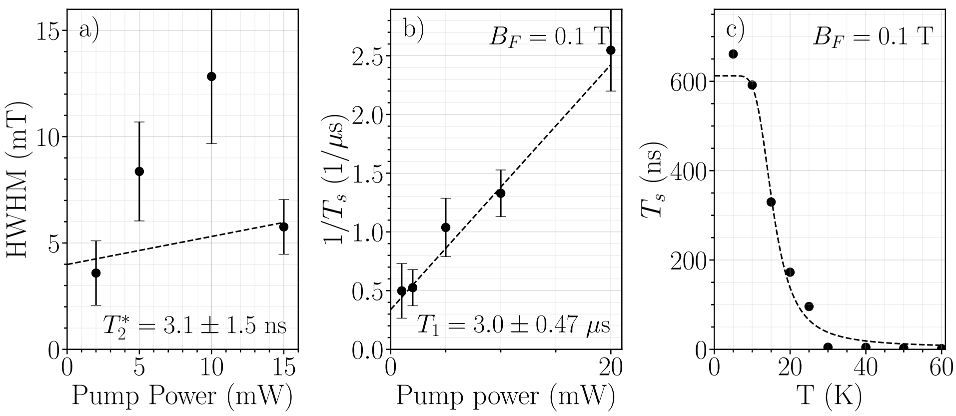

Figure 4.5: Spin dynamics measurements of quantum dots showing. (a) HWHM of the Hanle curve as a function of pump power, showing electron spin lifetime at zero power extrapolation. (b) Inverse electron spin lifetime versus pump power measured with a $B_F = 0.1$ T parallel magnetic field applied, with linear extrapolation to zero to obtain electron longitudinal spin relaxation time T_1. (c) Temperature dependence of electron spin lifetime with a 0.1 T parallel magnetic field applied, fitted with an Arrhenius equation (dashed line).

Figure 4.4(c) shows the relationship between the PRC and Hanle curve. Both PRC and Hanle curve were obtained by sweeping magnetic field strength and measuring Faraday ellipticity. For PRC, the magnetic field was parallel, and for Hanle, it was transverse. The PRC and Hanle curve can be fitted with the following model [141]:

$$H(\Omega_L) \approx \frac{\tau_c}{\tau_s} \frac{2\delta^2}{4\delta^2 + 3\Omega_L^2}, \tag{4.6}$$

$$P(\Omega_L) = \frac{\Omega_L^2}{\Omega_L^2 + \delta^2 \tau_s / \tau_c} \tag{4.7}$$

where P is the PRC curve, H is the Hanle curve, δ is the dispersion of nuclear fluctuations, τ_c is the nuclear spin correlation time and τ_s is the carrier spin relaxation time. This results in nuclear fluctuation dispersion value of $\delta = 430 \pm 40\, \mu s^{-1}$ and spin relaxation to nuclear spin correlation time ratio of $\tau_s/\tau_c = 7.1 \pm 1.3$. The PRC being relatively wide and V-shaped indicates that it is the spin dynamics of the electron that are being measured [139]. The implications of these parameters will be discussed in the discussion part.

Lastly, Fig. 4.5 shows the different spin times of our sample. Figure 4.5(a) is measured by performing Hanle measurements at different pump powers. The HWHM from the Hanle curves can then be extracted, and the intrinsic spin lifetime can be calculated by extrapolating to zero pump power and applying the following equation [138]:

$$T_s = \frac{\hbar}{g_e \mu_B B_{\text{HWHM}}}. \tag{4.8}$$

This results in a spin dephasing time of $T_2^* = 3.1 \pm 1.5\, ns$. In Fig. 4.5(b) T_1 is measured by using the spin inertia method [172]. A longitudinal magnetic field is applied to decouple the carrier spins from the fluctuations of the nuclear spins. Fixing the delay at a negative time delay, the modulation frequency is swept, and the Faraday ellipticity signal is measured. When the modulation period falls below the spin lifetime T_s, measured spin polarization decreases, causing the average signal amplitude to diminish. This can be described by the following equation [17]:

$$S(f_m) = \frac{S_0}{\sqrt{1 + (2\pi f_m T_s)^2}}, \tag{4.9}$$

where S_0 is the amplitude of the Faraday ellipticity signal and f_m is the EOM modulation frequency of the pump beam polarization. This allows the extraction of the spin lifetimes at different pump powers and obtaining the longitudinal spin relaxation by extrapolating to zero pump power, which is $T_1 = 3.0 \pm 0.47\, \mu s$. Finally, Fig. 4.5(c) shows the spin lifetime dependence on varying temperature. It is fitted with the Arrhenius equation, which shows similar activation energy to the electron activation energy seen in Fig. 4.4(a). This indicates that we are most likely measuring the spin lifetimes for electrons. In comparison, an MBE-grown InAs/InAlGaAs C-band QD sample shows $T_1 = 0.5\,\mu s$ [17] and another MBE-grown InAs/InAlGaAs/InP C-band QD sample shows $T_1 = 0.2\,\mu s$ [89]. Our sample shows an order-of-magnitude improvement, indicating that it is advantageous to use MOVPE DE for QD growth.

4.6 Discussion

There are several reasons why we assume that we are measuring resident carriers which are polarized by excited trions. It has been demonstrated that InAs/InP QD exciton recombination times can be up to 2 ns [173]. Looking at Fig. 4.1(d), it can be seen that hole dephasing times of nearly 10 ns have been measured, which indicates the presence of optically polarized resident holes, since, if there were no resident holes polarized by trions, the neutral exciton would radiatively recombine and spin dephasing would be limited at approximately 2 ns. The spin dephasing for resident electrons is below the exciton recombination time; however, electrons are impacted more by hyperfine interaction, as covered previously in Experimental Results, which is why the spin dephasing times for them are much shorter. Nonetheless, the V shape and width of the PRC seen in Fig. 4.5(c) indicate that the majority of resident carriers are electrons. If the measured electron component were a part of a positively charged trion, an M shape of the PRC would be observed [140]. Lastly, the fact that we can measure the PRC indicates the presence of resident carriers. The PRC curve is measured at negative pump-probe delay times, indicating that spin polarization is observed at times significantly longer (> 13 ns) than the exciton recombination times (< 2 ns).

Furthermore, an improvement in the T_1 time of electron spins is observed, approximately an order of magnitude larger than in other MBE SK grown telecom QD samples [17, 89]. However, there are 900 nm wavelength range QD samples that show T_1 times in the millisecond range [174]. One of the factors that influences T_1 times is the degree of confinement in the QD [175]. In the case of Ref. [174] there are two factors that increase the confinement of their QDs: an asymmetric AlGaAs barrier, where it has been shown that barriers with AlGaAs tend to increase confinement [171], and small QD size. In our sample, the barrier only consists of InP, and the size is larger, causing reduced confinement energy. Another contributing factor is the hyperfine interaction with nuclear spins. It has been demonstrated in a p-doped InAs sample that the hole T_1 time is limited to 1 μs due to coupling to nuclear spins [176]. In our case, we are measuring the electron T_1, however, as we have shown with Fig. 4.4(c) results, in our sample the nuclear spin correlation time is short enough to impact spin polarization, which reduces T_1 [141, 89].

To quantitatively analyze the nuclear spin correlation time observed in Fig. 4.4(c), we first consider the theoretical framework. In an ideal case, the data would be fit using a basic model [141]:

$$H(\Omega_L) \approx \frac{2}{3}\frac{\delta^2}{2\delta^2 + \Omega_L^2}, \tag{4.10}$$

$$P(\Omega_L) \approx \frac{1}{3}\frac{2\delta^2 + 3\Omega_L^2}{2\delta^2 + \Omega_L^2}, \tag{4.11}$$

but this model provides an incomplete description of the system, as the observed ratio between PRC and Hanle curves deviates from the expected 2:1 relationship. This basic model assumes that the distribution function of the nuclear spin precession frequency is isotropic. It also assumes that the nuclear spins on the timescale of electron precession are effectively static. These assumptions would result in the 2:1 distribution of PRC and Hanle as seen in Eqs. (4.10) and (4.11). However, in our case a 2:1 distribution is not seen. Sect. 4 of Ref. [141] provides a different model which still assumes that the hyperfine interaction is isotropic, which, if it was anisotropic, it would not have effect in our sample since it is of relevance only for heavy holes, whereas in our sample electrons are the resident carriers. However, in this model, the nuclear spin correlation times are shorter than the spin relaxation times, which decreases the electron dephasing time. The model with shorter τ_c contributions is seen in Eqs. (4.6) and (4.7).

Fitting these functions for our data shows spin relaxation to nuclear spin correlation time ratio of $\tau_s/\tau_c \approx 7$, which indicates that for our sample the carrier spin relaxation time is longer than the nuclear correlation time by 7 times. While this still allows for coherent electron spin, it introduces additional relaxation pathways, causing the spin polarization values to reduce and reducing T_1 time [141, 89]. Similar experimental results for p-doped (In,Ga)As/GaAs QDs are presented in Sec. VII D. of Ref. [141]. The main differences are in the shape of the PRC curve, which in their case is composed of two Lorentzians, indicating that the resident carrier in their sample are holes, and that they see depolarization partially due to hyperfine interaction anisotropy, g-factor anisotropy and potentially quantum anti-Zeno effect [177]. Otherwise, it is seen that the electron dispersion values between our sample and theirs are almost the same.

Additionally, it is worth noting that the theory of the model described in Sec. 4 of Ref. [141] does not fully apply to our case. The model describes how the nuclear correlation time indicates the time it takes for an electron to transition to a different nuclear environment. Since our sample is composed of QDs, the electrons stay within the same nuclear environment. This shows that the nuclear spins are fluctuating on a timescale faster than the carrier spin relaxation time. One possible cause of that is quadrupole interactions. It is known that the fundamental mechanism underlying quadrupolar interactions in quantum dots involves the coupling between nuclear quadrupole moments and electric field gradients generated by strain fields within the semiconductor lattice [178, 98]. Due to this coupling, the Overhauser field becomes time-dependent on the time scales comparable to the carrier spin relaxation time [98]. In Fig. 4.5(a) we have shown that our sample has an improved T_2^* compared to other telecom samples [17, 89], therefore, as an approximation, we assume that the same numerical model applies as in Ref. [141], except that it is related to quadrupolar interactions causing nuclear field fluctuations. This could also explain why the PRC amplitude observed in Ref. [141] is higher than in our case, since their sample shows shorter electron spin lifetimes than our sample [139].

Another important feature of our sample is the reduced electron g-factor magnitude. It should be said that the measurement method presented in Fig. 4.1 does not allow to determine the signs of the g-factor, however, the absolute value is still significantly different compared to other telecom QD samples, which display absolute electron g factors closer to 2 [65, 17]. This is related to the increased electron g-factor due to the QD shape asymmetry. Ref. [72] demonstrates lower g factors at higher excitation energies than in our case, which is attributed to the InAs/InP QDs having a structure similar to a flat disk [60]. Therefore, our MOVPE DE grown sample shows improvement in structural symmetry by having relatively better electron anisotropy properties and lower electron g-factor value, compared to MBE or MOVPE grown with strain methods InAs/InP quantum dots.

Additionally, the temperature dependence of T_1 in Fig. 4.5(c) is as expected. Assuming that at low temperatures the primary mechanism for spin relaxation is due to hyperfine interaction, we expect to see similar behavior for electron spin dephasing as in Fig. 4.4(a), where the relaxation would remain constant and limited by hyperfine interaction and at higher temperatures it would decay due to phonon interactions. However, the relaxation time starts decaying earlier compared to spin dephasing temperature dependence. This may be caused by hyperfine coupling variations mediated by lattice phonons [179]. It is mentioned in Ref. [179], that T_1 time is protected from the main inelastic-scattering mechanism due to confinement, however, as we have determined before, our sample's confinement is reduced, which is why it is possible that we are observing such temperature dependence.

The electron spin dephasing times at zero pump power show a further improvement compared to the times measured in Fig. 4.1(d). At this point, we approach the limit of dephasing caused by hyperfine interaction. To prove this, hyperfine interaction strength can be calculated by fitting the PRC curve with the following equation:

$$\bar{S}_z = S_0 \left[\frac{1}{3} + \frac{2}{3} \frac{B_{\text{ext}}^2}{B_{\text{ext}}^2 + B_f^2} \right] \tag{4.12}$$

where S_0 is the average electron-spin polarization at zero magnetic field, B_{ext} is the applied magnetic field and B_f is the averaged nuclear fluctuation field strength, which is defined as the HWHM of the PRC curve dip. However, this equation assumes that the nuclear field fluctuations are isotropic and non-fluctuating at the time scales of electron spin relaxation, but as we have shown, our sample exhibits time-varying nuclear field fluctuations. If, as an approximation, we assume that the nuclear field varies between z and (xy) directions, we can apply the τ_s/τ_c ratio for the distribution of the field directions. If we take the ratio to be 8 (within error bounds of the τ_s/τ_c, better fit with higher value), the equation becomes $\bar{S}_z = S_0 \left[\frac{1}{8} + \frac{7}{8} B_{\text{ext}}^2/(B_{\text{ext}}^2 + B_f^2) \right]$. Fitting this equation with the PRC data shown in Fig. 4.4 results in $B_f = 13\,\text{mT}$. From this, the spin dephasing time limited by hyperfine interaction can be calculated $T_2^* = 2\sqrt{3}\hbar/(g_e \mu_B B_f) = 3.2\,\text{ns}$, which is only slightly larger than the value we have obtained in Fig. 4.5(a). While Fig. 4.1(d) already shows the spin dephasing saturation at low applied magnetic field, which usually indicates that the values are limited by nuclear fluctuations, this further confirms that in our sample the electron spin dephasing time is limited mainly by hyperfine interaction and not any other factors.

We were not able to provide T_2 measurements as we could not observe the SML [17, 101]. One of the possible reasons is that T_2 is too short for SML to occur, however, seeing how an improvement in spin dynamics is observed, it would be expected that an improvement for T_2 would also be observed, which should make it long enough for SML to be present. Another possibility is that our signal to noise ratio was poor, which overshadowed the SML signal. Compared to MBE SK grown samples that we have previously measured, this sample exhibited increased noise and reduced signal strength. This degradation may result from point defects introduced during the stacking of multiple quantum dot layers. The sample in Ref. [17] also has 8 layers of QDs with a density of approximately $10^{10}\,\text{cm}^{-2}$, whereas our sample is 3 layers, which results in our sample having a significantly smaller effective QD density and in turn weaker signal.

4.7 Conclusions

We have characterized the spin properties of InAs/InGaAs/InP quantum dots grown by droplet epitaxy using MOVPE. Our measurements reveal several key findings that demonstrate the advantages of this growth method for telecom wavelength quantum dots. Most notably, we observed a longitudinal spin relaxation time $T_1 = 3.0\,\mu s$ for electrons, representing an order of magnitude improvement over comparable MBE-grown telecom QD samples [17, 89]. While we still observe significant electron g-factor anisotropy, we show that compared to other telecom samples, we see an improvement in anisotropy [72]. This enhancement is attributed to the improved structural symmetry achieved through MOVPE droplet epitaxy growth, which reduces the asymmetric growth profile common in both MOVPE and MBE strain-based growth methods [50].

5

Layer-dependent spin properties of charge carriers in vertically coupled telecom quantum dots

5.1 Preamble

This chapter reproduces the published manuscript on spin dynamics in Stranski-Krastanov grown InAs/InAlGaAs telecom-band quantum dots. The text, figures, and results are unchanged from the original paper. Only formatting, notation consistency, and layout adjustments have been applied so that the chapter fits the overall thesis style. Experimental measurements, data analysis and manuscript writing was done by me. Project conceptualization and initial setup was done by A. Greilich. Sample growth was done by A. Kors, J. P. Reithmaier and M. Benyoucef. Supervision, project management and manuscript editing was done by A. M. Fox, M. Bayer and A. Greilich. The corresponding publication is:

M.Cizauskas, A. Kors, J. P. Reithmaier, A. M. Fox, M. Benyoucef, M. Bayer, A. Greilich, "Layer-dependent spin properties of charge carriers in vertically coupled telecom quantum dots," *arXiv*, 2509.15051, Sep. 2025 [2].

5.2 Abstract

We investigate the spin properties of charge carriers in vertically coupled InAs/InAlGaAs quantum dots grown by molecular beam epitaxy, emitting at telecom C-band wavelengths, with a silicon δ-doped layer. Using time-resolved pump-probe Faraday ellipticity measurements, we systematically study single-, two-, and four-layer QD configurations to quantify how vertical coupling affects key spin-coherence parameters. Our measurements reveal distinct layer-dependent effects: (1) Adding a second QD layer flips the resident charge from electrons to holes, consistent with optically induced electron tunneling into lower-energy dots and resultant hole charging. (2) Starting from the four-layer sample, the pump-probe signal develops an additional non-oscillating, decaying component absent in single- and two-layer samples, attributed to multiple layer growth changing the strain environment, which reduces heavy-hole and light-hole mixing. (3) With four-layers or more, hole SML can be observed, enabling quantitative extraction of the hole coherence time $T_2 \approx 13$ ns from SML amplitude saturation. We also extract longitudinal spin relaxation (T_1) and transverse (T_2^*) spin dephasing times, g-factors, and inhomogeneous dephasing parameters for both electrons and holes across all layer configurations. The hole spin dephasing times T_2^* remain relatively constant (2.3-2.7 ns) across layer counts, while longitudinal relaxation times T_1 decrease with increasing layers (from 0.9 μs for single-layer to 0.32 μs for four-layer samples). These findings provide potential design guidelines for engineering spin coherence in telecom-band QDs for quantum information applications.

5.3 Introduction

The advancement of quantum information and communication technologies relies on the development of high-quality quantum systems that can maintain coherence over extended timescales while operating under practical conditions. Semiconductor QDs have emerged as versatile platforms for quantum information applications due to their potential for optical control of spin states, scalable fabrication, possibility of on-chip integration and use as high purity single-photon sources [180, 150, 151].

For quantum information applications, operation at telecom wavelengths (1.3-1.6 µm) offers practical advantages, which is the possibility to use existing telecom fiber infrastructure. Efficient QD coupling to single-mode fiber has been demonstrated with additional nanostructures designed to reduce losses [146, 147]. InAs/InGaAs/InP QDs are a promising solution for telecom-band quantum information applications, as they can be engineered to emit efficiently in the C-band while maintaining the spin coherence properties necessary for quantum applications [89, 17].

The ultimate performance of QD spin-based quantum information systems is governed by the coherence properties of the carrier spins, which are subject to decoherence from hyperfine interactions, phonon scattering, and structural asymmetries [89, 141]. MBE has been the predominant growth technique for high-quality QD, offering precise control over layer thickness, composition, and doping profiles [181]. However, the specific growth conditions and structural parameters can significantly influence the resulting spin coherence properties.

An important consideration in QD design is the impact of layer structure on spin dynamics. While single-layer QD structures offer simplicity, multi-layer configurations can provide enhanced optical signals and the potential for engineering inter-layer interactions [182, 183, 184]. The samples investigated in this work are InAs/InAlGaAs QDs grown by MBE, with a structure identical to that reported by Ref. [17], with the difference that in Ref. [17] the sample consists of eight-layers. We focus on comparing the spin properties of single-, two-, and four-layer stacks of QD configurations to quantify how additional layers affect key spin-coherence parameters. Using time-resolved pump–probe Faraday ellipticity, we extract longitudinal and transverse relaxation times, g-factors, and inhomogeneous dephasing for electrons and holes.

Across otherwise-identical stacks, we uncover clear layer-dependent trends. First, adding a second QD layer flips the effective optically-induced doping from electrons to holes, consistent with optically induced electron tunneling into lower-energy dots and resultant hole charging. Second, in four-layer stacks, the pump–probe signal exhibits an additional non-oscillatory decay component absent in one- and two-layer samples, which we attribute to potential inter-layer coupling that modifies the valence-band structure and reduces HH–LH mixing. Finally, the four-layer sample supports hole SML, enabling the quantitative extraction of the hole coherence time $T_2 \approx 13\,\mathrm{ns}$ from SML amplitude saturation.

This layer-resolved study identifies how vertical coupling reshapes spin properties in telecom-band QDs and provides design guidelines for engineered coherence. Since multiple-layer structures shift to holes as the primary charge carriers, coherence remains robust due to the weak hyperfine coupling of holes. In this paper, we present measurements and results that provide a systematic assessment of layer-dependent spin behaviour, essential for determining how multilayer QD structures can be used constructively in telecom-wavelength spin-photon platforms.

5.4 Experimental details

The QD samples investigated in this study are fabricated using MBE SK growth method on (100)-oriented InP substrates. The samples contain InAs QDs embedded within $In_{0.53}Al_{0.24}Ga_{0.23}As$ barrier layers, following the same structural design and growth parameters as reported by Ref. [17], see Fig. 5.1a. The only difference between our samples is the number of layers.

Each InAs layer consists of 5.5 monolayers (equivalent to approximately 1.65 nm) with QDs having a surface density of approximately 10^{10} cm^{-2}. A silicon δ-doped layer is positioned 15 nm below the QD layers with a doping concentration of 10^{10} cm^{-2} to provide resident electrons within the QDs. In the two-layer sample, the QD layers are separated by 15 nm of $In_{0.53}Al_{0.24}Ga_{0.23}As$ barrier material. The quaternary barrier composition serves the dual purpose of providing enhanced carrier confinemefnt.

Optical measurements are conducted using a liquid helium bath cryostat equipped with temperature control capabilities, allowing measurements across a temperature range from 6 K to 60 K. Magnetic field application is achieved through a superconducting magnet system capable of providing fields up to 4 T. The magnetic field orientation can be configured either parallel to the optical excitation axis (Faraday configuration) or perpendicular to it (Voigt configuration) by mechanical rotation of the sample mount and cryostat.

The optical excitation source consists of a mode-locked Ti:Sapphire laser (MiraHP) operating at a repetition frequency of 76.7 MHz, which pumps an optical parametric oscillator (APE OPO) to generate tunable pulses in the telecom wavelength range. The laser output provides pulses with approximately 2 nm spectral bandwidth. The generated beam is divided into pump and probe paths using a beam splitter, with the probe beam directed through a computer-controlled mechanical delay stage for temporal scanning.

Both pump and probe beams are focused onto the sample surface, with the pump beam diameter set to 150 µm and the probe beam focused to 100 µm diameter to ensure complete spatial overlap. The excitation energy is tuned to coincide with the photoluminescence peak at approximately 0.83 eV to achieve resonant excitation of the QD ensemble.

Spin polarization in the QDs is generated using circularly polarized pump pulses, achieved through an electro-optic modulator that alternates the pump polarization between σ^+ and σ^- states at frequencies ranging from 1 kHz to 2 MHz (with 10 kHz used for Voigt geometry measurements). The probe beam is linearly polarized, and the intensity is modulated using a photoelastic modulator

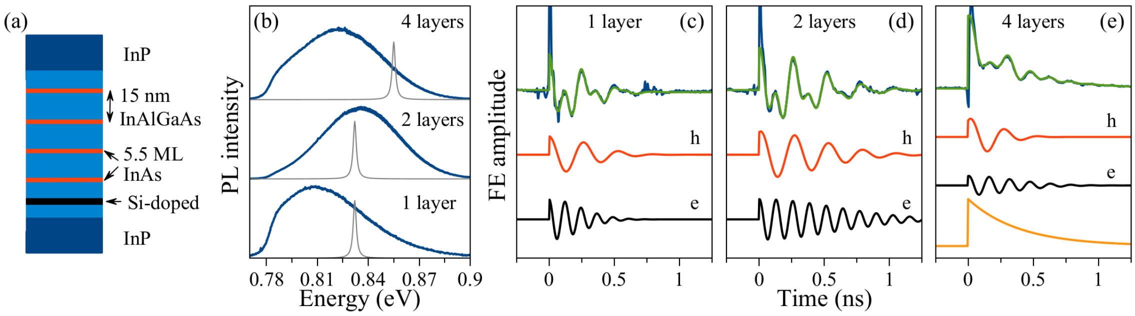

Figure 5.1: (a) Example of a four-layer InAs/InAlGaAs stacked QD sample structure. PL spectra and Faraday ellipticity measurements for QD samples with varying numbers of layers are presented in the subsequent plots. Panel (b) shows PL intensity spectra (offset for clarity), with the laser excitation spectrum shown as a gray line for each sample. All PL spectra were obtained with a 2.33 eV laser as the excitation source. For Faraday ellipticity, 0.832 eV excitation was used for the single- and two-layer samples, and 0.855 eV for the four-layer sample. Panels (c), (d), and (e) show time-resolved Faraday ellipticity amplitude measurements in blue color for the 1-layer, 2-layer, and 4-layer samples, respectively, with green color fitting using Eq. 5.9. The colored traces below show the fit decomposition, with red traces corresponding to hole spin precession, black traces to electron spin precession, and the orange trace (in panel e) representing an additional exponential decay component that may arise from inter-dot coupling or other multi-dot interactions. The component measurements were all done at a transverse magnetic field strength of 0.4 T. The pump and probe powers for the single-layer sample were 15 mW and 2 mW, for the two-layer sample 20 mW and 2 mW, and for the four-layer sample 10 mW and 2 mW. All measurements were done at 6 K.

operating at 86 kHz, followed by a Glan-Thompson polarizer.

Spin-dependent optical rotation of the probe beam is detected through Faraday ellipticity measurements [135]. Following interaction with the sample, the probe beam passed through a 10 μm diameter pinhole to minimize detection of scattered pump light. A quarter-wave plate converts the circular components of an elliptically polarized probe into linearly polarized components with orthogonal orientations. These components are separated using a Wollaston prism and directed onto balanced photodiodes for differential detection.

The photodiode signals are processed using lock-in amplification at the difference frequency between the pump and probe modulation frequencies, providing an enhanced signal-to-noise ratio and rejection of common-mode noise sources. This double-modulation detection scheme enables measurement of small spin-induced optical rotations with high sensitivity.

5.5 Experimental Results

Figure 5.1b shows the PL spectra of all the samples (blue curves, gray curves show excitation). The PL comparison of the different samples shows consistency; most of the change is observed in where the sample is excited. The pump-probe excitation energy was determined by recording the electron and hole precession signal intensities at different wavelengths, keeping the excitation power constant, and selecting the wavelength with the highest signal-to-noise ratio. For the 1- and 4-layer samples, the results are consistent and can be explained by the fact that at higher energies, more dots are excited, leading to higher signal amplitude. In the 4-layer sample, the excitation is shifted to higher energies to obtain a higher amplitude for the hole spin component due to the spin mode-locking effect discussed later in the paper. In a 2-layer sample, the excitation is placed at a lower energy than the PL center to obtain a robust signal.

When a transverse magnetic field is applied in the Voigt direction, the samples exhibit characteristic oscillatory Faraday ellipticity signals (blue curve and the signal fit in green in panels c-e of Fig. 5.1), as shown in Figs. 5.1c-e for a field of 0.4 T. These oscillations arise from the Larmor precession of electron (black curve) and hole (red curve) spins, with each carrier type contributing a distinct frequency component. The signals can be fitted and decomposed using:

$$S = \sum_i A_i \cos(\omega_i t) \exp\left(-\frac{t^2}{2T_{2,i}^{*2}}\right), \tag{5.1}$$

where i denotes the carrier type (electron or hole), A_i is the amplitude, ω_i is the Larmor precession frequency, and $T_{2,i}^*$ is the spin dephasing time. The Larmor frequency is related to the applied magnetic field through:

$$\omega_i = \frac{g_i \mu_B B_V}{\hbar} \tag{5.2}$$

where g_i is the g-factor of the respective carrier, μ_B is the Bohr magneton, B_V is the transverse magnetic field strength, and $\hbar$ is the reduced Planck constant. Holes have a higher effective mass than electrons, leading to more localized wavefunctions and correspondingly smaller g-factors, which results in lower precession frequencies. [185, 163].

A further result can be observed in Figure 5.1e, where, alongside the electron and hole precessions, there is an additional non-oscillating exponential decay element (orange curve in panel e), which is also observed in the 8-layer sample investigated in Ref. [17]. One possible explanation is the presence of a tilted magnetic field component, which provides an additional Faraday geometry component that causes the exponential decay. However, with further anisotropy measurements and the fact that this phenomenon is not observed in samples with 2 or 1 layers, we demonstrate that it is most probably related to inter-layer dot coupling and varying strain environment between the QD layers, which can affect heavy-hole and light-hole mixing.

Figure 5.2 shows the change of sample properties with varied excitation energy. The columns correspond to one-, two-, and four-layer structures, respectively, and the rows correspond to Faraday ellipticity, g-factor, and spin dephasing measurements, respectively. The black data points correspond to electrons and red to holes. In gray, the PL is shown, and in panels a, b, and c, the excitation spectra is displayed. The Faraday ellipticity measurements show the expected results: the highest amplitude at higher energies after the PL peak. The excitation is placed to account for both the Faraday ellipticity amplitude and the signal-to-noise ratio, which is why the excitation energy is offset from the amplitude maxima. The g-factor dependency shows the absolute electron g-factor decreasing and increasing for holes, which is in line with what is observed in similar telecom QD samples [17, 65, 66] and agrees with the Roth–Lax–Zwerdling relation for bulk semiconductors [74]. The spin dephasing measurements do not show any significant trends with changing excitation energy. It should be noted that all data displayed here is with error bars. However, in some cases, the error is small, so the error bars are not clearly visible.

The spin dephasing times (red data points correspond to holes and black to electrons), displayed in Figures 5.3a-c for single-, two- and four-layer structures respectively, show a characteristic dependence on the applied transverse magnetic field strength. At low magnetic fields, dephasing is dominated by hyperfine interactions with nuclear spins. In contrast, at higher fields, inhomogeneities in the QD ensemble, which cause a spread in the g-factor, become the limiting factor. This behavior is described by [17]:

$$T_{2,i}^{*} = \frac{\hbar}{\sqrt{(\Delta g_i \mu_B B_V)^2 + (g_i \mu_B \Delta B_i)^2}} \tag{5.3}$$

where Δg_i represents the g-factor spread due to variations in QD size and composition, and ΔB_i characterizes the magnetic field fluctuations resulting from hyperfine interactions.

From the fits to the dephasing equation in Eq. 5.3, we extract significantly different g-factor spreads for the three samples, shown in Table 5.1. The single-layer sample shows the largest g-factor spreads for both electrons and holes, along with considerable magnetic field fluctuation spreads. The two-layer sample exhibits reduced g-factor spreads for both carrier types, while magnetic-field fluctuation spreads remain similar. The four-layer sample demonstrates a similar electron g-factor spread compared to the two-layer sample, but shows a significant increase in hole g-factor spread, while magnetic field fluctuation spreads remain comparable to the previous samples. The magnetic field fluctuations, which reflect the strength of hyperfine interactions, show

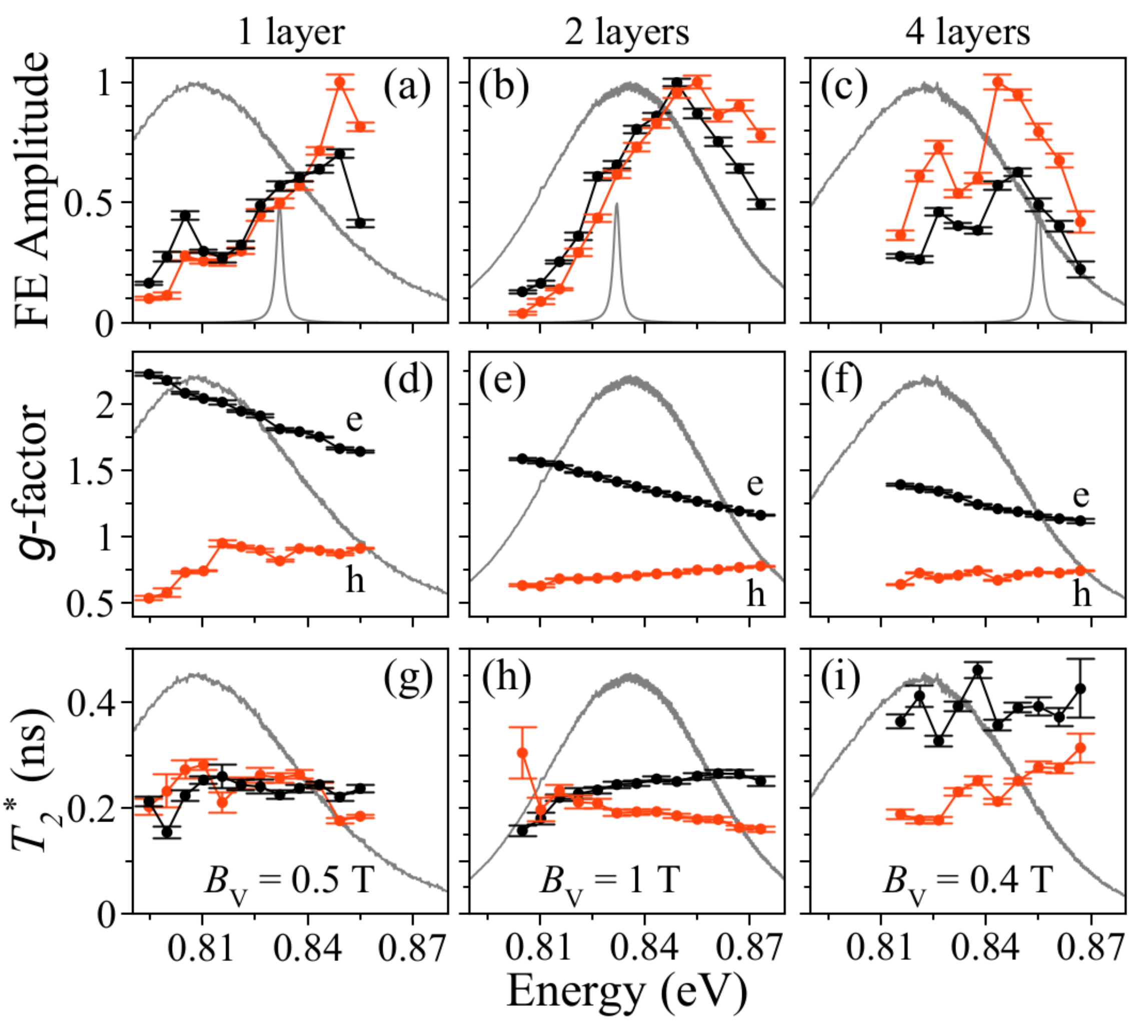

Figure 5.2: Energy dependent parameter characterization for QD samples with different numbers of layers (1, 2, and 4 layers). Panels (a), (b), and (c) display the normalized Faraday ellipticity amplitudes A_i from Eq. 5.9, red points represent holes and black ones electrons. Gray lines additionally show the PL and the laser pulse profile for later experiments. Panels (d), (e), and (f) show the extracted Lande g-factors. Panels (g), (h), and (i) show the spin dephasing times $T^*_{2,i}$ measured at magnetic field values shown in the panels. Pump powers for the 1-layer sample were 15 mW, and for 2- and 4-layer samples, 20 mW. All measurements were performed at 6 K and a probe power of 2 mW.

some variation between samples but stay in the same order of magnitude, suggesting similar nuclear spin environments in all three structures. There is a more significant difference between our three samples and the eight-layer sample in Ref. [17] in terms of magnetic field fluctuation values ΔB_i. This substantial deviation of the electron field fluctuation component might be related to the weaker localization of the tunneling electrons.

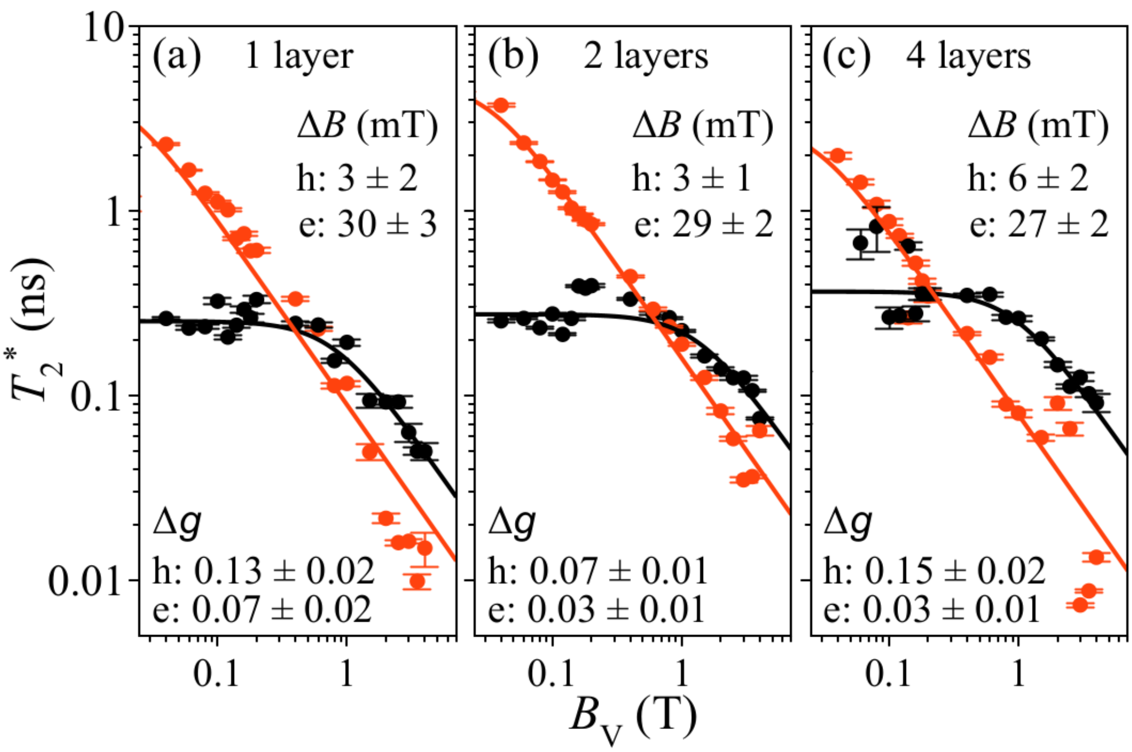

Figure 5.3: Spin dephasing time (T_2^*) measurements as a function of transverse magnetic field (B_V) for InAs/InAlGaAs QD samples with different numbers of layers. The data is presented on log-log scales for samples containing 1, 2, and 4 QD layers (panels a, b, and c, respectively). Red circles represent hole spin dephasing times, and black circles represent electron spin dephasing times. The solid lines show fits to the experimental data using a model that accounts for g-factor spread and magnetic field fluctuations. The fitting parameters, including magnetic field spreads (ΔB_h, ΔB_e) and g-factor spreads (Δg_h, Δg_e) are displayed for each sample. The measurement configuration is the same as in Fig. 5.1.

Sample	$\lvert g_e \rvert$	$\lvert g_h \rvert$	Δg_e	Δg_h	ΔB_e	ΔB_h
1-layer	**1.51** $\pm$ 0.01	**0.64** $\pm$ 0.01	**0.07** $\pm$ 0.02	**0.13** $\pm$ 0.02	**30** $\pm$ 3	**3** $\pm$ 2
2-layers	**1.42** $\pm$ 0.01	**0.72** $\pm$ 0.01	**0.03** $\pm$ 0.01	**0.07** $\pm$ 0.01	**29** $\pm$ 2	**3** $\pm$ 1
4-layers	**1.15** $\pm$ 0.01	**0.49** $\pm$ 0.01	**0.03** $\pm$ 0.01	**0.15** $\pm$ 0.02	**27** $\pm$ 2	**6** $\pm$ 2
8-layers [17]	**1.88** $\pm$ 0.02	**0.60** $\pm$ 0.01	**0.15** $\pm$ 0.03	**0.09** $\pm$ 0.01	**14** $\pm$ 2	**8** $\pm$ 2

Table 5.1: Different sample g-factor values, g-factor spreads, and magnetic field fluctuation spreads extracted from dephasing equation Eq. 5.9 and Eq. 5.3 fits for electron and hole carriers across four QD layer structures. ΔB_e and ΔB_h units are in mT.

The g-factor spread shows more significant variation compared to the magnetic field spread.

The reduced g-factor spread in the two-layer sample may indicate improved structural uniformity or different growth dynamics compared to the single-layer sample; however, the more likely explanation is that the excitation energy remains the same while the PL of the two-layer sample blue-shifts. This results in the effective excited PL width being significantly smaller than in the single-layer sample, indicating that the size distribution of the excited QDs is narrower than in the single-layer case, leading to a smaller g-factor spread. Another contributing factor is that due to the PL blue shift, higher-energy QDs are excited. It has been demonstrated that higher-energy transitions tend to have lower g-factor spreads [72], which is consistent with our reduced g-factor spread. A similar argument applies to the four-layer sample, where the PL is red-shifted and the excitation energy is higher than in the other two samples, thereby increasing the hole g-factor spread. It is of interest to note that in both cases, the electron g-factor spread is smaller than that of the hole, and even decreases relative to the hole g-factor spread in the two-layer and four-layer structures. Compared to Ref. [17], it would be expected that the electron g-factor spread would become larger than for holes with an increasing layer amount. This is further addressed in the Discussion.

Lastly, the obtained transverse g-factors for the different samples are shown in Table 5.1. There is minimal change in the g-factors between one- and two-layer samples. However, the four-layer sample shows a significant decrease in g-factors. This is related to the differences in excitation energy between the samples. It is demonstrated that with increasing excitation energy, the electron g-factor decreases [71, 65]. In our case, the excitation energy is significantly increased in the four-layer sample, leading to a decreased electron g-factor. The same applies to the eight-layer sample in Ref. [17], where the g-factors are $|g_e| = 1.88$ and $|g_h| = 0.60$. The electron g-factor is significantly larger, which is expected, since the excitation done is at lower energies due to a red shift of the sample PL.

Figures 5.4a-c show PRC and Hanle measurements for the single-, two-, and four-layer samples, respectively. Both Hanle (black data points and curve) and PRC (red data points and curve) measurements are performed by measuring Faraday ellipticity immediately before pump and probe overlap, ensuring sufficient spin decay and measurements of the resident carriers. The main difference is that Hanle is measured in Voigt geometry, while PRC in Faraday geometry.

As mentioned in the Experimental Details, our sample is doped to provide electrons as resident carriers. It has been demonstrated previously that PRCs exhibit a V-like shape for n-doped samples and an M-shape for p-doped samples [139]. From the single-layer sample PRC demonstrated in Fig. 5.4a, it can be seen that there are both electrons and holes as the resident carriers. However, in

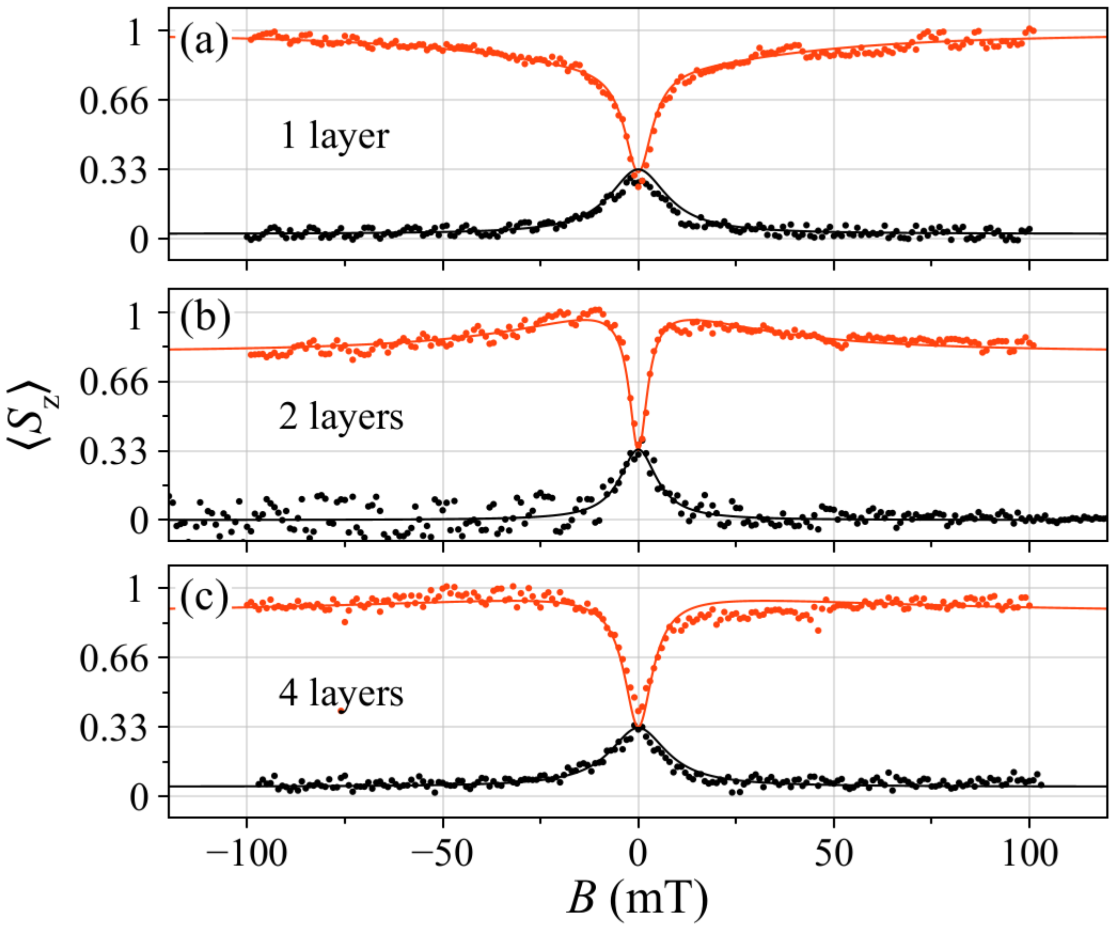

Figure 5.4: Polarization recovery curves (red) and Hanle effect measurements (black) for (a) single-layer sample, (b) two-layer sample, and (c) four-layer sample. The measurements show the total spin polarization $\langle S_z \rangle$ as a function of magnetic field strength. The fits for PRC are done with Eqs. 5.5. The pump power is 20 mW and probe power is 2 mW for both PRC and Hanle, for single and two-layer samples, and the pump power for the four-layer sample is 10 mW. All measurements are performed at 6 K.

the two and four-layer samples (Fig. 5.4b), a more prominent M shape is observed, indicating that the electrons are observed as part of trions and holes are becoming resident carriers, showing that by adding additional layers, the number of holes as resident carriers increases. This can be attributed to electrons tunneling out to occupy lower-energy QDs, due to their lower effective mass [186, 17], leading to optically induced hole doping.

The fits for both PRC and Hanle are done with Lorentzians that are provided by Ref. [141]:

$$H(\Omega_L) \approx \frac{2}{3}\frac{\delta^2}{2\delta^2 + \Omega_L^2} \tag{5.4}$$

$$P(\Omega_L) \approx \frac{1}{3}\frac{2\delta^2 + 3\Omega_L^2}{2\delta^2 + \Omega_L^2}, \tag{5.5}$$

where P – PRC, H – Hanle curve, δ – dispersion of the nuclear fluctuations, and $\Omega_L = g\mu_B B/\hbar$. This model is applied by first fitting the Hanle curve with the known transverse g-factor to obtain the dispersion δ, which is then used to fit the PRC's dispersion value and the carrier longitudinal g-factor. This basic model assumes that the hyperfine interaction is isotropic and that nuclear spin precession is significantly slower than electron spin precession. It should be noted that, due to the use of pulsed excitation, we are plotting total spin polarization rather than normalized spin polarization. In such case, the fit is $\langle S_z \rangle = S_0 P(\Omega_L)$, where S_0 is the initial spin polarization [141]. The reason for this is explained in Ref. [141] Section V. In the single-layer sample, the PRC fitting yields electron dispersion values of $\delta_e = 2870 \pm 100\,\mu s^{-1}$ and hole dispersion values of $\delta_h = 360 \pm 10\,\mu s^{-1}$. For the two-layer sample, the electron dispersion slightly increases to $\delta_e = 3180 \pm 100\,\mu s^{-1}$ and the obtained hole dispersion is $\delta_h = 261 \pm 10\,\mu s^{-1}$. As for the four-layer sample, the dispersion values remain similar $\delta_e = 3200 \pm 400\,\mu s^{-1}$ and $\delta_h = 326 \pm 10\,\mu s^{-1}$. These widths indicate how strong the hyperfine interaction is [141], which means that for holes, the hyperfine interaction is significantly lower, which is expected since the nuclear interaction hyperfine constant of a hole is an order of magnitude smaller than for the electron [95]. Moreover, an offset is seen in the Hanle curve of the four-layer sample. This indicates that spin mode-locking is present, which we confirm and discuss in the text below.

Returning to the aforementioned exponential decay component present in the four-layer sample and shown in Fig. 5.1e, Figs. 5.5a and 5.5b prove that the additional component is not related to Faraday geometry. Figure 5.5a shows the change of amplitude of the Faraday ellipticity signal, and Fig. 5.5b shows the change of the decay time of the non-oscillating component as the sample is

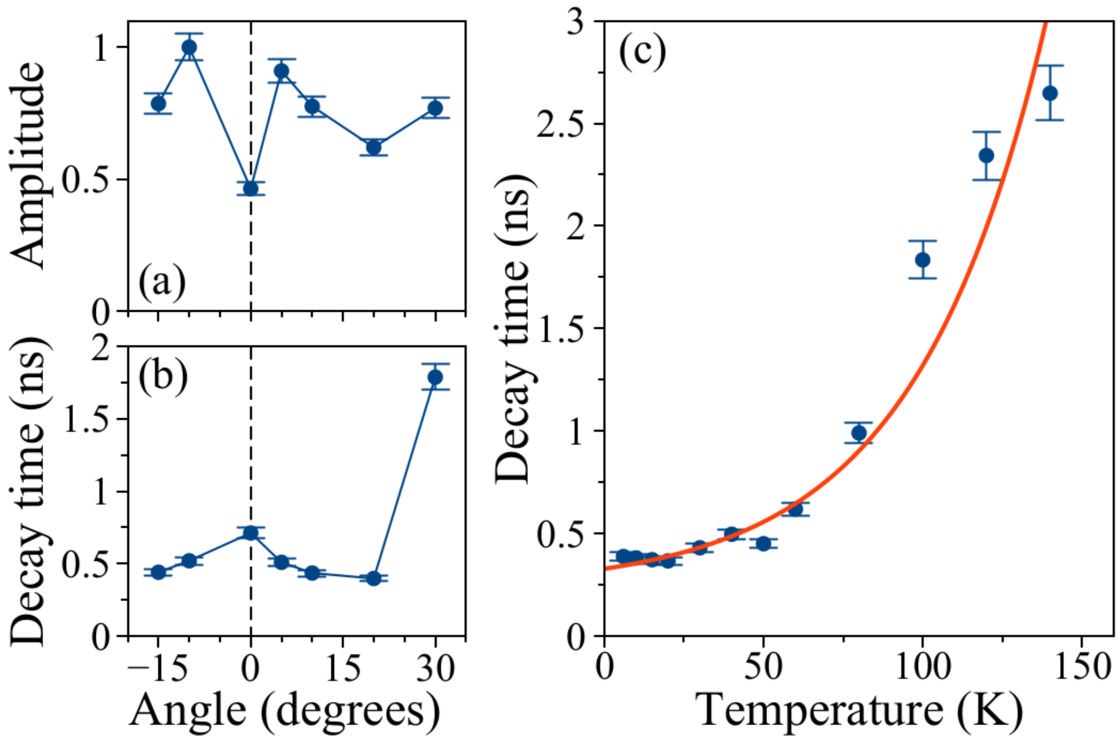

Figure 5.5: Characterization of the additional exponential decay component observed in a four-layer QD sample. (a) Normalized amplitude of the exponential component as a function of magnetic field angle measured away from the Voigt geometry. (b) Decay time of the exponential component as a function of magnetic field angle. (c) Temperature dependence of the exponential component decay time. All measurements are performed at a temperature of 6 K (except for (c)), a transverse magnetic field strength of 0.4 T, a pump power of 10 mW, and a probe power of 2 mW.

rotated. It can be seen that no matter the rotation angle, the non-oscillating exponential component remained present. It should be noted that, although the lowest decay time would be expected at a 0-degree angle due to the magnetic field being entirely in Voigt geometry, mechanical rotation of the sample introduces inaccuracies in determining the magnetic field angle.

Additionally, Fig. 5.5c shows the temperature dependence of the exponential decay time (red curve corresponds to the exponential fit). In a magnetic field applied in the Faraday geometry, one would expect the measurement to reflect spin lifetime T_1, which typically decreases with increasing temperature [1, 17, 89]. Instead, the decay time in our case remains nearly constant up to 50 K, after which it increases exponentially. A similar trend was reported in Ref. [187], where exciton lifetimes were measured in QD molecules using time-resolved micro-photoluminescence. These observations support the conclusion that the exponential decay component originates when additional QD layers are added. However, this is not necessarily related to inter-dot coupling effects. This is further addressed in the Discussion.

Figure 5.6 presents the different spin relaxation times for our samples. In Fig. 5.6a-c, Hanle measurements are performed at varying pump powers to extract the HWHM, from which the intrinsic spin dephasing time is determined by extrapolating to zero pump power using the following equation:

$$T_2^* = \frac{\hbar}{g\mu_B B_{\text{HWHM}}}. \tag{5.6}$$

The extrapolation to zero is done using a linear fit (red curve in Fig. 5.6a-c panels). The resulting spin dephasing times can be seen in Table 5.2, showing only slight increase between the different samples. However, the obtained dephasing times are lower than the theoretical limit imposed by hyperfine interaction. To evaluate this limit, the hyperfine interaction strength can be calculated by fitting the PRC curves of all the samples with the following equation [188]:

$$\bar{S}_z = S_0 \left[\frac{1}{3} + \frac{2}{3} \frac{B_{\text{ext}}^2}{B_{\text{ext}}^2 + B_f^2} \right] \tag{5.7}$$

where B_{ext} – applied magnetic field, S_0 – average electron-spin polarization at zero magnetic field, and B_f – averaged nuclear fluctuation field strength, which is HWHM of the PRC dip. This equation is used to fit two components of the PRC, since we observe both a hole and an electron component in all samples. The results of the fits for the hole component of the single-layer sample are $B_f = 5.2$ mT, $B_f = 2.4$ mT for the two-layer sample, and $B_f = 3.9$ mT for the four-layer sample.

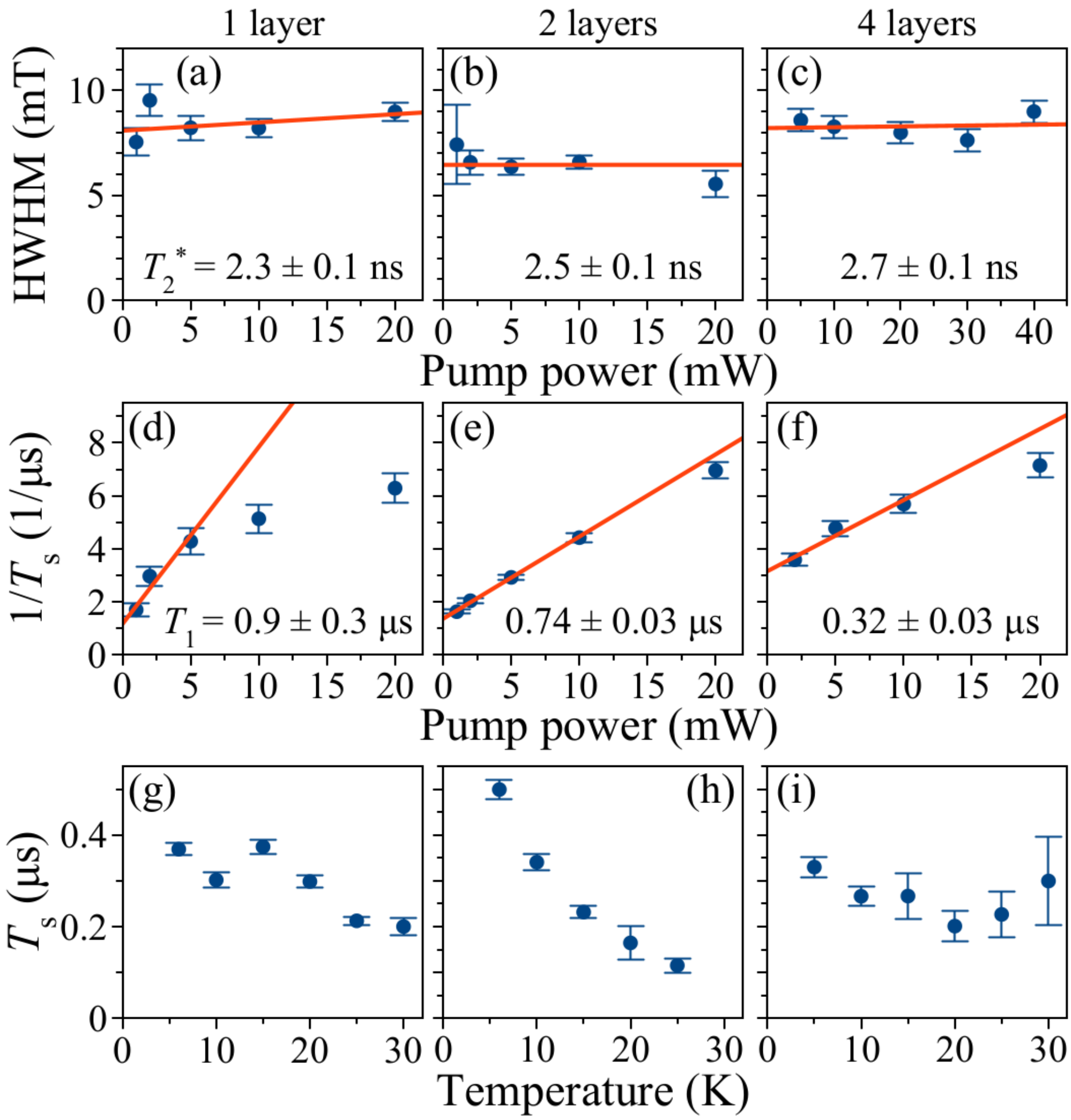

Figure 5.6: Spin dynamics measurements for QD samples with different numbers of layers (1, 2, and 4 layers). Panels (a), (b), and (c) display the HWHM of Hanle curves as a function of pump power, from which spin dephasing times T_2^* are extracted through linear extrapolation to zero pump power. Panels (d), (e), and (f) show the inverse spin lifetime ($1/T_s$) versus pump power measured under a longitudinal magnetic field of 0.1 T, with the intrinsic longitudinal spin relaxation times T_1 determined by extrapolating the linear fits to zero pump power. Red lines are linear fits for extrapolation to zero.

Panels (g), (h) and (i) show the spin lifetime in Faraday geometry dependency on the sample temperature, measured using the spin inertia method. All the samples are subjected to a magnetic field of 0.1 T. Pump power for the different panels is (g) 5 mW, (h) 2 mW, and (i) 2 mW. All measurements were performed at 6 K and a probe power of 2 mW.

With this, the spin dephasing time limited by hyperfine interaction for holes can be calculated with the following equation [169]:

$$T_2^* = 2\sqrt{3}\hbar/(g_h \mu_B B_f) \tag{5.8}$$

which results in 12 ns for the single-layer sample, 23 ns for the two-layer one and 20 ns for the four-layer sample. The T_2^* values obtained from Hanle measurements are significantly lower, indicating that effects beyond the hyperfine interaction further reduce the dephasing times. One possibility is strain-induced effects that give rise to nuclear quadrupolar interactions, which can significantly reduce spin coherence times [189]. The inherent lattice mismatch in InAs/InAlGaAs QDs grown by SK creates structural asymmetries that enhance these quadrupolar effects. This interpretation is supported by recent studies on InAs/InGaAs/InP QDs grown by MOVPE droplet epitaxy, which demonstrate substantially improved spin dephasing times approaching the hyperfine limit due to the reduced strain achieved through this growth technique [1]. It should be noted that these equations are usually applied for electrons rather than holes. Holes demonstrate significantly weaker hyperfine interactions compared to electrons [95], so this is only an approximation; however, such spin dephasing times are expected for holes [190].

Figures 5.6d-f show T_1 measurements obtained using the spin inertia method [172]. In this measurement approach, a longitudinal magnetic field decouples carrier spins from nuclear spin fluctuations. With the probe delay fixed at a negative time, the pump modulation frequency is varied while monitoring the Faraday ellipticity signal. As the modulation period approaches the spin lifetime, the measured spin polarization diminishes, reducing the average signal amplitude according to the relation [17]:

$$S(f_m) = \frac{S_0}{\sqrt{1 + (2\pi f_m T_s)^2}}, \tag{5.9}$$

where S_0 – initial amplitude of the Faraday ellipticity signal and f_m – pump beam polarization EOM modulation frequency. By measuring T_s at different pump powers with a parallel magnetic field applied, a linear fit can be applied (red curve in Fig. 5.6d-f panels), and it can be extrapolated to obtain the intrinsic longitudinal hole spin lifetime T_1. As the time relaxation rate saturates at higher powers, we only include the linear part of the dependence in the low power side of the data points for the fitting. The T_1 values across the samples can be seen in Table 5.2.

The difference in T_1 times between single- and two-layer samples is significant, but the error

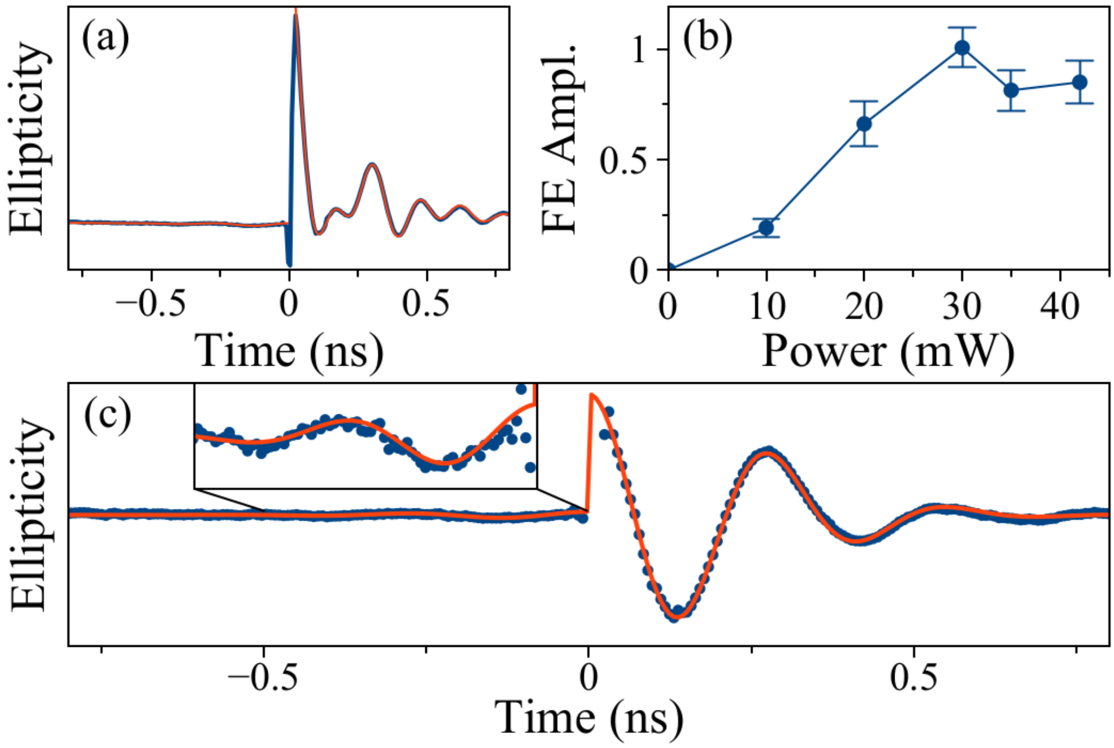

Figure 5.7: (a) Time-resolved pump-probe signal for the four-layer sample, where the blue trace represents the raw data and the red line is a fit. At negative time delays (on the left), the signal shows the characteristic SML revival, in which spin coherence is recovered before the arrival of the pump pulse. At positive time delays (right side), normal spin precession is observed in Voigt geometry following optical excitation. (b) Normalized amplitude of the SML signal as a function of pump power, showing how the mode-locking effect strengthens with increasing excitation power until reaching saturation around 25-30 mW. (c) The extracted SML data for holes (blue data points) fitted with a theoretical model curve (red line). All measurements were performed at 6 K, 0.4 T transverse magnetic field, and 2 mW probe power.

Sample Type	$T^*_{2,h}$ **(ns)**	$T_{1,h}$ **(μs)**
Single-layer	**2.3** $\pm\,0.1$	**0.9** $\pm\,0.3$
Two-layer	**2.5** $\pm\,0.1$	**0.74** $\pm\,0.03$
Four-layer	**2.7** $\pm\,0.1$	**0.32** $\pm\,0.03$
Eight-layer [17]	-	**0.50** $\pm\,0.04$

Table 5.2: Spin dephasing times (T^*_2) and longitudinal spin relaxation times (T_1) measured for hole spin carriers across the different QD layer structures. The T^*_2 value was not measured by Hanle in Ref. [17].

in the single-layer sample T_1 is large enough to put it within the range of the two-layer sample. However, the four-layer sample shows a further reduction compared to both the single- and two-layer samples. The eight-layer sample in Ref. [17] also exhibits a reduced T_1 of 0.5 μs, indicating that the shift from two- to four-layers causes a reduction in T_1 times. Figure 5.4 demonstrates that with added layers, the effective carriers become holes; therefore, it is also safe to assume that the T_1 measurements are for holes when additional layers are added. This transition to hole-dominated charging contributes to the observed reduction in T_1 times, as holes exhibit enhanced spin-orbit coupling compared to electrons, which accelerates spin relaxation processes [191, 88]. Moreover, the hole spin lifetime also shows a strong dependence on QD size. It was demonstrated that larger InAs/GaAs dots exhibit longer T_1 times [192]. The particularly low T_1 observed in the four-layer sample can be understood through the interplay of these effects: the resident carriers are holes, which have an inherently shorter lifetime, and the sample was excited at a higher energy compared to the single and two-layer samples, which excite smaller QDs within the ensemble, leading to shorter T_1 times for holes. In contrast, the eight-layer sample in Ref. [17] was excited at a lower energy, corresponding to larger QDs with longer T_1 times. However, this value remains lower than those of single- and two-layer samples because holes are the dominant carriers.

Figures 5.6g-i show the spin lifetime dependence on temperature with a magnetic field applied in Faraday geometry for single-, two-, and four-layer samples, respectively. The spin lifetime values in Fig. 5.6i are significantly lower because of using higher pump power, where it is known that increasing pump power speeds up spin relaxation due to photogenerated carriers, causing delocalization of resident carriers [193]. Another factor is the intrinsically lower T_1 time for the four-layer structure, shown in Fig. 5.6f. The measurements were done up to 25-30 K because the signal weakened as the temperature increased, making the fitting error too large at higher temperatures. The changing trend across different layer count structures is further addressed in the Discussion.

Lastly, in Fig. 5.7a, the signal of the four-layer sample and its fit (red curve) are displayed. In this case, a weak, single-frequency oscillation can be observed (see Fig. 5.7c and zoom-in). This effect is called SML. In SML, coherent spin dynamics are sustained across multiple pump-pulse cycles via a feedback mechanism. When the spin coherence time T_2 exceeds the laser repetition period T_R, spins that precess commensurate with the pulse repetition frequency can maintain phase coherence between successive excitation pulses [17, 101]. This manifests as a revival of the spin signal at negative time delays, where the probe pulse arrives before the pump pulse. In this case, the SML signal frequency corresponds to holes, since the SML signal frequency is the same as the hole precession frequency seen at positive time delays.

The existence of SML allows us to estimate T_2 for the four-layer sample. The hole spin coherence time T_2 was extracted by modeling the SML signal amplitude ratio before and after pump pulse excitation. The modeling incorporated experimentally determined hole g-factors, g-factor spreads (Δg_h), and assumed a Gaussian distribution of g-factors across the QD ensemble. Refs. [135, 194, 17, 101] go into more details about how the modeling is done.

In Ref. [17], the authors were only able to estimate the range of T_2 times due to not observing SML amplitude saturation or Rabi oscillations. In our case, we can determine it much more accurately by observing saturation of the SML amplitude, as shown in Fig. 5.7b. To determine it, we model the QD ensemble using a Gaussian g-factor distribution with a width of $\Delta g_h = 0.11$ and g-factor $|g_h| = 0.65$. The amplitude ratio of SML and the amplitude of the signal after excitation then depends on T_2 time and the pulse area Θ. Since we observe saturation, the pulse area is $\Theta = \pi$, and thus the coherence time is $T_2 = 13\,\text{ns}$. The plotted model (red curve corresponds to the model fit) can be seen in Fig. 5.7c overlayed with the extracted hole spin contribution of the real signal given in Fig. 5.7a.

5.6 Discussion

Several noteworthy effects emerge when additional QD layers with narrow barrier separations are incorporated. First, the n-doped sample becomes effectively p-doped when a second layer is added, and with four layers, there is indication that there is again more electron carriers, which is possible due to variances in doping between samples. However, holes are still present, as shown in Figs. 5.4a-c. In the previous section, we mentioned that the cause of this is the tunneling of excited electrons to lower-energy QDs. The reason is likely that, as additional layers grow, the QDs on that layer have lower energy. This has been demonstrated for InAs/GaAs QDs, where as layers are stacked, the QD size increases since the strain distribution from the underlying layers causes the preferential localization of QDs on top [195, 196]. Moreover, although the barrier thickness is 15 nm, it is not measured from the top of the QDs. The QD height is estimated to be between 9-13 nm [72], which makes the effective distance between the QDs short enough (3-6 nm) for tunneling to occur efficiently.

These samples would benefit from added charge-control structures not only because of being able to confidently determine whether the seen changes in doping are truly related to tunneling, but also for extending carrier lifetimes and enabling controlled tuning of tunneling. However, implementing charge control in multi-layer structures is challenging because doping can only be applied above and below the QD layer stack. Due to this, deterministic charging of each layer is hard to achieve due to the lack of uniformity of the electric field and the Fermi level.

In addition to tunneling, we see an additional non-oscillating decaying exponential starting to appear in the four-layer structure, seen in Fig. 5.1d, which is also seen in the eight-layer structure in Ref. [17] Fig. 2a. In the referenced paper, the authors attribute this additional component to either a molecular or an excitonic state caused by coupling between the QDs. In our case, we also attribute it to coupling-related effects, since we exclude the possibility of the exponential resulting from Faraday geometry by performing anisotropy measurements shown in Figs. 5.5a-b, and also because we do not see the additional component in either single or two-layer samples.

We hypothesize that there are two effects associated with this non-oscillating component. It is known that, due to QD confinement, there is significant LH and HH mixing [197], which affects the optical and spin properties of QDs, in particular, causing significant g-factor anisotropy and non-zero in-plane g-factor values for the corresponding hole component[66]. However, for some quantum well samples, a pure HH state has been observed, which shows transverse g-factor values near zero [198] or even effectively zero when considering thin quantum wells, in which case the splitting between the LH and HH is relatively large when ignoring cubic symmetry [199]. Therefore, we attribute the non-oscillating component to reduced heavy-hole-light-hole mixing, caused by the addition of multiple layers that change the strain environment and, in turn, reduce symmetry, resulting in greater splitting between LH and HH. This is further confirmed by examining the eight-layer structure in Ref. [17], where the non-oscillating component exhibits an increase in both decay time and amplitude, suggesting that additional layers may further reduce HH and LH mixing.

Subsequently, Fig. 5.5c demonstrates an unexpected result where both the electron and the potential HH dephasing times increase with temperature. These results show substantial similarity to time-resolved microphotoluminescence exciton lifetime measurements in InAs/InP QDs [187] and in InAs/GaAs QDs [200, 201, 202], where the lifetime increases with temperature due to the carriers being excited to *p*-shell states with increased temperature, causing lowered radiative rates since the carriers have to relax back to *s*-shell before recombining. Moreover, indirect excitons in coupled QD systems have been demonstrated via photoluminescence measurements, using an electric field to place the electron and hole in resonance [203]. Therefore, as we have confirmed that tunneling in our sample is a possibility due to the effective distances between the QDs and due to the results shown in Fig. 5.4, we then assume that the increasing dephasing times of exciton and heavy-hole seen in Fig. 5.5c is due to the formation of an indirect exciton.

In our case, we do not need to perform electric-field tuning because our measurements show spin polarization rather than photoluminescence. However, the previously discussed measurements in Refs. [187, 200, 201, 202] show increased exciton lifetime, rather than investigating spin dephasing. The observed dephasing pattern arises because holes in indirect excitons experience primarily hyperfine interactions as their dominant dephasing mechanism [204]. This hyperfine-interaction-limited dephasing directly correlates the hole spin dephasing time with the exciton lifetime. Therefore, as temperature increases, exciton lifetimes increase, and the dephasing time increases proportionally. As to why this is not observed for the direct excitons in either the four-layer or lower count layer samples, this is due to the indirect excitons having an inherently longer lifetime because of their reduced wavefunction overlap [205], making them more affected by the aforementioned radiative overlap.

Another emerging effect arising from multiple layers of QDs is evident in Figs. 5.6g-i. In the Figs. 5.6g and h, the tendencies are expected, where in panel g, a more or less constant spin lifetime is observed up to 20 K and then starts reducing, which indicates that the resident carriers are electrons [89]. In plot h, the lifetime starts to decrease immediately at 10 K, suggesting that the resident carriers are then holes [89]. The PRC results in Figs. 5.4a and 5.4b further confirm these two plots. In the case of Fig. 5.6i, it is expected that it would be the same as in plot h, due to the resident carriers being holes; however, the spin lifetime remains nearly constant through the whole range. Almost identical behavior is observed in the eight-layer sample investigated in Ref. [17], indicating that this effect, like SML and the non-oscillating component, only appears at 4 layers or more.

Lastly, along with the additional component observed in the four-layer sample, we also observe spin mode-locking. Moreover, we can see improvements in T_2 times from a four-layer sample to an eight-layer sample, as shown in Ref. [17]; however, these are relatively marginal and, in this case, are attributed to error. As to the reason for SML's appearance, it can be explained by the aforementioned tunneling. As more and more layers are added, there are more QDs for electrons to tunnel to, leaving more holes behind. This greatly increases the hole population, which allows us to observe SML. As for the T_2 values themselves, they are relatively low compared to $T_2 = 1.1\,\mu s$ of AlAs/GaAs QDs [206]. However, hole-spin coherence times have not been reported previously in telecom QDs. Therefore, this shows that multi-layer QD structures have potential for quantum information applications. To gain better insight not only into T_2 but also into other phenomena we have observed in this paper, additional measurements and analyses are needed.

5.7 Conclusions

This layer-resolved study identifies how vertical stacking of MBE-grown telecom C-band QDs impacts spin properties, revealing several phenomena that emerge with increasing layer count in InAs/InAlGaAs QD configurations. The transition from electron-dominated to hole-dominated resident carriers with increasing layers represents a fundamental shift in spin dynamics: single-layer samples exhibit both electron and hole components, whereas two- and four-layer samples show predominantly hole-like behavior due to electron tunneling to lower-energy dots in additional layers. Four-layer structures exhibit distinctive inter-layer coupling effects, including an additional non-oscillatory exponential-decay component that persists across all magnetic field angles, with an unusual temperature dependence in which spin relaxation times increase rather than decrease with temperature, attributed to indirect exciton effects. Also, the emergence of spin mode locking that enables direct measurement of hole coherence times $T_2 \approx 13\,\text{ns}$. While transverse dephasing times T_2^* remain relatively stable across layer counts (2.3-2.7 ns), they fall short of hyperfine-limited theoretical values, suggesting additional dephasing mechanisms such as strain-induced quadrupolar interactions. The reduction in longitudinal relaxation time T_1 with increasing layers (from 0.9 μs to 0.3 μs) highlights the trade-off between optical signal enhancement and spin-lifetime preservation.

Across all layer numbers studied, the results show that the relevant spin properties, carrier type, and coherence behavior do not degrade (except T_1) with increasing layer count. Instead, multilayer stacks support hole spins with stable coherence characteristics, indicating that vertical coupling can be used as a design parameter rather than a limitation. These findings demonstrate that multilayer telecom QDs remain a viable platform for spin–photon schemes and guide engineering stacked structures where hole-spin coherence is the operative resource.

6

33 Gbps source device independent QRNG with real-time extraction

6.1 Preamble

This chapter reproduces the published manuscript on high-bandwidth quantum random number generation based on heterodyne measurement of vacuum fluctuations with real-time randomness extraction. The text, figures, and results are unchanged from the original paper. Only formatting, notation consistency, and layout adjustments have been applied so that the chapter fits the overall thesis style. The experimental measurements, data analysis, FPGA digital logic design, software design and manuscript writing was done by me. Project conceptualization and initial setup was done by A. Greilich. The source device-independent (SDI) theory was developed by H. Tebyanian. Supervision, project management and manuscript editing was done by A. M. Fox, M. Assmann and A. Greilich. The corresponding publication is:

M. Cizauskas, H. Tebyanian, A. M. Fox, M. Bayer, M. Assmann, A. Greilich, "33 Gbit/s source-device-independent quantum random number generator based on heterodyne detection with real-time FPGA-integrated extraction," *arXiv*, 2512.07319, Dec. 2025 [3].

6.2 Abstract

We present a high-speed continuous-variable QRNG based on heterodyne detection of vacuum fluctuations. The scheme follows a SDI security model in which the entropy originates from quantum measurement uncertainty and no model of the source is required; security depends only on the trusted measurement device and the calibrated discretization, and thus remains valid even under adversarial state preparation. The optical field is split by a 90° optical hybrid and measured by two balanced photodiodes to obtain both quadratures of the vacuum state simultaneously. The analog outputs are digitized using a dual-channel 12-bit analog-to-digital converter operating at a sampling rate of 3.2 GS/s per channel, and processed in real time by an FPGA implementing Toeplitz hashing for randomness extraction. The quantum-to-classical noise ratio was verified through calibrated power spectral density measurements and cross-checked in the time domain, confirming vacuum-noise dominance within the 1.6 GHz detection bandwidth. After extraction, the system achieves a sustained generation rate of $R_{\text{net}} = 33.92$ Gbit/s of uniformly distributed random bits, which pass all NIST and Dieharder statistical tests. The demonstrated platform provides a compact, FPGA-based realization of a practical heterodyne continuous-variable source-independent QRNG suitable for high-rate quantum communication and secure key distribution systems.

6.3 Introduction

Random numbers serve as fundamental building blocks across numerous fields, from Monte Carlo simulations in scientific research [207] to quantum key distribution based cryptographic protocols [208] of which the purpose is to provide unbreakable secure encrypted communication [209]. In cryptographic applications, the quality and unpredictability of random numbers directly determine the security of encryption schemes, since they are used in one-time pad encryption, where the key length must match the message length and cannot be reused [208]. While classical random number generators based on deterministic algorithms can satisfy many computational needs, they fundamentally cannot provide the true unpredictability required for security-critical applications, as their outputs are ultimately predictable given sufficient computational resources and knowledge of the algorithm's internal state [210].

Quantum mechanics offers a fundamental solution to this limitation through the intrinsic randomness present in quantum measurements. QRNGs exploit the fundamental uncertainty principle of quantum mechanics to produce truly unpredictable random numbers, providing a level of security that classical systems cannot achieve. The measurement of quantum observables yields outcomes that are fundamentally non-deterministic, even with complete knowledge of the quantum state prior to measurement. There are several established QRNG methods, such as measuring single photons going through a 50:50 beamsplitter [116], measurements of laser phase fluctuations [211], amplified spontaneous emission in fiber amplifiers [212], vacuum fluctuations [213, 214] and etc. QRNGs are further divided into two main categories. There are DV QRNGs, where the random numbers are formed by quantum measurements that yield binary results, such as single-photon measurements, and there are CV QRNGs, where continuous quantum mechanical properties are measured.

Work (Year)	Security Model	Bit Rate	Extraction	Entropy Generation Method
Avesani et al. (2018) [131]	Source-device-independent	17.42 Gbps	Offline	Heterodyne vacuum noise measurements
Zheng et al. (2019) [214]	Device-dependent	6 Gbps	Online (FPGA)	Homodyne vacuum noise measurements
Bruynsteen et al. (2023) [120]	Device-dependent	100 Gbps	Offline	Homodyne vacuum noise measurements
Bertapelle et al. (2023) [215]	Source-device-independent	20 Gbps	Offline	On-chip heterodyne vacuum noise
Qiu et al. (2025) [216]	Source-device-independent	347 Mbps	Online (FPGA)	Fiber beamsplitter statistics, device imperfection tolerant
Cheng et al. (2024) [217]	Semi-device-independent	580 Mbps	Offline	Entropy from squeezed light states
Zhang et al. (2025) [218]	One-sided device-independent	7.06 Mbps	Offline	Entropy from quantum steering
Yang et al. (2025) [219]	Device-dependent	156 Gbps	Offline	Laser phase noise
Crampton et al. (2025) [220]	Device-dependent	2 Gbps	Online (FPGA)	Phase-diffusion in two gain-switched lasers
This work	Source-device-independent	33.92 Gbps	Online (FPGA)	Heterodyne vacuum noise measurements

Table 6.1: Comparison of recent experimental QRNG demonstrations (2018–2025) focusing on security assumptions, achieved random bit rate, extraction mode, and entropy estimation method.

The critical distinction between online and offline extraction is operationally significant: offline schemes require intermediate data storage and batch post-processing, so the advertised rate represents a peak throughput that cannot be sustained on demand. Online extraction, by contrast, produces certified random bits continuously at line rate, enabling direct integration with high-speed cryptographic applications. In recent times, QKD systems have been improving and are operating in the GHz range [221, 222]. With the increasing QKD operating frequency, higher bandwidth QRNGs are needed to match the data transmission rates. There are already implementations showing bandwidths of more than a hundred Gbits/s [120, 121]. However, these systems are not fully secure. The sources or the measurement devices can be tampered, which reduces the quality of QRNG, allowing for potential attacks [223]. There are DI QRNGs, which assume that both source and measurement devices cannot be trusted and apply self-testing algorithms to ensure that the QRNG cannot be tampered with. However, due to how complicated DI schemes are, the achievable bandwidths range is only up to kbits/s [133]. A good trade-off is a SDI QRNG, where only the measurement device is assumed to be completely trusted. There are already implementations of SDI QRNGs with bandwidth rates in the 10-30 Gbits/s range [131, 224, 225]. However, in those cases, the processing is performed offline, making the effective bandwidth significantly lower. Therefore, higher bandwidths can be achieved by performing the processing fully on FPGA.

In this paper, we present a SDI QRNG based on heterodyne measurements of vacuum fluctuations, with acquisition, extraction and data transfer performed entirely on FPGA in real time. While we adopt the SDI security framework established by [131], our security analysis extends it in several respects necessary for real-time operation: explicit treatment of analog-to-digital converter (ADC) clipping as trusted post-selection, conservative inflation factors for excess noise, temporal-mode definition addressing sample correlations, and security composition including calibration uncertainty. Together with the engineering implementation, this constitutes the first demonstration of SDI-certified random number generation with online extraction exceeding 30 Gb/s. By using an FPGA together with a dual-channel analog-to-digital converter (ADC12DJ5200RFEVM) operating at a sampling rate of $f_s = 3.2$ GHz per channel (up to 5.2 GHz maximum), both heterodyne detection channels are digitized in parallel to generate random numbers. A net extracted throughput of $R_{\text{net}} = 33.92$ Gbit/s is achieved on this set up. In the subsequent sections we cover the experimental setup, including the FPGA implementation, the results of the QRNG and its statistical tests.

6.4 Experimental details

6.4.1 General Setup

The experimental setup, shown in Fig. 6.1, implements a heterodyne detection scheme for vacuum fluctuation-based quantum random number generation. The system is built on a continuous-wave laser source LPSC-1550-FC with CLD1010LP laser diode driver from Thorlabs operating at wavelength $\lambda = 1550\,nm$ with output powers up to 30 mW. The laser output serves as the LO. It passes

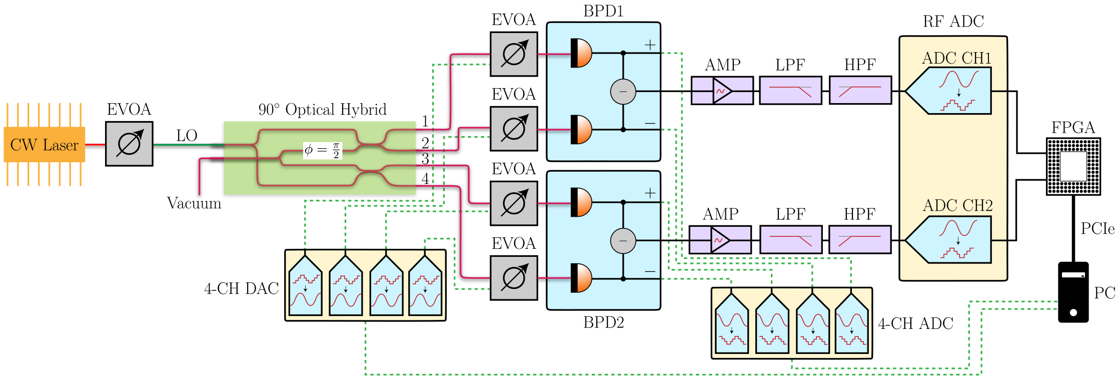

Figure 6.1: Schematic diagram of the vacuum fluctuation-based quantum random number generator using heterodyne detection. The setup consists of a laser source followed by a variable optical attenuator (VOA) for power control and stabilization. The laser output is mixed with vacuum fluctuations in a 90° optical hybrid, which simultaneously measures both X and P quadratures of the electromagnetic field. Each of the four hybrid outputs are individually controlled by electronically variable optical attenuators (EVOAs) with electrical control inputs before being detected by balanced photodiode detectors (BPD1 and BPD2). The analog electrical signals from both detectors are first filtered by a low-pass and high-pass filters to filter out as much classical electrical noise as possible and then digitized by a 2-channel ADC and processed in real-time by an FPGA connected via an FPGA Mezzanine card (FMC) interface.

through a VOA EVOA1550A to precisely control the LO power and to ensure its stability. The VOA is set to limit the detector-plane LO power to $\leq$ 15 mW for the variance–slope calibration range.

The LO is input to a 90° optical hybrid Optoplex model HB-C0AFAS066 operating in the telecom C-band. This device implements a 2×4 optical hybrid coupler that mixes the LO E_{LO} with the reference signal (vacuum in this case) E_{vac} from the environment to generate four quadratural states in the complex-field space.

Each of the four hybrid outputs is individually controlled by EVOAs Thorlabs V1550A. These devices enable real-time gain balancing which allows for 90° optical hybrid outputs to be properly balanced. This ensures equal power distribution to maintain the quadrature measurement accuracy and compensate for any asymmetries in the optical path.

The four EVOA outputs are paired and fed into two Thorlabs PDB480C-AC balanced photodiodes (BPDs). Each BPD consists of a pair of matched photodiodes operated in differential mode. The 90° optical hybrid routes the LO and the signal (vacuum at the signal port) so that ports (1,2) and (3,4) form two balanced pairs with a relative phase shift of 180° within each pair and 90° between the two pairs. With the diodes in differential mode, these two balanced differences implement a simultaneous measurement of orthogonal quadratures (heterodyne). Denoting the differential voltages by A and B (for the two BPDs), we model

$$\begin{aligned} A \equiv V_X \; &= \; \kappa_X \sqrt{P_{\mathrm{LO}}^{(\mathrm{det})}}\, X \; + \; n_{e,X}, \\ B \equiv V_P \; &= \; \kappa_P \sqrt{P_{\mathrm{LO}}^{(\mathrm{det})}}\, P \; + \; n_{e,P}, \end{aligned} \tag{6.1}$$

where $\kappa_{X/P}$ are responsivities [V/$\sqrt{\mathrm{W}}$], X, P are heterodyne quadrature outcomes with $\langle X \rangle = \langle P \rangle = 0$ and $\mathrm{Var}(X) = \mathrm{Var}(P) = \frac{1}{2}$, and $n_{e,X/P}$ are electronics noises (V).

Hence the shot-noise slopes satisfy

$$m_X = \frac{\kappa_X^2}{2}, \qquad m_P = \frac{\kappa_P^2}{2}. \tag{6.2}$$

Consequently, the variances scale linearly with LO power,

$$\begin{aligned} \mathrm{Var}(A) &= m_X P_{\mathrm{LO}}^{(\mathrm{det})} + \sigma_{e,X}^2, \\ \mathrm{Var}(B) &= m_P P_{\mathrm{LO}}^{(\mathrm{det})} + \sigma_{e,P}^2, \end{aligned} \tag{6.3}$$

where $\sigma_{e,X}^2$, $\sigma_{e,P}^2$ are the classical electronics noise variances (amplifier thermal noise, photodiode dark current, ADC quantization), measured with the LO blocked. These correspond to the intercepts $c_X = \sigma_{e,X}^2$ and $c_P = \sigma_{e,P}^2$ in the slope–offset calibration of Sec. 6.4.2.

The analog electrical signals from both BPDs, representing the X and P quadratures, first go through a ZX60-P105LN+ 15 dB amplifier to ensure that most of the ADC input range is covered, then they go through a series connected low-pass filter (LPF) and high-pass filter (HPF). The LPF is a SLP-1650+ with a bandwidth of DC-1650 MHz and the HPF is a SHP-200+ with a bandwidth of 185-3000 MHz, yielding an effective bandpass filter with a bandwidth of 185-1650 MHz. The upper limit was chosen at 1650 MHz since the diodes have a bandwidth of up to 1600 MHz and the sampling rate is 3.2 GHz, which puts the bandwidth slightly outside the Nyquist frequency; the *LPF* nominal passband is DC-1400 MHz with a -3 dB point at 1650 MHz. The lower bound was chosen at 185 MHz to reduce the classical lower frequency noise originating in the diodes. Lastly, the diode outputs are digitized by a 2-channel ADC ADC12DJ5200RFEVM with a sampling rate of $f_s = 3.2$ GHz set for both channels and a resolution of 12 bits. The digitized quadrature data streams are transmitted to a FPGA Virtex Ultrascale+ VCU118 development board via a high-speed FMC interface. The FPGA implements a real-time randomness extraction algorithm via Toeplitz hashing to generate provably random bit sequences from the quantum vacuum fluctuations by flattening the Gaussian distribution of the data.

6.4.2 Randomness Generation and Extraction

Security model

We model the QRNG as a prepare–measure protocol on n_{eff} temporal modes $A^{n_{\text{eff}}}$ impinging on a trusted receiver. The optical input is treated as fully untrusted: an adversary may prepare an arbitrary joint state $\rho_{A^{n_{\text{eff}}}E}$ of the incoming modes and a quantum memory E, allowing arbitrary entanglement and arbitrary inter-round correlations. The receiver is trusted and fixed prior to acquisition: the 90° hybrid, balanced detection, analogue front-end, ADC digitisation, the discretisation map (binning and the clipping rule), and the extractor circuit are treated as trusted. The Toeplitz seed is assumed uniform and independent of the measured data; Toeplitz hashing is a strong (universal$_2$) extractor.

In the SDI setting adopted here, security is enforced by the trusted receiver measurement rather than by a model of the optical source. The trusted receiver implements a discretised heterodyne POVM $\{M_z\}$ whose elements are determined by the calibrated discretisation in phase space; the resulting entropy bound depends only on these trusted bin regions through operator-norm bounds on $\|M_z\|_\infty$.

Minimum entropy quantifies the worst-case unpredictability of a random variable in the presence of an adversary. For a random variable X with probability distribution $p(x)$,

$$H_{min}(X) = -\log_2 \big(\max_x p(x)\big). \tag{6.4}$$

In QRNG security we use the smooth conditional min-entropy $H^{\varepsilon_s}_{\text{min}}(\cdot|E)$ where E denotes adversary's (quantum) side information; we write H for classical protocol history when needed. Let Z denote the discretised heterodyne outcome (ADC bin index). For a classical outcome Z correlated with quantum side information E, the (non-smooth) conditional min-entropy is defined operationally by the adversary's optimal guessing probability

$$\begin{aligned} H_{\text{min}}(Z|E) &= -\log_2 P_{\text{guess}}(Z|E), \\ P_{\text{guess}}(Z|E) &= \max_{\{E_z\}} \sum_z \text{Tr}[(M_z \otimes E_z)\rho_{AE}]\,, \end{aligned} \tag{6.5}$$

where $\{M_z\}$ is the trusted positive operator valued measurement (POVM) implemented on the

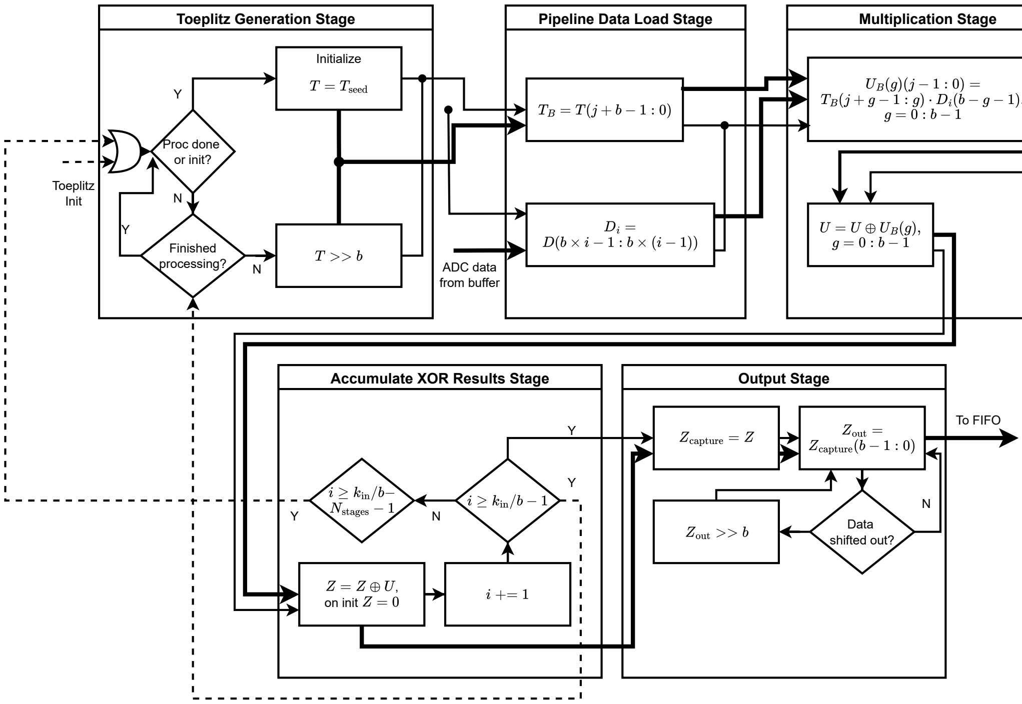

Figure 6.2: The pipelined Toeplitz extraction scheme. The scheme consists of separate pipeline stages. The dashed arrows indicate binary signals, the normal lines indicate the flow of the program and the bold, larger lines indicate flow of data. The square blocks represent operations and the diamond blocks represent conditionals.

optical mode and $\{E_z\}$ is an arbitrary POVM on E. Defining

$$c \;:=\; \max_z \|M_z\|_\infty, \tag{6.6}$$

the inequality $M_z \leq \|M_z\|_\infty \mathbb{I} \leq c\,\mathbb{I}$ implies, for any ρ_{AE},

$$\sum_z \mathrm{Tr}[(M_z \otimes E_z)\rho_{AE}] \leq \mathrm{Tr}\left[\left(c\,\mathbb{I} \otimes \sum_z E_z\right)\rho_{AE}\right] = c, \tag{6.7}$$

and hence $P_{\text{guess}}(Z|E) \leq c$ and $H_{\text{min}}(Z|E) \geq -\log_2 c$. For discretised heterodyne, Lemma 1 bounds $\|M_z\|_\infty$ in terms of the trusted bin area, yielding the state-independent bound used below.

Smooth conditional min-entropy evaluates non-smooth entropies on the optimal state within an ϵ-neighbourhood of the measured state, where ϵ is the security parameter, while the per-round heterodyne discretization bound is state-independent and holds *unsmoothed* [131]:

$$H_{min}(X|E) \geq -\log_2\left(\min\{\tfrac{\delta'_X \delta'_P}{2\pi}, 1\}\right), \tag{6.8}$$

The heterodyne POVM is $\Pi(\alpha) = |\alpha\rangle\langle\alpha|/\pi$, so $Q_\rho(\alpha) = \langle\alpha|\rho|\alpha\rangle/\pi$ and $\sup_\rho Q_\rho = 1/\pi$.

With $\mathrm{Var}(X) = \mathrm{Var}(P) = \frac{1}{2}$ we have $\alpha = (X + iP)/\sqrt{2}$ and $d^2\alpha = dX\, dP/2$. If the ADC defines rectangles $\{R_{mn}\}$ of area $\delta'_X \delta'_P$ in (X, P), then $\mathrm{Area}_\alpha(R_{mn}) = \delta'_X \delta'_P/2$. Hence (using $d^2\alpha = dX\, dP/2$ for vacuum units $\mathrm{Var}(X) = \mathrm{Var}(P) = 1/2$)

$$p_{\max} := \max_{m,n} \int_{R_{mn}} Q_\rho(\alpha)\, d^2\alpha \;\le\; \min\Big\{\tfrac{\delta'_X \delta'_P}{2\pi},\, 1\Big\}, \tag{6.9}$$

and

$$h^{(1)}_{\min} \;\ge\; -\log_2\Big(\min\big\{\tfrac{\delta'_X \delta'_P}{2\pi},\, 1\big\}\Big). \tag{6.10}$$

For any (possibly adversarial) preparation and any past transcript,

$$\max_{m,n} \Pr\big[(X, P) \in R_{mn} \,|\, \text{history}, \mathcal{E}\big] \le \min\Big\{\tfrac{\delta'_X \delta'_P}{2\pi},\, 1\Big\}, \tag{6.11}$$

and thus $h^{(1)}_{\min} \;\ge\; -\log_2\Big(\min\{\tfrac{\delta'_X \delta'_P}{2\pi},\, 1\}\Big)$ holds per round without independent and identically distributed (IID) assumptions and is adaptivity-robust.

Lemma 1. *Let $M_R = \int_R |\alpha\rangle\langle\alpha|\, \frac{d^2\alpha}{\pi}$ be the heterodyne POVM element for a measurable bin $R \subset \mathbb{C}$. Then*

$$\|M_R\|_\infty \;\le\; \min\Big\{\tfrac{\mathrm{Area}(R)}{\pi},\, 1\Big\}. \tag{6.12}$$

Proof. For any unit vector $|\psi\rangle$, $\langle\psi|M_R|\psi\rangle = \int_R Q_\psi(\alpha)\, d^2\alpha$ with $Q_\psi(\alpha) = |\langle\psi|\alpha\rangle|^2/\pi \le 1/\pi$; hence $\langle\psi|M_R|\psi\rangle \;\le\; \mathrm{Area}(R)/\pi$. Completeness of the POVM gives $\int_{\mathbb{C}} |\alpha\rangle\langle\alpha|\, \frac{d^2\alpha}{\pi} = \mathbb{I}$, so $0 \le M_R \le \mathbb{I}$ and $\|M_R\|_\infty \le 1$. Taking the tighter of the two bounds yields the stated minimum. □

Boundary (rail-adjacent but non-clipped) bins are treated as truncated rectangles with their actual area used in (6.9). ADC *clipping* codes result from voltages outside the input range $[-V_{\mathrm{pp}}/2,\, V_{\mathrm{pp}}/2]$ of the ADC. They correspond to semi-infinite regions and are excluded. Dropping clips is a post-selection on the event $\Omega_{\mathrm{acc}} := \{\text{no clip}\}$ determined solely by the trusted ADC range. For security we upper bound the rejection probability by a conservative value $f^{\max}_{\mathrm{clip}}$ fixed by the trusted ADC range and operating point (with any estimation uncertainty absorbed into β), so that $\Pr[\Omega_{\mathrm{acc}}] \ge 1 - f^{\max}_{\mathrm{clip}}$. Consequently, the single-round bound for the post-selected data becomes

$$h^{(1)}_{\mathrm{min,no\ clip}} \;\ge\; -\log_2\Big(\min\big\{\tfrac{\delta'_X \delta'_P}{2\pi(1 - f_{\mathrm{clip}})},\, 1\big\}\Big). \tag{6.13}$$

and the extraction length obeys

$$\begin{aligned} \ell \;\le\; n_{\text{valid}}\, h^{(1)}_{\text{min, no clip}} \;-\; 2\log_2 \frac{1}{\varepsilon_{\text{PA}}}, \\ n_{\text{valid}} = n(1 - f_{\text{clip}}), \end{aligned} \tag{6.14}$$

where n is the total number of rounds entering extraction.

Calibration and vacuum-unit resolutions

The bound depends only on the discretization induced by the apparatus. We determine the raw resolutions $\delta_{X/P}$ and the conservative resolutions $\delta'_{X/P}$ from a slope–offset calibration and the ADC's effective code width as follows.

$$\begin{aligned} \sigma^2_{V,X}(P_{\text{LO}}) = m_X P_{\text{LO}} + c_X, \\ \sigma^2_{V,P}(P_{\text{LO}}) = m_P P_{\text{LO}} + c_P, \end{aligned} \tag{6.15}$$

with $m_{X/P}$ in V^2/W and $c_{X/P} \ge 0$ in V^2. To exclude LO relative-intensity-noise leakage due to residual imbalance, we fit

$$\begin{aligned} \sigma^2_{V,X}(P_{\text{LO}}) = m_X P_{\text{LO}} + c_X + \eta_X P^2_{\text{LO}}, \\ \sigma^2_{V,P}(P_{\text{LO}}) = m_P P_{\text{LO}} + c_P + \eta_P P^2_{\text{LO}}, \end{aligned} \tag{6.16}$$

and test $\eta_{X/P} = 0$ via lack-of-fit. We found $|\eta_{X/P}| P_{\text{LO,max}} \ll m_{X/P}$ within the calibration range; thus linear shot-noise slopes are valid. If $\eta \neq 0$, its effect is absorbed by increasing $\gamma_{X/P}$ in (6.22).

Here $c_X = \sigma^2_{e,X}$ and $c_P = \sigma^2_{e,P}$, consistent with the detector model in (6.1). Since $\text{Var}(X) = \text{Var}(P) = \frac{1}{2}$ for vacuum, the conversion factors to vacuum units are:

$$\alpha_X = \sqrt{2 m_X P^{(\text{det})}_{\text{LO}}}, \quad \alpha_P = \sqrt{2 m_P P^{(\text{det})}_{\text{LO}}}, \tag{6.17}$$

here $P^{(\text{det})}_{\text{LO}}$ denotes the *per-BPD* LO power at the photodiodes *after* the 90° hybrid and EVOA balancing (i.e., the sum incident on the two diodes of a given BPD). All power readings used in (6.17) are taken at this plane. We define per-sample vacuum-unit coordinates by

$$\hat{X} := \frac{A}{\alpha_X}, \qquad \hat{P} := \frac{B}{\alpha_P}, \tag{6.18}$$

so that for vacuum $\text{Var}(\hat{X}) = \text{Var}(\hat{P}) = \frac{1}{2}$. With ADC peak-to-peak range $V_{\text{pp}} = 0.5\,\text{V}$ after the analog front end, define the effective code width

$$\Delta V_{\text{eff}} = \frac{V_{\text{pp}}}{2^{\,n_{\text{ENOB}}}}, \tag{6.19}$$

where $n_{\text{ENOB}} = 10.2$ (X channel) and 10.3 (P channel) is the measured effective number of bits of the ADC (sine-wave histogram method, averaged over 185–1600 MHz). Datasheet effective number of bits (ENOB) variation is absorbed into β. The raw resolutions are

$$\delta_X = \frac{\Delta V_{\text{eff}}}{\alpha_X}, \qquad \delta_P = \frac{\Delta V_{\text{eff}}}{\alpha_P}. \tag{6.20}$$

Let σ_X^2 and σ_P^2 denote the measured quadrature variances expressed in vacuum units after applying the gains $\alpha_{X/P}$ from (6.17). To conservatively include excess noise or calibration uncertainty, define

$$\begin{aligned} \gamma_X &:= \max\left\{1, \sqrt{\sigma_X^2/(1/2)}\right\}, \\ \gamma_P &:= \max\left\{1, \sqrt{\sigma_P^2/(1/2)}\right\}, \end{aligned} \tag{6.21}$$

$$\delta'_X = \gamma_X\,\delta_X, \qquad \delta'_P = \gamma_P\,\delta_P. \tag{6.22}$$

More generally, the single-shot bound reduction is $\log_2(\gamma_X\gamma_P)$. With the measured (σ_X^2, σ_P^2), the single-shot penalty is

$$\begin{aligned} \Delta h_{\text{min}}^{(1)} &= \log_2(\gamma_X\gamma_P) \\ &= \tfrac{1}{2}\log_2\!\big(\max\{1, 2\sigma_X^2\}\big) + \tfrac{1}{2}\log_2\!\big(\max\{1, 2\sigma_P^2\}\big). \end{aligned} \tag{6.23}$$

For $(\sigma_X^2, \sigma_P^2) = (0.616, 0.647)$ this gives $\Delta h_{\text{min}}^{(1)} \approx 0.336$ bits/round. In the symmetric case $\sigma_X^2 = \sigma_P^2 = \frac{1}{2}(1+\xi)$, where ξ is the relative excess noise above the vacuum variance, one has $\gamma_X = \gamma_P = \sqrt{1+\xi}$ and the reduction equals $\log_2(1+\xi)$. The guard $\gamma \geq 1$ prevents artificial entropy gain if $\sigma^2 < 1/2$ due to calibration uncertainty. Imperfections in the 90° optical hybrid and detection chain (non-ideal phase shift, unequal splitting ratios, detector gain mismatch) can induce correlation between the X and P quadratures. We measured the raw cross-quadrature correlation to be $|\rho_{XP}| = 0.012 \pm 0.004$ at zero lag. To verify no correlation structure exists at nonzero delays, we computed the full cross-correlation function as a function of sample lag (Fig. 6.8); the cross-correlation remains below 10^{-3} at all measured delays, confirming that coupling is confined to the zero-lag term and does not introduce temporal structure.

This correlation does not compromise the security bound. The per-round bound $p_{\max} \leq \delta'_X \delta'_P/(2\pi)$ derives from the operator norm of the POVM element (Lemma 1), which depends only on the bin area in phase space, not on the correlation structure of the input state. An adversary could prepare an arbitrarily correlated state, and the bound would still hold because it is a property of the trusted measurement, not the source. At our measured $|\rho_{XP}| = 0.012$, a hypothetical correlation penalty would be $\Delta h_{\text{corr}} = -\frac{1}{2}\log_2(1-\rho_{XP}^2) < 10^{-4}$ bits/round, which is negligible. No decorrelation step is required.

We propagate uncertainties in $(m_{X/P}, c_{X/P}, V_{\text{pp}}, n_{\text{ENOB}})$ to (δ'_X, δ'_P) and to $h_{\text{min}}^{(1)}$ by first-order error propagation; error bars for $\delta'_{X/P}$ and the net rate include these calibration contributions.

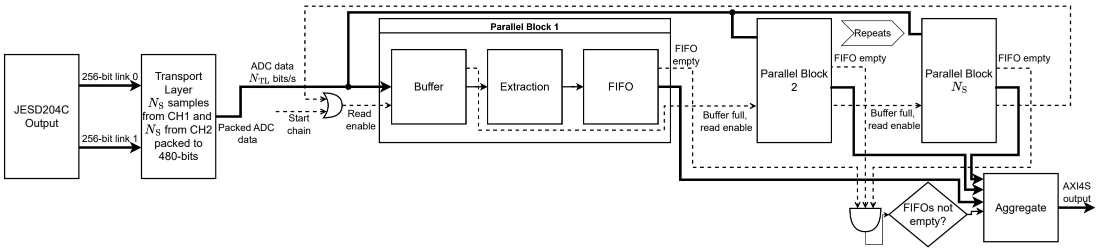

Figure 6.3: The overall schematic of the FPGA design. All parallel blocks contain the same functions and I/O, only the first block is fully drawn to make the diagram more compact. The dashed arrows indicate binary signals, the normal lines indicate the flow of the program and the bold, larger lines indicate flow of data.

The security proof relies on the fact that for any quantum state, the Husimi function $Q_\rho(q+ip)$ is upper bounded by $1/\pi$. This fundamental quantum mechanical constraint ensures that even if an adversary prepares an optimal quantum state to maximize their guessing probability, the conditional min-entropy remains bounded by the measurement resolution alone [131]. This bound is independent of the actual quantum state prepared by the potentially malicious source, providing information-theoretic security guarantees. Practical implementations must account for device imperfections that can compromise this security. Imbalanced heterodyne detection, arising from non-ideal beam splitter ratios or photodiode efficiency mismatches, introduces local oscillator fluctuation that contributes excess noise. Under imbalanced conditions, LO fluctuation cannot be eliminated and affects the calibration of vacuum fluctuations [226]. Without proper consideration of these fluctuations, the extractable randomness can be overestimated, creating security vulnerabilities. For this reason, we use additional EVOAs at the 90° optical hybrid, since it does not show perfect 50:50 splitting ratio.

As mentioned before, upon initial measurements of this system, the resulting distribution is Gaussian, which makes it easier to predict the generated random numbers. For this reason, a randomness extractor has to be used to flatten the distribution and extract the QRNG which is mixed with classical noise sources. One of the more commonly used extractors is Toeplitz hashing [213, 214, 227, 120, 131, 225], belonging to universal$_2$ family and hence a *strong* extractor [228, 229]: for a public, uniform, independent seed S, $(S, \mathrm{Ext}(Z^n, S)) \approx (S, U_j)$.

We reuse the same public seed S across all parallel output blocks within one extractor invocation; Toeplitz hashing is a strong (universal$_2$) extractor, and our single-round heterodyne min-entropy bound is independent of S and the classical transcript. Hence, by a hybrid/triangle-inequality argument applied block by block, the joint trace distance satisfies

$$\begin{aligned} &\Big\|(S, \mathrm{Ext}(Z^n_{(1)}, S), \ldots, \mathrm{Ext}(Z^n_{(B)}, S), E) - \\ &(S, U_{\ell_1}, \ldots, U_{\ell_B}, E)\Big\|_{\mathrm{tr}} \;\le\; \sum_{i=1}^{B} \big(\varepsilon_s^{(i)} + \varepsilon_{\mathrm{PA}}^{(i)}\big) \end{aligned} \tag{6.24}$$

where $\varepsilon_s^{(i)}$ is the smoothing error of a block and $\varepsilon_{\mathrm{PA}}^{(i)}$ is the privacy amplification error of a block. In this way we allocate $(\varepsilon_s^{(i)}, \varepsilon_{\mathrm{PA}}^{(i)})$ so that the sum over blocks equals the advertised $\varepsilon_{\mathrm{sec}}$.

The two 12-bit ADC codes are concatenated into a single 24-bit symbol $D_i := (X_i \| P_i)$ at each sampling instant. This concatenation is mandated by the security model: the heterodyne POVM $\Pi(\alpha) = |\alpha\rangle\langle\alpha|/\pi$ is a joint measurement on 2D phase space that cannot be factored into independent marginal measurements. The min-entropy bound (Eq. 6.10) certifies entropy of the pair (X, P) via the joint bin area; treating the quadratures as separate streams would require a different security analysis based on marginal distributions rather than the joint Husimi bound.

The heterodyne bound is state- and history-independent: for every retained round $t \le n_{\mathrm{eff}}$ and any classical transcript H,

$$p_{\max}^{(t)} \;\le\; \min\Big\{\tfrac{\delta_X' \delta_P'}{2\pi},\, 1\Big\}. \tag{6.25}$$

Because the trusted device applies the same per-round POVM $\{M_z\}$ to each temporal mode and does not adapt to H, one has for any cq state with arbitrary inter-round correlations

$$\begin{aligned} H_{\min}^{\varepsilon_s}(Z^{n_{\mathrm{eff}}}|E, H) \;&\ge\; n_{\mathrm{eff}}\, h_{\min}^{(1)}, \\ h_{\min}^{(1)} &= -\log_2\Big(\min\{\tfrac{\delta_X' \delta_P'}{2\pi}, 1\}\Big). \end{aligned} \tag{6.26}$$

where n_{eff} is the number of temporal modes on which the trusted POVM $\{M_z\}$ acts identically.

We report integrated autocorrelation time τ_{int} as a diagnostic of classical correlations in the sampled voltage stream. A conservative way to enforce approximate factorization is to define rounds on a decimated stream with spacing D samples (e.g. $D \geq \lceil \tau_{\text{int}} \rceil$), leading to $n_{\text{eff}} = n/D$ and an effective sampling rate $f_s^{(\text{eff})} = f_s/D$. In our reported security analysis and rates, we instead apply a fixed unit-Jacobian orthonormal transform on blocks before discretization, so that the n samples are mapped to n orthonormal temporal modes measured by the same POVM $\{M_z\}$; in this case we take $n_{\text{eff}} = n$ and $f_s^{(\text{eff})} = f_s$, and τ_{int} is used purely as a diagnostic check that residual correlations after extraction are within statistical error. The analog front-end and sampling chain are trusted and absorbed into the calibration that defines $\delta'_{X/P}$. After enforcing factorization as above, the product-POVM structure holds on the retained temporal modes and we use $H_{\min}(Z^{n_{\text{eff}}}|E) \geq n_{\text{eff}}\, h_{\min}^{(1)}$.

We separate the secrecy parameter from statistical-estimation error, thus we define

$$\varepsilon_{\text{sec}} = \varepsilon_s + \varepsilon_{\text{PA}} + \beta, \tag{6.27}$$

where β upper-bounds the probability that calibration parameters deviate outside their quoted confidence intervals. Privacy amplification obeys

$$\ell \leq H_{\min}^{\varepsilon_s}(Z^{n_{\text{eff}}}|E) - 2\log_2 \frac{1}{\varepsilon_{\text{PA}}}. \tag{6.28}$$

Here E denotes adversarial (quantum) side information. Since $H_{\min}^{\varepsilon_s}(\cdot|E) \geq H_{\min}(\cdot|E)$ for any $\varepsilon_s \in [0, 1)$, our unsmoothed lower bound $H_{\min}(Z^{n_{\text{eff}}}|E) \geq n_{\text{eff}}\, h_{\min}^{(1)}$ also lower-bounds the smoothed quantity used in privacy amplification.

Here β upper-bounds the probability that the calibration parameters $(m_{X/P}, c_{X/P}, \Delta V_{\text{eff}}, n_{\text{ENOB}})$ deviate outside their quoted confidence intervals; it is set via conservative concentration bounds for the variance fits and datasheet limits. We set $\varepsilon_s = \varepsilon_{\text{PA}} = \beta = 2^{-64}$, yielding $\varepsilon_{\text{sec}} = 3 \cdot 2^{-64}$. If the data are output in N_{blk} extractor invocations (fresh or reused public seed), we allocate per-block parameters $(\varepsilon_s/N_{\text{blk}},\ \varepsilon_{\text{PA}}/N_{\text{blk}},\ \beta/N_{\text{blk}})$ so that a union bound guarantees the advertised global bound on ε_{sec}.

6.4.3 FPGA Implementation

The FPGA receives 20 samples for each channel per 160 MHz clock cycle, or 480-bits of data, over 16 JESD204C data lanes. This results in a total data rate of 76.8 Gbps at 3.2 GHz sample rate and 2-channel acquisition. Therefore, both pipelining and parallelization were applied to ensure that the data is processed in real-time. Fig. 6.2 shows how the Toeplitz extraction scheme was implemented. In the figure shown, there are 5 pipelines stages, however, there is an additional initial stage for buffering ADC input, which is covered in further text.

Once there is data available in the input buffer, the pipeline starts with the Toeplitz generation stage. It can be seen that there is an OR gate for two signals, one which is triggered when Toeplitz extraction is done and another called Toeplitz init, which is only set when the FPGA is reset, so as to ensure proper Toeplitz matrix initialization on FPGA power on. If one of these signals is triggered, the initial Toeplitz vector signal T is set from the independently generated seed. When neither of the two aforementioned signals is triggered, it indicates that Toeplitz extraction is running, therefore T is shifted to the right by the combined bit-depth b. The right shift is needed because a block of the Toeplitz matrix T_B is taken in the next pipeline data loading stage. A total of $j + b$ bits are taken for a block, which effectively corresponds to b columns of the Toeplitz matrix, since, if the column size is j, the next column can be formed by $T_B(j + 1 : 1)$ (T_B here denotes a block of the Toeplitz matrix). When T is shifted to the right by b, it results in taking further b columns of the Toeplitz matrix. In the same block, the b-bit ADC word D_i is taken every cycle from the buffer D.

Following is the multiplication stage, where first, the multiplication is done for the block of Toeplitz matrix, which is then stored in an intermediate two-dimensional vector U_B. As mentioned before, the numbers in the matrices are in binary, therefore mod 2 arithmetic applies. Therefore, the multiplication is calculated by applying AND bitwise operation on a single column of the Toeplitz matrix by a single bit of the ADC data D_i. This operation is done over a range of 0 to $b - 1$ so as to multiply all b columns in the same cycle. Afterwards, a XOR reduction is done on U_B, which corresponds to the b-column multiplication sum, and is stored in U. After this, U goes to the XOR accumulation stage, where each clock cycle U is accumulated in the final result vector Z. This is done k_{in}/b times, until the ADC input buffer is fully processed. In this stage there are also two conditions: $i \geq k_{\text{in}}/b - 1$ is used to signal when Z is fully accumulated and it can be output, and $i \geq k_{\text{in}}/b - N_{\text{stages}} - 1$, where N_{stages} is the number of stages between the Toeplitz generation and accumulation stages (in this case 3), which is necessary to ensure timely initialization of T, since the Toeplitz generation stage operates ahead of the accumulation stage due to pipelining created latency.

When the $i \geq k_{\text{in}}/b - 1$ condition is satisfied, the output stage is started, where firstly Z is captured to Z_{capture} to ensure that the extracted value is not overridden by further calculations in the pipeline. The data is output in pieces of b bits for j/b cycles by shifting Z_{out} to the right by b. Lastly, it should be mentioned that between all these stages there's a single clock cycle latency and that initially all stages are inactive until the first Toeplitz stage becomes active.

Fig. 6.2 shows only the extraction diagram of a single block. If f_{ADC} is the ADC sampling frequency (per channel), the total input rate is $b\,f_{\text{ADC}}$ bits/s, where $b = 2\,n_{\text{ADC}} = 24$ bits/round. The FPGA receives N_{S} samples per cycle per channel, so the reference clock is $f_{\text{ref}} = f_{\text{ADC}}/N_{\text{S}}$. A single block processes b bits per clock cycle, i.e., $b\,f_{\text{ref}}$ bits/s. Thus the number of parallel blocks required for full throughput is $N_{\text{B}} = \frac{b f_{\text{ADC}}}{b f_{\text{ref}}} = N_{\text{S}}$. In our setup $N_{\text{S}} = 20$, so 20 blocks are used to extract randomness in real time.

Fig. 6.3 shows the full implementation of the FPGA design. Starting on the left, there is the JESD204C protocol output of the ADC, which goes into the transport layer, where first JESD204C lanes are appropriately mapped, then samples are extracted from the frames and finally the values are packed into 480-bit AXI4 Stream buses, where both CH1 and CH2 samples are interleaved in 24-bit words. This data is then sent to all the extraction blocks. All the blocks are interconnected by the buffering logic. The buffer is an additional pipeline stage part of the extraction schematic shown in Fig. 6.2. It consists of additional logic that ensures that the right amount of data is being read and to allow for proper operation with other parallel extraction blocks. More specifically, the buffer block additionally has a read enable input and a buffer full output. The buffer does not take any data until read enable is asserted and the buffer full output is asserted when the buffer is filled.

Such a design allows for daisy chaining the blocks and allow them to work in parallel. As seen in Fig. 6.3 the read enables and the buffer full signals are chained together, with the exception of the first block, where there is an OR gate to the input of read enable. Initially, all of the blocks are inactive. Once ADC data becomes valid, the start chain signal connected to the OR gate of the first block read enable is asserted, which starts the ADC sample collection in the first block's buffer. Once the buffer is full, the buffer full signal is asserted and the collection starts in the second block and continues until the last block, where the buffer full signal is fed back to the first one, repeating the chain again. Finally, after extraction, the random bits are sent into a first in - first out (FIFO). The FIFO empty signals from each block are checked and when the condition of all FIFOs not being empty is satisfied, the FIFO outputs are read and are collated into a single vector signal.

To realize the full potential of the high bandwidth QRNG, the extracted data is sent over x16 PCIe to a computer. The PCIe interface on the FPGA runs with a clock speed of 250 MHz and 512-bit depth. To ensure proper clock domain crossing (CDC), the QRNG data first goes into an asynchronous FIFO, from which the PCIe interface reads. PCIe on the FPGA is handled by the XDMA IP provided by AMD. The computer that the FPGA is connected to runs Linux and uses the AMD provided XDMA driver to stream the data from the FPGA to the computer over an AXI4 Stream interface. There is an additional, not shown channel of the PCIe used to also transfer the raw, unextracted data to the computer. It is used both for security analysis and for monitoring the system during operation. The full implementation was successfully placed and routed without any timing issues. The used resources for a Toeplitz extraction for $j = 1272$, $k = 2880$ and 20 parallel blocks can be seen in Table 6.2. The most significant usage is seen in the look-up tables (LUTs), which is expected, since even though the operations are not applied on a full matrix, the vector widths are still relatively large and therefore a lot of LUTs are needed to perform the bitwise operations over 20 independent extraction blocks. The matrix size could be slightly increased, however, at higher resource usage values the design has higher likelihood to fail implementation, since when usage is over 75 %, congestion becomes an issue, making the placement and routing of logic challenging [230].

Resource	Used	Available	Utilization (%)
LUT	596422	1182240	50.4
LUTRAM	12697	591840	2.1
FF	329457	2364480	13.9
BRAM	197	2160	9.1
DSP	20	6840	0.3
IO	24	832	2.9
GT	32	52	61.5
BUFG	25	1800	1.4
MMCM	1	30	3.3
PCIe	1	6	16.7

Table 6.2: FPGA resource utilization for $j = 1272$ and $k_{\text{in}} = 2880$ Toeplitz matrix extraction algorithm with 20 parallel blocks.

6.5 Results and Discussion

Security Analysis

The SDI security of our QRNG derives from the measurement-device characterization, not from statistical properties of the output. Specifically, the per-round min-entropy bound (Eq. 6.10) follows from the operator norm of heterodyne POVM elements (Lemma 1), which holds for *any* input state—including states prepared adversarially to maximize the guessing probability. The security-critical parameters are therefore the calibrated bin dimensions δ'_X, δ'_P and the privacy amplification composition $\varepsilon_{\text{sec}} = \varepsilon_s + \varepsilon_{\text{PA}} + \beta$. In Fig. 6.4 we show the power spectral density (PSD) of both ADC channels when measuring with LO and without LO. The results are similar to other heterodyne and homodyne set-ups, where we see an LO-induced noise-power increase of ≈ 7.5 dB (X) and ≈ 6.5 dB (P) [214, 224, 231], indicating that quantum noise is present, not only the classical noise. In particular,

$$\Delta_{\text{dB}}^{(X)} = 10\log_{10}\left(\frac{m_X P_{\text{LO}}^{(\text{det})} + c_X}{c_X}\right), \qquad \Delta_{\text{dB}}^{(P)} = 10\log_{10}\left(\frac{m_P P_{\text{LO}}^{(\text{det})} + c_P}{c_P}\right), \tag{6.29}$$

which follow from (6.15). With $m_X = 2.41\times10^{-1}\,\text{V}^2/\text{W}$, $c_X = 4.35\times10^{-4}\,\text{V}^2$, $m_P = 2.33\times10^{-1}\,\text{V}^2/\text{W}$, $c_P = 5.60\times10^{-4}\,\text{V}^2$, and $P_{\text{LO}}^{(\text{det})} = 8.4\,\text{mW}$,

$$\Delta_{\text{dB}}^{(X)} \approx 7.52\ \text{dB}, \qquad \Delta_{\text{dB}}^{(P)} \approx 6.52\ \text{dB}. \tag{6.30}$$

One difference compared to the other references is the dip in intensity we see below 0.2 GHz, which is caused by the HPF we have added which has a bandwidth of 185 to 3000 MHz. The resulting filter band (185–1650 MHz) lies only slightly outside of Nyquist frequency for $f_s = 3.2\,\text{GHz}$ ($f_s/2 = 1.6\,\text{GHz}$), so residual aliasing into the analysis region is negligible. Another inconsistency is the observation of spikes in the spectrum. The spikes at the highest frequency are related to spurious codes of the ADC at $f_s/2$. The spikes at lower frequencies are related to electromagnetic interference resulting from surrounding electronics because they can be seen with LO off or on, indicating that their source is not related to the optics. These spikes are narrow in bandwidth and do not impact the security after extraction.

As a consistency check, we integrate the PSD difference (LO on minus LO off) over the analysis band (185–1600 MHz) to obtain the quantum-to-classical noise ratio (QCNR), reported with uncertainty. This cross-check is consistent with the slope-based calibration used for $\delta'_{X/P}$ and is not used directly in the entropy bound.

PSD estimates were obtained using a one-sided periodogram with a Hann window (equivalent noise bandwidth, ENBW $= 1.5\,\Delta f$). The fast Fast Fourier Transform (FFT) length was set to $N = 2^{20}$, with a sampling rate of $f_s = 3.2\,\text{GS/s}$, resulting in a frequency bin width of $\Delta f = f_s/N$. Each spectrum was averaged over $M = 64$ blocks, and the error is $\pm 1.96/\sqrt{M}$ confidence interval on the dB scale, which is not shown due to being negligibly small.

To further characterize the QRNG, we measure the Husimi Q function and the variance dependence on LO power. With the vacuum-unit axes from Eqs. (6.15)–(6.22), the 2D histogram H_{mn}

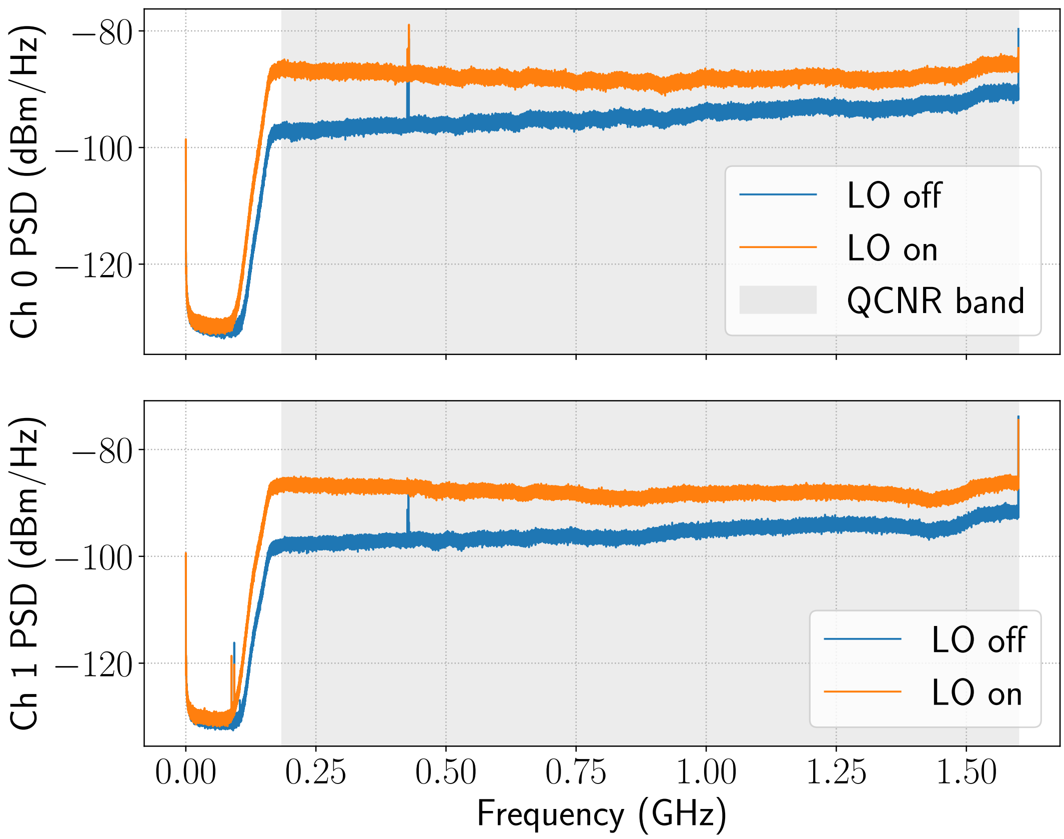

Figure 6.4: PSD of both ADC channels that are connected to the balanced diodes. The blue curve corresponds to no laser power and the orange curve to a local-oscillator power of 8.4 mW. The gray colored area shows over which range the PSD is integrated for QCNR.

over bin area $\delta'_X \delta'_P$ is converted via

$$\widehat{Q}_{mn} := \frac{2\,H_{mn}}{N\,\delta'_X \delta'_P}, \qquad \sum_{m,n} \widehat{Q}_{mn}\,\frac{\delta'_X \delta'_P}{2} = 1. \tag{6.31}$$

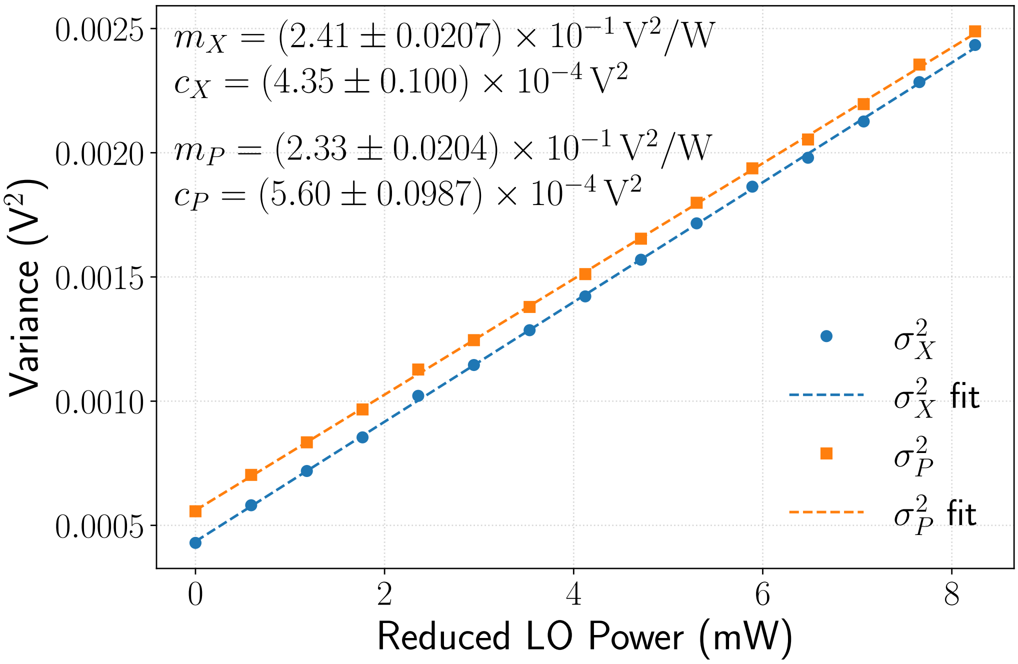

Figure 6.5: The dependence of both quadrature measured signal variance on the local oscillator laser power.

The calibration curve is shown in Fig. 6.5. The resulting fit values are:

$$\begin{aligned} m_X &= (2.41 \pm 0.0207) \times 10^{-1}\,\mathrm{V}^2/\mathrm{W}\ (95\%\ \mathrm{CI}), \\ c_X &= (4.35 \pm 0.100) \times 10^{-4}\,\mathrm{V}^2\ (95\%\ \mathrm{CI}), \\ m_P &= (2.33 \pm 0.0204) \times 10^{-1}\,\mathrm{V}^2/\mathrm{W}\ (95\%\ \mathrm{CI}), \\ c_P &= (5.60 \pm 0.0987) \times 10^{-4}\,\mathrm{V}^2\ (95\%\ \mathrm{CI}) \end{aligned}$$

At the operating LO power $P_{\mathrm{LO}}^{(\mathrm{det})} = 8.4\,\mathrm{mW}$ we obtain dimensionless vacuum-unit variances (e.g., $\sigma_X^2 \simeq 0.616$, $\sigma_P^2 \simeq 0.647$) and the conservative resolutions

$$\delta'_X = 0.0300 \quad \text{and} \quad \delta'_P = 0.0319 \tag{6.32}$$

(with uncertainties), computed via Eqs. (6.17)–(6.22). These resolutions are then used to convert the voltage histogram to the phase-space representation shown in Fig. 6.6. From these resolutions,

$$
\begin{aligned}
h_{\text{min}}^{(1)} &= -\log_2\Big(\min\{\tfrac{\delta'_X\delta'_P}{2\pi},\, 1\}\Big)\\
&= \log_2\left(\frac{2\pi}{0.0300\times 0.0319}\right) \approx 12.681 \text{ bits/round.}
\end{aligned}
\tag{6.33}
$$

For $n_{\text{eff}} = k_{\text{in}}/b = 2880/24 = 120$ rounds per block, this gives

$$
H_{\text{min}}(Z^{n_{\text{eff}}}|E) \geq 1521 \text{ bits/block.} \tag{6.34}
$$

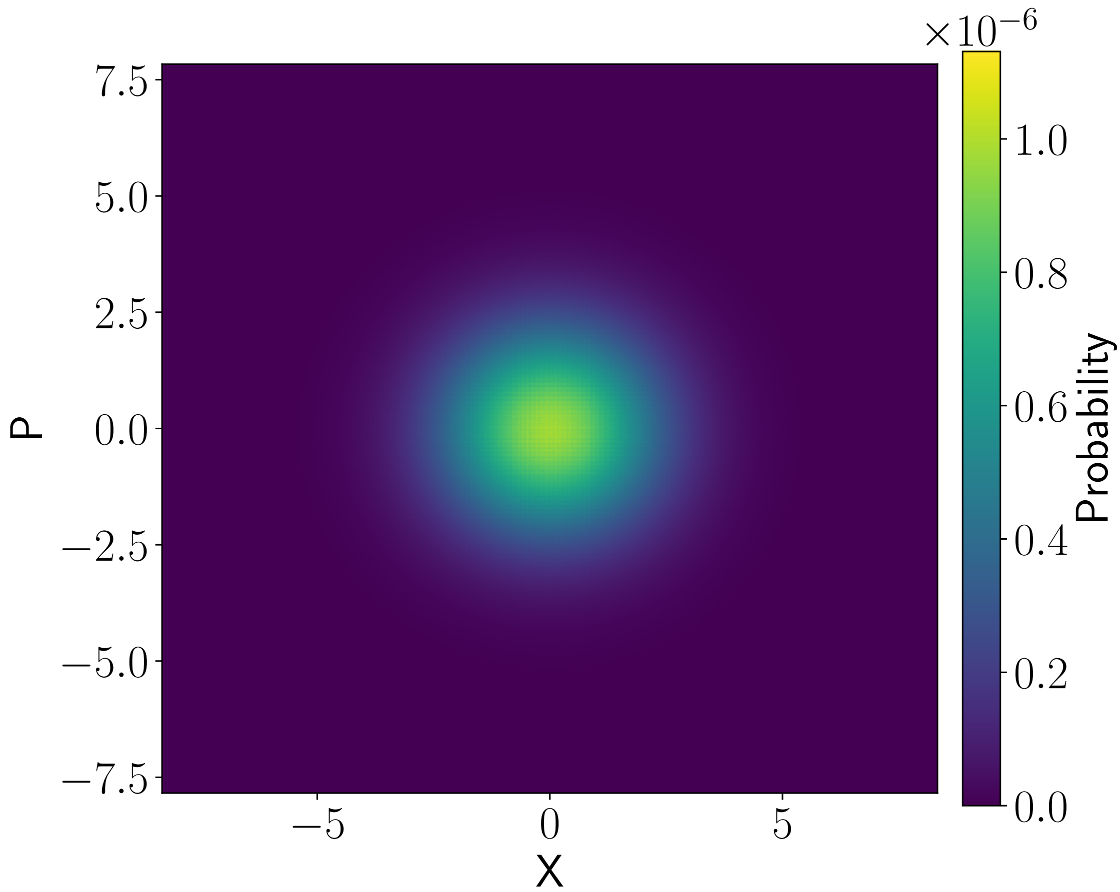

Figure 6.6: Husimi–Q distribution in quadrature space: horizontal axis shows the in-phase quadrature X and vertical axis the orthogonal quadrature P. The color scale encodes the normalized probability per pixel.

We verified that the empirical bin frequencies f_{mn} satisfy $f_{mn} \leq \min\{\delta'_X\delta'_P/(2\pi),\, 1\} + \Delta$ with high confidence, using a multiplicative Chernoff bound at significance $\alpha = 10^{-6}$ together with a union bound over all bins (m, n); violations signal a calibration error in $(\alpha_{X/P}, \delta'_{X/P})$.

Several discrepancies can be seen compared to Ref. [131]. Firstly, we show an increased variance value in vacuum units. The most likely reason is the difference in set-ups. Ref. [131] immediately measures the quadrature signals from the diode with an oscilloscope that has a low enough measurement range to capture the low diode voltages. In our case, the lowest voltage that can be measured with the ADC without measurement quality deterioration is 0.5 V peak-to-peak (from -0.25 to 0.25 V), therefore, we have used an amplifier, which may have different noise characteristics, potentially causing an increase in the noise.

The second difference is that in our case the power dependencies of both quadratures do not completely overlap. This is also related to the difference in set-ups. Together with amplifiers we used hardware filters to reduce the complexity of the FPGA implementation. While the components models were the same between the two quadratures, there can still be variations between the same devices in insertion loss, gain, and other characteristics that can cause a reduction in the signal. To increase the overlap, we used the EVOAs before the photodiodes to reduce the power of one of the quadratures.

With the power calibration complete, we obtain $H_{\text{min}} \geq 1521$ per block; we extract $\ell = 1272$ bits per block, i.e. $(\ell/k_{\text{in}}) \approx 0.442$, using a 1272×2880 Toeplitz matrix. The next step is to confirm whether the Toeplitz extraction algorithm is flattening the distribution seen in Fig. 6.6. This can be partially done by looking at the autocorrelation of the numbers before and after extraction, which is shown in Fig. 6.7. The gap between the min-entropy bound (1521 bits) and extracted length (1272 bits) is deliberate. The leftover hash lemma requires a privacy amplification penalty of $2\log_2(1/\varepsilon_{\text{PA}}) = 128$ bits for $\varepsilon_{\text{PA}} = 2^{-64}$, yielding a theoretical maximum of 1393 bits. We extract $\ell = 1272 = 24 \times 53$ bits, which aligns with the 24-bit word boundaries required by the parallel FPGA pipeline. The remaining 121-bit margin provides robustness against calibration drift during continuous operation.

The net extracted bit rate is

$$R_{\text{net}} = \frac{\ell}{n_{\text{eff}}} f_s^{(\text{eff})}, \tag{6.35}$$

where n_{eff} is the number of retained rounds after enforcing factorization (by fixed-ratio decimation or an invertible whitener). For decimation by D, $n_{\text{eff}} = n/D$ and $f_s^{(\text{eff})} = f_s/D$; for an orthonormal (unit-Jacobian) transform $n_{\text{eff}} = n$ and $f_s^{(\text{eff})} = f_s$. Clipped samples are dropped, so n_{eff} already counts valid rounds and no separate Δ_{clip} term is needed. The measured clipping fraction at the operating point is $f_{\text{clip}} = 2.3 \times 10^{-6}$ (95% confidence interval (CI)).

There is a clear correlation observed in the random data before extraction, which is also seen in other QRNGs [131, 214, 232]. It is caused partially by noise introduced by the sampling de-

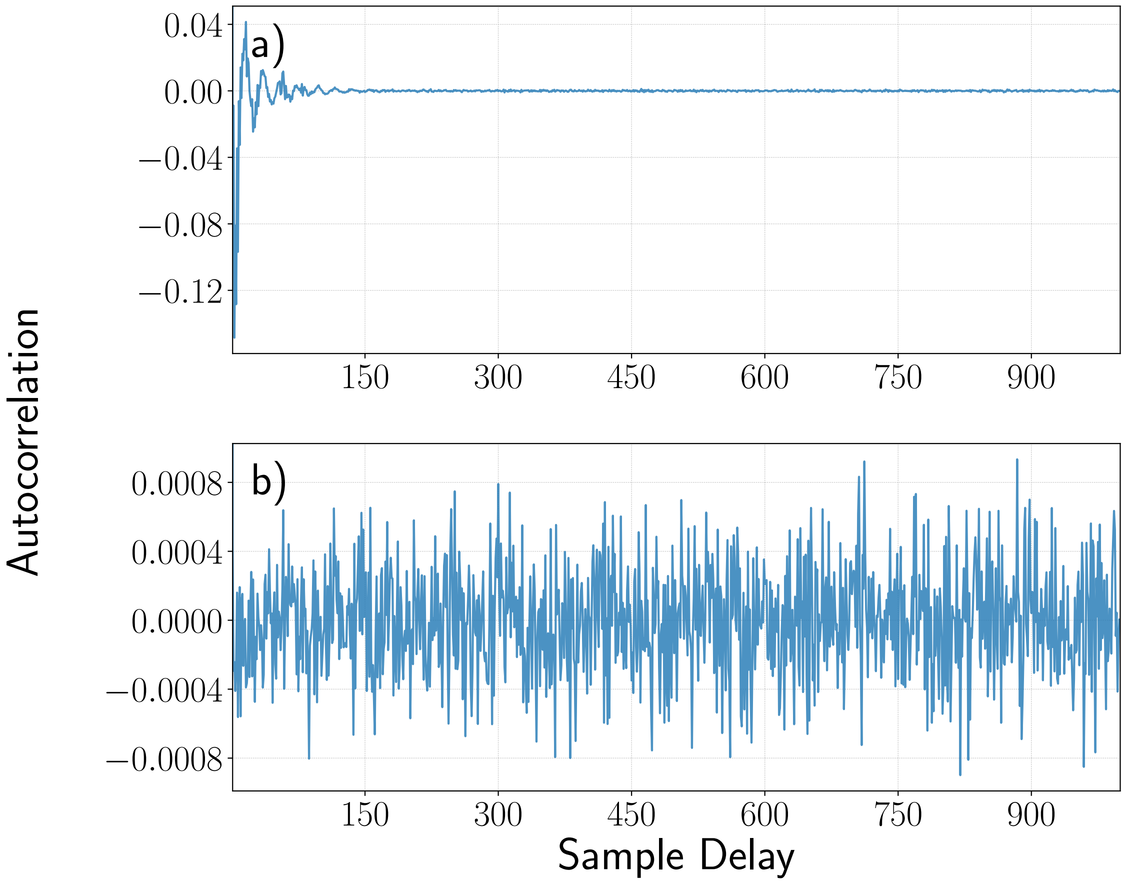

Figure 6.7: Autocorrelation comparison between (a) raw quadrature data and (b) extracted random bits. Panel (a) shows significant positive correlation at short lags, decaying over ≈3 samples consistent with the band-limited detection bandwidth ($\tau_c \sim 1/\Delta f$). Panel (b) shows residual correlations after Toeplitz extraction at the 10^{-4} level, indistinguishable from statistical noise, confirming successful removal of correlated structure. This comparison serves as a diagnostic verifying that the extractor operates as designed. Lag axis is in units of 10^3 samples; optical power 8.4 mW; 10^7 samples used.

vice [131], however, the most significant contributor in this case is the sample rate related to the filtering that we apply. Band-limitation induces temporal correlations. We estimate the normalized autocorrelation function (ACF) $\rho(k)$ and define the integrated autocorrelation time

$$\tau_{\text{int}} := \max\Big\{1,\ 1 + 2\sum_{k=1}^{K^\star} \rho(k)\Big\}, \\ K^\star = \min\{k \geq 1 : |\rho(k)| < 2/\sqrt{N_{\text{samp}}}\}. \tag{6.36}$$

In our data we obtain

$$\tau_{\text{int}} = 2.68 \pm 0.00011 \text{ (95\% CI)},$$

using $B = 10^4$ bootstrap resamples with block length $\ell_B = 10^5$ to keep the calculation time reasonable. Nyquist-rate sampling ($f_s = 2\Delta f$) prevents aliasing but does not yield independent samples; approximate independence would require $f_s \lesssim \Delta f$, reducing throughput by at least half. We instead sample at $f_s = 3.2$ GS/s and let the extractor compression ratio $\ell/k_{\text{in}} \approx 0.44$ absorb the correlation structure. This is consistent with the security model: the per-round bound derives from the glsPOVM operator norm (Lemma 1), which holds for any input state including states correlated with previous rounds. The accumulation $H_{\min}(Z^n|E) \geq n \cdot h^{(1)}_{\min}$ requires only that the trusted measurement applies identical non-adaptive POVMs, a condition satisfied by fixed ADC discretization regardless of temporal correlations. The quantity τ_{int} thus serves as a diagnostic confirming the analog chain behaves as characterized, not as an input to the min-entropy bound. After extraction, residual autocorrelations are consistent with statistical fluctuations (we do not reduce the security bound by τ_{int} since it can be minimized by decimating the sampling frequency). We inspected higher-order autocorrelations (Ljung–Box) up to a fixed lag window, finding no statistically significant residual structure at the 95% level. The experimental cross-quadrature correlation was $|\rho_{XP}| = 0.012 \pm 0.004$, consistent with the negligible correlation penalty reported in Section II. This completes the security-relevant calibration; the min-entropy bound and extraction parameters are now fully determined.

Statistical Diagnostics

The following tests serve as implementation diagnostics to verify that the hardware operates as modeled. We emphasize that statistical tests are necessary but not sufficient for security: a deterministic pseudorandom number generator with sufficient state size will pass all such tests while possessing zero min-entropy against an adversary who knows the algorithm. The security of our

QRNG is established by the calibration and min-entropy analysis of Section 6.5, not by the tests below.

We additionally inspected cross-correlation between X and P quadratures of the raw data to confirm there is no correlation introduced by the ADC sampling or the electrical filtering. The correlation computation was performed in the same method as for autocorrelation. The result can be seen in Fig. 6.8, which shows that the cross-correlation between X and P is negligible.

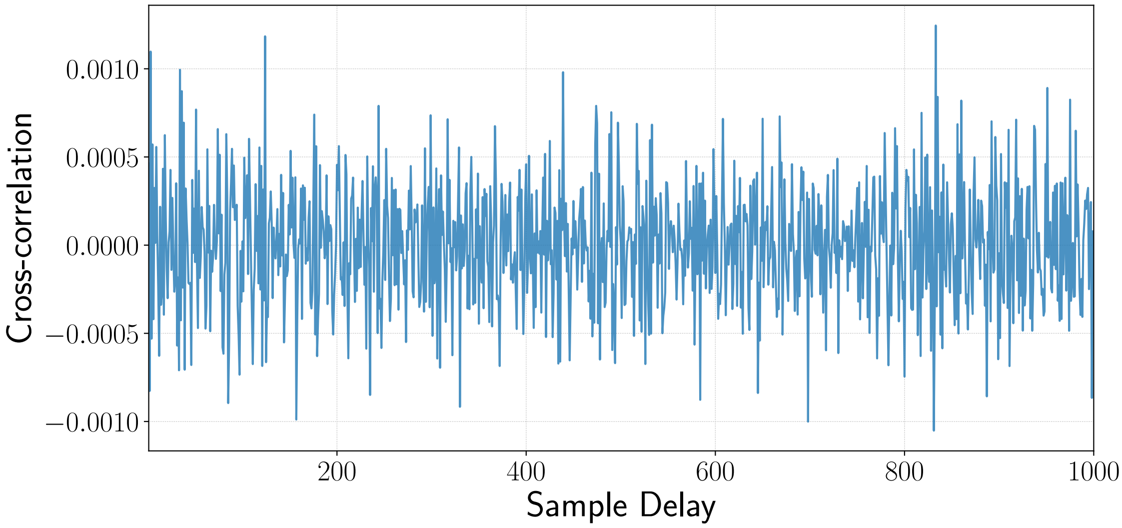

Figure 6.8: Cross-correlation between X and P quadratures of the raw data. The autocorrelation and lag is applied in terms of 1000 12-bit samples. The optical power is 8.4 mW. A total of 10^7 samples were taken for calculation.

Statistical quality of the generated random numbers was evaluated using both the GNU Dieharder suite [233] and the NIST SP 800-22 Statistical Test Suite [111]. For Dieharder, all available tests were executed on binary input files of size 16 GB, with the generator set to file input and the analysis configured to apply the Kolmogorov–Smirnov test with two rejections for failure determination and full reporting of p-values. We also sorted the resulting p-values from the Dieharder tests and plotted them on a Q-Q plot. For the NIST tests, we run it configured to do 1000 iterations with 100 p-values per iteration, using sequences of 1,000,000 bits each. The results from the tests are shown in Fig. 6.9. As can be seen, the NIST tests are all passing and the dieharder test p-values are all uniformly distributed along the diagonal reference line, indicating that no patterns were detected. These tests confirm that no obvious implementation defects (stuck bits, periodic patterns, unexpected correlations from the analog chain) are present. However, passing statistical tests does not establish security—the information-theoretic guarantees derive solely from the SDI framework and calibration analysis of Section 6.5.

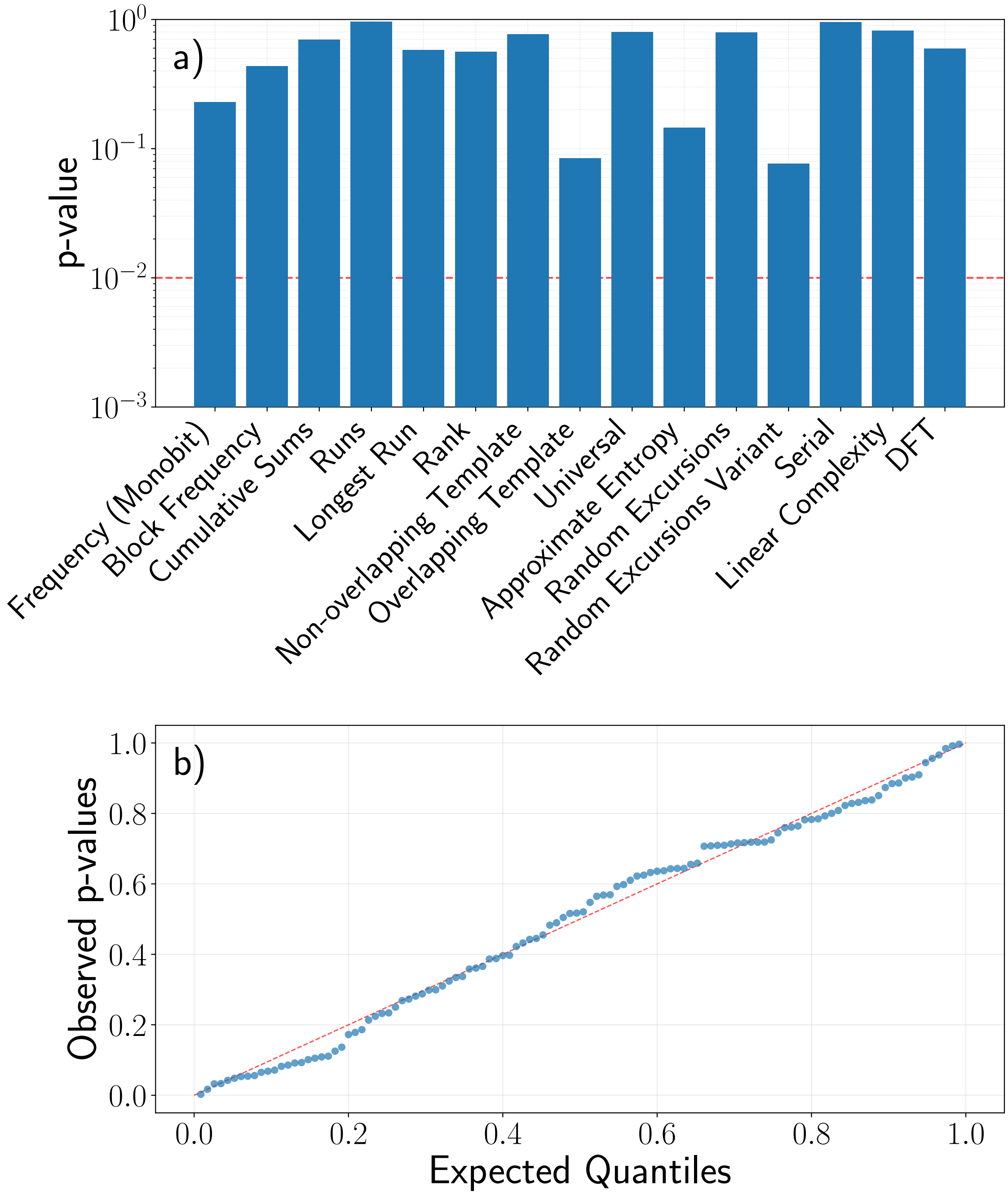

Figure 6.9: Statistical test results for quantum random number generator output. (a) NIST Statistical Test Suite results showing p-values for individual randomness tests on a logarithmic scale. The dashed red line indicates the significance threshold ($\alpha = 0.01$). Tests with single occurrences show individual p-values, while tests with multiple instances show Kolmogorov-Smirnov test p-values comparing the distribution of individual p-values against a uniform distribution. (b) Quantile-quantile plot of Dieharder test suite p-values against expected uniform quantiles. Points following the diagonal reference line (dashed red) indicate p-values consistent with a uniform distribution expected from a true random source.

6.6 Conclusions

We have presented a fully hardware-integrated, SDI QRNG based on heterodyne detection of vacuum fluctuations. The SDI framework, which derives security from the POVM structure rather than source characterization, was established by [131]; our contribution lies in extending the security analysis to address real-time operational requirements (clipping, excess noise, temporal correlations, calibration uncertainty) and demonstrating the first online SDI-certified extraction at rates exceeding 30 Gb/s. We realize the random number acquisition and Toeplitz hashing based randomness extraction entirely on FPGA logic. We also do an extensive security analysis, which shows that the source-device independent model that we consider does not rely on a model of the source, but rather on the properties of the measurement itself, which is useful in the case where the source characteristics drift or when they may be adversarially controlled.

We demonstrate a system with a real-time random number generation rate of 33.92 Gbit/s with all the security bounds taken into account. To quantify this claim, we decompose the contributions to the certified rate. The single-round min-entropy $h^{(1)}_{\text{min}} = \log_2(2\pi/\delta'_X\delta'_P) \approx 12.68$ bits/round receives the following corrections: (i) excess noise inflation reduces this by $\Delta h_\gamma = \log_2(\gamma_X\gamma_P) \approx 0.34$ bits/round (-2.7%); (ii) clipping contributes $< 10^{-5}$ bits/round (negligible); (iii) cross-correlation penalty is $< 10^{-4}$ bits/round (negligible). In contrast, the raw bin width scales as $\delta \propto 2^{-n_{\text{ENOB}}}$, so a 1-bit improvement in ENOB would increase $h^{(1)}_{\text{min}}$ by 2 bits/round ($+15.8\%$). The ENOB contribution thus dominates other effects by a factor of ≈ 6, confirming that higher-ENOB ADCs offer the most direct path to increased rates. We additionally explore additional security limiting factors, such as ADC clipping, inter-quadrature correlation and time autocorrelation. We find that these quantities do not significantly impact the security and therefore we only present them as diagnostics.

Most importantly, this set-up shows that high bandwidth true RNG can be achieved with commonly available components. Moreover, the PCIe interface allows for high speed transfer of the random numbers into another platform, allowing easy access to the QRNG for different applications.

7

Summary and Outlook

7.1 Summary

In this thesis two distinct but conceptually related quantum technologies were investigated: spin dynamics in telecom C-band quantum dots and continuous variable quantum random number generation. Though the physical platforms differ, both investigations share a common motivation of realizing quantum optics concepts for secure communications. Telecom QDs with long spin lifetimes are of interest for the potential application of quantum repeaters, which is essential for long range QKD [234]. High bandwidth, secure QRNGs are of relevance for realizing high speed QKD systems [235], as detailed in Section 2.5.1. In this work we have shown improvement in both parts compared to previous literature.

In Chapter 4, an MOVPE DE telecom C-band InAs/InGaAs/InP QD ensemble sample was examined. By using time-resolved Faraday ellipticity, the spin dynamics of the sample were investigated. It was found that the DE growth mode shows significant improvements in telecom QD spin properties. In particular, a substantial improvement in the electron T_1 time (measured to be $3.0\,\mu$s) was shown in comparison to similar telecom SK grown QDs. Moreover, reduced electron g-factor anisotropy was measured, which is an indicator of improved structural symmetry. Therefore, the improvements are attributed to the DE growth mode, which shows that there is potential to achieve even better properties by further looking into different composition QDs grown by the same method. Unexpectedly, from the PRC and Hanle curves it is seen that nuclear spin lifetimes are close to the electron spin lifetimes. Seeing how measurements were done at cryogenic temperatures and how the electrons in QDs are stationary, this is attributed to quadrupolar effects. Nuclear quadrupole effects arise mostly from strain [97]. However, as explained in Section 2.2.3, DE is a strain-free growth method. In the case of this sample, interdiffusion of Ga and In atoms can also cause loss of symmetry, which results in quadrupole effects [157]. Overall, DE shows significant potential for improving spin properties and different composition QDs can possibly produce better results.

In Chapter 5, MBE SK grown multi-layer telecom C-band InAs/InAlGaAs QDs were investigated. Particularly, one-, two- and four-layer samples were examined. This was done since previous measurements of the same composition eight-layer sample has shown properties which were of interest [17]. Therefore, measurements were done with different layer counts to find out whether the seen effects were real and what dependencies they have. Some noteworthy observations were: a shift from electron resident carriers to holes as layer count increased, even with a Si-doping layer; the appearance of SML at four and above layer count samples; and an additional, non-oscillating component appearing when measuring four- or higher-layer samples. The shift of the resident carriers from electrons to holes is attributed to the fact that the separation of the layers is small enough to allow the electrons to tunnel out to upper layers which have lower energy QDs. SML then becomes a consequence of the tunneling, since the observed SML signal is attributed to the holes, meaning that electrons do not have a long enough coherence time, meaning that hole coherence is longer than electron. That is why SML only shows up when there is a more significant population of holes as resident carriers. As for the non-oscillating component, the exact cause was not known. The primary proposed explanation was that with several layer structures the symmetry is broken, reducing HH-LH mixing. Since HH have a very low or zero g-factor, the signal shows up as a non-oscillating component, since the dephasing time is too short to observe an oscillation.

Comparing the two differently grown QD samples reveals that, in general, MOVPE DE structures exhibit improved spin-dynamical properties compared to MBE SK dots. Although most measured quantities for the DE samples show clear enhancement relative to the multi-layer SK structures, no SML was observed in the DE case. The absence of SML is significant, as the transverse coherence time T_2 extracted from such measurements represents a key figure of merit for quantum repeater operation, determining the number of coherent spin manipulations that can be performed [34]. Consequently, multi-layer samples remain advantageous in this respect, as they exhibit clear SML. The lack of SML in the DE sample may result from shorter coherence times but could also arise from differences in dot density or carrier type. Specifically with electrons being the resident carriers rather than holes, stronger homogeneous dephasing is expected due to nuclear quadrupolar effects. Nevertheless, the overall improvement of the DE structures in most spin-related parameters indicates that this growth approach holds substantial promise for achieving longer coherence times, warranting further systematic investigation.

Lastly, a source DI QRNG with real-time randomness extraction was developed and demonstrated. A total bandwidth of 33.91 Gbit/s was achieved, which is not the highest that has been achieved in QRNGs. However, as mentioned in Chapter 6, the other implementations are either based on less secure, trusted device models or perform offline extraction. In this case, the developed model provides more security since it does not assume that the source device (laser) is safe and so the QRNG is safe even in the case with a malicious third party controlling the source. Moreover, an FPGA was used to implement a real-time Toeplitz extraction algorithm together with random number transfer over PCIe, contrary to the usual case in heterodyne source-DI QRNGs, where an oscilloscope is used to stream data to a computer and then extracted, as mentioned in Chapter 6.

Taken together, the results presented in this thesis contribute to the advancement of secure quantum communication technologies on two complementary parts. The telecom C-band QDs studies demonstrate material and structural pathways toward longer spin lifetimes and improved coherence, both critical for realizing practical quantum repeaters and spin-photon interfaces. In parallel, the developed source-DI QRNG provides a hardware efficient and verifiable entropy source suitable for high-speed QKD implementations. By addressing both the physical storage and the cryptographic randomness requirements, this work establishes experimental approaches that support the long-term goal of scalable, fiber-compatible quantum networks necessary for establishing secure communication channels.

7.2 Future Work

As mentioned previously, there is substantial potential for realizing improved spin properties using DE growth. One of the ways it can be done is by realizing a sample with doping. Applying p-doping to DE grown QDs would allow the observation of the spin dynamics of holes. Since holes are affected by hyperfine interaction significantly weaker than electrons [95], it would reduce the nuclear quadropolar effects, potentially resulting in observable SML. Furthermore, different samples with different material compositions should be investigated to provide a clearer picture on quadrupolar effects. Ref. [89] measures an SK grown InAs/InAlGaAs/InP QD sample with electrons as resident carriers and with a similar PRC curve as was shown in Section 4.5. In their case, the quadrupolar effects are attributed to strain resulting from SK growth. Seeing how strain is present in the DE samples measured in this thesis, which should have no or minimal strain, and how it is not seen in the SK grown InAs/InAlGaAs, this indicates that quadrupolar effects either result from the presence of InP or from another nuclear related effect which appears with addition of InP. For this reason, it would be beneficial to investigate different composition DE grown samples, as there was already a significant improvement in spin properties with DE growth compared to the SK grown sample in Ref. [89]. It would also help with understanding the underlying effect causing the effectively short nuclear spin lifetimes in these DE samples.

For the multi-layer structures most of the future work lies in more detailed investigation of the non-oscillating component and the appearance of SML with increasing layer count, since SK growth for QDs is already researched in detail. One of the more unusual results was the non-oscillating component, which was attributed to reduced HH-LH mixing, which in turn causes the non-oscillating component due to low HH g-factor in Voigt geometry. However, due to HH still having some anisotropy in QDs [236], as the magnetic field is rotated, the g-factor should increase and show oscillations, assuming a strong enough magnetic field is applied. In this thesis, that was done by mechanically rotating the sample holder. This can cause issues when trying to measure anisotropy since the rotation is inaccurate and can result in the sample shifting vertically and horizontally, which can cause measurement issues due to sample inhomogeneity. To ensure proper anisotropy measurements, the use of a vector superconducting magnet is necessary, since then the magnetic field can be rotated without adjusting the sample itself.

In terms of sample development for the multi-layer structures, there are two primary changes that can be made: doping and barrier thickness. Both of these changes can be used to investigate the potential tunneling effects when additional layers are added. In the samples used in this thesis, only a single Si-doping layer, so it is not entirely clear whether the switch of resident carriers was due to tunneling of electrons or whether the additionally added layers intrinsically had holes as resident carriers. Varied barrier thickness is also an additional measure that can help ascertain this, since with increasing barrier thickness tunneling should decrease and stop altogether. Therefore with additional layers no change in resident carriers should be seen if it was indeed caused by tunneling. Moreover, with tunneling blocked, potentially different behavior would be seen for the non-oscillating component. Specifically, it was shown that the component's lifetime increases with temperature, which was attributed to indirect exciton effects, partially caused by tunneling and partially by reduced HH-LH mixing. By blocking tunneling, indirect excitons cannot form and so this kind of behavior would not be the observed then.

For the QRNG, there are further security improvements that can be done without making significant changes to the set-up. Firstly, the monitoring of the QRNG can be improved upon. Currently, there are two outputs over PCIe, one for the extracted random data and another for the raw data. It is necessary to monitor the raw data, since if, for example, the source laser is shut off, it is no longer the quadratures that are being measured, but rather the classical noise of the electronics and so the security model breaks down. In this case, the extracted data does not show indications that the laser is off. However, by measuring the variance of the raw data, it could be seen that the laser was turned off or the power was reduced. While this can be monitored on a computer, the data transfer and analysis takes time and with high bandwidth a lot of insecure random numbers can already be transferred. This can be improved by designing logic that runs in parallel to the extraction in the FPGA which would monitor variance in real time. By doing this, the extracted random numbers could be placed in a buffer while variance is calculated and only when it is seen that the variance is within bounds, the transfer of the extracted numbers would be allowed, ensuring that insecure data does not get transferred.

Lastly, successful fabrication and use of DE QD samples opens the possibility for using these QDs for measure-only QKD protocols. As mentioned in Section 2.1.1, QDs can be approximated as two-level systems. This means that if a QD is resonantly excited (excitation energy matches the band gap energy), the QD emits only a single photon. This makes QDs a good single-photon source. DE QDs already have been shown to have very high single photon emission in the telecom range [55]. For QKD measure-only protocol, entangled states are needed, prefferably in telecom wavelengths to use existing fiber networks. To create entangled states, high single-photon purity and indistinguishability is needed [237], which DE QDs exhibit due to their improved structural properties. More specifically, fine-structure splitting is one of the main factors that reduces entangled photon creation. It has been shown that due to the improved DE QD symmetry, the fine-structure splitting is significantly reduced, which is highly promising for entangled photon pair generation [56, 238]. Therefore, DE QDs can be used then to created polarization entangled pairs for QKD by utilizing biexciton recombination cascade [237]. While using single photon methods for QRNG or QKD suffers from low bandwidths due to low single photon emission rate, it can be improved by embeddeding QDs in photonic crystal cavities. QDs placed in photonic crystal cavities results in increased light confinement, which in turn increases the Q-factor [239] and reduces the light mode volume [240], which results in high Purcell enhancement. Purcell enhancement denotes how excitons radiatively recombine faster [241], so a QD placed in a cavity can have significantly increased emission rate, which would improve the bandwidth limitations for the prepare-measure QKD protocol.

Abbreviations

ACF autocorrelation function

ADC analog-to-digital converter

Al aluminum

AlGaAs aluminum gallium arsenide

As arsenic

BPD balanced photodiode

CDC clock domain crossing

CI confidence interval

CSPRNG cryptographically secure pseudorandom number generator

CV continuous-variable

CW continuos wave

DE droplet epitaxy

DI device-independent

DV discrete-variable

EFG electric field gradient

ENOB effective number of bits

EOM electro-optic modulator

EVOA electronically variable optical attenuator

FFT Fast Fourier Transform

FIFO first in - first out

FMC FPGA Mezzanine card

FPGA field programmable gate array

Ga gallium

GaAs gallium arsenide

HH heavy-hole

HPF high-pass filter

HWHM half width at half maximum

IID independent and identically distributed

In indium

InAlGaAs indium aluminum gallium arsenide

InAs indium arsenide

InGaAs indium gallium arsenide

InP indium phosphide

LH light-hole

LO local oscillator

LPF low-pass filter

LUT look-up table

MBE molecular beam epitaxy

MOCVD metalorganic chemical vapour deposition

MOVPE metalorganic vapour-phase epitaxy

ND neutral density

OPO optical parametric oscillator

OTP one-time pad

P phosphorus

PEM photoelastic modulator

PL photoluminescence

POVM positive operator valued measurement

PRC polarization recovery curve

PRNG pseudorandom number generator

PSD power spectral density

QCNR quantum-to-classical noise ratio

QD quantum dot

QKD quantum key distribution

QRNG quantum random number generator

RNG random number generators

SDI source device-independent

SK Stranski-Krastanov

SML spin mode locking

VOA variable optical attenuator

VTI variable temperature insert

WL wetting layer

XOR exclusive-or

Bibliography

[1] M. Cizauskas, E. M. Sala, J. Heffernan, A. M. Fox, M. Bayer, and A. Greilich, "Spin properties in droplet epitaxy grown telecom quantum dots," *Phys. Rev. B*, vol. 112, p. 165412, Oct. 2025.

[2] M. Cizauskas, A. Kors, J. P. Reithmaier, A. M. Fox, M. Benyoucef, M. Bayer, and A. Greilich, "Layer-dependent spin properties of charge carriers in vertically coupled telecom quantum dots," *arXiv*, Sep. 2025.

[3] M. Cizauskas, H. Tebyanian, M. Fox, M. Bayer, M. Assmann, and A. Greilich, "33 gbit/s source-device-independent quantum random number generator based on heterodyne detection with real-time fpga-integrated extraction," *arXiv*, Dec. 2025.

[4] D. Browne, S. Bose, F. Mintert, and M. Kim, "From quantum optics to quantum technologies," *Progress in Quantum Electronics*, vol. 54, pp. 2–18, 2017. Special issue in honor of the 70th birthday of Professor Sir Peter Knight FRS.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, p. 1484–1509, 1997.

[6] R. Bavdekar, E. Jayant Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post quantum cryptography: A review of techniques, challenges and standardizations," in *2023 International Conference on Information Networking (ICOIN)*, pp. 146–151, Jan 2023.

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, p. 1301–1350, 2009.

[8] Y. Yu, S. Liu, C.-M. Lee, P. Michler, S. Reitzenstein, K. Srinivasan, E. Waks, and J. Liu, “Telecom-band quantum dot technologies for long-distance quantum networks,” *Nature Nanotechnology*, vol. 18, p. 1389–1400, Dec. 2023.

[9] S. Wilksen, F. Lohof, I. Willmann, F. Bopp, M. Lienhart, C. Thalacker, J. Finley, M. Florian, and C. Gies, “Gate-based protocol simulations for quantum repeaters using quantum-dot molecules in switchable electric fields,” *Advanced Quantum Technologies*, vol. 7, no. 3, p. 2300280, 2024.

[10] S. van Enk and O. Hirota, “Entangled coherent states: Teleportation and decoherence,” *Physical Review A*, vol. 64, no. 2, 2001.

[11] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, “Quantum repeaters and quantum key distribution: Analysis of secret-key rates,” *Phys. Rev. A*, vol. 87, p. 052315, May 2013.

[12] C. Simon, Y.-M. Niquet, X. Caillet, J. Eymery, J.-P. Poizat, and J. M. Gerard, “Quantum communication with quantum dot spins,” *Physical Review B*, vol. 75, p. 081302, 2006.

[13] D. Buterakos, E. Barnes, and S. E. Economou, “Deterministic generation of all-photonic quantum repeaters from solid-state emitters,” *Phys. Rev. X*, vol. 7, p. 041023, Oct 2017.

[14] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991.

[15] B. J. Riel, “An introduction to self-assembled quantum dots,” *American Journal of Physics*, vol. 76, pp. 750–757, Aug. 2008.

[16] C. Kittel, *Introduction to Solid State Physics*. Wiley, 2004.

[17] E. Evers, N. E. Kopteva, V. Nedelea, A. Kors, R. Kaur, J. Peter Reithmaier, M. Benyoucef, M. Bayer, and A. Greilich, “Hole spin coherence in InAs/InAlGaAs self-assembled quantum dots emitting at telecom wavelengths,” *physica status solidi (b)*, vol. 262, no. 1, p. 2400174, 2025.

[18] M. Valín-Rodríguez and R. G. Nazmitdinov, “Model for spin-orbit effects in two-dimensional semiconductors in magnetic fields,” *Physical Review B*, vol. 73, p. 235306, 2005.

[19] W. Gutiérrez, J. H. Marín, and I. D. Mikhailov, "Charge transfer magnetoexciton formation at vertically coupled quantum dots," *Nanoscale Research Letters*, vol. 7, pp. 585 – 585, 2012.

[20] W. Que, "Excitons in quantum dots with parabolic confinement," *Phys. Rev. B*, vol. 45, pp. 11036–11041, May 1992.

[21] S. Tarucha, D. G. Austing, T. Honda, R. J. van der Hage, and L. P. Kouwenhoven, "Shell filling and spin effects in a few electron quantum dot," *Phys. Rev. Lett.*, vol. 77, pp. 3613–3616, Oct. 1996.

[22] A. Fox, *Optical Properties of Solids*. Oxford master series in condensed matter physics, Oxford University Press, 2001.

[23] E. Chekhovich, M. Glazov, A. Krysa, M. Hopkinson, P. Senellart, A. Lemaître, A. Tartakovskii, and M. Skolnick, "Element-sensitive measurement of the hole–nuclear spin interaction in quantum dots," *Nature Physics*, vol. 9, p. 74, Feb. 2013.

[24] M. I. Dyakonov, *Basics of Semiconductor and Spin Physics*, pp. 1–37. Springer International Publishing, 2017.

[25] G. Slavcheva and P. Roussignol, *Optical Generation and Control of Quantum Coherence in Semiconductor Nanostructures*. Jan. 2010.

[26] P. Lodahl, S. Mahmoodian, and S. Stobbe, "Interfacing single photons and single quantum dots with photonic nanostructures," *Reviews of Modern Physics*, vol. 87, pp. 347–400, 2013.

[27] A. J. Ramsay, "A review of the coherent optical control of the exciton and spin states of semiconductor quantum dots," *Semiconductor Science and Technology*, vol. 25, p. 103001, Sep. 2010.

[28] T. Belhadj, T. Amand, A. Kunold, C.-M. Simon, T. Kuroda, M. Abbarchi, T. Mano, K. Sakoda, S. Kunz, X. Marie, and B. Urbaszek, "Impact of heavy hole-light hole coupling on optical selection rules in GaAs quantum dots," *Applied Physics Letters*, vol. 97, p. 051111, Aug. 2010.

[29] E. Harbord, P. Spencer, E. Clarke, and R. Murray, "Radiative lifetimes in undoped and p-doped InAs/GaAs quantum dots," *Phys. Rev. B*, vol. 80, p. 195312, Nov. 2009.

[30] S. Grijseels, J. van Bree, P. Koenraad, A. Toropov, G. Klimko, S. Ivanov, C. Pryor, and A. Silov, "Radiative lifetimes and linewidth broadening of single InAs quantum dots in an AlxGa1−xAs matrix," *Journal of Luminescence*, vol. 176, pp. 95–99, 2016.

[31] I. Vurgaftman, J. R. Meyer, and L. R. Ram-Mohan, "Band parameters for III–V compound semiconductors and their alloys," *Journal of Applied Physics*, vol. 89, pp. 5815–5875, Jun. 2001.

[32] K. H. Schmidt, G. Medeiros-Ribeiro, J. Garcia, and P. M. Petroff, "Size quantization effects in InAs self-assembled quantum dots," *Applied Physics Letters*, vol. 70, pp. 1727–1729, Mar. 1997.

[33] A. Kurzmann, A. Ludwig, A. D. Wieck, A. Lorke, and M. Geller, "Auger recombination in self-assembled quantum dots: Quenching and broadening of the charged exciton transition.," *Nano letters*, vol. 16, pp. 3367–72, Apr. 2016.

[34] P. L. McMahon and K. De Greve, *Towards Quantum Repeaters with Solid-State Qubits: Spin-Photon Entanglement Generation Using Self-assembled Quantum Dots*, pp. 365–402. Cham: Springer International Publishing, 2015.

[35] S. Cortez, O. Krebs, S. Laurent, M. Senes, X. Marie, P. Voisin, R. Ferreira, G. Bastard, J.-M. Gérard, and T. Amand, "Optically driven spin memory in n-doped InAs-GaAs quantum dots," *Phys. Rev. Lett.*, vol. 89, p. 207401, Oct. 2002.

[36] M. A. Herman, W. Richter, and H. Sitter, *Molecular Beam Epitaxy*, pp. 131–170. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004.

[37] S. Irvine and P. Capper, *Introduction to Metalorganic Vapor Phase Epitaxy*, ch. 1, pp. 1–18. John Wiley & Sons, Ltd, 2019.

[38] N. Papež, R. Dallaev, S. Ţălu, and J. Kaštyl, "Overview of the current state of gallium arsenide-based solar cells," *Materials*, vol. 14, p. 3075, Jun. 2021.

[39] P. A. Wroński, P. Wyborski, A. Musiał, P. Podemski, G. Sęk, S. Höfling, and F. Jabeen, "Metamorphic buffer layer platform for 1550 nm single-photon sources grown by MBE on (100) GaAs substrate," *Materials*, vol. 14, p. 5221, Sep. 2021.

[40] J. Prieto and I. Markov, "Stranski–Krastanov mechanism of growth and the effect of misfit sign on quantum dots nucleation," *Surface Science*, vol. 664, pp. 172–184, 2017.

[41] H. Dobbs, D. Vvedensky, and A. Zangwill, “Theory of quantum dot formation in Stranski-Krastanov systems,” *Applied Surface Science*, vol. 123-124, pp. 646–652, 1998.

[42] J. Johansson, W. Seifert, T. Junno, and L. Samuelson, “Sizes of self-assembled quantum dots – effects of deposition conditions and annealing,” *Journal of Crystal Growth*, vol. 195, no. 1, pp. 546–551, 1998.

[43] R. Vengrenovich, I. Gudyma, and S. Yarema, “Ostwald ripening of quantum-dot nanostructures,” *Semiconductors*, vol. 35, pp. 1378–1382, Dec. 2001.

[44] A. Hospodková, “Capping of InAs/GaAs quantum dots for GaAs based lasers,” in *Quantum Dots* (A. Al-Ahmadi, ed.), ch. 2, Rijeka: IntechOpen, 2012.

[45] C. P. Dietrich, A. Fiore, M. G. Thompson, M. Kamp, and S. Höfling, “Gaas integrated quantum photonics: Towards compact and multi-functional quantum photonic integrated circuits,” *Laser & Photonics Reviews*, vol. 10, no. 6, pp. 870–894, 2016.

[46] T. D. Park, J. S. Colton, J. K. Farrer, H. Yang, and D. J. Kim, “Annealing-induced change in quantum dot chain formation mechanism,” *AIP Advances*, vol. 4, p. 127142, Dec. 2014.

[47] M. Liao, W. Li, M. Tang, A. Li, S. Chen, A. Seeds, and H. Liu, “Selective area intermixing of III–V quantum-dot lasers grown on silicon with two wavelength lasing emissions,” *Semiconductor Science and Technology*, vol. 34, p. 085004, Jul. 2019.

[48] D. Fricker, P. Atkinson, X. Jin, M. Lepsa, Z. Zeng, A. Kovács, L. Kibkalo, R. Dunin-Borkowski, and B. Kardynał, “Effect of surface gallium termination on the formation and emission energy of an InGaAs wetting layer during the growth of InGaAs quantum dots by droplet epitaxy,” *Nanotechnology*, vol. 34, p. 145601, Jan. 2023.

[49] M. Gawełczyk, “Atypical dependence of excited exciton energy levels and electron-hole correlation on emission energy in pyramidal InP-based quantum dots,” *Scientific Reports*, vol. 12, p. 164, Jan. 2022.

[50] R. S. Gajjela, E. Sala, J. Heffernan, and P. Koenraad, “Control of morphology and substrate etching in InAs/InP droplet epitaxy quantum dots for single and entangled photon emitters,” *ACS Applied Nano Materials*, vol. 5, p. 8070, May 2022.

[51] K. Reyes, P. Smereka, D. Nothern, J. M. Millunchick, S. Bietti, C. Somaschini, S. Sanguinetti, and C. Frigeri, "Unified model of droplet epitaxy for compound semiconductor nanostructures: Experiments and theory," *Physical Review B*, vol. 87, p. 165406, 2012.

[52] M. Abbarchi, T. Mano, T. Kuroda, A. Ohtake, and K. Sakoda, "Polarization anisotropies in strain-free, asymmetric, and symmetric quantum dots grown by droplet epitaxy," *Nanomaterials*, vol. 11, p. 443, Feb. 2021.

[53] M. Anderson, T. Müller, J. Skiba-Szymanska, A. B. Krysa, J. Huwer, R. M. Stevenson, J. Heffernan, D. A. Ritchie, and A. J. Shields, "Coherence in single photon emission from droplet epitaxy and Stranski–Krastanov quantum dots in the telecom c-band," *Applied Physics Letters*, vol. 118, p. 014003, Jan. 2021.

[54] S. Bietti, F. Basset, A. Tuktamyshev, E. Bonera, A. Fedorov, and S. Sanguinetti, "High–temperature droplet epitaxy of symmetric GaAs/AlGaAs quantum dots," *Scientific Reports*, vol. 10, p. 6532, Apr. 2020.

[55] P. Holewa, S. Kadkhodazadeh, M. Gawełczyk, P. Baluta, A. Musiał, V. G. Dubrovskii, M. Syperek, and E. Semenova, "Droplet epitaxy symmetric InAs/InP quantum dots for quantum emission in the third telecom window: morphology, optical and electronic properties," *Nanophotonics*, vol. 11, pp. 1515 – 1526, Jan. 2021.

[56] J. Skiba-Szymanska, R. M. Stevenson, C. Varnava, M. Felle, J. Huwer, T. Müller, A. J. Bennett, J. P. Lee, I. Farrer, A. B. Krysa, P. Spencer, L. E. Goff, D. A. Ritchie, J. Heffernan, and A. J. Shields, "Universal growth scheme for quantum dots with low fine-structure splitting at various emission wavelengths," *Phys. Rev. Appl.*, vol. 8, p. 014013, Jul. 2017.

[57] Z. Yan and Q. Li, "Recent progress in epitaxial growth of dislocation tolerant and dislocation free III–V lasers on silicon," *Journal of Physics D: Applied Physics*, vol. 57, p. 213001, Feb. 2024.

[58] Z. M. Wang, K. Holmes, Y. I. Mazur, K. A. Ramsey, and G. J. Salamo, "Self-organization of quantum-dot pairs by high-temperature droplet epitaxy," *Nanoscale Research Letters*, vol. 1, pp. 57 – 61, 2006.

[59] E. M. Sala, M. Godsland, Y. I. Na, A. Trapalis, and J. Heffernan, “Droplet epitaxy of InAs/InP quantum dots via MOVPE by using an InGaAs interlayer,” *Nanotechnology*, vol. 33, p. 065601, Nov. 2021.

[60] E. G. Banfi, E. M. Sala, R. S. R. Gajjela, J. Heffernan, and P. M. Koenraad, “An atomically resolved study of droplet epitaxy InAs quantum dots grown on InGa(As,P)/InP by MOVPE for quantum photonic applications,” *Journal of Applied Physics*, vol. 137, p. 134401, Apr. 2025.

[61] F. Meier and B. P. Zakharchenia, *Optical orientation / [edited by] F. Meier, B.P. Zakharchenya.* Modern problems in condensed matter sciences ; v. 8, Amsterdam ;: North-Holland, 1984.

[62] O. Krebs, B. Eble, A. Lemaître, P. Voisin, B. Urbaszek, X. Marie, and T. Amand, “Hyperfine interaction in inas/gaas self-assembled quantum dots: dynamical nuclear polarization versus spin relaxation,” *Comptes Rendus Physique*, vol. 9, pp. 874–884, 2008.

[63] B. Venitucci and Y.-M. Niquet, “Simple model for electrical hole spin manipulation in semiconductor quantum dots: Impact of dot material and orientation,” *Phys. Rev. B*, vol. 99, p. 115317, Mar 2019.

[64] D. R. Yakovlev and M. Bayer, *Coherent Spin Dynamics of Carriers*, pp. 155–206. Cham: Springer International Publishing, 2017.

[65] V. V. Belykh, A. Greilich, D. R. Yakovlev, M. Yacob, J. P. Reithmaier, M. Benyoucef, and M. Bayer, “Electron and hole g factors in InAs/InAlGaAs self-assembled quantum dots emitting at telecom wavelengths,” *Phys. Rev. B*, vol. 92, p. 165307, Oct. 2015.

[66] V. V. Belykh, D. R. Yakovlev, J. J. Schindler, E. A. Zhukov, M. A. Semina, M. Yacob, J. P. Reithmaier, M. Benyoucef, and M. Bayer, “Large anisotropy of electron and hole g factors in infrared-emitting InAs/InAlGaAs self-assembled quantum dots,” *Phys. Rev. B*, vol. 93, p. 125302, Mar. 2016.

[67] V. Jovanov, T. Eissfeller, S. Kapfinger, E. C. Clark, F. Klotz, M. Bichler, J. G. Keizer, P. M. Koenraad, G. Abstreiter, and J. J. Finley, “Observation and explanation of strong electrically tunable exciton g-factors in composition engineered In(Ga)As quantum dots,” *Physical Review B*, vol. 83, p. 161303, Apr. 2011.

[68] C. Pryor and M. Flatté, "Landé g factors and orbital momentum quenching in semiconductor quantum dots," *Physical Review Letters*, vol. 96, p. 026804, Feb. 2006.

[69] T. Nakaoka, T. Saito, J. Tatebayashi, and Y. Arakawa, "Size, shape, and strain dependence of the g factor in self-assembled In(Ga)As quantum dots," *Phys. Rev. B*, vol. 70, p. 235337, Dec. 2004.

[70] W. Sheng, "Landé g factors in elongated InAs/GaAs self-assembled quantum dots," *Physica E: Low-dimensional Systems and Nanostructures*, vol. 40, no. 5, pp. 1473–1475, 2008.

[71] D. Kim, W. Sheng, P. J. Poole, D. Dalacu, J. Lefebvre, J. Lapointe, M. E. Reimer, G. C. Aers, and R. L. Williams, "Tuning the exciton g factor in single InAs/InP quantum dots," *Phys. Rev. B*, vol. 79, p. 045310, Jan. 2009.

[72] V. V. Belykh, D. R. Yakovlev, J. J. Schindler, J. van Bree, P. M. Koenraad, N. S. Averkiev, M. Bayer, and A. Y. Silov, "Dispersion of the electron g factor anisotropy in InAs/InP self-assembled quantum dots," *Journal of Applied Physics*, vol. 120, p. 084301, Aug. 2016.

[73] J. van Bree, A. Y. Silov, P. M. Koenraad, M. E. Flatté, and C. E. Pryor, "g factors and diamagnetic coefficients of electrons, holes, and excitons in InAs/InP quantum dots," *Phys. Rev. B*, vol. 85, p. 165323, Apr. 2012.

[74] L. M. Roth, B. Lax, and S. Zwerdling, "Theory of optical magneto-absorption effects in semiconductors," *Phys. Rev.*, vol. 114, pp. 90–104, Apr. 1959.

[75] A. Greilich, *Spin coherence of carriers in (In,Ga)As/GaAs quantum dots and quantum wells*. Dissertation, Institute of Physics, Technical University of Dortmund, Dortmund, Germany, 2007.

[76] T. M. Godden, J. H. Quilter, A. J. Ramsay, Y. Wu, P. Brereton, S. J. Boyle, I. J. Luxmoore, J. Puebla-Nunez, A. M. Fox, and M. S. Skolnick, "Coherent optical control of the spin of a single hole in an InAs/GaAs quantum dot," *Phys. Rev. Lett.*, vol. 108, p. 017402, Jan. 2012.

[77] P. A. Dalgarno, J. M. Smith, J. McFarlane, B. D. Gerardot, K. Karrai, A. Badolato, P. M. Petroff, and R. J. Warburton, "Coulomb interactions in single charged self-assembled quantum dots: Radiative lifetime and recombination energy," *Phys. Rev. B*, vol. 77, p. 245311, Jun. 2008.

[78] R. J. Elliott, “Theory of the effect of spin-orbit coupling on magnetic resonance in some semiconductors,” *Phys. Rev.*, vol. 96, pp. 266–279, Oct. 1954.

[79] Y. Yafet, “g factors and spin-lattice relaxation of conduction electrons,” in *Solid State Physics* (F. Seitz and D. Turnbull, eds.), vol. 14 of *Solid State Physics*, pp. 1–98, Academic Press, 1963.

[80] S. Bandyopadhyay, “Chapter 9 - quantum information science from the perspective of a device and materials engineer,” in *Advanced Semiconductor and Organic Nano-Techniques* (H. Morkoç, ed.), pp. 441–502, San Diego: Academic Press, 2003.

[81] M. I. Dyakonov and V. I. Perel, “Spin orientation of electrons associated with the interband absorption of light in semiconductors,” *Sov. Phys. JETP*, vol. 33, pp. 1053–1059, 1971. Zh. Eksp. Teor. Fiz. 60, 1954 (1971).

[82] M. I. D’yakonov and V. I. Perel’, “Spin relaxation of conduction electrons in noncentrosymmetric semiconductors,” *Sov. Phys. Solid State*, vol. 13, pp. 3023–3026, 1972. Fiz. Tverd. Tela 13, 3581 (1971).

[83] S. V. Nekrasov, Y. G. Kusrayev, I. A. Akimov, V. L. Korenev, L. Langer, and M. Salewski, “Negative circular polarization dynamics in InP/InGaP quantum dots,” *Journal of Physics: Conference Series*, vol. 741, p. 012189, Aug. 2016.

[84] G. L. Bir, A. G. Aronov, and G. E. Pikus, “Spin relaxation of electrons due to scattering by holes,” *Sov. Phys. JETP*, vol. 42, pp. 705–712, 1975. Zh. Eksp. Teor. Fiz. 69, 1382 (1975).

[85] G. E. Pikus and G. L. Bir, “Exchange interaction in excitons in semiconductors,” *Sov. Phys. JETP*, vol. 33, pp. 108–115, 1971. Zh. Eksp. Teor. Fiz. 60, 195 (1971).

[86] M. Krzykowski, K. Gawarecki, and P. Machnikowski, “Hole spin-flip transitions in a self-assembled quantum dot,” *Phys. Rev. B*, vol. 102, p. 205301, Nov. 2020.

[87] K. Gawarecki and P. Machnikowski, “Phonon-assisted relaxation between triplet and singlet states in a self-assembled double quantum dot,” *Scientific Reports*, vol. 11, p. 15256, Jul. 2021.

[88] L. Chirolli and G. Burkard, “Decoherence in solid-state qubits,” *Advances in Physics*, vol. 57, pp. 225 – 285, 2008.

[89] A. V. Mikhailov, V. V. Belykh, D. R. Yakovlev, P. S. Grigoryev, J. P. Reithmaier, M. Benyoucef, and M. Bayer, "Electron and hole spin relaxation in InP-based self-assembled quantum dots emitting at telecom wavelengths," *Phys. Rev. B*, vol. 98, p. 205306, Nov. 2018.

[90] J. Li, B. Venitucci, and Y.-M. Niquet, "Hole-phonon interactions in quantum dots: Effects of phonon confinement and encapsulation materials on spin-orbit qubits," *Physical Review B*, vol. 102, p. 075415, 2020.

[91] G. Gillard, I. Griffiths, G. Ragunathan, A. Ulhaq, C. McEwan, E. Clarke, and E. Chekhovich, "Fundamental limits of electron and nuclear spin qubit lifetimes in an isolated self-assembled quantum dot," *npj Quantum Information*, vol. 7, p. 43, Dec. 2021.

[92] A. W. Overhauser, "Polarization of nuclei in metals," *Phys. Rev.*, vol. 92, pp. 411–415, Oct. 1953.

[93] I. A. Merkulov, A. L. Efros, and M. Rosen, "Electron spin relaxation by nuclei in semiconductor quantum dots," *Phys. Rev. B*, vol. 65, p. 205309, Apr. 2002.

[94] E. Evers, *Nuclear-Electron Spin Interaction in Low-Dimensional Semiconductors*. Dissertation, Technical University of Dortmund, Dortmund, Germany, Dec. 2021. Dr. rer. nat. thesis.

[95] C. Testelin, F. Bernardot, B. Eble, and M. Chamarro, "Hole–spin dephasing time associated with hyperfine interaction in quantum dots," *Phys. Rev. B*, vol. 79, p. 195440, May 2009.

[96] C. Slichter, *Principles of Magnetic Resonance*. Springer Series in Solid-State Sciences, Springer Berlin Heidelberg, 1996.

[97] M. S. Kuznetsova, R. V. Cherbunin, I. Y. Gerlovin, I. V. Ignatiev, S. Y. Verbin, D. R. Yakovlev, D. Reuter, A. D. Wieck, and M. Bayer, "Spin dynamics of quadrupole nuclei in ingaas quantum dots," *Phys. Rev. B*, vol. 95, p. 155312, Apr. 2017.

[98] A. Bechtold, D. Rauch, F. Li, T. Simmet, P.-L. Ardelt, A. Regler, K. Müller, N. A. Sinitsyn, and J. J. Finley, "Three-stage decoherence dynamics of an electron spin qubit in an optically active quantum dot," *Nature Physics*, vol. 11, no. 12, p. 1005–1008, 2015.

[99] M. Wu, J. Jiang, and M. Weng, "Spin dynamics in semiconductors," *Physics Reports*, vol. 493, no. 2, pp. 61–236, 2010.

[100] L. M. K. Vandersypen, H. Bluhm, J. S. Clarke, A. S. Dzurak, R. Ishihara, A. Morello, D. J. Reilly, L. R. Schreiber, and M. Veldhorst, "Interfacing spin qubits in quantum dots and donors—hot, dense, and coherent," *npj Quantum Information*, vol. 3, p. 34, Sep. 2017.

[101] A. Greilich, D. R. Yakovlev, A. Shabaev, A. L. Efros, I. A. Yugova, R. Oulton, V. Stavarache, D. Reuter, A. Wieck, and M. Bayer, "Mode locking of electron spin coherences in singly charged quantum dots," *Science*, vol. 313, no. 5785, pp. 341–345, 2006.

[102] F. Fras, B. Eble, B. Siarry, F. Bernardot, A. Miard, A. Lemaître, C. Testelin, and M. Chamarro, "Hole spin mode locking and coherent dynamics in a largely inhomogeneous ensemble of p-doped InAs quantum dots," *Phys. Rev. B*, vol. 86, p. 161303, Oct. 2012.

[103] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[104] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[105] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, p. 025002, May 2020.

[106] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. D. Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 967–1002, 2024.

[107] M. Mosca, D. Stebila, and B. Ustaoğlu, "Quantum key distribution in the classical authenticated key exchange framework," in *Post-Quantum Cryptography* (P. Gaborit, ed.), (Berlin, Heidelberg), pp. 136–154, Springer Berlin Heidelberg, 2013.

[108] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The universal composable security of quantum key distribution," in *Theory of Cryptography* (J. Kilian, ed.), (Berlin, Heidelberg), pp. 386–406, Springer Berlin Heidelberg, 2005.

[109] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, "Quantum repeaters and quantum key distribution: Analysis of secret-key rates," *Phys. Rev. A*, vol. 87, p. 052315, May 2013.

[110] N. P. Landsman, *Born Rule and its Interpretation*, pp. 64–70. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[111] L. E. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, and N. Heckert, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Tech. Rep. Special Publication 800-22 Rev. 1a, National Institute of Standards and Technology, Gaithersburg, MD, 2010.

[112] P. L'Ecuyer and R. Simard, "Testu01: A c library for empirical testing of random number generators," *ACM Trans. Math. Softw.*, vol. 33, pp. 1–40, 01 2007.

[113] P. L'Ecuyer, "Random numbers for simulation.," *Commun. ACM*, vol. 33, pp. 85–97, 10 1990.

[114] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Documentation and analysis of the Linux random number generator," technical report, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022.

[115] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *Journal of Modern Optics*, vol. 47, no. 4, pp. 595–598, 2000.

[116] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, pp. 1675–1680, Apr. 2000.

[117] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Applied Physics Letters*, vol. 104, p. 051110, 02 2014.

[118] R. Uppu, F. T. Pedersen, Y. Wang, C. T. Olesen, C. Papon, X. Zhou, L. Midolo, S. Scholz, A. D. Wieck, A. Ludwig, and P. Lodahl, "Scalable integrated single-photon source," *Science Advances*, vol. 6, no. 50, p. eabc8268, 2020.

[119] Y. Zhang, X. Ding, Y. Li, L. Zhang, Y.-P. Guo, G.-Q. Wang, Z. Ning, M.-C. Xu, R.-Z. Liu, J.-Y. Zhao, G.-Y. Zou, H. Wang, Y. Cao, Y.-M. He, C.-Z. Peng, Y.-H. Huo, S.-K. Liao, C.-Y. Lu, F. Xu, and J.-W. Pan, "Experimental single-photon quantum key distribution surpassing the fundamental weak coherent-state rate limit," *Phys. Rev. Lett.*, vol. 134, p. 210801, May 2025.

[120] C. Bruynsteen, T. Gehring, C. Lupo, J. Bauwelinck, and X. Yin, “100-Gbit/s integrated quantum random number generator based on vacuum fluctuations,” *PRX Quantum*, vol. 4, p. 010330, Marc. 2023.

[121] S. Q. Ng, G. Zhang, C. Wang, and C. C. W. Lim, “240 Gbps quantum random number generator with photonic integrated chip,” *2023 Conference on Lasers and Electro-Optics (CLEO)*, p. AM4N.6, 2023.

[122] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, “6 gbps real-time optical quantum random number generator based on vacuum fluctuation,” *Review of Scientific Instruments*, vol. 90, p. 043105, 04 2019.

[123] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, “Ultrafast quantum random number generation based on quantum phase fluctuations,” *Opt. Express*, vol. 20, pp. 12366–12377, May 2012.

[124] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, “Fast physical random number generator using amplified spontaneous emission,” *Opt. Express*, vol. 18, pp. 23584–23597, Nov. 2010.

[125] S. Olivares, “Introduction to generation, manipulation and characterization of optical quantum states,” *Physics Letters A*, vol. 418, p. 127720, 2021.

[126] U. Leonhardt, *Essential Quantum Optics: From Quantum Measurements to Black Holes*. Cambridge University Press, 2010.

[127] A. I. Lvovsky and M. G. Raymer, “Continuous-variable optical quantum-state tomography,” *Rev. Mod. Phys.*, vol. 81, pp. 299–332, Mar. 2009.

[128] T. Gehring, C. Lupo, A. Kordts, D. Solar Nikolic, N. Jain, T. Rydberg, T. Pedersen, S. Pirandola, and U. Andersen, “Homodyne-based quantum random number generator at 2.9 gbps secure against quantum side-information,” *Nature Communications*, vol. 12, p. 605, 01 2021.

[129] U. Leonhardt and H. Paul, “Measuring the quantum state of light,” *Progress in Quantum Electronics*, vol. 19, no. 2, pp. 89–130, 1995.

[130] V. Mannalatha, S. Mishra, and A. Pathak, “A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness,” *Quantum Information Processing*, vol. 22, no. 12, p. 439, 2023.

[131] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, “Source-device-independent heterodyne-based quantum random number generator at 17 Gbps,” *Nature Communications*, vol. 9, p. 5365, Dec. 2018.

[132] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, “High speed self-testing quantum random number generation without detection loophole,” in *Frontiers in Optics 2017*, p. FTh2E.1, Optica Publishing Group, 2017.

[133] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, “Device-independent randomness expansion against quantum side information,” *Nature Physics*, vol. 17, pp. 448 – 451, 2019.

[134] P. R. Berman, “Optical faraday rotation,” *American Journal of Physics*, vol. 78, pp. 270–276, 03 2010.

[135] I. Yugova, M. Glazov, E. Ivchenko, and A. Efros, “Pump-probe Faraday rotation and ellipticity in an ensemble of singly charged quantum dots,” *Physical Review B*, vol. 80, p. 104436, May 2009.

[136] M. Atatüre, J. Dreiser, A. Badolato, and A. Imamoglu, “Observation of Faraday rotation from a single confined spin,” *Nature Physics*, vol. 3, p. 101–106, Jan 2007.

[137] L. N. Novikov, G. V. Skrotskiĭ, and G. I. Solomakho, “The Hanle effect,” *Soviet Physics Uspekhi*, vol. 17, p. 542, Apr. 1975.

[138] C. Rittmann, M. Y. Petrov, A. N. Kamenskii, K. V. Kavokin, A. Y. Kuntsevich, Y. P. Efimov, S. A. Eliseev, M. Bayer, and A. Greilich, “Unveiling the electron-nuclear spin dynamics in an n-doped InGaAs epilayer by spin noise spectroscopy,” *Phys. Rev. B*, vol. 106, p. 035202, Jul. 2022.

[139] E. A. Zhukov, E. Kirstein, D. S. Smirnov, D. R. Yakovlev, M. M. Glazov, D. Reuter, A. D. Wieck, M. Bayer, and A. Greilich, “Spin inertia of resident and photoexcited carriers in singly charged quantum dots,” *Phys. Rev. B*, vol. 98, p. 121304, Sep. 2018.

[140] D. S. Smirnov, E. A. Zhukov, E. Kirstein, D. R. Yakovlev, D. Reuter, A. D. Wieck, M. Bayer, A. Greilich, and M. M. Glazov, "Theory of spin inertia in singly charged quantum dots," *Phys. Rev. B*, vol. 98, p. 125306, Sep. 2018.

[141] D. S. Smirnov, E. A. Zhukov, D. R. Yakovlev, E. Kirstein, M. Bayer, and A. Greilich, "Spin polarization recovery and Hanle effect for charge carriers interacting with nuclear spins in semiconductors," *Phys. Rev. B*, vol. 102, p. 235413, Dec. 2020.

[142] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics*, vol. 4, p. 82, Oct. 2002.

[143] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "Corrigendum: A comprehensive design and performance analysis of low earth orbit satellite quantum communication (2013 new j. phys. 15 023006)," *New Journal of Physics*, vol. 16, p. 069502, Jun. 2014.

[144] D. Giggenbach and A. Shrestha, "Atmospheric absorption and scattering impact on optical satellite-ground links," *International Journal of Satellite Communications and Networking*, vol. 40, no. 2, pp. 157–176, 2022.

[145] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, "Experimental demonstration of memory-enhanced quantum communication," *Nature*, vol. 580, no. 7801, p. 60–64, 2020.

[146] S. Bauer, D. Wang, N. Hoppe, C. Nawrath, J. Fischer, N. Witz, M. Kaschel, C. Schweikert, M. Jetter, S. L. Portalupi, M. Berroth, and P. Michler, "Achieving stable fiber coupling of quantum dot telecom c-band single-photons to an SOI photonic device," *Applied Physics Letters*, vol. 119, p. 211101, 11 2021.

[147] M. H. Rahaman, S. Harper, C.-M. Lee, K.-Y. Kim, M. A. Buyukkaya, V. J. Patel, S. D. Hawkins, J.-H. Kim, S. J. Addamane, and E. Waks, "Efficient, indistinguishable telecom c-band photons using a tapered nanobeam waveguide," *ACS Photonics*, vol. 11, p. 2738–2744, Jun 2024.

[148] J. Huwer, R. M. Stevenson, J. Skiba-Szymanska, M. B. Ward, A. J. Shields, M. Felle, I. Farrer, D. A. Ritchie, and R. V. Penty, "Quantum-dot-based telecommunication-wavelength quantum relay," *Phys. Rev. Appl.*, vol. 8, p. 024007, Aug. 2017.

[149] E. M. Sala, Y. I. Na, M. Godsland, and J. Heffernan, "Self-assembled InAs quantum dots on InGaAsP/InP(100) by modified droplet epitaxy in metal–organic vapor phase epitaxy around the telecom C-band for quantum photonic applications," *physica status solidi (RRL) – Rapid Research Letters*, vol. 18, p. 2300340, Sep. 2023.

[150] T. Miyazawa, K. Takemoto, Y. Nambu, S. Miki, T. Yamashita, H. Terai, M. Fujiwara, M. Sasaki, Y. Sakuma, M. Takatsu, T. Yamamoto, and Y. Arakawa, "Single-photon emission at 1.5 µm from an InAs/InP quantum dot with highly suppressed multi-photon emission probabilities," *Applied Physics Letters*, vol. 109, p. 132106, Sep. 2016.

[151] P. Holewa, A. Sakanas, U. M. Gur, P. Mrowi'nski, A. Huck, B.-Y. Wang, A. Musiał, K. Yvind, N. Gregersen, M. Syperek, and E. Semenova, "Bright quantum dot single-photon emitters at telecom bands heterogeneously integrated on Si," *ACS Photonics*, vol. 9, pp. 2273 – 2279, Jun. 2021.

[152] P. Laccotripes, T. Müller, R. M. Stevenson, J. Skiba-Szymanska, D. A. Ritchie, and A. J. Shields, "Spin-photon entanglement with direct photon emission in the telecom c-band," *Nature Communications*, vol. 15, p. 9740, Nov. 2023.

[153] E. M. Sala, Y. I. Na, M. Godsland, A. Trapalis, and J. Heffernan, "InAs/InP quantum dots in etched pits by droplet epitaxy in metalorganic vapor phase epitaxy," *physica status solidi (RRL) – Rapid Research Letters*, vol. 14, p. 2000173, May 2020.

[154] A. Greilich, R. Oulton, E. A. Zhukov, I. A. Yugova, D. R. Yakovlev, M. Bayer, A. Shabaev, A. L. Efros, I. A. Merkulov, V. Stavarache, D. Reuter, and A. Wieck, "Optical control of spin coherence in singly charged $(\mathrm{In,Ga})\mathrm{As}/\mathrm{GaAs}$ quantum dots," *Phys. Rev. Lett.*, vol. 96, p. 227401, Jun. 2006.

[155] M. Syperek, D. R. Yakovlev, A. Greilich, J. Misiewicz, M. Bayer, D. Reuter, and A. D. Wieck, "Spin coherence of holes in $\mathrm{GaAs}/(\mathrm{Al,Ga})\mathrm{As}$ quantum wells," *Phys. Rev. Lett.*, vol. 99, p. 187401, Oct. 2007.

[156] M. M. Glazov, I. A. Yugova, S. Spatzek, A. Schwan, S. Varwig, D. R. Yakovlev, D. Reuter, A. D. Wieck, and M. Bayer, "Effect of pump-probe detuning on the Faraday rotation and ellipticity signals of mode-locked spins in (In,Ga)As/GaAs quantum dots," *Phys. Rev. B*, vol. 82, p. 155325, Oct. 2010.

[157] B. Urbaszek, X. Marie, T. Amand, O. Krebs, P. Voisin, P. Maletinsky, A. Högele, and A. Imamoglu, "Nuclear spin physics in quantum dots: An optical investigation," *Reviews of Modern Physics*, vol. 85, no. 1, p. 79–133, 2013.

[158] M. M. Glazov, "Coherent spin dynamics of electrons and excitons in nanostructures (a review)," *Physics of the Solid State*, vol. 54, no. 1, pp. 1–27, 2012. Translated from Russian "Fizika Tverdogo Tela", Vol. 54, No. 1.

[159] M. Bayer, A. Greilich, and D. R. Yakovlev, "Coherent electron spin dynamics in quantum dots," in *Single Semiconductor Quantum Dots*, NanoScience and Technology, pp. 121–143, Springer Berlin Heidelberg, 2009. Chapter 4.

[160] M. Syperek, D. R. Yakovlev, I. A. Yugova, J. Misiewicz, M. Jetter, M. Schulz, P. Michler, and M. Bayer, "Electron and hole spins in InP/(Ga,In)P self-assembled quantum dots," *Phys. Rev. B*, vol. 86, p. 125320, Sep. 2012.

[161] V. V. Belykh, D. R. Yakovlev, M. M. Glazov, P. S. Grigoryev, M. Hussain, J. Rautert, D. N. Dirin, M. V. Kovalenko, and M. Bayer, "Coherent spin dynamics of electrons and holes in CsPbBr3 perovskite crystals," *Nature Communications*, vol. 10, p. 673, Feb. 2019.

[162] I. A. Yugova, A. Greilich, E. A. Zhukov, D. R. Yakovlev, M. Bayer, D. Reuter, and A. D. Wieck, "Exciton fine structure in InGaAs/GaAs quantum dots revisited by pump-probe faraday rotation," *Phys. Rev. B*, vol. 75, p. 195325, May 2007.

[163] L. Sapienza, R. M. Al-Khuzheyri, A. C. Dada, A. Griffiths, E. Clarke, and B. D. Gerardot, "Magneto-optical spectroscopy of single charge-tunable InAs/GaAs quantum dots emitting at telecom wavelengths," *Physical Review B*, vol. 93, p. 155301, 2016.

[164] I. Hapke-Wurst, U. Zeitler, R. Haug, and K. Pierz, "Mapping the g factor anisotropy of InAs self-assembled quantum dots," *Physica E: Low-dimensional Systems and Nanostructures*, vol. 12, pp. 802–805, Jan. 2002. Proceedings of the Fourteenth International Conference on the Electronic Properties of Two-Dimensional Systems.

[165] C. Carmesin, M. Schowalter, M. Lorke, D. Mourad, T. Grieb, K. Müller-Caspary, M. Yacob, J. P. Reithmaier, M. Benyoucef, A. Rosenauer, and F. Jahnke, "Interplay of morphology, composition, and optical properties of InP-based quantum dots emitting at the $1.55\ \mu$m telecom wavelength," *Phys. Rev. B*, vol. 96, p. 235309, Dec. 2017.

[166] N. A. J. M. Kleemans, J. van Bree, M. Bozkurt, P. J. van Veldhoven, P. A. Nouwens, R. Nötzel, A. Y. Silov, P. M. Koenraad, and M. E. Flatté, "Size-dependent exciton g factor in self-assembled InAs/InP quantum dots," *Phys. Rev. B*, vol. 79, p. 045311, Jan. 2009.

[167] W. Sheng and A. Babinski, "Zero g factors and nonzero orbital momenta in self-assembled quantum dots," *Phys. Rev. B*, vol. 75, p. 033316, Jan. 2007.

[168] S. A. Crooker, J. Brandt, C. Sandfort, A. Greilich, D. R. Yakovlev, D. Reuter, A. D. Wieck, and M. Bayer, "Spin noise of electrons and holes in self-assembled quantum dots," *Phys. Rev. Lett.*, vol. 104, p. 036601, Jan. 2010.

[169] A. Greilich, A. Pawlis, F. Liu, O. A. Yugov, D. R. Yakovlev, K. Lischka, Y. Yamamoto, and M. Bayer, "Spin dephasing of fluorine-bound electrons in ZnSe," *Phys. Rev. B*, vol. 85, p. 121303, Mar. 2012.

[170] S. Varwig, A. Ren'e, A. Greilich, D. R. Yakovlev, D. Reuter, A. D. Wieck, and M. Bayer, "Temperature dependence of hole spin coherence in (In,Ga)As quantum dots measured by mode-locking and echo techniques," *Physical Review B*, vol. 87, p. 115307, Mar. 2013.

[171] D. Das, H. Ghadi, B. Tongbram, S. Singh, and S. Chakrabarti, "The impact of confinement enhancement algaas barrier on the optical and structural properties of InAs/InGaAs/GaAs submonolayer quantum dot heterostructures," *Journal of Luminescence*, vol. 192, pp. 277–282, 2017.

[172] F. Heisterkamp, E. A. Zhukov, A. Greilich, D. R. Yakovlev, V. L. Korenev, A. Pawlis, and M. Bayer, "Longitudinal and transverse spin dynamics of donor-bound electrons in fluorine-doped ZnSe: Spin inertia versus Hanle effect," *Phys. Rev. B*, vol. 91, p. 235432, Jun. 2015.

[173] M. Gong, W. Zhang, Z. Han, G. Guo, and L. He, "Atomistic pseudopotential theory of optical properties of exciton complexes in InAs/InP quantum dots," *Applied Physics Letters*, vol. 99, p. 231106, 2010.

[174] M. Kroutvar, Y. Ducommun, D. Heiss, M. Bichler, D. Schuh, G. Abstreiter, and J. J. Finley, “Optically programmable electron spin memory using semiconductor quantum dots,” *Nature*, vol. 432, pp. 81–84, 2004.

[175] W. I. L. Lawrie, N. W. Hendrickx, F. van Riggelen, M. Russ, L. Petit, A. Sammak, G. Scappucci, and M. Veldhorst, “Spin relaxation benchmarks and individual qubit addressability for holes in quantum dots,” *Nano Letters*, vol. 20, no. 10, p. 7237–7242, 2020.

[176] F. Fras, B. Eble, P. Desfonds, F. Bernardot, C. Testelin, M. Chamarro, A. Miard, and A. Lemaître, “Two-phonon process and hyperfine interaction limiting slow hole-spin relaxation time in InAs/GaAs quantum dots,” *Phys. Rev. B*, vol. 86, p. 045306, Jul. 2012.

[177] V. Nedelea, N. V. Leppenen, E. Evers, D. S. Smirnov, M. Bayer, and A. Greilich, “Tuning the nuclei-induced spin relaxation of localized electrons by the quantum Zeno and anti-Zeno effects,” *Phys. Rev. Res.*, vol. 5, p. L032032, Sep. 2023.

[178] N. A. Sinitsyn, Y. Li, S. A. Crooker, A. Saxena, and D. L. Smith, “Role of nuclear quadrupole coupling on decoherence and relaxation of central spins in quantum dots,” *Phys. Rev. Lett.*, vol. 109, p. 166605, Oct. 2012.

[179] F. G. G. Hernandez, A. Greilich, F. Brito, M. Wiemann, D. R. Yakovlev, D. Reuter, A. D. Wieck, and M. Bayer, “Temperature-induced spin-coherence dissipation in quantum dots,” *Phys. Rev. B*, vol. 78, p. 041303, Jul. 2008.

[180] D. A. Vajner, L. Rickert, T. Gao, K. Kaymazlar, and T. Heindel, “Quantum communication using semiconductor quantum dots,” *Advanced Quantum Technologies*, vol. 5, no. 7, p. 2100116, 2022.

[181] X. Li, Q. Xu, and Z. Zhang, “Molecular beam epitaxy growth of quantum wires and quantum dots,” *Nanomaterials*, vol. 13, p. 960, Mar. 2023.

[182] E. A. Stinaff, M. Scheibner, A. S. Bracker, I. V. Ponomarev, V. L. Korenev, M. E. Ware, M. F. Doty, T. L. Reinecke, and D. Gammon, “Optical signatures of coupled quantum dots,” *Science*, vol. 311, no. 5761, pp. 636–639, 2006.

[183] D. Kim, S. E. Economou, c. C. Bădescu, M. Scheibner, A. S. Bracker, M. Bashkansky, T. L. Reinecke, and D. Gammon, “Optical spin initialization and non-destructive measurement in a quantum dot molecule,” *Physical Review Letters*, vol. 101, no. 23, p. 236804, 2008.

[184] D. Wigger, J. Schall, M. Deconinck, N. Bart, P. Mrowiński, M. Krzykowski, K. Gawarecki, M. von Helversen, R. Schmidt, L. Bremer, F. Bopp, D. Reuter, A. D. Wieck, S. Rodt, J. Renard, G. Nogues, A. Ludwig, P. Machnikowski, J. J. Finley, S. Reitzenstein, and J. Kasprzak, "Controlled coherent coupling in a quantum dot molecule revealed by ultrafast four-wave mixing spectroscopy," *ACS Photonics*, vol. 10, p. 1504–1511, May 2023.

[185] J. H. Prechtel, F. M. Maier, J. Houel, A. V. Kuhlmann, A. Ludwig, A. D. Wieck, D. Loss, and R. J. Warburton, "Electrically tunable hole g factor of an optically active quantum dot for fast spin rotations," *Physical Review B*, vol. 91, p. 165304, 2014.

[186] I. Mikhailov, L. García, and J. Marín, "Vertically coupled quantum dots charged by exciton," *Microelectronics Journal*, vol. 39, no. 3, pp. 378–382, 2008. The Sixth International Conference on Low Dimensional Structures and Devices.

[187] R. Hostein, A. Michon, G. Beaudoin, N. Gogneau, G. Patriache, J.-Y. Marzin, I. Robert-Philip, I. Sagnes, and A. Beveratos, "Time-resolved characterization of InAsP/InP quantum dots emitting in the C-band telecommunication window," *Applied Physics Letters*, vol. 93, p. 073106, 08 2008.

[188] M. Y. Petrov, I. V. Ignatiev, S. V. Poltavtsev, A. Greilich, A. Bauschulte, D. R. Yakovlev, and M. Bayer, "Effect of thermal annealing on the hyperfine interaction in InAs/GaAs quantum dots," *Phys. Rev. B*, vol. 78, p. 045315, Jul. 2008.

[189] R. Stockill, C. Le Gall, C. Matthiesen, L. Huthmacher, E. Clarke, M. Hugues, and M. Atatüre, "Quantum dot spin coherence governed by a strained nuclear environment," *Nature Communications*, vol. 7, p. 12745, Sep. 2016.

[190] T. M. Godden, J. H. Quilter, A. J. Ramsay, Y. Wu, P. Brereton, S. J. Boyle, I. J. Luxmoore, A. P. Heberle, M. S. Skolnick, and A. M. Fox, "Coherent optical control of the spin of a single hole in an InAs/GaAs quantum dot," *Phys. Rev. Lett.*, vol. 108, p. 017402, Jan. 2012.

[191] D. V. Bulaev and D. Loss, "Spin relaxation and decoherence of holes in quantum dots.," *Physical review letters*, vol. 95, p. 076805, Aug. 2005.

[192] H. Wei, M. Gong, G. Guo, and L. He, "Atomistic pseudopotential theory of spin relaxation in self-assembled In1−xGaxAs/GaAs quantum dots at zero magnetic field," *Physical Review B*, vol. 85, p. 045317, 2010.

[193] E. A. Zhukov, D. R. Yakovlev, M. Bayer, M. M. Glazov, E. L. Ivchenko, G. Karczewski, T. Wojtowicz, and J. Kossut, “Spin coherence of a two-dimensional electron gas induced by resonant excitation of trions and excitons in CdTe/(Cd,Mg)Te quantum wells,” *Physical Review B*, vol. 76, p. 205310, 2007.

[194] I. Yugova, M. Glazov, D. Yakovlev, A. Sokolova, and M. Bayer, “Coherent spin dynamics of electrons and holes in semiconductor quantum wells and quantum dots under periodical optical excitation: Resonant spin amplification versus spin mode locking,” *Physical Review B—Condensed Matter and Materials Physics*, vol. 85, no. 12, p. 125304, 2012.

[195] H. J. Krenner, S. Stufler, M. Sabathil, E. C. Clark, P. Ester, M. Bichler, G. Abstreiter, J. J. Finley, and A. Zrenner, “Recent advances in exciton-based quantum information processing in quantum dot nanostructures,” *New Journal of Physics*, vol. 7, pp. 184 – 184, 2005.

[196] M. Usman, T. Inoue, Y. Harda, G. Klimeck, and T. Kita, “Experimental and atomistic theoretical study of degree of polarization from multilayer InAs/GaAs quantum dot stacks,” *Physical Review B*, vol. 84, p. 115321, 2011.

[197] J. Luo, G. Bester, and A. Zunger, “Supercoupling between heavy-hole and light-hole states in nanostructures,” *Physical Review B*, vol. 92, p. 165301, Oct. 2015.

[198] X. Marie, T. Amand, P. Le Jeune, M. Paillard, P. Renucci, L. E. Golub, V. D. Dymnikov, and E. L. Ivchenko, “Hole spin quantum beats in quantum-well structures,” *Phys. Rev. B*, vol. 60, pp. 5811–5817, Aug. 1999.

[199] M. A. Semina, A. A. Golovatenko, and A. V. Rodina, “Cubic anisotropy of hole Zeeman splitting in semiconductor nanocrystals,” *Physical Review B*, vol. 108, p. 235310, Dec. 2023.

[200] H. Yu, S. Lycett, C. Roberts, and R. Murray, “Time resolved study of self-assembled inas quantum dots,” *Applied Physics Letters*, vol. 69, pp. 4087–4089, 12 1996.

[201] A. Fiore, P. Borri, W. Langbein, J. M. Hvam, U. Oesterle, R. Houdré, R. P. Stanley, and M. Ilegems, “Time-resolved optical characterization of InAs/InGaAs quantum dots emitting at 1.3 µm,” *Applied Physics Letters*, vol. 76, pp. 3430–3432, 06 2000.

[202] G. Wang, S. Fafard, D. Leonard, J. E. Bowers, J. L. Merz, and P. M. Petroff, “Time-resolved optical characterization of InGaAs/GaAs quantum dots,” *Applied Physics Letters*, vol. 64, pp. 2815–2817, 05 1994.

[203] J. M. Daniels, P. Machnikowski, and T. Kuhn, “Excitons in quantum dot molecules: Coulomb coupling, spin-orbit effects, and phonon-induced line broadening,” *Physical Review B*, vol. 88, p. 205307, 2013.

[204] J. Rautert, T. S. Shamirzaev, S. V. Nekrasov, D. R. Yakovlev, P. Klenovsk’y, Y. G. Kusrayev, and M. Bayer, “Optical orientation and alignment of excitons in direct and indirect band gap (In,Al)As/AlAs quantum dots with type-I band alignment,” *Physical Review B*, vol. 99, p. 195411, May 2019.

[205] K. Sivalertporn, L. Mouchliadis, A. L. Ivanov, R. Philp, and E. A. Muljarov, “Direct and indirect excitons in semiconductor coupled quantum wells in an applied electric field,” *Physical Review B*, vol. 85, p. 045207, 2011.

[206] K. D. Greve, P. L. McMahon, D. Press, T. D. Ladd, D. Bisping, C. Schneider, M. Kamp, L. Worschech, S. Hoefling, A. Forchel, and Y. Yamamoto, “Ultrafast coherent control and suppressed nuclear feedback of a single quantum dot hole qubit,” *Nature Physics*, vol. 7, pp. 872–878, 2011.

[207] V. Martín, J. P. Brito, C. Escribano, M. Menchetti, C. White, A. Lord, F. Wissel, M. Gunkel, P. Gavignet, N. Genay, O. L. Moult, C. Abellán, A. Manzalini, A. A. P. Perales, V. López, and D. R. López, “Quantum technologies in the telecommunications industry,” *EPJ Quantum Technology*, vol. 8, p. 19, Jul. 2021.

[208] O. Alkhazragi, H. Lu, W. Yan, N. Almaymoni, T.-Y. Park, Y. Wang, T. K. Ng, and B. S. Ooi, “Semiconductor emitters in entropy sources for quantum random number generation,” *Annalen der Physik*, vol. 535, p. 2300289, Aug. 2023.

[209] E. Başar, “Kirchhoff meets Johnson: In pursuit of unconditionally secure communication,” *Engineering Reports*, vol. 6, p. e12958, Jun. 2023.

[210] A. M. Garipcan and E. Erdem, “Hardware implementation of chaotic zigzag map based bitwise dynamical pseudo random number generator on field-programmable gate array,” *Informacije MIDEM - Journal of Microelectronics, Electronic Components and Materials*, vol. 50, p. 243–253, 2021.

[211] J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, "5.4 Gbps real time quantum random number generator with simple implementation.," *Optics express*, vol. 24, pp. 27475–27481, 2016.

[212] C. R. S. Williams, J. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission.," *Optics express*, vol. 18, pp. 23584–23597, 2010.

[213] B. Bai, J. Huang, G.-R. Qiao, Y.-Q. Nie, W. Tang, T. Chu, J. Zhang, and J.-W. Pan, "18.8 Gbps real-time quantum random number generator with a photonic integrated chip," *Applied Physics Letters*, vol. 118, p. 264001, Jun. 2021.

[214] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, "6 Gbps real-time optical quantum random number generator based on vacuum fluctuation.," *The Review of scientific instruments*, vol. 90, p. 043105, Apr. 2018.

[215] T. Bertapelle, M. Avesani, A. Santamato, A. Montanaro, M. Chiesa, D. Rotta, M. Artiglia, V. Sorianello, F. Testa, G. D. Angelis, G. Contestabile, G. Vallone, M. Romagnoli, and P. Villoresi, "High-speed source-device-independent quantum random number generator on a chip," *Optica Quantum*, vol. 3, pp. 111–118, Feb 2025.

[216] K. Qiu, Y. Cai, N. H. Y. Ng, and J. Y. Haw, "Fully passive quantum random number generation with untrusted light," *APL Quantum*, vol. 2, p. 046105, 10 2025.

[217] J. Cheng, S. Liang, J. Qin, J. Li, Z. Yan, X. Jia, C. Xie, and K. Peng, "Semi-device-independent quantum random number generator with a broadband squeezed state of light," *NPJ Quantum Inf.*, vol. 10, Feb. 2024.

[218] J. Zhang, Y. Li, M. Zhao, D. Han, J. Liu, M. Wang, Q. Gong, Y. Xiang, Q. He, and X. Su, "One-sided device-independent random number generation through fiber channels," *Light Sci. Appl.*, vol. 14, p. 25, Jan. 2025.

[219] J. Yang, M. Wu, Y. Zhang, Y. Li, W. Huang, H. Wang, Y. Pan, Q. Su, Y. Bian, H. Jiang, S. Yu, B. Xu, B. Luo, and H. Guo, "An ultra-fast quantum random number generation scheme based on laser phase noise," *Commun. Phys.*, vol. 9, Dec. 2025.

[220] O. M. Crampton, T. J. Dowling, T. Roger, P. R. Smith, J. F. Dynes, M. S. Winnel, D. G. Marangon, M. Sanzaro, R. Singh, C. Perumangatt, J. A. Dolphin, T. K. Paraiso, and A. J.

Shields, "A 2-gbps low-SWaP quantum random number generator with photonic integrated circuits for satellite applications," *NPJ Quantum Inf.*, vol. 11, p. 153, Sept. 2025.

[221] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution," *Applied Physics Letters*, vol. 117, p. 144003, Oct. 2020.

[222] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nature Photonics*, vol. 1, pp. 343–348, 2007.

[223] J. Thewes, C. Lüders, and M. Aßmann, "Eavesdropping attack on a trusted continuous-variable quantum random-number generator," *Phys. Rev. A*, vol. 100, p. 052318, Nov. 2019.

[224] M. Shrivastava, M. Mittal, I. Kumari, and V. Abhignan, "Randomness in quantum random number generator from vacuum fluctuations with source-device-independence," *Applied Physics B*, vol. 131, p. 111, May 2025.

[225] X. Guo, W. Zhou, Y. Luo, X. Meng, J. Li, Y. Bian, Y. Guo, and L. Xiao, "Deep learning-based min-entropy-accelerated evaluation for high-speed quantum random number generation," *Entropy*, vol. 27, p. 786, Jul. 2025.

[226] Y. Li, Y. Fei, W. Wang, X. Meng, H. Wang, Q. Duan, Y. Han, and Z. Ma, "Practical security analysis of a continuous-variable source-independent quantum random number generator based on heterodyne detection," *Opt. Express*, vol. 31, pp. 23813–23829, Jul. 2023.

[227] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Review of Scientific Instruments*, vol. 86, p. 063105, 06 2015.

[228] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5524–5535, 2011.

[229] H. Krawczyk, "Lfsr-based hashing and authentication," in *Advances in Cryptology — CRYPTO '94* (Y. G. Desmedt, ed.), (Berlin, Heidelberg), pp. 129–139, Springer Berlin Heidelberg, 1994.

[230] AMD, *UltraFast Design Methodology Guide (UG949)*, May 2025.

[231] Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," *Phys. Rev. A*, vol. 81, p. 063814, Jun. 2010.

[232] J. Li, Z. Huang, C. Yu, J. Wu, T. Zhao, X. Zhu, and S. Sun, "Quantum random number generation based on phase reconstruction.," *Optics express*, vol. 32 4, pp. 5056–5071, 2024.

[233] R. G. Brown, *DieHarder: A GNU Public License Random Number Tester*. Duke University (Physics Department), Durham, NC, 2006.

[234] K. Sharman, F. Kimiaee Asadi, S. C. Wein, and C. Simon, "Quantum repeaters based on individual electron spins and nuclear-spin-ensemble memories in quantum dots," *Quantum*, vol. 5, p. 570, Nov. 2021.

[235] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, p. 595–604, Jul. 2014.

[236] A. Bogucki, T. Smoleński, M. Goryca, T. Kazimierczuk, J. Kobak, W. Pacuski, P. Wojnar, and P. Kossacki, "Anisotropy of in-plane hole g factor in CdTe/ZnTe quantum dots," *Phys. Rev. B*, vol. 93, p. 235410, Jun. 2016.

[237] P. Senellart, G. S. Solomon, and A. White, "High-performance semiconductor quantum-dot single-photon sources.," *Nature nanotechnology*, vol. 12, pp. 1026–1039, Nov. 2017.

[238] N. J. Martin, A. J. Brash, A. Tomlinson, E. M. Sala, E. O. Mills, C. L. Phillips, R. Dost, L. Hallacy, P. Millington-Hotze, D. Hallett, K. A. O'Flaherty, J. Heffernan, M. S. Skolnick, A. M. Fox, and L. R. Wilson, "Stark tuning and charge state control in individual telecom c-band quantum dots," *Applied Physics Letters*, vol. 127, p. 194001, Nov. 2025.

[239] K. Debnath, M. Clementi, T. D. Bucio, A. Z. Khokhar, M. Sotto, K. M. Grabska, D. Bajoni, M. Galli, S. Saito, and F. Y. Gardes, "Ultrahigh-Q photonic crystal cavities in silicon rich nitride," *Opt. Express*, vol. 25, pp. 27334–27340, Oct. 2017.

[240] L. Rickert, B. Fritsch, A. Kors, J. P. Reithmaier, and M. Benyoucef, "Mode properties of telecom wavelength InP-based high-(Q/V) L4/3 photonic crystal cavities," *Nanotechnology*, vol. 31, p. 315703, May 2020.

[241] E. M. Purcell, "Spontaneous Emission Probabilities at Radio Frequencies," *Physical Review*, vol. 69, p. 681, 1946.