Worldwide, enormous efforts are directed toward the development of the so-called quantum internet. Turning this long-sought-after dream into reality is a great challenge that will require breakthroughs in quantum communication and computing. To establish a global, quantum-secured communication infrastructure, photonic quantum technologies will doubtlessly play a major role, by providing and interfacing essential quantum resources, for example, flying- and stationary qubits or quantum memories.

Over the last decade, significant progress has been made in the engineering of on-demand quantum light sources based on semiconductor quantum dots, which enable the generation of close-to-ideal single- and entangled-photon states, useful for applications in quantum information processing. This review focuses on implementations of, and building blocks for, quantum communication using quantum-light sources based on epitaxial semiconductor quantum dots. After reviewing the main notions of quantum communication and introducing the devices used for single-photon and entangled-photon generation, an overview of experimental implementations of quantum key distribution protocols using quantum dot based quantum light sources is provided. Furthermore, recent progress toward quantum-secured communication networks as well as building blocks thereof is summarized. The article closes with an outlook, discussing future perspectives in the field and identifying the main challenges to be solved.

1. Introduction

The task of storing and exchanging information lies at the heart of our society. In many cases, information has to be transmitted in a secure fashion. Numerous examples can be found, where secure information exchange is crucial, ranging from sensitive private, financial, or medical data as well as information related to critical infrastructure. While various encryption schemes, as well as the strategies of breaking them, have been employed over time (see Singh for a historic overview[1]), most current security standards rely on the computational complexity of so-called one-way functions.[2]

However, considering the steady increase in computational power, today’s secrets might not stay secret forever. Additionally, breakthroughs in the fields of quantum computing might endanger security schemes such as the Rivest-Shamir-Adleman (RSA) scheme, which is based on prime factorization of large numbers, a problem that could be solved efficiently on future quantum computers using Shor’s algorithm.[3]

In addition, classical encryption protocols do exist, which claim to be post-quantum secure—but none of them offers ultimate security.[4]

This is where quantum key distribution (QKD) comes into play, which is a method of establishing a random bitstring, securely shared between authenticated parties. This key can then be used to encrypt messages with a key that is protected not by computational complexity, but by the laws of quantum mechanics. If the so-called one-time-pad (OTP) scheme is used for data encryption, information-theoretical security is possible[5, 6] (see details further below). In brief, the communicating parties exchange quantum two-level systems, known as quantum bits or qubits, prepared in one of two incompatible bases. Any eavesdropping attempt requires measurement on the qubits, for which an eavesdropper must choose one specific basis since quantum states cannot be copied.[7] As a result, errors are introduced in the key material in cases where the attacker uses the wrong basis. Detected by the communicating parties, these errors reveal eavesdropping attempts already during key generation and the corresponding bit string can be discarded for data encryption. Also, in contrast to classical encryption schemes, a postponed measurement of the transmitted qubit is not possible. Hence, securely transmitted data will remain secure also in the future. Photonic quantum channels do however not only provide a means of perfectly secure communication but also enable other quantum technologies. “Flying” qubits, that is, photons, are vital for distributed quantum computing schemes and to interface different parts of a future quantum computer, as formulated in the seminal DiVincenzo criteria.[8] Connecting several quantum computing nodes securely, a quantum network can be realized ideally all over the world—a vision called the quantum
Figure 1. Principle of QKD: Prepare and Measure based a) and entanglement based b) protocols can be used to generate a secret key that can be used with the OTP c) for absolutely secure communications. d) Common eavesdropping strategies of an adversary (Eve) intercepting the quantum channel.

internet.[9] This review intends to summarize and discuss some of the progress made toward achieving that vision, with a focus on implementations of quantum communication using quantum light sources based on epitaxial semiconductor quantum dots (QDs).

Let us begin by introducing QKD in more detail. Historically, the ideas of quantum cryptography date back to the late 1960s, when Stephen Wiesner first formulated his ideas on conjugate coding, a work published more than a decade later in 1983.[10] We refer to Bennett et al.[11] for a first-hand historical review. Motivated by the ideas of Wiesner, Charles H. Bennett and Gill Brassard proposed the first actual key distribution protocol in 1984, later referred to as the BB84 protocol, using the quantum mechanical properties of single photons to detect eavesdropping attempts.[12] In their seminal work, the authors proposed to use the polarization of single photons to encode the bits in different, randomly chosen bases (see Figure 1a) and detect adversaries by comparing a subset of the results. Many QKD protocols follow the same generic steps introduced in the BB84 protocol and outlined in the following:

1. **Qubit exchange:** The sending party (Alice) encodes photons in one of at least two randomly selected, non-commuting bases and sends them via a quantum channel to the receiving party (Bob), who detects the photons in randomly chosen bases on his side. Accordingly, this configuration is referred to as a prepare-and-measure setting, in contrast to entanglement-based schemes (see further below). The transmitted bit string is referred to as the raw key.

2. **Sifting:** If Alice and Bob are authenticated (see below), they can share their lists of used bases settings over a classical, public channel and keep only measurement results where both used the same basis (a process called “key sifting”), without communicating the actual measurement results. The bit string obtained after the sifting step is called sifted key and should be perfectly correlated in the absence of experimental imperfections and eavesdropping by an adversary (Eve).

3. **Parameter Estimation:** By comparing a subset of the sifted key, potential eavesdropping can be detected. According to the laws of quantum mechanics, every measurement of an adversary on the transmitted photons, performed in the wrong basis, perturbs the quantum state, which leads to detectable errors in the sifted key. These errors can be quantified by the quantum bit error ratio (QBER), which is the probability that a bit of Alice and Bob differs, even though they used the same measurement basis. Note, that a more widely used term in the literature is the quantum bit error rate in units of s⁻¹. As the QBER entering the key rate equations must be a probability (see Eq. 4), we consistently use the quantum bit error ratio in this work. As discussed further below, the QBER is mainly affected by the qubit-state preparation and discrimination fidelities, as well as by detector noise.

4. **Error correction:** In a classical post-processing step, the errors introduced by the quantum channel, insufficient state preparation, and the detection setup need to be corrected. Hereby, a finite amount of information leaks to the adversary, which must be compensated during the last step.

5. **Privacy Amplification:** The secrecy of the final key can be enhanced in another classical post-processing step, by applying hash functions that reduce the key length but increase its security. The remaining bits form the secure key shared between Alice and Bob. The number of secure bits per time is called...
the secure key rate and a positive key rate means that secure key exchange is possible.

Note that the aforementioned steps require an authenticated classical channel to be established between both parties in advance. For this purpose, a small amount of secret key needs to be available before the first quantum-key exchange,\footnote{This initially available key can be renewed once the quantum key exchange was successful.} which is why QKD is also referred to as a “secret growing scheme”. This initially available key can be renewed once the quantum key exchange was successful. The authenticated classical channel is needed to communicate the used measurement bases in the BB84 protocol, the exchanged bits for the error correction, and the choice of random numbers during the privacy amplification step. Without authentication, an eavesdropper could always perform a man-in-the-middle-attack by impersonating Alice or Bob. In the most common authentication scheme, the parties use the initially shared secret bits as seeds to select a hash function from a fixed family. The party that wants to send an authenticated message computes the hash of the message and sends the message and hash together. The second party can then confirm the value of the hash, by applying the same hash function, to authenticate the message. If the used hash functions are universal (like those also used for privacy amplification), this authentication scheme is provably secure.\footnote{Authentication can also be done without an initially shared secret key, via a trusted third party. An example of this would be the authority-based authentication scheme, where both Alice and Bob talk to an authority. An example of this would be the authority-based authentication scheme, where both Alice and Bob talk to an authority that confirms their identities.} In addition to that, authentication is possible by combining methods from classical cryptography and post-quantum cryptography. The basic idea is that only short-term security needs to be assumed for the authentication step, to enable a QKD protocol, which then establishes a key with long-term security.\footnote{Authentication is possible by combining methods from classical cryptography and post-quantum cryptography.} This can lead to an increase in efficiency, especially in multi-user networks, as recently demonstrated experimentally by Wang et al.\footnote{Note furthermore, that in most of the QKD protocols random numbers are needed, either to encode a random bit, to pick a measurement basis, or to select the hash functions randomly. Thus, true random number generators are essential for QKD schemes to be absolutely secure (see Section 4.5).} A few years after C. H. Bennett and G. Brassard proposed their BB84 protocol, Artur Ekert proposed the first QKD protocol using entangled photon pairs in 1991\footnote{It is used only once (hence the name one-time-pad).} (Figure 1b). The E91 protocol relies on detecting an eavesdropper by monitoring the amount of violation of a Bell-like inequality,\footnote{It is used only once (hence the name one-time-pad).} which quantifies the degree of remaining entanglement. In addition, one can also use the distributed entangled photons directly for measurements in the BB84 bases, compare some of the results and deduce the security from the identified error rates just as in the BB84 protocol—a protocol known as BBM92.\footnote{If these requirements are met, the secret key can be applied to the message using an XOR \textsc{eXclusive OR} logical operation (a modulo-2 addition). The resulting encrypted message appears to third parties as random as the key itself and therefore does not disclose any useful information. Then, the encrypted message can be sent over a public channel. The other party can now use the same key and apply it with an XOR operation to the received, encrypted bit string, by which the original message is recovered. The problem for any classical key distribution process however is to guarantee the secrecy of the key distribution. Exactly this secrecy can be guaranteed using QKD.} Note, that sending single photons from Alice to Bob in a prepare-and-measure setting, or Alice and Bob each receiving one photon from a central source in an entanglement-based setting are equivalent. One can also imagine QKD with entangled photons in the way that Alice measures a photon, which then travels backward in time to the source and then forward in time to Bob.\footnote{Quantum cryptography is physically secure in the sense that eavesdropping attempts can always be detected. The most basic eavesdropping scenario is the intercept-resend strategy, where an adversary measures Alice’s photons in a random basis and resends photons prepared in the same state to Bob (c.f. Figure 1d, upper panel). In the symmetric BB84 protocol, the wrong basis is chosen in 50% of all cases, resulting in a disturbance of the quantum states. When an eavesdropping attempt is detected, it can either be compensated (if the error is low enough) by distilling a shorter key that is again secure, or the key is discarded and} the problem for any classical key distribution process however is to guarantee the secrecy of the key distribution. Exactly this secrecy can be guaranteed using QKD. The total distance to be covered in secure communication, however, can be doubled by placing the source in the center of Alice and Bob (although at asymptotically small rates), as the ultimate limit is given by the attenuation at which the detection rate at each individual detector equals its dark count rate (see, e.g., Figure 3 in ref. \cite{24}).

Nowadays, numerous other QKD protocols are known, for example, decoy protocols for attenuated lasers, asymmetric versions of the BB84 protocol, protocols with more or fewer states, multi-dimensional protocols, fully or partially device-independent protocols, two-way protocols and coherent-one-way protocols, reference-frame independent protocols, twin-field protocols, continuous variable protocols, and many more. For a recent overview, we refer to Pirandola et al.\footnote{Quantum cryptography is physically secure in the sense that eavesdropping attempts can always be detected. The most basic eavesdropping scenario is the intercept-resend strategy, where an adversary measures Alice’s photons in a random basis and resends photons prepared in the same state to Bob (c.f. Figure 1d, upper panel). In the symmetric BB84 protocol, the wrong basis is chosen in 50% of all cases, resulting in a disturbance of the quantum states. When an eavesdropping attempt is detected, it can either be compensated (if the error is low enough) by distilling a shorter key that is again secure, or the key is discarded and}

After establishing a secure key through a QKD protocol, how can the two parties exchange a message and be sure that no one but them knows its content? The only provably secure—in an information theoretical sense—encryption method known to date is the OTP\footnote{Quantum cryptography is physically secure in the sense that eavesdropping attempts can always be detected. The most basic eavesdropping scenario is the intercept-resend strategy, where an adversary measures Alice’s photons in a random basis and resends photons prepared in the same state to Bob (c.f. Figure 1d, upper panel). In the symmetric BB84 protocol, the wrong basis is chosen in 50% of all cases, resulting in a disturbance of the quantum states. When an eavesdropping attempt is detected, it can either be compensated (if the error is low enough) by distilling a shorter key that is again secure, or the key is discarded and} (see Figure 1c). This symmetric encryption method, first postulated by G. Vernam in 1926,\footnote{Quantum cryptography is physically secure in the sense that eavesdropping attempts can always be detected. The most basic eavesdropping scenario is the intercept-resend strategy, where an adversary measures Alice’s photons in a random basis and resends photons prepared in the same state to Bob (c.f. Figure 1d, upper panel). In the symmetric BB84 protocol, the wrong basis is chosen in 50% of all cases, resulting in a disturbance of the quantum states. When an eavesdropping attempt is detected, it can either be compensated (if the error is low enough) by distilling a shorter key that is again secure, or the key is discarded and} is based on four requirements:

- The key of Alice and Bob is secret
- It is randomly generated
- It has at least the same length as the message to be encrypted
- It is used only once (hence the name one-time-pad).

If these requirements are met, the secret key can be applied to the message using an XOR \textsc{eXclusive OR} logical operation (a modulo-2 addition). The resulting encrypted message appears to third parties as random as the key itself and therefore does not disclose any useful information. Then, the encrypted message can be sent over a public channel. The other party can now use the same key and apply it with an XOR operation to the received, encrypted bit string, by which the original message is recovered. The problem for any classical key distribution process however is to guarantee the secrecy of the key distribution. Exactly this secrecy can be guaranteed using QKD.

Quantum cryptography is physically secure in the sense that eavesdropping attempts can always be detected. The most basic eavesdropping scenario is the intercept-resend strategy, where an adversary measures Alice’s photons in a random basis and resends photons prepared in the same state to Bob (c.f. Figure 1d, upper panel). In the symmetric BB84 protocol, the wrong basis is chosen in 50% of all cases, resulting in a disturbance of the quantum states. When an eavesdropping attempt is detected, it can either be compensated (if the error is low enough) by distilling a shorter key that is again secure, or the key is discarded and
a new key exchange is initiated, until the final key is provably secure.

Generally speaking, quantum cryptography is the art of using quantum mechanical effects to perform cryptographic tasks, which cover many scenarios going beyond the mere exchange of a secret key. Important examples for other cryptographic primitives with corresponding quantum implementations include bit commitment, coin flipping, oblivious transfer (see, e.g., Broadbent et al. for an overview). While the focus of this review article is set on QKD, the required building blocks (sources, channels, memories, repeaters, random numbers, etc.) also enable quantum cryptographic applications beyond QKD.

When implementing a QKD protocol, one of the first choices to take is the technology platform and the respective qubits used. To realize a “flying” qubit, photons are the obvious choice. They can be transmitted over long distances in optical fibers or through free-space links and hardly interact with their environment which leads to unmatched coherence properties. Due to the photon’s coherence properties, speed, and the possibility to encode information in various degrees of freedom (e.g., polarization, time-bin, energy, path, phase or orbital angular momentum, see for an overview), they are a promising candidate for many quantum information tasks such as quantum computing, sensing, metrology, and of course quantum cryptography. Noteworthy, other physical realizations for qubits are possible, which may have advantages for specific tasks. One example are electrons in wires, which however suffer from high losses and decoherence strongly limiting the achievable distance for quantum information transfer. Another alternative are microwave photons propagating in cryogenic waveguides, enabling interfaces between superconducting qubits in quantum computation tasks. In this context, Magnard et al. recently demonstrated a microwave quantum link between two remote transmon qubits separated by 5 m.

For implementations of QKD using optical photons, different encoding schemes have been developed, which will be briefly summarized in the following. It is straightforward to encode qubits in the polarization states of photons, which is why the very first demonstration of QKD in 1992 as well as the first field experiment used polarization encoding (Figure 2a). With polarization optics, arbitrary polarization states can be prepared, both in optical fibers and in free space. Typically, the rectilinear and the circular bases are used for the two non-commuting BB84 bases, as they can be prepared actively in a random fashion with fast electro-optical modulators on the sender side. On the receiver side, a beam splitter followed by polarization optics projecting the incoming photons in two different bases can be used to realize a passive random basis choice. Alternatively, the basis choice can also be performed actively, requiring a second electro-optical modulator at Bob. It is crucial to maintain the polarization state in this encoding scheme, which is why effects such as polarization mode dispersion in optical fibers must be compensated and the quantum channel must be stabilized to compensate polarisation drifts over time.

A coding scheme that is better suited for fiber-based communication is phase encoding. In the simplest case, a single Mach-Zehnder-Interferometer (MZI) is spanned between Alice and Bob via two optical fibers and two couplers, at which each of the parties can apply phase shifts to their half of the MZI. The chosen bases are compatible and the events survive the sifting if the phase difference is 0 or π, thus the beamsplitter exit port determines the detected bit. As the path length stability required in the single MZI phase encoding scheme is difficult to achieve in practice, QKD is typically done with a double MZI phase encoding. Here, two unbalanced MZI are set in series, with one being controlled by Alice and one by Bob (Figure 2b). If the imbalance of both MZIs is exactly matched, paths including one short and one long arm are indistinguishable, leading to the occurrence of interference depending on the applied phase shifts at Alice and Bob. The phase shifts represent the encoded bits. As the photons are in a superposition of different time bins, this can also be seen as a way of time-bin encoding. An interesting variation of this scheme uses photons traveling back and forth to improve the stability of the interferometer, as phase distortions are compensated, however at the cost of a reduced communication distance.

Several other encoding schemes exist, such as encoding in the relative phase between sidebands of a central optical frequency, the photon path, using correlations between time bins and photon energy, enabling high-dimensional encoding. Also, several ways exist to convert the different encoding types into each other. Ideally, all these encoding schemes require practical, high-performance single-photon sources (SPSs) or entangled photon pair sources (EPSs).
In the last step we have expanded the denominator for $\mu << 1$ up to first order and the enumerator up to second order, while keeping only terms up to $\mathcal{O}(\mu^2)$. This shows that the probability that a non-empty pulse contains more than a single photon can be made arbitrarily small, however at the cost of an extremely low number of photons in the quantum channel as for small $\mu$ we also have $P(n = 0, \mu) \approx 1 - \mu$. QKD experiments with WCPs typically use $\mu = 0.1$, a mean photon number at which about 5% of the non-empty pulses still contain more than a single photon. This opens security loopholes in the protocol, for example, for photon number splitting attacks (Figure 1d) or more realistic beam splitting attacks. Here, an adversary replaces the quantum channel with one of lower loss. Measuring only the photon number without significantly disturbing other degrees of freedom of the quantum state, by blocking pulses containing one photon and eavesdropping $n-1$ photons from pulses containing $n$ photons. In this way, the eavesdropper possesses a copy of all photons that Bob receives and can measure them according to the basis information disclosed via the public channel. For an ideal SPS, the photon number splitting attack is not applicable, as the source never emits more than a single photon per pulse. Figure 3 compares the photon number distribution of WCPs (Poissonian) and SPSs for different mean photon numbers. While for a typical average number of 0.1 photons per pulse both sources have a similar number of single-photon events, the attenuated laser still has a considerable amount of multi-photon contributions. One might argue that a solution is to strongly reduce the mean photon number in WCP setups and, in turn, increase the repetition rate. In this case, however, the photon detectors receive many
empty pulses significantly increasing the influence of detector noise.

Using so-called decoy state protocols,[54] the photon number splitting attack can be mitigated for WCP-based implementations. Instead of sending pulses of equal intensity, the pulse intensities are randomly modulated using fast intensity modulators (Figure 2c). In addition to sending the signal pulses, decoy pulses with different intensities are allowed for the detection of the photon number splitting attacks, by comparing the decoy state distributions at the transmitter and the receiver, respectively. An adversary, that attempts to eavesdrop lacks knowledge about which pulse intensity is sent at which time. Thus, the attacker unambiguously disturbs the intensity distribution, which can be detected statistically once Alice announces the pulses used for the decoy states during the sifting step. Furthermore, vacuum pulses are sent on purpose to quantify the dark count contributions. While the original proposal ideally required an infinite number of decoy state intensities,[55,56] it became clear that a few decoy state intensity levels are sufficient,[57] while recent results even shown that a single decoy state can be enough.[58] Employing decoy protocols, however, typically the achievable secret key rate is reduced due to the additional protocol overhead (i.e. usage of dim decay pulses). Provided a single-photon source (in contrast to attenuated laser pulses) with high efficiency, that is, with an average number of photons per pulse $\mu_{SPS}$ Comparable to average intensities typically used for signal states in decoy protocols (e.g., $\mu_{WCP} = 0.4$), the reduced protocol overhead gives a clear benefit for the SPS. For an overview of the state-of-the-art in attenuated laser QKD covering decoy and other types of protocols, we refer the reader to ref. [58].

More generally, for WCPs obeying Poisson statistics, the maximum probability for observing a single photon in a given pulse is limited to 37%, which means that a QD-SPS with an average photon number in the quantum channel exceeding this number will outperform the WCP source using the same system parameters except the source statistics (e.g., repetition rate, system losses). In the case of EPSs, these arguments in addition to others lead to even higher potential advantages, as will be discussed further below. Sending laser pulses to nonlinear crystals, spontaneous parametric down-conversion (SPDC) can be used to generate entangled photon pairs.[59,60] This process, however, is not only inefficient (conversion rates of $10^{-6}$ are typical) but also does not provide entangled photon pairs with single-photon statistics. The number of photon pairs follows a thermal distribution on a timescale below the coherence time and a Poisson distribution at longer times.[61,62] As a consequence, the maximum number of photon pairs generated via an SPDC source is limited, since the fidelity to the maximally entangled states reduces with increasing multi-pair contributions. As a consequence, the higher probability to emit more than one entangled photon pair in the down-conversion process ultimately limits the key rate, independent of the clock rate, as recently shown by Hosak et al.[63] QD-SPSs on the other hand can provide entangled photon pairs with single-photon pair statistics via the biexciton-exciton emission cascade (see Section 2.1) which have already exceeded the fundamental limits of SPDC sources.[64–66]

Even more important, when considering realistic finite key lengths, the number of secure bits reduces significantly due to finite-size corrections, which arise from statistical errors due to the reduced size of the parameter estimation set. These corrections, which are necessary for secure communication using finite-sized keys, are expected to have larger impact in implementations using attenuated laser pulses compared to SPS-based systems[67,68] making SPSs advantageous even at lower average photon numbers. Such finite-size effects are especially important in scenarios where the key length is strongly limited, for example in satellite links or mobile systems.[69,70]

Moreover, in many advanced protocols (e.g., measurement-device-independent (MDI) and fully device-independent (DI) QKD, see Section 3.3) or essential building blocks of quantum networks (e.g., quantum repeaters, see Section 4.2), successful Bell state measurements are essential. These, however, suffer strongly from multi-photon input states, which occur more often in WCP systems due to the Poisson statistics. These measurements also require high two-photon interference visibility, which can in principle reach up to 100% for quantum light sources, while it is fundamentally limited to 50% for WCPs.[71] Thus, also in this case, SPSs provide a clear advantage.

Another aspect is that even state-of-the-art single-photon detectors limit the achievable detection rates to below 100 MHz.[72] The repetition rates of modern QKD systems however have already reached the GHz regime, hence many QKD system clock rates are already limited by the photon detector.[73,74] In such a case and following the arguments presented above, using SPSs with relatively low brightness can already increase the secret key rate. Semiconductor QDs are a promising candidate for such a SPS and are therefore at the core of this review.

Before focusing on the experimental advances in the field, we concisely discuss major advances in the theoretical framework since the proposal of the BB84 protocol in the following (see ref. [75] for a recent review article). First rigorous security proofs were soon extended to more realistic scenarios, also considering the imperfections of Alice and Bob, unavoidable in physical implementations. A common way of calculating asymptotic secure key rates for imperfect photon sources was introduced in the so-called GLLP paper by D. Gottesman, H.-K. Lo, N. Litkenhaus, and J. Preskill.[76] Typically, secure key rates are calculated in the asymptotic regime, that is, assuming that an infinite amount of exchanged qubits is available so that protocol parameters can be estimated without errors from an infinite set. In that case, the secure key rate $K_{sec}$ is simply the clock rate of the QKD experiment $R_0$ multiplied by the mean photon number coupled into the quantum channel $\mu$, the channel transmissivity $t$, the detection setup transmission $\eta_{det}$, the detector efficiency $\eta_{\text{det}}$, the sifting factor $q$, and the secure bit fraction $r$ as

$$K_{sec} = R_0 \cdot \mu \cdot q \cdot t \cdot \eta_{\text{det}} \cdot r \cdot \eta_{\text{bob}} \cdot (1 - e^{-\frac{1}{e} e})$$

The secure bit fraction $r$, following the GLLP security proof, is the amount of uncertainty an adversary has over the key, reduced by the information leakage due to the error correcting code with an efficiency of $I_{\text{sec}}$. The uncertainty of the adversary and also the information leakage due to error correction is quantified by the binary Shannon entropy $H_2(e) = -e \log_2(e) - (1 - e) \log_2(1 - e)$ as a function of the QBER $e$. Finally, the secure bit fraction is corrected for multi-photon emission events $A$ that may enable
photon number splitting attacks. This leads to a secure bit fraction of

\[ r = A \left[ 1 - h_r \left( \frac{e}{A} \right) \right] - f_{dc} \cdot h_e(e) \] (4)

Here, A is the correction factor used to incorporate multi-photon emission events as \( A = P_f / P_{\text{click}} \), which describes the ratio of detector clicks resulting from single-photon events with probability \( P_f \) to all detector clicks \( P_{\text{click}} \). The QBER \( e \) is the number of erroneous detection events normalized by the sum of all detection events within a given basis. It can be estimated from an intrinsic system error \( e_{\text{det}} \), i.e. the probability that a photon encoded as one state is erroneously detected as the orthogonal state within the same basis (assumed to be similar for both bases here), and the number of dark counts \( P_{dc} \) as\(^{[77]}\)

\[ e = e_{\text{false clicks}} + e_{\text{dark counts}} = \frac{P_{\text{click}} \cdot e_{\text{det}} + \frac{1}{2} \cdot P_{dc}}{P_{\text{click}} + P_{dc}} \] (5)

Note, that errors resulting in detection events in the wrong basis are filtered out in the shifting event, and therefore do not contribute to the QBER. Contributions to the sifted key due to detector noise result in a bit error in 50% of the cases, as there are two possible states per basis. Refined channel models also take further detector imperfections into account (e.g., the detector’s dead-time or the after-pulsing probability) and allow for channel multiplexing.\(^{[78]}\) The GLLP rate equations (3-5) discussed above will be used at the end of Section 3.2 to put the QKD experiments reported to date into perspective. An important development in the field of QKD rate calculations over the last decade was to consider even more realistic settings beyond the asymptotic limit, in which only a finite number of qubits can be exchanged. This becomes crucial in practical scenarios using free-space optical communication links to, and between, moving platforms such as aircrafts or satellites. Several adaptations have to be made to the estimate of the secure key rate, which are due to intrinsic system errors, as shown by Chiavonga et al.\(^{[77]}\) Importantly, incorporating finite-size effects is not just a theoretical consideration to certify the security of the scheme more precisely. On the contrary, not incorporating these effects entails actual security risks, as shown by Sciarrini et al.\(^{[72,78,79]}.\) Noteworthy, secure key rates can also be calculated numerically, by maximizing Eve’s information over all attacks that are allowed by the laws of physics,\(^{[82]}\) which reproduces the results obtained analytically.\(^{[83,84]}\)

2. Quantum Dot Based Quantum Light Sources

Even though the notion of “single photons” has been around for 100 years,\(^{[85,86]}\) the concepts and practical realizations of light sources emitting single photons by one object took their fair time to be developed. While an atomic system is a good approximation of a driven two-level system, enabling single-photon generation,\(^{[87,88]}\) this route is not always practical for applications. This motivated researchers to consider low-dimensional solid-state systems, which mimic atoms but provide advantages for device integration. Important first steps toward solid-state-based SPSs have been achieved in the 1990s when research groups succeeded in embedding small islands of semiconductor material in another semiconductor with a larger bandgap. This created a potential well effectively forming a quasi zero-dimensional structure—the QD.\(^{[89,90]}\) After their discovery, QDs quickly gained interest, with applications ranging from laser physics\(^{[91]}\) to quantum information.\(^{[92]}\) Many excellent review articles and books on epitaxial semiconductor QDs and QD-based quantum light sources have been published over the years, for example, refs. [93, 94, 95, 96, 97, 98]. This section, therefore, intends to briefly summarize the most important properties of QDs and engineered QD-based quantum light sources used for implementations of quantum communication to date.

2.1. Semiconductor Quantum Dots

In QDs (see Figure 4a–d) the three-dimensional confinement of charge carriers in a small volume of typically a few nanometers\(^{[99]}\) leads to quantized energy levels in the valence and conduction band, resulting in discrete atom-like transitions. The lowest energy levels are referred to as s-shell (in analogy to atoms) and can be approximated as a two-level system (cf. Figure 4a). Adding an electron-hole pair, or exciton, to the QD potential using optical or electrical excitation, the energy levels can be occupied. After a characteristic time, that is, the spontaneous emission lifetime (typically \( \approx 1 \) ns), the exciton recombines radiatively under emission of a single photon, leaving the empty QD in its ground state. As long as the exciton has not recombined, the electronic state is occupied, thus providing the basic mechanism required for a SPS emitting photons one by one, as first demonstrated by Michler et al. in 2000.\(^{[100]}\)

For the epitaxial growth of QDs, different methods can be employed. Most of them exploit self-organized processes, like in the Stranski-Krastanov growth-mode\(^{[101–103]}\) (cf. Figure 4b,c), during heteroepitaxy of one material onto another.\(^{[104]}\) By controlling the thickness of the deposited QD material, different QD densities can be achieved. A fundamentally different approach uses etched nanoholes in an AlGaAs layer, which are subsequently filled with the GaAs QD material before final capping\(^{[105,106]}\) (cf. Figure 4d). This droplet-etching technique allows for a high degree of control over the properties of the QD ensemble.\(^{[107]}\)

Due to the semiconductor environment, QDs can host multiple charge carriers in different combinations of excited states, resulting in various distinct emission lines (Figure 4e,f). The most common states are the neutral exciton (X), the charged excitons (X±), and the biexciton (XX). Spectrally selecting one of the corresponding QD emission lines results in single-photon emission which can be experimentally verified via second-order photon auto-correlation experiments, analogous to the Hanbury-Brown-Twiss (HBT) experiment.\(^{[108]}\) The highest single-photon purity achieved for QDs to date was reported by Schweickert et al.\(^{[109]}\) with \( g^{(2)}(0) = (7.5 \pm 1.6) \times 10^{-5} \) (cf. Figure 4g).

Semiconductor QDs can be used for the generation of single photons featuring excellent quantum-optical properties (high purity and high indistinguishability), which were demonstrated to be superior to any other known type of SPS. Additionally, they offer the possibility to realize engineered devices with designed emission wavelength (see also Section 2.2). This is highly
beneficial for applications in quantum information, as the generated quantum light states can be spectrally matched to the telecom O- and C-band at wavelengths centered around 1300 nm and 1550 nm, suitable for long-distance communication in optical fibers, or atomic transitions in Alkali vapor cells for quantum memory applications (see Section 4.3).

As the growth of high-quality QDs emitting at telecom wavelengths remains technologically challenging, despite recent progress, they are less widespread compared to their shorter wavelength counterparts. Fabrication methods for telecom-compatible QDs include the bimodal-growth technique, strain-relaxing layers, the growth on metamorphic buffers or using InP based QDs. An alternative approach is the conversion of single photons emitted from a QD at lower wavelengths to the telecom range exploiting nonlinear optical effects. The state-of-the-art in the field of quantum frequency conversion enables conversion efficiencies of 35%. Importantly, again thanks to the semiconductor environment, different schemes are available for the optical excitation of excitonic states in QDs. The most basic method is non-resonant excitation using photons with an energy exceeding the bandgap of the matrix material, which results in the excitation of free electron-hole pairs. From this reservoir, single charge carriers can, relax to the QD states and subsequently recombine radiatively emitting single photons. While non-resonant excitation is technically the most simple excitation scheme, it imposes limitations to the quantum optical properties of the emitted photons—mostly due to phonon-induced dephasing, fluctuating charge traps, and relaxation-induced timing jitter. Alternatively, in quasi-resonant excitation, also referred to as resonant p-shell excitation, the closest energy level above the emission state is resonantly excited, which reduces the excitation of excess charge carriers and non-radiative relaxation induced dephasing.
To further improve the quantum optical properties of single photons from QDs, strict resonant excitation of the exciton state can be applied with the excitation laser matching the QD emission wavelength.\cite{124} This scheme, however, requires a suppression of the scattered laser light of typically six orders of magnitude, using, for example, cross-polarized excitation and collection paths,\cite{125} side-excitation of the sample,\cite{126} also via coupling to photonic waveguides,\cite{127} or bichromatic excitation pulses.\cite{128} Note that, compared to some of the other coherent excitation schemes discussed further below, such resonant excitation schemes are still not ideal in terms of photon purity due to possible re-excitation processes.\cite{131}

The physics of QDs, however, are by far not limited to single-photon emission. When exciting two (or more) excitons, cascaded emissions are possible, where the individual photons have slightly different energies due to the Coulomb interaction of the confined excitons and can thus be separated.\cite{129–134} Due to the two possible decay paths that are correlated in polarization (Figure 5a), photon pairs emitted via the XX-X radiative emission cascade are polarization-entangled and form $|\Psi^\pm\rangle$ Bell states. This was predicted theoretically in ref. [135], followed by numerous experimental demonstrations, for example, refs. [65, 136, 137, 138] (Figure 5d–g). To generate entanglement on-demand via the XX-X cascade, as it is most beneficial for practical applications, the so-called fine-structure-splitting (FSS) must ideally vanish. The FSS quantifies the amount of energy splitting of the X state due to intrinsic anisotropies in the QD, (Figure 5b). For non-zero FSS the different decay paths are non-degenerate and the interference of their respective probability amplitudes leads to a precession between the two different maximally entangled Bell states $|\Psi^\pm\rangle$ and $|\Psi^\mp\rangle$.\cite{138,139} This can be observed when the fidelity to a specific maximally entangled state is measured, which then oscillates as a function of the temporal detuning between the detection of the X and XX photons.\cite{112} To enhance the measured fidelity to one of the Bell states, temporal filtering can be employed, to select only the photons corresponding to that Bell state.\cite{140} The measured fidelity is then referred to as peak fidelity. While the two-photon state emitted by the XX-X radiative cascade is typically limited to the $|\Psi^\pm\rangle$ Bell states, schemes for the generation of arbitrary entangled states were recently proposed.\cite{141,142} Importantly, several in-situ or post-growth techniques can be used to tune the FSS to zero, with piezo-induced strain tuning being one of the most powerful approaches to date.\cite{143} The possibility to generate polarization entanglement—being one crucial ingredient for many schemes of quantum communication—is a major advantage of using engineered QD devices. We refer the interested reader to ref. [144] for a recent perspectives article on this topic. Noteworthy, also other configurations of the energy level scheme can be realized so that the emission cascade enables the generation of polarization-entanglement via time-reordering\cite{145} or so-called twin photon states.\cite{146,147}

Making use of the XX-X emission cascade, QDs can also be excited coherently without the need for complex methods to suppress the reflected laser light as it is the case for the resonant excitation scheme mentioned above. In so-called two-photon-excitation schemes, the QD is excited by two photons, each with...
an energy between the X and XX state energy levels, such that two photons together can excite the XX state. As the excitation photons differ in energy from the photons emitted by the X and XX state, this two-photon excitation allows for less stringent requirements for the spectral filter.\textsuperscript{[148–150]} Since the emission happens via the XX-X cascade, two-photon excitation is especially useful for entanglement generation. While such a two-photon excitation results in a reduced re-excitation probability and hence higher single-photon purity compared to the resonant excitation scheme mentioned above,\textsuperscript{[109,151]} the indistinguishability of the excited photons is intrinsically limited due to temporal correlations,\textsuperscript{[152]} as discussed in more detail in Section 4.2. However, two-photon excitation was recently combined with a trigger pulse to stimulate emission of highly polarized, indistinguishable photons.\textsuperscript{[153,154]}

While the coherent control of QD excitons in the form of Rabi oscillations was first observed in pump-probe experiments,\textsuperscript{[155,156]} a variety of coherent excitation schemes is nowadays available. Examples range from adiabatic rapid passage,\textsuperscript{[157–159]} over bichromatic excitation,\textsuperscript{[128,160]} to recent theory proposals for swing-up schemes using frequency-modulated or spectrally far detuned laser pulses.\textsuperscript{[161]} As QDs are embedded in the semiconductor host matrix, the quantized lattice vibrations, that is, phonons, play a crucial role in the preparation process, often adding decoherence to the coherent excitation schemes discussed above.\textsuperscript{[162–165]} Therefore, regimes should be sought, where the phonon impact is minimal.\textsuperscript{[166,167]} On the other hand, phonon-assisted schemes for the single- \textsuperscript{[168]} or two-photon\textsuperscript{[169,170]} excitation can be exploited to coherently populate excitonic states via thermalization with the photon bath, showing prospects for improved single-photon purities\textsuperscript{[171]} and the efficient while robust generation of linearly polarized photons.\textsuperscript{[172]}

Note, that the efficient trapping of excitons in most QD systems requires cryogenic temperatures in the range of 4 to 70 K. Some material systems (e.g., CdSe and Nitride materials), however, feature higher exciton binding energies resulting in operating temperatures up to room temperature.\textsuperscript{[173–177]} In addition, also cryotechnologies advanced significantly in recent years, nowadays enabling compact and benchtop cryogenic quantum light sources as demonstrated first by Schlehahn et al.\textsuperscript{[178]} (see Section 4.1).

Another important development in the field of QD-device engineering refers to the availability of several deterministic fabrication technologies, where the QDs are either grown directly at a pre-determined location (site-controlled growth) or QDs are pre-selected post-growth (according to the optical properties) and subsequently integrated into photonic devices (see refs. [98, 179] for recent review articles). These deterministic technologies turned out to become a game-changer enabling high device yields for applications in photonic quantum technologies.

How QDs compare to other SPSs, such as defects, carbon nanotubes, or atomic-vacancy centers in crystals, was reviewed by Aharonovich et al.,\textsuperscript{[46]} with the result that QDs show the best overall performance in terms of a short radiative lifetime as well as high single-photon purity and indistinguishability. Noteworthy, several novel materials, including monolayers of transition metal dichalcogenides\textsuperscript{[180]} and defects in GaN crystals\textsuperscript{[181]} attracted increasing interest in the field of quantum light generation, but are not yet competitive with QD sources in terms of brightness and photon indistinguishability. Overall, QD-based sources are the closest there is to ideal quantum light sources today.

2.2. Engineered Quantum Light Sources for Quantum Communication

As mentioned in the previous section, QDs provide all assets to achieve fast emission of single, indistinguishable, and entangled photons at high rates. To further boost their performance in terms of the photon extraction efficiency and emission rate, QDs can be integrated into photonic structures.\textsuperscript{[182]} This section will provide an overview of engineered QD-based SPSs previously employed in the QKD experiments to be discussed in Section 3.

Micropillar (or micropost) cavities have been widely used to enhance the emission of optically excited QD-based SPSs.\textsuperscript{[183,184]} Meanwhile, they have also been employed in QKD experiments.\textsuperscript{[185,186]} A scanning electron microscope (SEM) image of micropillar cavities is shown in Figure 6a. The etched pillars consist of a QD layer sandwiched between two distributed Bragg reflector (DBR) mirror sections. The top DBR mirror is usually designed to have lower reflectivity than the bottom DBR mirror, to promote emission into the upper hemisphere toward collecting optics. Purcell enhancements of factor 5-6 of the emission rate and extraction efficiencies above 60% can be typically achieved with micropillar structures.\textsuperscript{[187–190]}

Micropillar structures were also used to realize electrically triggered QD-based SPSs emitting in the near-infrared (900 nm)\textsuperscript{[191]} (Figure 6b,c) or visible (650 nm)\textsuperscript{[192]} (Figure 6d) spectral range. These highly engineered devices have in turn been employed for the first QKD experiments with electrically injected QD-devices.\textsuperscript{[195]} In both device approaches a layer of self-organized QDs is embedded in an undoped (intrinsinc) section of a micropillar structure sandwiched between a top p-doped and a bottom n-doped DBR mirror forming a p-i-n diode structure electrically contacted via gates.\textsuperscript{[196]} The operation wavelength can thereby be determined by the choice of the QD-material, being InAs/GaAs and InP/GaAs for the devices emitting in the near-infrared and visible spectral range respectively, highlighting the flexibility QDs offer for applications in quantum technologies. Electrically driven micropillar-based SPSs were reported to reach overall efficiencies (including electrical losses) exceeding 60%\textsuperscript{[197]} and Purcell enhancement of close to 5\textsuperscript{[191]} values comparable to their optically excited counterparts, but with the advantage of a straightforward implementation of GHz excitation pulse repetition rates.\textsuperscript{[197,198]}

In another approach, QDs were embedded in diode structures to electrically generate polarization-entangled photon pairs via the XX-X radiative cascade (see Section 2.1).\textsuperscript{[193,199]} This so-called entangled light-emitting diode (ELED) has later been employed for the first entanglement-based QKD experiments using QD-devices.\textsuperscript{[200]} The fabrication scheme to realize InP-based ELEDs for entangled photon emission in the telecom C-Band is shown in Figure 6e.

A different type of photonic structure that was used for QKD experiments in the telecom C-Band\textsuperscript{[201]} is a so-called optical horn (Figure 6f). It consists of a QD embedded in a fabricated nano-cone on a substrate. The horn acts as a reflector, directing photons upwards through the anti-reflection coated substrate.
and towards the collection optics. The horn structure did not show Purcell enhancement, but photon collection efficiencies of close to 11% were achieved.\(^\text{[194]}\)

The last type of QD-device that shall be mentioned here was used for a recent implementation of entanglement-based QKD experiments\(^\text{[202,203]}\) and utilized optically pumped symmetric GaAs QDs grown by the droplet-etching method (Figure 4d). Featuring short radiative lifetimes and small FSSs, these QDs enable large entanglement fidelities,\(^\text{[107]}\) while reaching out-coupling efficiencies of about 8% if combined with a solid immersion lens.

Other types of photonic structures used to enhance the performance of QD-based quantum light sources include nanowires,\(^\text{[204]}\) photonic crystal cavities,\(^\text{[205,206]}\) circular Bragg gratings,\(^\text{[207,65,66]}\) open cavity systems,\(^\text{[208]}\) on-chip waveguide based structures,\(^\text{[209]}\) and monolithic microlenses.\(^\text{[210]}\) The latter proved to be useful for the development of practical plug&play SPSSs\(^\text{[178,211]}\) as well as tools for the performance optimization of single-photon QKD,\(^\text{[212]}\) both evaluated very recently in a QKD-testbed operating at O-band wavelengths\(^\text{[213]}\) (see Section 4 for details).

3. Implementations of Quantum Key Distribution Using Quantum Dot Devices

In the previous section, we introduced QD-based quantum light sources as promising candidates for applications in quantum information. In this section, we review the implementations of QKD based on respective QD-devices reported to date. Noteworthy, also other types of quantum emitters have been used successfully for QKD experiments with sub-Poissonian light states. Among the two very first demonstrations of the BB84 protocol with single photons in 2002, Beveratos et al. used Nitrogen vacancy (NV) centers in diamond as quantum emitter\(^\text{[214]}\)—work to be complemented by a free-space experiment of the same group 2 years later.\(^\text{[215]}\) Meanwhile also Silicon vacancy (SiV) centers were used to implement QKD protocols.\(^\text{[216]}\) Compared to QDs, the longer radiative lifetimes typically observed for atomic vacancies in diamond limit the clock rates and secure key rates achievable for QKD. In the following we restrict ourselves to QD-based implementations of QKD. As discussed in Section 1, QDs can either be used in a prepare-and-measure type setting (cf. BB84 protocol) or an entanglement-based setting (cf. E91 protocol) for QKD. We will start with discussing first BB84-type of implementations in the following.

### 3.1. Quantum Key Distribution Using Single Photons

The very first implementation of single-photon QKD reported by Waks et al. dates back to 2002.\(^\text{[185]}\) The authors implemented the BB84 protocol with the bits being polarization-encoded in single-photon states from a triggered QD source.\(^\text{[187]}\) Here, InAs QDs were encapsulated in micro-pillar cavities made from distributed Bragg reflectors (cf. Figure 6a). In their setup (Figure 7a), the QD
sample was mounted to the coldfinger of a liquid-Helium flow cryostat, optically excited using a pulsed Titan:Sapphire laser and spectrally filtered via a grating spectrometer. The single-photon pulses were modulated in their polarization using an electro-optical modulator (EOM) placed after a polarizing beam splitter (PBS). The non-resonant optical excitation at a rate of 76 MHz resulted in a mean photon number of $\mu = 0.007$ injected into the quantum channel, as deduced from a measurement using a single-photon detector on Alice’s side. Using a short free-space link containing a variable attenuator, the photons were sent to Bob for polarization-state discrimination. Here, a polarization decoder was implemented with passive random basis choice using a 50:50 beam splitter (BS) in combination with two PBSs and a quarter-waveplate. The detection events and the photon statistics were analyzed using a time interval analyzer (TIA). The experimental data acquired with this setup, namely the bit rates and QBER under variation of the link attenuation, were used to calculate the asymptotic key rate according to ref. [217]—in good agreement with the simulated rate-loss dependence (cf. Figure 7b). In their work, the authors introduced an upper bound on the probability of multi-photon events used by the SPS in the future could further increase the advantage sub-Poissonian SPSs can have over attenuated laser pulses in implementations of QKD.

Additionally, the authors performed a comparative study with attenuated laser pulses, however, without applying decoy states at that time. The comparison revealed, that the QD SPS was able to outperform the attenuated laser at link losses exceeding 16 dB, as the compensation for potential photon number splitting attacks used up more bits for the attenuated laser pulses. [27] Overall, the SPS could tolerate about 4 dB higher losses than the laser in this experiment. Using the secret key from their experiment, Waks et al. encoded and decoded an image of Stanford University Memorial’s Church (Figure 7c). It should be noted, that nowadays decoy-state protocols allow for the in-situ estimation of the multi-photon contribution to mitigate photon number splitting attacks and hence much higher average photon numbers in the laser pulses, [34] which is why the asymptotic rate of Waks et al. would not beat a decoy-state implementation using WCPs. On the other hand, according to recent discussions in the literature, [213] the upper bound on the probability of multi-photon events used by Waks et al. is not tight, but a rather pessimistic estimate. Therefore, finding tighter bounds to $P_{\text{in,SPS}}$ in the future could further increase the achievable key rate. Using a Michelson-interferometer on Alice side, a relative temporal delay was introduced between both photons (time-multiplexing), enabling the polarization modulation of each photon individually, before coupling both to the same free-space quantum channel. On Bob’s side, a second Michelson interferometer was used to demultiplex both photons for independently measuring their polarization state. Note that the multiplexing and demultiplexing were performed in the time domain, rather than the spectral domain, to make the implementation robust against spectral fluctuations of the QD. Using this approach, Aichele et al. demonstrated a rate of secure bits per pulse of $5 \cdot 10^{-4}$, which results in a communication rate of 38 kbit/s at the given laser repetition rate (76 MHz).

While these first implementations used short laboratory-scale free-space optical (FSO) links as quantum channels, being a good choice to cover large distances in air-to-ground [69] or space-to-ground [220-222] link scenarios, the use of optical fibers has many practical advantages for ground-based communication scenarios. Firstly, it requires no direct line of sight being susceptible to environmental fluctuations, for example, weather conditions and atmospheric turbulence. Secondly, fiber-based technologies can be integrated into existing infrastructures of fiber-based communication networks, at least in principle. The deployed optical fibers are suitable for quantum light sources operating at wavelengths in the telecom O- or C-band, [222] enabling the coexistence of classical and quantum traffic via wavelength division multiplexing. [224-227] Several QD-based QKD experiments using optical fibers as quantum channels for single-photon pulses have been reported to date. The first experiment was conducted by Collins et al. using QD-generated single photon pulses.
Since the transmission losses in optical fibers are lowest at wavelengths in the second and third telecom window (O- and C-band), it was soon considered to use QDs operating at these wavelengths, as first fabricated by Ward et al. In 2009, Intallura et al. demonstrated single-photon QKD at 1300 nm using QDs integrated into micropillar cavity optically excited above the bandgap. The quantum channel was represented by a standard SMF-28 optical fiber of 35 km length. As mentioned in Section 1, it can be difficult to maintain polarization states over long transmission distances in optical fibers. For this reason, Intallura et al. used a phase encoding scheme, which made use of a multiplexed reference laser to match the path differences in Alice’s and Bob’s MZIs (Figure 8a). For the QKD demonstration, the entire system ran at a clock rate of 1 MHz, limited by the single-photon detectors’ response and dead time. Using the asymptotic GLLP rate equations 3-5 incorporating multi-photon events, a measured QBER of 5.9%, and an error correction efficiency of 1.17, the authors calculated a maximum secure key rate of about 160 bit/s and achieved a positive key rate at a distance of 35 km, overcoming the distance limit of a WCP-source (without decoy states) in their setup (Figure 8b).

Just 1 year later, Takemoto et al. reported the first implementation of single-photon QKD in the telecom C-band (1560 nm), benefiting from even lower losses in optical fibers. In their experimental setup designed for phase encoding (see Figure 9a), the SPS was represented by a QD incorporated into a horn-like structure (cf. Figure 6f and ref. [194]). The authors achieved a maximum secure communication distance of 50 km using the asymptotic GLLP rate equations, setting a new record for single-photon QKD at that time.

A few years later, the same group presented an improved version of their QKD implementation, using better detectors and QDs of higher quality. Close to the distance limit of a given QKD system, that is, strong channel losses, the detected signal photons are on the order of the events due to detector noise, ultimately limiting the achievable communication distance. Using single-photon detectors based on superconducting nanowires, the dark count contribution could be significantly reduced and hence the maximum achievable distance increased. Moreover, the authors also improved the single-photon purity of their QD source \( g^{(2)}(0) = 0.005 \) using pulse shaping techniques, which reduced the protocol overhead required for the correction of multi-photon emission events. Overall, these improvements resulted in a maximal communication distance of 120 km reported by Takemoto et al. in 2015—the longest transmission distance achieved in fiber-based single-photon QKD to date (cf. Figure 9b).

All QKD experiments discussed so far used pulsed laser systems to optically excite the QD devices. A major advantage of semiconductor-based quantum light sources, however, is the
possibility to realize complex engineered devices including diode structures for electrical charge carriers injection, enabling the electrical triggering of QD emission. This is highly beneficial for applications, not only because higher degrees of device integration become possible, as bulky laser systems become obsolete, but also the clock rate of quantum cryptographic implementations can easily be adjusted and pushed to their limits (see also Section 4.1). While the first electrically injected QD-based SPS was reported in 2002 by Yuan et al., it took one decade until the first QKD experiments were reported.

In the work by Heindel et al. in 2012, three research groups joined forces to demonstrate lab-scale BB84-QKD experiments using two different types of single-photon emitting diodes operating in the near-infrared (NIR) and visible (VIS) spectral range, at 897 nm and 653 nm, respectively (see Figure 10a–c). Employing engineered QD devices based on different material systems and growth techniques, their work highlighted the flexibility semiconductor-based quantum light sources offer for implementations of quantum communication. The NIR-SPS was based on an electrically contacted micropillar cavity exploiting the Purcell effect to enhance the photon extraction efficiency (cf. Figure 6b,c). In case of the VIS-SPS, QDs were integrated into a quasi-planar DBR cavity structure (cf. Figure 6d). Using the NIR-SPS, the authors achieved sifted key rates of 27.2 kbit/s (35.4 kbit/s) at a QBER of 3.9% (3.8%) and a $g^2(0)$ value of 0.35 (0.49) at moderate (high) excitation under pulsed current injection at a clock-rate of 182.6 MHz. The VIS-SPS was triggered at 200 MHz, delivering sifted keys at a rate of 95.0 kbit/s at a QBER of 4.1% and a $g^2(0)$ value of 0.49. While the achieved performance, in terms of single-photon purity and key rates, left room for future improvements, these first proof-of-principle QKD experiments using electrically operated semiconductor SPSs were considered as a major step forward in photonic quantum technologies. Shortly after the lab-scale QKD experiments reported in 2012, the authors integrated the NIR-emitting SPS in a, at that time, compact quantum transmitter setup to be employed for QKD field experiments in downtown Munich (see Figure 10d). As reported by Rau et al., the QKD experiments comprised a 500 m FSO link between two buildings of the Ludwigs-Maximilians-Universität Munich, with the transmitter and receiver units synchronized via GPS-disciplined oscillators. Using their single-photon light-emitting diode modulated at a clock-rate of 125 MHz, the authors achieved sifted key rates of 7.4 kbit/s (11.6 kbit/s) at a quantum bit error ratio of 7.2% (6.3%) and a $g^2(0)$ value of 0.39 (0.46) at low (moderate) excitation.

To become competitive with attenuated laser systems using decoy-state protocols both, the efficiency and the clock rate of electrically injected QD-SPSs have to be further improved. Promising steps in this direction were reported by Schleihahn et al. by achieving a photon extraction efficiency of up to 61% (into the first lens) using a GHz-clocked single-photon light-emitting diode. A promising route to further improve the mean photon number per pulse $\mu$ injected into the quantum channel, is to pursue a tighter integration of the SPSs, for example, via the direct coupling to optical fibers allowing for practical plug-and-play quantum light sources (see Section 4.1 for details). Along this route, Rickert et al. succeeded very recently to directly fiber-pigtailing electrically injected QD-microcavities to single-mode optical fibers and demonstrate low-temperature operation.

### 3.2. Quantum Key Distribution Using Entangled Photon Pairs

While the QKD implementations discussed in the previous section were performed in a prepare-and-measure configuration, this section will review QKD experiments using QD-based entangled photon pair sources. Here, the communicating parties, Alice and Bob, independently perform a measurement on one photon of an entangled two-photon state using randomly selected bases. They keep only results in which both used the same basis, thus obtaining perfectly correlated bitstrings. By quantifying the remaining degree of entanglement after the photon transmission, for example, by verifying the violation of the Bell-type CHSH inequality, eavesdropping attempts can be uncovered, as described by the E91 protocol (see Section 1). Entanglement monogamy thereby guarantees that if Alice’s and Bob’s photons are maximally entangled, their photons cannot be entangled with any other quantum system. Hence an adversary’s state is separable from the state of Alice and Bob, which is why the adversary cannot have any information. Based on the measured deviation from a maximally entangled state, the required amount of privacy amplification can be deduced.

As discussed in Section 2.1, QDs can also be used for the generation of triggered polarization-entangled photon pairs via the XX-X emission cascade. Since the photons obey single-photon statistics, higher generation rates of entangled photons are possible compared to SPDC sources. Thus QDs can be used for entanglement-based implementations of QKD, where the entangled photons can either be distributed via FSO or fiber-optical links.

The first proof-of-concept demonstration of QD-based entanglement QKD based on the BBM92 protocol was reported by Dzurnak et al. in 2015. The authors performed an in-lab experiment using entangled photons generated via an electrically triggered QD-device, referred to as an entangled-light emitting diode (ELED) as introduced first by Salter et al. Using the experimental setup depicted in Figure 11a, the entangled photon pairs were distributed via optical fibers connected to the receiver stations of Alice and Bob, analyzing the polarization state of the XX- and X-photon, respectively. For this purpose, the photons emitted by the biexciton- and exciton-state were first spatially separated using a spectral filter (Figure 11b), before coupling them to the individual fiber links connected to Alice and Bob. Polarization-entanglement of the photon pairs was verified by violating the CHSH inequality, yielding a $S$-parameter $> 2$ for vanishing time delays (cf. Figure 11c). Note, that an optimal trade-off between the entanglement fidelity and the sifted key fraction required a narrow temporal filter of 400 ps to be applied as post-process. In their experiment, the authors succeeded in transferring a sifted key of 2053 bits with a bit error rate of 9.8%, just below the threshold of 11% required for the security of the BBM92 protocol. After performing an error correction step, Alice and Bob shared a secret key of 949 bits. The sifted key rate achieved in the experiment was about 10 bits/min.

Recently, two other successful implementations of entanglement based-QKD were reported. Both experiments used
Figure 10. a) Demonstration of lab-scale single-photon QKD.\cite{195} Two different electrically triggered QD-SPSs were implemented: b) InAs QDs emitting at 900 nm and c) InP QDs emitting at 650 nm. Red arrows in the spectra indicate the width of the bandpass filter used. Inset display the corresponding auto-correlation measurements proving single-photon emission. d) In a follow-up experiment, the micropillar-cavity based single-photon emitting diode operating at 900 nm was employed for field experiments in downtown Munich using a 500 m free-space optical (FSO) link connecting two buildings of the Ludwig-Maximilians-University Munich.\cite{232} (a–c) Reproduced with permission.\cite{195} Copyright 2012, IOP Publishing.

the same type of optically excited QD-source, comprising a GaAs QD fabricated by the droplet-etching technique (cf. Figure 4d) embedded between a bottom DBR and a solid immersion lens on top. Importantly, and in contrast to all previous QD-based implementations of QKD, both groups used a two-photon resonant excitation scheme for entangled photon pair generation. This enabled a significant improvement in the single-photon purity and entanglement fidelity compared to the first-time demonstration discussed above.

Schimpf et al.\cite{203} distributed the entanglement of their QD-source using a 350 m optical fiber, resulting in an asymptotic secure key rate of 86 bits/s (Figure 12a). Basso Basset et al.\cite{202}
Figure 11. a) Experimental setup of the first demonstration of entanglement-based QKD using an electrically triggered QD-device. Using a spectral filter, polarization-entangled photon pairs emitted by the XX-X radiative cascade were spatially separated and distributed via optical fibers connected to Alice and Bob. c) Entanglement was verified by violating the CHSH inequality with an $S$-parameter $> 2$. Reproduced with permission.\cite{200} Copyright 2015, AIP Publishing.

Figure 12. Two entanglement-based QKD experiments: Schimpf et al. realized the BBM92 QKD protocol.\cite{203} Their setup a) allowed them to achieve secure key transmission with the rate shown in (c) and a QBER (d) far below the maximum allowed value for secure transmission. Basso Basset et al. used an asymmetric Ekert protocol\cite{202} to perform QKD between two buildings b) and the photons were transmitted both through an optical fiber (top panel in e) and a free-space (bottom panel in e) and the degree of entanglement (second column in e) and the key rate (third column in e) were compared. (a,c,d) Reproduced under the terms of the Creative Commons CC-BY license.\cite{203} Copyright 2021, The Authors, some rights reserved; exclusive licensee American Association for the Advancement of Science. (b,e) Reproduced with permission.\cite{202} Copyright 2021, The Authors, some rights reserved; exclusive licensee American Association for the Advancement of Science.

realized a fiber link (250 m) as well as a free-space link (270 m) with comparable transmission lengths, allowing for a direct comparison of both channel types operated with the same QD-source (Figure 12b). The authors observed better performance in terms of larger Bell parameters and fewer fluctuations for the entanglement distribution via the fiber-based link, as seen in Figure 12e. Also, the average raw key rate achieved was higher in the case of the fiber-link (486 bits/s) compared to the FSO-link (60 bits/s), due to the challenge of correcting instabilities and drifts in the FSO channel. Polarization-state distortions in the fiber-link were compensated by an active feedback loop.

Interestingly, slightly different protocols were implemented in the entanglement QKD experiments of both groups. Basso Basset et al. implemented an asymmetric version of the original...
E91 protocol. Using a subset of the transmitted bits, the violation of the CHSH inequality was evaluated to quantify the amount of entanglement left after the transmission of the photons. This in turn quantifies the amount of eavesdropping that could have occurred, which determines the amount of privacy amplification required for distillation of the secret key. For this purpose, the authors measured the photons on Alice’s side in the basis set known to maximally violate the CHSH inequality, while Bob measured in the conventional BB84 bases. This asymmetric approach reduces the number of detectors required compared to the original E91 protocol. Schimpf et al.,[201] on the other hand, implemented the BBM92 protocol,[22] being the entanglement-based analog of the BB84 protocol. Here, Alice and Bob measure their respective halves of the entangled state in two conjugate bases. The amount of privacy amplification required is determined solely from evaluating the deviations of a subset of results measured and compared by Alice and Bob (as in the BB84). Hence, the degree of entanglement in terms of the S-parameter is not actively monitored during the key generation in this case.

Noteworthy, entanglement-based QKD has so far not been implemented with QD-sources operating at telecom wavelengths. The generation of polarization-entangled photon pairs at 1550 nm was first reported by Olbrich et al.[224] using optically excited InAs-QDs grown on a metamorphic buffer. More recently, Shooter et al. demonstrated a GHz-clocked electrically triggered QD entanglement source operating in the telecom C-band based on InAs droplet QDs grown on InP substrate.[235] The generated entangled photon pairs, showing a peak fidelity to the maximally entangled state of 89% after temporal post-selection, were distributed at record-high rates over a fiber link of 4.6 km length, representing an important step toward high-performance QKD systems exploiting sub-Poissonian entanglement sources. The same type of QDs has been used to demonstrate entanglement generation up to 93 K[193]—a temperature enabling operation at liquid nitrogen or the integration into compact Stirling cryocoolers[236] (see also Section 4.1). Furthermore, Xiang et al. achieved a peak fidelity of 91% to the maximally entangled state using an electrically pumped QD-device, after the polarization-entangled photons propagated over an 18 km long deployed optical fiber.[140] Note, that in the case of a non-vanishing fine structure splitting the term “peak fidelity” is important. Here, the fidelity to a specific maximally entangled Bell state oscillates in time, due to the interference of the non-degenerate decay channels of the cascaded emission (see Section 2.1).[122,139] Hence, to maximize the fidelity to one Bell state, the authors employed a tight temporal filter of 48 ps width, accepting only 3% of the entire signal. Using active polarization stabilization, the authors were able to demonstrate entanglement distribution via the deployed optical fiber over 7 days of operation.

Another interesting experiment on fiber-based entanglement distribution used a 96 km long submarine optical fiber between Malta and Sicily employing an SPDC-source.[237] Although a probabilistic source was used here, the stability observed for the distribution of entangled photons pairs over such long distances in a real-world scenario is impressive and highlights the prospects entanglement-based QKD offers for applications in existing fiber networks. For the sake of completeness, it should be mentioned that the longest distance covered by entanglement distribution to date was achieved in a space-to-ground link between the quantum satellite ‘Micius’ and a ground station on earth.[238] Here, photons generated via an SPDC source propagated over a distance of up to 1200 km with an entanglement fidelity of 86%. Using the same satellite, also entanglement-based QKD in a satellite-to-ground[239] as well as ground-satellite-ground[221] configuration was demonstrated. Satellite-based experiments employing deterministic sub-Poisson quantum light sources have yet to be explored.

Table 1 summarizes the status quo in the field of QD-based QKD experiments, listing all implementations reported to date. A few points should be considered if comparing the different implementations. While some experiments were proofs-of-concept with a fixed communication distance and/or lab-based experiments, others were performed at varying distances or attenuation to simulate different channel losses. In these cases, we give a range of parameters. Moreover, some references quote an average value for the QBER in their system, while this value, in general, depends on the channel loss. Furthermore, some of the quoted parameters rely either on assumptions made in the key rate calculations (e.g., which imperfections to include and which attacks to consider), while others depend highly on the equipment used (such as the number of detector dark counts), making a direct comparison difficult. Key rates we calculated using the asymptotic GLLP equation (cf. equation 3, Section 1) based on the parameters given in the respective publication are indicated by footnotes.

To put the QKD implementations reviewed above into perspective, we address the question of which performance, in terms of secure key rates and communication distances, is within reach using QD-based SPSS in fiber-based implementations of BB84-QKD. For this purpose, we use equations (3-5) to extrapolate the achievable asymptotic key rate from parameters reported in the literature as described in the following and assuming an operation wavelength of 1550 nm. Note that, while the values stated in the following were not yet demonstrated at C-band wavelengths, the advances in the development of QD-based telecom-wavelength quantum light sources show prospects that this can be achieved in the future.

For the probability of multi-photon events we use the upperbound of $P_{\mu,SPS} \leq \frac{1}{2} \mu \cdot n_{B}(0)$ introduced by Waks et al.[227] Assuming a mean photon number of $\mu = 0.3$ and an antibunching value of $g^{(2)}(0) = 7.5 \cdot 10^{-5}$[199] an upper bound for the achievable multi-photon contribution can be calculated. Note that even larger values of $\mu$ were already demonstrated.[172,208] In this regime, however, the increase of multi-photon contributions might effectively reduce the key rate at large loss on Bob’s side. We further assume a setup transmission of $\eta_{\text{det}} = 0.3$,[240] alignment errors of $\delta_{\text{align}} = 1\%$,[271] and superconducting nanowire detectors with an detection efficiency of $\eta_{\text{det}} = 0.9$[72] and a few dark counts per second, that is, $P_{\text{dc}} = 10^{-6}$ dark counts per pulse at a clock rate of $R_{\text{c}} = 100 \text{MHz}$. Using state-of-the-art optical fibers, losses in the quantum channel of $\alpha = 0.17 \text{dB/km}$ are possible at 1550 nm.[37] We further assume a value of $f_{\text{EC}} = 1.1$ for the efficiency of the error correction protocol[241] (with $f_{\text{EC}} = 1$ being the ideal Shannon limit) and $q = 0.5$ for the sifting factor of the symmetric BB84 protocol.

Using these parameters, we deduce an asymptotic secure key rate exceeding 3 Mbits s$^{-1}$ at a short distance, a key rate
exceeding 1 kbit s⁻¹ after a distance of 200 km in optical fiber, and a maximum achievable communication distance beyond 250 km. These realistic extrapolations, for which none of the parameters was pushed to its physical limits, highlight the prospects for substantial advances in the field of sub-Poissonian QKD also for schemes of quantum communication beyond direct point-to-point links. Importantly, this performance can be improved much further, for example, by using higher clock rates, asymmetric bases choices allowing for larger sifting rates, or temporal filtering as will be detailed in Section 4.6. One should keep in mind, however, that such high asymptotic key rates can only be achieved when sufficiently large block sizes of qubits are transmitted (about 10¹⁵). Otherwise finite-size effects drastically reduce the secure key rate.

3.3. Advanced QKD protocols—Toward Device Independence

In recent years numerous novel, advanced types of protocols have been proposed with a special emphasis on device independence. The quantum cryptographic protocols discussed so far, for example, the BB84 or the E91 protocol, are provably secure in an information theoretical sense. In experimental implementations, however, imperfect devices can open loopholes making side-channel attacks possible which compromises the protocol’s security. Prominent examples are faked-states attacks, blinding-attacks, or attacks using spatial side-mode channels (see ref. 58 for a review covering also quantum hacking strategies). Device-independent (DI), or partially DI, QKD protocols are designed such, that imperfections of all, or some, of the devices used for the implementation, do not compromise the security of the protocol—a major advantage for practical applications. While fully DI-QKD is extremely challenging to realize (see further below), partially device-independent protocols have been invented, which are already very useful. Knowing for instance, that many quantum hacking attacks target the receiver side, it is already a huge advantage if those attacks could be excluded. This becomes possible in measurement-device-independent (MDI) QKD protocols.

Here the protocol security can be guaranteed independent of the measurement device, that is, the detection setup, which could in principle be even controlled by an adversary. MDI-QKD can be thought of as a time-reversed version of the E91 protocol. It requires that Alice and Bob each send single and indistinguishable photons to a central receiver station (Charly), where both photons are projected into an entangled two-photon state via a Bell measurement. By learning the outcome of the Bell measurement and by communicating the preparation bases, Alice and Bob can establish a secret key. Knowing only the outcome of the Bell state measurement does not disclose any information about the key, which is why the detector does not need to be trusted.

MDI-QKD has so far only been implemented using attenuated laser pulses or in proof-of-concept experiments using stored and released photons from down-conversion sources. However, substantial quantum advantages can be expected, when employing deterministic SPSs for MDI-QKD. The crucial prerequisite for implementations of MDI-QKD is the two-photon interference at a beam splitter. As will be reviewed in Section 4.2, single photons emitted by spatially separated QD-SPSs enable two-photon interference visibilities which exceed the fundamental limit of 50% for WCPs, thus making Bell measurements more efficient. The secure key rates achievable in MDI-QKD have so far been studied analytically for attenuated laser pulses in the asymptotic limit as well as the finite-size regime. Theoretical studies for MDI-QKD using deterministic SPSs enable photon indistinguishabilities up to unity have yet to be conducted. Importantly, MDI-QKD protocols are intrinsically suited for starlike network topologies, which is particularly useful for the realization of scalable multi-user QKD networks in metropolitan areas. An experimental demonstration of this type of quantum network with a sub-Poissonian quantum light source would be a major step toward the quantum internet.
The challenge in the practical realization of fully DI-QKD is the requirement for loophole-free Bell measurements across remote locations with high entanglement fidelity. Experimentally, DI-QKD has therefore only been explored very recently using two trapped single Rubidium atoms separated by 400 m [264] and two Strontium ions separated by about 2 m [265]—work to be considered as major steps toward untrusted QKD networks.

4. Recent Progress on Building Blocks for Quantum Networks

The establishment of QKD-secured communication links discussed above is only the first step toward a worldwide quantum internet [266]. In this section, we review recent advances in building blocks necessary for extending quantum networks both in terms of distance and functionality (see Figure 13). Noteworthy, many of the building blocks discussed in the following are equally important for distributed and optical quantum computing, quantum sensing, and quantum metrology, thus representing so-called cross-cutting challenges. While many excellent review articles are available on building blocks for future quantum technologies [267,268,29] we intend to highlight recent advances specifically in the context of QD-based quantum communication networks. This includes practical QD-SPSs (4.1), quantum memories compatible with QD sources (4.3), teleportation of single photon states (4.4), and quantum repeater schemes suitable for entangled photons from QDs (4.2). For completeness, we also highlight recent advances in random number generation (4.5) and tools for the optimization of quantum networks (4.6).

4.1. Toward practical quantum light sources

Practical QD-based quantum light sources should ideally feature “plug-and-play” operation, that is, they can be operated without laboratory infrastructure (e.g., liquid coolants or bulky laser systems) and provide the generated quantum light “ready-to-use” via an optical single-mode fiber. In addition, devices should be robust, durable, as compact as possible, and ideally operate with standard power plugs. Not least, practical quantum light sources need to be benchmarked regarding their long-term stability.

A key to the integration of QD-SPSs into practical modules are techniques for their permanent coupling to optical fibers typically requiring a precise alignment. Starting with the probabilistic coupling of QDs using bundles of hundreds of single-mode fibers [269] over exploring deterministic coupling techniques using open cavity systems [270] or selected nanowire SPSs [271] respective technologies have been developed for more than a decade. More recently, fiber-scanning techniques in combination with epoxy resist or optical adhesives cured via ultraviolet (UV) light proved useful tools for the permanent fiber-coupling of QD-SPSs based on micropillar cavities [233,272,273] microcavities or microcavities [179,211,274] as well as nanowires [275]. Figure 14 depicts a schematic of an electrically controlled fiber-coupling micropillar-cavity used to demonstrate resonant excitation by Snijders et al. in 2018 [273]. While overall efficiencies of permanently fiber-coupled devices reported to date were limited to a few percent, microcavities based on hybrid circular Bragg gratings (hCBG's) have recently been evaluated as a promising strategy to achieve fiber coupling efficiencies close to unity. In their study, Rickert et al. presented numerically optimized designs for devices operating...
at O-band wavelengths, indicating that overall efficiencies exceeding 80% are possible using off-the-shelf single-mode fibers.

An illustration of a single-mode fiber-coupled hCBG is shown in Figure 14b together with corresponding simulation results. Considering the recent experimental advances in the development of state-of-the-art SPSs based on hCBGs, this device approach appears particularly promising.

Alternatively, QDs integrated into optical nanobeams or a photonic crystal cavity can be fiber-coupled using an adiabatic mode transfer between tapered waveguide-to-fiber couplers. Using this approach, end-to-end efficiencies exceeding 10% have been achieved for extracting single photons from QDs while proof-of-concepts demonstrated the approach also at telecom wavelengths. Noteworthy, adiabatic fiber tapers were recently also employed in diamond-based spin-photon interfaces for demonstrating memory-enhanced quantum communication.

The QD-based SPSs used for QKD experiments to date entirely relied on laboratory infrastructure including bulky cryotechnology in particular. A more practical solution for the operation of QD-SPSs at cryogenic temperatures was pioneered by Schlehahn et al. in 2015, using for the first time a Stirling-cryocooler combined with free-space optics. This type of cryocooler can be operated with an electrical power of 100 W via standard net supply voltage achieving a base temperature below 30 K within a cool-down time of about 20 min. Three years later, the authors reported the integration of a multimode fiber-coupled QD-based SPS emitting around 925 nm into a compact one-piston Stirling cryocooler—proving that practical QD-based quantum light sources are within reach. The cryocooler, achieving a base temperature below 40 K, was compact enough to be integrated into a standard 19-inch rack module. More recently, Musiał, et al. adopted this approach to demonstrate the first compact QD-SPSs emitting at O-band wavelengths by integrating a single-mode fiber-coupled QD. Based on these developments, Gao et al. very recently pioneered the application of plug&play QD-SPSs for quantum communication. Here, the authors realized the, to date, most compact telecom-wavelength...
QD-SPS providing single-photon pulses via an SMF-28 fiber, with a pulsed diode laser and a fiber-based bandpass filter integrated together with the Stirling cryocooler in a 19-inch rack module (Figure 14c). Implemented in a simple BB84-QKD testbed, the source performance was evaluated in terms of the secure key rate, QBER, and maximal tolerable losses expected in full implementations of QKD—work representing an important step forward in the field of photonic quantum technologies.

While the reports discussed in the previous paragraph used external laser systems for above-band or quasi-resonant optical excitation of the QD-SPSs, also other more compact solutions for driving the quantum emitters have been envisioned. The possibility to electrically inject carriers in QD light-emitting diodes is one advantage of semiconductor-based quantum light sources, which is one route to achieve higher degrees of device integration. Electrical pumping, however, excludes the possibility to apply resonant excitation schemes in most device layouts. For this reason, sophisticated device technologies have been developed enabling the optical driving of QDs using microlasers integrated on the same chip next to the quantum light emitting device. Stock et al. proposed in 2013 to use electrically driven on-chip whispering-gallery-mode microlasers to excite nearby QD micropillar cavities and showed Purcell enhancement of the QD emission in a micropillar excited in such a way. In 2017 Munnely et al. used this approach to demonstrate the Purcell-enhanced triggered single-photon emission at excitation repetition rates of up to 190 MHz using on-chip microlasers. Additionally, the authors demonstrated the possibility of independently tuning the emission wavelength of the QD micropillar exploiting the quantum-confined Stark-effect via additional electrical gates. Using a similar approach, Lee and coworkers realized a QD-SPS excited by an on-chip integrated light-emitting diode (LED) in the same year, that was using the quantum-confined Stark effect to tune the FSS of the emitting QD. Based on this approach, the same group reported recently on an on-chip driven QD entangled-photon pair source emitting at O-band wavelengths, which was implemented in a deployed urban fiber network. While resonant excitation of a QD has not yet been demonstrated using an on-chip pumped device, the approaches discussed above show prospects for the realization of high-performance quantum light sources at ultimate degrees of device integration.

The advances in the realization of plug-and-play quantum light sources discussed above show prospects for practical applications of QD-based devices in photonic quantum technologies. Future work in this direction needs to demonstrate that these technologies can be implemented in a way fully exploiting the potential QD-based quantum light sources offer in terms of device efficiency, single-photon purity, and photon indistinguishability.

4.2. Toward Quantum Repeaters

The communication distance in direct point-to-point QKD is limited by photon loss, both in free space and in fiber optical links. Larger distances can be covered by introducing intermediate trusted nodes, however at the cost of reduced overall security. Note, that large multi-user networks based on trusted nodes are already in use. To cover arbitrary distances without compromises on the security, quantum repeaters are the ultimate choice. Exploiting entangled photon pair sources and entanglement swapping as key resources, quantum information can be transferred over arbitrary distances by dividing the quantum channel into shorter segments. This subsection first briefly introduces quantum repeater protocols before highlighting recent advances in one required key ingredient—two-photon interference from remote, that is, spatially separated, QD-based SPSSs.

The first quantum repeater scheme, known as BDCZ protocol, was proposed by Briegel, Dür, Cirac, and Zoller in 1998, to overcome the exponential scaling of errors with the transmission length in noisy quantum channels. The BDCZ protocol enables the distribution of a maximally entangled photon pair, for example, the well-known Einstein-Podolski-Rosen (EPR) state, over arbitrary distances. Later, a physical implementation of a quantum repeater scheme, known as the DLCZ protocol, has been proposed, which uses atomic ensembles both as the memory and the photon source. The entangled photon pair can then be used directly, to realize QKD protocols (e.g., the E91 protocol), or, to teleport a quantum state from one end to the other (see Section 4.4 for a discussion on quantum teleportation). To distribute the entanglement, Briegel et al. proposed to use multiple EPR sources along the quantum channel each sending entangled photons in opposite directions, thus dividing the complete quantum channel into shorter segments. At intermediate nodes, photons from two neighboring EPR sources are stored in a quantum memory and then used for swapping the entanglement to the two outer photons via a joint Bell state measurement (BSM) of the photons at the intermediate station. Repeating the swapping in a nested fashion, arbitrary distances can be covered in principle (Figure 15a). Within a successful protocol run, all photons together propagated over the complete length of the quantum channel. An improvement of the photon loss sensitivity is therefore only possible if quantum memories are used at the intermediate nodes. In this case, redundant EPR pairs can be sent until the memory is loaded to perform a successful BSM, thus preventing loss between two nodes. In other words, the quantum channel is cut into shorter segments and over each segment, entanglement purification can create maximally entangled, distributed photon pairs in a memory before entanglement swapping connects all these segments.

For a physical implementation of the BDCZ quantum repeater protocol, different quantum emitter platforms can be used as discussed in detail in ref. 290. For implementations using QD-based entangled photon pair sources, quantum memories compatible with photons emitted by QDs are required, which is a challenge in itself (see Section 4.3). To realize the entanglement swapping step, two photons must be projected into a Bell state, as first demonstrated by Pan et al. using an SPDC source. Here, the authors created two entangled photon pairs, performed a projective BSM via two-photon-interference (TPI), and verified entanglement of the remaining two photons that never interacted before. A quantum repeater node implementing the BDCZ protocol was first experimentally realized by Yuan et al. using two atomic ensembles as quantum memories. By projecting photons, entangled with the states of their respective memory, in a joint Bell state, the entanglement was swapped, entangling the two atomic ensembles, which was confirmed by measuring the entanglement between the photons emitted from the memories.
In addition to memory-based quantum repeaters, all-photonic measurement-based quantum repeater schemes have been proposed, which do not require storage and retrieval of photon states.\[^{[292–295]}\] As key resources these types of repeater protocols require photonic cluster states as used recently in a proof-of-principle quantum repeater experiment.\[^{[296]}\] Photonic cluster states are also of large importance for photonic quantum computing\[^{[297]}\] and have already been generated using QD-SPSs.\[^{[298,299]}\]

One crucial ingredient for all quantum repeater protocols and many other schemes in quantum information is a successful BSM implemented via TPI experiments at a beam splitter. Before discussing recent advances in QD-based TPI experiments, a few general remarks shall be made. The Bell basis is the natural basis of the four-dimensional Hilbert space in which a joint two-qubit state is described. It consists of four maximally entangled states, that is, the Bell states, that are non-separable superpositions of the tensor products of the respective one-particle Hilbert space bases. Assuming two polarization qubits in the rectilinear \{H, V\}-basis, which are indistinguishable with respect to all other quantum numbers, the Bell states can be written as \(|\Psi^\pm\rangle = \frac{1}{\sqrt{2}} (|HV\rangle \pm |VH\rangle)\) and \(|\Phi^\pm\rangle = \frac{1}{\sqrt{2}} (|HH\rangle \pm |VV\rangle)\). Using linear optical elements, only two out of four Bell states can be discriminated resulting in a success rate of 50\%. Braunstein et al.\[^{[100]}\] first introduced the notion that TPI at a beam splitter in a generalized Hong-Ou-Mandel (HOM) experiment\[^{[101]}\] is equivalent to a BSM since the Bell states are eigenstates of the unitary operation that describes the beam splitter. If both photons exit the beam splitter at different output ports, the two-qubit state is projected into the \(|\Psi^+\rangle\) Bell state (Figure 15b) being the only antisymmetric state under particle exchange (thus characterized by fermionic anti-bunching statistics). This results in a successful BSM in 25\% of all cases. The indistinguishability of both photons (in all quantum numbers other than their polarization) is a crucial prerequisite, as otherwise erroneous \(|\Psi^-\rangle\) coincidence events would also result from the projection into the other Bell states. But if the photons are indeed indistinguishable and not projected into the \(|\Psi^+\rangle\) state, they will exit the beam splitter via the same output port, as observed in the famous HOM effect. Adding polarization beam splitters to both output ports of the TPI beam splitter, both \(|\Psi^\pm\rangle\) states can be discriminated, which increases the efficiency of the BSM to 50\% (Figure 15c).

Note that if the interfering photons are not perfectly indistinguishable, erroneous coincidences in the PBS basis can be detected, while states prepared in any other basis (that are randomly projected at the PBS) lead to false coincidences. This was observed by Basso Basset et al. by comparing the teleportation fidelities achieved in BSMs with 25\% and 50\% efficiency, respectively, as well as with high and low indistinguishability\[^{[302]}\] (see Section 4.4). As QD-based SPSs enable higher photon indistinguishabilities compared to SPDC sources, the fraction of erroneous coincidence events can be reduced, resulting in a higher fidelity of the BSM. Furthermore, also multi-photon contributions in WCP-based implementations result in lower measurement fidelities compared to deterministic SPSs.\[^{[261]}\] Therefore, many schemes of quantum information relying on high-fidelity BSMs benefit from remote SPSs with high TPI visibilities.

The photon indistinguishability is quantified by the coalescence probability (for pure states the maximum wave packet overlap) of the two photons \(P_{\text{coal}} = |\langle \phi_1 | \phi_2 \rangle|^2\), which can be estimated by measuring the TPI visibility \(V\) in HOM-type interference experiments.\[^{[301]}\] While the TPI visibility is fundamentally limited to 0.5 for phase-randomized Poissonian light,\[^{[71]}\] it can in principle reach unity for single photons generated via deterministic quantum light sources.

To achieve high TPI visibilities between photons emitted from remote solid-state sources is particularly challenging, as both emitters must be as indistinguishable as possible in all their quantum numbers. To date, TPI from remote quantum emitters has been demonstrated for many types of photon sources, for example, SPDC sources\[^{[303,304]}\] trapped atoms\[^{[305]}\] and ions,\[^{[306]}\] NV- and SiV-centers in diamond,\[^{[307–309]}\] as well as organic
Techniques for the spectral tuning of QDs for remote TPI experiments. a) and b) Patel et al. exploited the quantum-confined Stark effect to electrically tune a QD embedded in a diode-structure.\cite{320} c) and d) Zhai et al. employed piezo actuators to apply strain to the QD.\cite{329} e) A similar approach was used earlier by Reindl et al. for matching the emission energies of two QDs.\cite{317} f) Giesz et al. used the temperature to tune the QD emission into resonance with the optical mode of a micropillar cavity.\cite{313} (a,b) Reproduced by permission.\cite{320} Copyright 2010, Springer Nature. (c,d) Reproduced with permission.\cite{329} Copyright 2020, AIP Publishing. (e) Reproduced under the terms of the Creative Commons CC-BY license.\cite{317} Copyright 2017, The Authors, published by the American Chemical Society. (f) Reproduced with permission.\cite{313} Copyright 2015, American Physical Society.

Figure 16. Techniques for the spectral tuning of QDs for remote TPI experiments. a) and b) Patel et al. exploited the quantum-confined Stark effect to electrically tune a QD embedded in a diode-structure.\cite{320} c) and d) Zhai et al. employed piezo actuators to apply strain to the QD.\cite{329} e) A similar approach was used earlier by Reindl et al. for matching the emission energies of two QDs.\cite{317} f) Giesz et al. used the temperature to tune the QD emission into resonance with the optical mode of a micropillar cavity.\cite{313} (a,b) Reproduced by permission.\cite{320} Copyright 2010, Springer Nature. (c,d) Reproduced with permission.\cite{329} Copyright 2020, AIP Publishing. (e) Reproduced under the terms of the Creative Commons CC-BY license.\cite{317} Copyright 2017, The Authors, published by the American Chemical Society. (f) Reproduced with permission.\cite{313} Copyright 2015, American Physical Society.

Table 2. Chronological overview of achieved visibilities in remote QD TPI experiments.

| Wavelength (nm) | Tuning mechanism         | TPI visibility (%) | Reference                  |
|-----------------|--------------------------|--------------------|-----------------------------|
| 940             | Electrical               | 33 ± 1             | Patel et al. 2010\cite{320} |
| 920             | Piezo strain             | 18 ± 1             | Flagg et al. 2010\cite{315} |
| 930             | Temperature              | 39 ± 2             | Gold et al. 2014\cite{323}  |
| 945             | Temperature              | 40 ± 4             | Giesz et al. 2015\cite{313} |
| 955             | Electrical               | 91 ± 6             | Delteil et al. 2016\cite{322} |
| 1250            | Laser-induced evaporation| 33 ± 1             | Kim et al. 2016\cite{323}   |
| 933             | Temperature              | 29 ± 6             | Thoma et al. 2017\cite{314} |
| 750             | Piezo strain             | 51 ± 5             | Reindl et al. 2017\cite{317} |
| 968             | Electrical               | 93 ± 1             | Stockill et al. 2017\cite{324} |
| 795             | Piezo strain             | 41 ± 5             | Zopf et al. 2018\cite{325}  |
| 1550            | Frequency conversion     | 29 ± 3             | Weber et al. 2019\cite{326} |
| 780             | Electrical               | 93 ± 1             | Zhai et al. 2021\cite{327}  |
| 1583            | Frequency conversion     | 67 ± 2             | You et al. 2021\cite{328}   |

* Used temporal post-selection (CW experiment); † with active feedback; ‡(93 ± 4)% with temporal filtering.

In the following, we review recent advances in TPI experiments using remote QD-based quantum light sources. In the case of QDs, the spectral properties are of particular importance, due to the self-organized nature and the semiconductor environment of the quantum emitters. The first demonstration of indistinguishable photons from the same QD was reported in a seminal work by Santori et al. in 2002.\cite{187} Since then, TPI visibilities close to unity have been reported many times for photons emitted by single QDs.\cite{188–190,311,312} Large photon indistinguishabilities from remote QDs; however, have only been achieved recently, as discussed further below. This requires firstly a coarse spectral matching of quantum emitters using pre-selection of suitable QDs. Using deterministic fabrication technologies, the yield for identifying suitable candidates can be increased significantly.\cite{179,98} Additionally, a spectral fine-tuning of one of the QDs is typically required, for which several techniques can be used (see Figure 16). Prominent examples are the tuning via the temperature,\cite{313,314} strain,\cite{315–319} or electrical gates by exploiting the quantum-confined Stark effect.\cite{320} The TPI visibilities achieved by spectrally matching two remote QDs are summarized in Table 2 further below.

A conceptually different technique was employed by Weber et al. using quantum frequency conversion of the single-photon emission of two spectrally unmatched QDs (see Figure 17b).\cite{326} To perform their remote TPI experiment at telecom C-band wavelengths, the emission of both QDs was converted from the near-infrared to 1550 nm (cf. Figure 17c). During the upconversion process, the spectral mismatch between both QDs (about 6 GHz) was compensated for using two independently tunable lasers, resulting in a remote TPI visibility of 29%.

However, even if the emission energies of two QDs are matched perfectly, several effects can limit the achievable TPI visibility. Most importantly, phonon-induced dephasing, nuclear spin fluctuations, and charge fluctuations can lead to emission...
Remote TPI visibilities exceeding the classical limit of 50% were achieved in several experiments using QD quantum light sources. A summary of TPI experiments using single photons emitted by remote QDs is given in Table 2 in chronological order. Very recently, Zhai et al.\cite{327} achieved remote TPI visibilities of up to 93% representing the current state-of-the-art. The authors used GaAs QDs fabricated via the droplet-etching technique and applied electrical gates for reducing spectral diffusion, which was sufficient to achieve an unprecedentedly low level of dephasing.\cite{319,329} Interestingly, the high visibility was achieved without employing Purcell enhancement, tight spectral filtering, post-selection, or active stabilization, therefore even leaving room for further improvement. In another recent experiment, You et al. demonstrated TPI of remote QD-SPSs separated by 300 km of optical fiber using quantum frequency conversion to 1583 nm,\cite{328} thus setting a remarkable distance record for the interference of quantum light sources. Before discussing recent advances in entanglement swapping experiments, it should be noted that indistinguishable flying qubits also enable the generation of entanglement between remote solid-state spin qubits.\cite{334} Two prominent experimental realizations demonstrated heralded entanglement between two hole-\cite{322} and electron-\cite{324} spin qubits confined in distant QDs.

Proof-of-concept experiments on entanglement swapping using polarization-entangled photon pairs generated via the XX-X radiative cascade in QDs were reported by Zopf et al.\cite{335} and Basso Basset et al.\cite{336} in 2019 (see Figure 18a). Both experiments used entangled photon pairs subsequently emitted by the same QD to demonstrate entanglement swapping, enabling higher TPI visibilities compared to a full-fledged remote experimental setting. The entangled XX- and X-photons of two subsequent photon pairs were spatially separated using spectral filters, before sending one photon of each pair (originating from the same transition) to a receiver performing a partial BSM on the two-photon state (Figure 18b). Note, that due to the binding energy of the XX-state, either two X- or two XX-photons must be used for the BSM, as both photons are distinguishable in their energy otherwise.

Zopf et al. used the XX-photons for the BSM in their experiment,\cite{335} where coincidence detections indicate the projection into the $|Ψ^+\rangle$ Bell state in 25% of the TPI events at best. Note, that although the photons leave the beam splitter via different output ports, a phase shift of $\pi$ rotates them into the $|Ψ^-\rangle$ state. Detecting the $|Ψ^-\rangle$-state, the two corresponding X-photons become entangled with each other, which can be verified by violating the CHSH inequality. Thus, entanglement has been swapped from the two photons within one XX-X pair
Figure 18. a) Schematic of a proof-of-concept entanglement swapping experiment using entangled XX-X photon pairs subsequently emitted by a single QD. b) The experimental setup used by Zopf et al.\cite{335} c) and d) Quantum state tomography verifies that the two X-photons are projected in the $|\Psi^-\rangle$ Bell state after performing a successful partial BSM using two XX-photons. Without the BSM, the density matrix remains maximally mixed. e) Fidelity $f_{|\Psi^-\rangle}$ to the $|\Psi^-\rangle$-state after entanglement swapping as a function of TPI visibility and the FSS.\cite{336} [a–d] Reproduced with permission.\cite{335} Copyright 2019, American Physical Society. (e) Reproduced under the terms of the Creative Commons CC-BY license.\cite{336} Copyright 2019, The Authors, published by American Physical Society.

(having different energies) to two X-photons (having the same energy) from subsequent pairs, as verified via quantum state tomography (cf. Figure 18d). Without performing the BSM, however, the density matrix was observed to be maximally mixed (cf. Figure 18c). From their experimental data, Zopf et al. extracted a fidelity of the entanglement-swapped two-photon state to the Bell state $|\Psi^-\rangle$ of 81%. The entanglement swapping experiment by Basso Basset et al. is conceptually very similar.\cite{336} But here, the authors used the X-photons for the partial BSM, that is, the entanglement was swapped to two XX-photons of subsequent pairs. Moreover, the BSM detected the $|\Psi^-\rangle$ Bell state, in this case, using coincidences from two different outputs of a beam splitter. Furthermore, the authors showed that the entanglement fidelity obtained after the swapping experiment is mainly limited by the photon-indistinguishability and the initial degree of entanglement present in the XX-X photon pairs. For this purpose, a theoretical model was introduced, reproducing the experimental findings (Figure 18e).

Additionally, the entanglement swapping experiments discussed above were conducted using QDs emitting around 780 nm close to the Rubidium $D_2$-transition, showing prospects for the implementation of quantum memories (see Section 4.3). Noteworthy in this context, Schöll et al. recently showed that the indistinguishability of photons emitted via the XX-X radiative cascade is intrinsically limited for a given QD due to the underlying three-level system.\cite{152} Firstly, the shorter radiative lifetime of the XX state results in a spectral line broadening, and secondly, photons emitted by the X state acquire an additional temporal jitter due to the preceding spontaneous decay of the XX state. Both effects reduce the achievable TPI visibility compared to a two-level system. If one realizes larger quantum networks including several entanglement swapping nodes, the effect of the limited indistinguishability will increase with every node. However, these effects could be mitigated by spectrally filtering the XX photons, or by nanoengineering of the excited state’s lifetimes. Alternatively, fabricating microcavities selectively enhancing the biexciton emission, the effect of the temporal jitter could also be reduced.\cite{144}

Using the parameters of state-of-the-art QD entangled photon sources,\cite{65,66} Basso Basset et al. predict a maximum achievable fidelity of the swapped entanglement of 84% with current technology. Even higher values can be expected with further improvements in the foreseeable future, opening up the route for entanglement swapping using remote QD sources and ultimately quantum repeaters based on sub-Poissonian quantum light sources.

The high fabrication quality and degree of control possible with QD quantum light sources today resulted in substantial advances in TPI experiments using remote sources. As reviewed in this subsection, remote photon indistinguishabilities exceeding the fundamental limit of 50% set for WCPs were demonstrated several times, showing prospects for breakthroughs in advanced implementations of quantum communication. Future work in this direction will also need to transfer these achievements to more practical scenarios outside shielded laboratories.
4.3. Quantum Memories

Quantum memories are another important building block for many applications in quantum information. An ideal noiseless quantum memory enables the storage and on-demand retrieval of a quantum state with zero decoherence and over arbitrary timescales. Many applications in photonic quantum technologies benefit or even rely on quantum memories, including quantum computation, quantum metrology, quantum machine learning, single-photon detectors (see ref. [341] for a comprehensive review). Specifically in quantum communication, quantum memories can enhance the performance and functionality of many types of protocols (e.g., ref. [342]), including memory-assisted QKD or memory-built-in quantum teleportation, and most prominently, quantum repeater protocols allowing for entanglement distribution over arbitrary distances (cf. Section 4.3). While all-photonic quantum repeater schemes without the necessity for a quantum memory do exist, these protocols are demanding in other ways, for example, by requiring multiple multiplexed quantum channels or relying on photonic cluster states, which are challenging to realize in a scalable fashion.

Various types of memories have been proposed and experimentally demonstrated, including solid-state systems, trapped atoms and alkali vapor cells. For an extensive overview of memory protocols and platforms, we refer to ref. [349].

A particularly interesting route for the realization of large quantum networks is to combine quantum memories with high-performance QD-based quantum light sources. For interfacing QD single-photons with quantum memories, several characteristics are important to consider besides the key parameters of storage time and fidelity. The quantum memory should for instance support the high clock rates achievable with QD sources and feature a low noise operation for reliably retrieving single photons despite the background noise. In the following, we will review recent advances in this context, also considering aspects of practicality for the implementation in scalable optical quantum networks.

Alkali vapor cells are promising candidates to realize QD-compatible memories (see Figure 19a). Here, the group velocity of light pulses propagating through the atomic ensemble can be reduced, that is, they are slowed down, allowing for photon storage. Warm atomic vapor cells are especially interesting due to their practicality, as their operation does not require complex cryotechnologies or laser cooling schemes, as is the case for solid-state-based and atomic implementations, respectively. In addition, they offer sufficiently long coherence times and benefit from a large set of existing memory protocols. On the other hand, solid-state memories and ultra-cold atoms experience typically less noise and offer longer storage times, making them more desirable for some applications.

To store photons in an ensemble of alkali atoms, transitions in a so-called $\lambda$-system can be used, where two spectrally close lower states together with one excited state enable the effect of electromagnetically induced transparency (EIT) (cf. Figure 19b). While the quantum state to-be-stored is resonant with one transition, a control pulse enables the excitation by driving the other transition. On the atomic level, all atoms are first prepared in a joint ground state. Subsequent excitation via a signal photon in combination with a control pulse results in an atom-spin-wave storing the coherence. A second control pulse then retransforms the spin-wave into an optical excitation, enabling retrieval of the original photon (Figure 19c).
Typically, the signal- and control-pulse are detuned from the resonant atomic transition, reducing noise arising from immediate fluorescence. For detuning the pulses while still driving the transitions, Raman scattering can be used. The detuning; however, not only reduces the noise floor but also affects the memory efficiency, typically requiring a trade-off between low noise and efficient excitation.

First theoretical investigations on atom-based quantum memories for QD single photons were reported by Rakher et al. considering ensembles of ultra-cold Rubidium atoms. Here, the authors highlighted steps necessary toward the storage and retrieval of single photons in a high bandwidth quantum memory and also discussed the impact of imperfections of QD-SPSs, for example, spectral diffusion and finite photon indistinguishabilities. Experimentally, a quantum memory with a bandwidth of 0.66 GHz suitable for QD single photons was demonstrated by Wolters et al., using a warm Rubidium vapor cell exploiting EIT and laser photons. The authors achieved an end-to-end efficiency of 3.4% for a storage time of 50 ns.

Early demonstrations of quantum memories based on vapor cells showed that a photon can be stored and retrieved with finite efficiency. That the retrieved photon is indeed identical to, that is, indistinguishable from, the input photon, had yet to be demonstrated. This was first achieved by Hosseini et al. in 2011, where the authors reported a 98% process fidelity by performing quantum state tomography on the retrieved photons. More recently, Guo et al. demonstrated a quantum memory based on a warm Rubidium vapor cell with an efficiency exceeding 82% using the Raman-detuned quantum memory scheme and attenuated laser pulses as signal photons—work representing the current state-of-the-art for this type of memory.

Exploiting standard EIT in vapor cells, however, is not useful for storing and retrieving polarization qubits, as the EIT memory preserves the phase, but not the polarization. The first solution was presented by England et al. where a dual-rail memory based on a Cesium vapor cell was implemented achieving up to 97% process fidelity and 1.5 μs storage time for polarized photons. Based on the dual-rail approach, 5 years later Namazi et al. demonstrated a quantum memory based on a Rubidium vapor cell achieving low-noise storage and retrieval of polarized photons with a fidelity to the original polarization state exceeding 90% and storage times of about 50 μs. This quantum memory was in turn employed for QKD experiments using WCP-based polarization qubits. To maintain the polarization state of the photons, both groups used polarization-dependent displacement optics (Glan-laser polarizers), which converted the polarization- into a path-encoding, defining two different spatial paths through the memory. After the atomic vapor cell, the qubits are reconverted to polarization-states again (Figure 19d). Hereby, each polarization component is stored individually in a different path within the atomic vapor. Similar experiments were also conducted using cold-atom ensembles also demonstrating storage and retrieval of polarization-entangled photon pairs.

An important task to address on side of the QD source concerns the spectral matching to the atomic quantum memory, requiring a precise tuning of the emission energy of the artificial atom relative to its natural counterpart. This challenge was first addressed experimentally by Akopian et al. in 2011 by exploiting the Zeeman effect. The authors used a magnetic field to tune the wavelength of QD single photons relative to the optical D2-transition in a Rubidium vapor cell and exploited the strong dispersion in the atomic medium to slow down the single photons. This experiment triggered more work in this direction also using different approaches for spectral matching. Jahn et al. used strain-tuning via piezo-electric material to shift the QD emission energy through resonance with the optical transitions in atomic vapor. As demonstrated by Ulrich et al., the spectral tuning can also be performed all-optically using “dressed state” resonance fluorescence. Recently, also deterministically fabricated QD-devices were interfaced with atomic vapor. Here, the authors used temperature tuning of the QD emission energy, achieving dispersion-induced temporal delays in the atomic medium exceeding 15 ns. Another insightful work in this context was reported by Vural et al., performing TPI experiments between two photons emitted by a QD, where either both or one propagated through an alkali vapor cell. The authors showed that the photons had a significant degree of indistinguishability, even though one of them acquired a dispersion-induced temporal shift and broadening.

Finally, we would like to stress that although single photons from QDs have been slowed down in vapor cell experiments, quantum memory operation has not been demonstrated yet. The on-demand storage and retrieval of QD-generated quantum light states is therefore an important next step in the field.

Solid-state-based quantum memories, on the other hand, are particularly interesting for device integration. Two concepts can be distinguished here: atomic ensembles embedded in a solid-state system or single spin-photon interfaces.

Ensembles of rare-earth ions in crystals enable photon storage in the solid-state with low decoherence showing prospects for long storage times, especially at low temperatures. The quantum storage is typically realized via the controlled reversible inhomogeneous broadening (CRIB) protocol, an extension of the classical photon echo effect, but without its inherent noise problem. Using the CRIB protocol, rare-earth-based quantum memories with GHz-bandwidth should be possible. To maintain a high storage efficiency even at larger bandwidths, the noise issue can also be mitigated using atomic frequency combs, as demonstrated in several experiments to date. Polarization qubits have been successfully stored and retrieved using solid-state quantum memories based on rare-earth ions, both, in a dual-rail memory approach with two different paths through the ion ensemble, or using two rare-earth crystals of Nd:YVO₄ with a halve-wave plate in between. While early work used laser pulses attenuated to the single- or few-photon level, Tang et al. demonstrated in 2015 the storage of a sequence of single photons from a QD.

A single spin embedded in a solid-state matrix and acting as spin-photon interface is another interesting candidate for the realization of solid-state quantum memories. Possible physical implementations are single spins or dark-excitations in QDs, defects in two-dimensional materials, or NV- and SiV-centers in diamond. Using a quantum memory based on a SiV-center in diamond, Bhaskar et al. recently demonstrated memory-enhanced quantum communication. Alternatively, nuclear spins can be used for the realization of quantum memories. This has the advantage of better shielding from the environment, due to the small magnetic moments of...
the nuclei. Long-term storage of quantum bits for realizing a so-called quantum hard-drive is thus more likely in nuclear-spin-based solid-state memories. The limiting factor, in this case, is the dipole-dipole interaction among the nuclear spins, which can be suppressed as demonstrated by Kurucz et al. Although solid-state memories show excellent properties for photon storage, their reduced coupling to the environment makes the processes of reading and writing more difficult. A different quite elegant way of transferring the qubit state from a single photon onto a solid-state quantum memory is by teleporting its state using an entangled photon pair. In this scheme, one photon of the entangled state would be stored in a local solid-state quantum memory, while the other one is sent to the to-be-stored flying qubit. By performing a projective BSM, the flying qubit is teleported into the quantum memory. This concept was experimentally demonstrated by Bussiò et al. in 2014 using telecom-wavelength entangled-photon pairs generated via an SPDC source interfaced with a quantum memory based on a rare-earth-ion-doped crystal. A completely different approach to realize quantum memories are nanofabricated mechanical resonators that allow for operation at telecom wavelengths as recently demonstrated by Walsucks et al. As seen in this subsection, significant progress has been achieved in the realization of optical quantum memories, also in terms of their compatibility with QD-based sources. For an in-depth discussion of this topic, we refer the interested reader to ref. [405]. In future work the efficiency and the signal-to-noise ratio must be further improved to allow for the on-demand storage and retrieval of QD single photons.

4.4. Quantum Teleportation

Quantum teleportation is a quantum information protocol by which the unknown quantum state of one particle can be transferred to another distant particle (Figure 20a). The resources required for a photonic implementation are an entangled photon...
pair shared between Alice and Bob, a projective BSM by Alice, and the exchange of two bits of classical information from Alice to Bob. Performing a BSM at Alice location with two input photons, one being the state to be teleported and the other being one of the entangled photon pair, the to-be-teleported state is projected into the Bell basis. The result of the BSM determines the unitary that must be applied to the other half of the entangled state by Bob to retrieve the teleported state at Bob’s side.

Quantum teleportation is a vital and particularly fascinating building block for future quantum networks. It enables non-local quantum computations and the transfer of qubit states into a solid-state quantum memory (cf. Section 4.3). Teleportation can also be directly used for QKD (given a shared entangled state) by teleporting an encoded state from Alice to Bob, which is known as a quantum relay. Quantum relays using entangled photons from QDs have been demonstrated by Varnava et al. over a distance of 1 km and later by Huwer et al. using photons at telecom wavelengths. In the following, we discuss advances in quantum teleportation enabled by QD-based quantum light sources.

As discussed earlier, the efficiency of a BSM is reduced by multi-photon events unavoidable in implementations using WCP or SPDC sources. Therefore, also teleportation can benefit from the use of entangled photons created by deterministic QD-SPSs. The first QD-based proof-of-concept teleportation experiment was reported by Nilsson et al. in 2013 using a QD entangled-light-emitting diode. The authors used the entangled photon pair emitted in one pulse to teleport a photon from the subsequent photon pair (Figure 20b) and obtained a maximum teleportation fidelity above the classical threshold of 2/3. Although the teleported photon and the entangled photon pair were generated by the same device, the authors emphasized that the teleported photon can in principle also stem from an external source. In fact, their QD emission energy was tunable, to match the wavelength of an incoming external photon, to facilitate TPI and enable teleportation. The operation wavelength of 890 nm was, however, not yet compatible with standard fiber-optical communication networks.

Teleporting external photons with a QD entangled-photon source emitting in the telecom C-band was recently demonstrated by Anderson et al. using an attenuated laser pulse (Figure 20c). The authors observed a HOM visibility of up to 70% for the TPI between the attenuated laser pulse and single photons emitted from their non-resonantly excited QD, a value exceeding the fundamental limit of 50% for TPI between WCPs only. The average teleportation fidelity achieved after temporal post-selection was (88.3 ± 4.0)% (Figure 20d).

Another quantum teleportation experiment was performed by Reindl et al. in which entangled photons from an optically excited GaAs/AlGaAs QD were used to teleport the state of the X-photon from the same source. The polarization state after the teleportation was compared to the prepared polarization state, which showed an average teleportation fidelity of 75% without temporal filtering or post-selection. Moreover, the authors proposed a model for predicting the process fidelity of the teleportation protocol from the properties (FSS and photon-indistinguishability) of a given QD.

While enormous research efforts have been devoted to the optimization of QD-based quantum light sources, Basso Basset et al. recently demonstrated teleportation experiments with photons from QDs, for which they deliberately chose a QD of below-average quality. The authors used one photon from every second entangled photon pair as the to-be-teleported input state. In contrast to their previous work in Reindl et al. the BSM projected into two Bell states instead of one (Figure 21a). The experiments revealed, that this does not only increase the efficiency of the partial BSM, but, importantly, also reduces the impact of finite indistinguishability. Moreover, by improving the photon indistinguishability using spectral filtering, the authors enhanced the teleportation fidelity (see Figure 21c)

Note worthy, also single-mode teleportation protocols have been proposed, which do not require entangled photon pairs and are related to the proposal of linear optics quantum computation. This has been experimentally demonstrated by Fattal et al. in 2004 using QD single photons. Quantum teleportation and quantum repeaters rely on the same resources and will thus benefit similarly from the advances achieved in the development of QD-based quantum light sources. In particular, the substantial improvements achieved in the TPI visibility between remote sources discussed in Section 4.2 show prospects for near-term breakthroughs, including entanglement swapping and quantum teleportation of photonic states from spatially distant QD-sources.

4.5. Quantum Random Number Generation

Among the building blocks required for quantum networks, quantum random number generators (QRNG) were the first to be realized, using for instance a radioactive decay. As a result, the technology readiness level is the highest among all building blocks, as confirmed by its widespread commercial availability—recently even in consumer smartphones—and standardization efforts are also underway. For an in-depth review of random number generation we refer to ref. [417].

All existing QKD protocols require reliable sources of randomness, either for qubit state preparation and detection or for the choice of 2-universal-hash functions during privacy amplification requiring an initial random seed. Moreover, true random numbers are vital for many other domains ranging from simulation and computing to online casinos. It has been shown that ideal QRNGs are the only perfect source of random numbers, as opposed to pseudo-random number generators. While computers typically rely on pseudo-randomness using random seeds and algorithms for random number generation, or classical physical randomness based on the complexity of classical systems, only quantum processes can provide true sources of randomness. This boils down to the proof of having no hidden variables so that the outcome of a single projective measurement cannot be predicted by any means, which is why randomness can be certified via the violation of Bell-like inequalities. The simplest optical QRNG can be described as a photon impinging on a beam splitter with its wave function collapsing on a single-photon detector—a concept that was the first to be implemented for an optical QRNG. In such a setup, it has been demonstrated that a true SPS can provide a larger amount of randomness than a bright laser.
By now, several other schemes for QRNGs emerged, which provide even faster random bit rates using for instance the photon arrival time as the random variable.\cite{425-427} The quantum phase fluctuation and vacuum state schemes achieve Gbps bandwidths\cite{428-430} and do not rely on SPSs. Even faster QRNGs are available\cite{431} which are however limited by the electronics that are not capable of handling the amount of data in real-time—similar to the issue of classical key reconciliation in practical QKD applications. In parallel to the developments in QKD, also the research on QRNGs shifted its focus from trusted devices to the development of device-independent (DI) approaches.\cite{440,441} While semi-device-independent\cite{443} or self-certifying approaches have been realized, a fully DI-QRNG has yet to be demonstrated.

Concerning QD-based QRNGs, it should be noted that QKD protocols are agnostic toward where the random numbers come from, as long as their rate is sufficiently high to keep up with QD emission rates. Nevertheless, it is interesting to note that specific ways of creating QRNG with QDs exist, which could in the future be combined with their SPS property to generate random numbers as well as true single photons on the same platform.\cite{434,435} While QDs can improve many ingredients of future quantum networks, they appear to be not the optimal choice for the generation of random numbers in terms of practicality and possible advantages.

### 4.6. Toward Quantum Networks—Practical Challenges

To build functional quantum networks in real-world settings, several practical challenges beyond the development of the aforementioned building blocks need to be addressed. This subsection reviews research efforts in the monitoring, stabilization, and optimization of protocol implementations and quantum networks in general.

One important practical challenge concerns the stability of quantum channels over long periods of time, which should maintain the performance in terms of data throughput.\cite{436} For this purpose, active stabilization schemes have been developed for both, FSO- and fiber-optical links, for example, using beacon lasers multiplexed spatially or spectrally with quantum signals. This has been demonstrated by Ursin et al. in 2007 using a 144 km FSO link between the Canary Island of La Palma and Tenerife by employing entangled photon-pairs generated via a SPDC source.\cite{437} Similar stabilization approaches have been used to improve or enable QKD experiments employing ground-based FSO,\cite{438} and even satellite,\cite{238} links. Using QD-generated entangled photon pairs at telecom wavelengths, an advanced stabilization scheme has recently been demonstrated by Xiang et al.\cite{140} by continuously exchanging entangled photon pairs over 18 km of optical fiber over an entire week (see Figure 22a).

The current state-of-the-art for mechanical stabilization of free-space links was recently reported by Liu et al.\cite{239} exchanging SPDC-generated qubits between flying drones.\cite{439} Moreover, it is important to define a joint reference frame for the measurement of the qubits (unless reference-frame independent schemes are employed\cite{440,441}), which is possible via auxiliary multiplexed lasers.\cite{69}

In addition, the quantum channels should be characterized (or calibrated) well, in terms of transmission losses and polarization-mode dispersion, to optimize the protocol implementation for maximum performance. This can be addressed experimentally via optimization routines, numerically via key rate predictions, or using machine learning approaches.\cite{442}

Another practical challenge concerns the synchronization between sender and receiver stations. For this purpose, pre-defined laser pulse pattern, multiplexed synchronization signals, clock-recovery,\cite{443} or GPS-disciplined oscillators\cite{432} can be used.

For fast stabilization and high key rates, it is important to achieve a fast modulation of the qubit's polarization or phase\cite{236,444}—a task for which integrated photonics seems to be the most promising route—\cite{445,447}—and to use high-speed detectors with low dead times, especially at telecom wavelengths (see, e.g., ref. \cite{448} for a recent perspectives article).

In addition, many QKD protocols benefit from a monitoring of the security parameters in respective system implementations. As mentioned before, multi-photon pulses enable photon number splitting attacks, which is why sources have to be well characterized to compensate for their non-ideal photon statistics. The amount of multi-photon contributions however might change over time, either due to system-intrinsic fluctuations or actions of an external eavesdropper. To still operate the QKD system at optimal performance, the multi-photon

---

**Figure 21.** Quantum teleportation with polarization-entangled photon pairs from QDs: Teleportation fidelities were measured with a efficiency of the partial BSM of a) 25% and b) 50%. c) Comparison of the average teleportation fidelities using the BSM from a), b), and with spectral filtering using an extra etalon to increase the TPI visibility. d) Teleportation fidelity as a function of the TPI visibility, FSS S, and the efficiency of the BSM. Reproduced under the terms of the Creative Commons CC-BY license.\cite{302} Copyright 2020, The Authors, published by Springer Nature.
contributions need to be monitored during the key exchange, as demonstrated by Kupko et al. in a real-time security monitoring approach (Figure 22b). In their work, the authors also demonstrated how temporal filtering on the receiver side can enhance the signal-to-noise ratio to optimize the secure key rate for a given channel loss. When implementing such approaches, however, special care must be taken not to open the door for other side-channel attacks, as an adversary could otherwise unnoticely steal photons outside the temporal acceptance window. Hence, for an implementation to benefit not only from the improved signal-to-noise ratio, but also from estimating a lower $g^{(2)}(0)$, active temporal filtering (e.g., using an intensity modulator) has to be applied on the sender side (or $g^{(2)}(0)$ needs at least to be monitored at Alice location). In addition, a minimum block size must be reached before post-processing due to finite-key size effects—as implemented nowadays in commercial systems.

The availability of a classical authenticated channel is always assumed implicitly in QKD protocols. Even if an initial secret is shared, authentication has to be repeated regularly which uses up a fraction of the key, which is why protocols for efficient authentication are necessary. Alternatively, QKD can be combined with other post-quantum cryptography schemes supporting the authentication. A challenge that gains importance with the growing maturity of the developed QKD systems refers to security certification. One could either rely on device-independent schemes or use special protocols to confirm that a QKD system is working properly. That includes the certification of the initial randomness, the integrity of the quantum channel, the purity of the source, as well as the correctness of the post-processing steps.

Finally, in order to benchmark different QKD protocols and different technology platforms, a general framework beyond stating only the maximum secure key rate or the maximum achieved distance must be developed, since these parameters are highly dependent on the specific laboratory setup used with a specific source and under certain conditions. Therefore, testing standards are envisioned, to reliably compare different approaches. For example, different QKD systems should be benchmarked according to the same amount of overall $\epsilon$-security (c.f. discussion on security definitions in ref. 80). Another useful figure-of-merit might be the “security-per-dollar-spent”, as different QKD architectures, which in principle promise different levels of security, have different technological requirements and hence costs. Last but not least, while the ultimate aim is to achieve unconditional security, ruling out even the most unlikely attacks (that are practically highly unlikely but allowed by the laws of quantum mechanics), a reduced but more practicable security level might be sufficient for some specific use-cases. This could either be a deliberate tradeoff between security gain and implementation-costs, or an intermediate step toward unconditional security.

The approach of assuming realistic restrictions on an adversary is known and even required in the field of cryptographic primitives beyond QKD, especially in untrusted settings (e.g., the noisy storage model in quantum oblivious transfer), representing crucial building blocks for modern quantum communication networks.
5. Conclusion

This article reviewed the progress made in recent years in the field of quantum communication using quantum light sources based on semiconductor QDs. After revisiting the foundations of QKD and introducing semiconductor QDs as promising candidates for photonic quantum technologies, we comparatively discussed single-photon- and entangled-photon-based QKD experiments implemented with QD devices. Moreover, we discussed recent advances in the development of important building blocks for future quantum networks and their application in practical settings. Considering the tremendous progress achieved in the field, functional quantum networks and real-world applications appear to be within reach in the not too distant future. To this end, several important ingredients require further research and engineering efforts. The superior performance QD sources offer in terms of high efficiency, high brightness, high single-photon purity, large photon indistinguishability, and large entanglement fidelities, need to be combined with recently established approaches for the realization of practical quantum light sources operable outside shielded laboratory environments. Another important challenge concerns the development of efficient quantum memories with on-demand retrieval suitable for QD sources. Further challenges refer to the implementation of protocols enabling an efficient multi-user operation of quantum-secured networks as well as the development of schemes and standards for the security certification.

An important topic which was only slightly touched upon in this review article concerns the implementation of cryptographic primitives beyond QKD and in distrustful settings exploiting quantum means. Primitives such as coin flipping, bit commitment, or oblivious transfer represent important building blocks for many sensitive tasks in modern communication networks, including the secure authentication at a bank’s ATM. These advanced cryptographic tasks might benefit substantially by the use of deterministic QD-based quantum light sources, opening up an entirely new field of research to be addressed in future work.

Finally, future quantum networks will most likely not be constituted of a single technology or a specific protocol. On the contrary, many different platforms and schemes will most probably be combined and coexist, including deterministic quantum light sources as well as WCP- and SPDC-based sources, two-party quantum cryptographic primitives like QKD and beyond, multiparty primitives, classical and post-quantum cryptography, different encoding schemes, and various network architectures, each of which optimized for specific use-cases. Reviewing the achievements and success since the advent of the field of quantum cryptography driven by the ideas of S. Wiesner in the late 1960s, it seems reasonable to expect major steps toward the quantum internet within this decade.

Acknowledgements

The authors gratefully acknowledge financial support from the German Federal Ministry of Education and Research (BMBF) via the project “QuSecure” (Grant No. 13N14876) within the funding program Photonic Research Germany and by the Einstein Foundation via the Einstein Research Unit “Quantum Devices”.

Open access funding enabled and organized by Projekt DEAL.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

engineered devices, quantum communication, quantum key distribution, quantum light sources, semiconductor quantum dots

Received: August 30, 2021
Revised: March 16, 2022
Published online: April 15, 2022

[1] S. Singh, The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, Doubleday Books, New York 1999.
[2] R. Impagliazzo, M. Luby, in 30th Annual Symposium on Foundations of Computer Science, IEEE, Piscataway, NJ 1989, pp. 230–235. http://ieeexplore.ieee.org/document/63483/.
[3] P. W. Shor, SIAM J. Comput. 1997, 26, 1484.
[4] D. J. Bernstein, T. Lange, Nature 2017, 549, 188.
[5] P. W. Shor, J. Preskill, Phys. Rev. Lett. 2000, 85, 441.
[6] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. 2002, 74, 145.
[7] W. K. Wootters, W. H. Zurek, Nature 1982, 299, 802.
[8] D. P. DiVincenzo, Fortschr. Phys. 2000, 48, 9-1171.
[9] H. J. Kimble, Nature 2008, 453, 1023.
[10] S. Wiesner, ACM Sigact News 1983, 15, 78.
[11] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology 1992, 5, 3.
[12] C. H. Bennett, G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, Piscataway, NJ 1984, pp. 175–179.
[13] C.-H. F. Fung, X. Ma, H. Chau, Phys. Rev. A 2010, 81, 012318.
[14] J. L. Carter, M. N. Wegman, J. Comput. Syst. Sci. 1979, 18, 143.
[15] M. N. Wegman, J. L. Carter, J. Comput. Syst. Sci. 1981, 22, 265.
[16] D. Ljunggren, M. Bourennane, A. Karlsson, Phys. Rev. A 2000, 62, 022305.
[17] M. Mosca, D. Stebila, B. Ustaöglu, in International Workshop on Post-Quantum Cryptography, Springer, Berlin Heidelberg 2013, pp. 136–154.
[18] L.-J. Wang, K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu, Q. Zhang, J.-W. Pan, npj Quantum Inf. 2021, 7, 1.
[19] A. K. Ekert, Phys. Rev. Lett. 1991, 67, 661.
[20] J. S. Bell, Phys. Phys. Fiz. 1964, 1, 195.
[21] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, Phys. Rev. Lett. 1969, 23, 880.
[22] C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. 1992, 68, 557.
[23] A. Boaron, G. Bosu, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, Phys. Rev. Lett. 2018, 121, 190502.
[24] X. Ma, C.-H. F. Fung, H.-K. Lo, Phys. Rev. A 2007, 76, 012307.
[25] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunard, R. Colbeck, D. Englund, T. Gehring, C. Lupu, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Valiron, P. Villioresi, P. Walden, Adv. Opt. Photonics 2020, 12, 1012.
[26] C. E. Shannon, Bell Syst. Tech. J. 1949, 28, 656.
[27] G. S. Vernam, J. A.I.E.E. 1926, 45, 109.
[28] A. Broadbent, C. Schaffner, Des. Codes Cryptogr. 2016, 78, 351.
[29] J. L. O’Brien, A. Furusawa, J. Vučković, Nat. Photonics 2009, 3, 687.
Daniel Aleksander Vajner studied physics in Berlin and Paris, accompanied by research stays at Yale University and University of St. Andrews, after which he obtained his joint M.Sc. degree from Freie Universität Berlin and Université Paris Saclay. He is currently pursuing his Ph.D. at the Technical University of Berlin working on implementations of quantum communication using solid-state quantum light sources. Here, he investigates the physics of quantum dot light sources, the advantage of single photons over attenuated laser pulses, and works toward implementing advanced QKD protocols.

Lucas Rickert completed his master’s degree in nanoscience at the Institute of Nanostructure Technologies and Analytics of the University of Kassel, Germany. He joined the Technical University of Berlin in autumn 2018 as a Ph.D. student working on the fabrication of deterministic quantum-dot-based single-photon sources for quantum communication. His research interests are, among others, the integration of quantum dots into photonic structures, nanofabrication techniques, and the development of compact user-friendly quantum light sources.

Tobias Heindel is head of the group Quantum Communication Systems at the Technical University of Berlin (TU Berlin), Germany. His current research focuses on implementations of quantum communication and quantum information science using engineered solid-state quantum light sources as well as the development of respective building blocks. After completing a Ph.D. in physics at Julius-Maximilians-Universität Würzburg, he worked as a postdoctoral researcher at TU Berlin. He had multiple research stays at the Technion Haifa, Israel, and Ludwigs-Maximilians-Universität Munich, Germany. In 2018, he established an independent junior research group at the Institute of Solid State Physics of TU Berlin.