Letter

ADVANCED PHOTONICS

Entanglement-based quantum key distribution with a blinking-free quantum dot operated at a temperature up to 20 K

Christian Schimpf,*,† Santanu Manna,*,† Saimon F. Covre da Silva, Maximilian Aigner, and Armando Rastelli
Johannes Kepler University Linz, Institute of Semiconductor and Solid State Physics, Linz, Austria

Abstract. Entanglement-based quantum key distribution (QKD) promises enhanced robustness against eavesdropping and compatibility with future quantum networks. Among other sources, semiconductor quantum dots (QDs) can generate polarization-entangled photon pairs with near-unity entanglement fidelity and a multiphoton emission probability close to zero even at maximum brightness. These properties have been demonstrated under resonant two-photon excitation (TPE) and at operation temperatures below 10 K. However, source blinking is often reported under TPE conditions, limiting the maximum achievable photon rate. In addition, operation temperatures reachable with compact cryocoolers could facilitate the widespread deployment of QDs, e.g., in satellite-based quantum communication. We demonstrate blinking-free emission of highly entangled photon pairs from GaAs QDs embedded in a p-i-n diode. High fidelity entanglement persists at temperatures of at least 20 K, which we use to implement fiber-based QKD between two buildings with an average raw key rate of 55 bits/s and a qubit error rate of 8.4%. We are confident that by combining electrical control with already demonstrated photonic and strain engineering, QDs will keep approaching the ideal source of entangled photons for real world applications.

Keywords: quantum optics; quantum dots; nanophotonics; quantum cryptography.

Received Aug. 31, 2021; revised manuscript received Nov. 25, 2021; accepted for publication Nov. 26, 2021; published online Dec. 17, 2021.

[DOI: 10.1117/1.AP.3.6.065001]

1 Introduction

Quantum key distribution (QKD) relying on single photons is regarded as one of the most mature quantum technologies.[1,2] However, the impossibility of amplifying single photons sets restrictions on the transmission distance. Entanglement-based QKD schemes are able to overcome these range limitations when embedded in quantum networks,[3,4] while also exhibiting a lower vulnerability to eavesdropping attacks.[1,5–8] For both fiber-based[9] and satellite-based[10] quantum cryptography, the most prominent sources of entangled photon pairs to date are based on the spontaneous parametric downconversion (SPDC) process. These sources are commercially available and can be operated in a large temperature range.[11] As a drawback, SPDC sources exhibit approximately Poissonian photon pair emission characteristics,[12] which severely limits their brightness when a high degree of entanglement—and thus a low qubit error rate (QBER)—is demanded. The biexciton–exciton (XX-X) spontaneous decay cascade in epitaxially grown semiconductor quantum dots (QDs) has been demonstrated to be a viable alternative to SPDC sources due to the sub-Poissonian entangled photon pair emission statistics.[13] In particular, GaAs QDs obtained by the Al droplet etching technique[14] are capable of emitting polarization-entangled photon pairs with a fidelity to the $|\phi^+\rangle$ Bell state beyond 0.98,[15,16] owing to an intrinsically low exciton fine structure splitting (FSS),[17] a low exciton lifetime of about 230 ps, and a near-zero multiphoton emission probability even at maximum brightness.[18] This allowed the demonstration of entanglement-based QKD with a QBER as low as 1.9%.[16,19]

Independent of the QD materials used, the best performances in terms of entanglement fidelity and biexciton state-preparation efficiency have been obtained by operating the QD sources at

*Address all correspondence to Christian Schimpf, christian.schimpf@jku.at; Santanu Manna, santanu.manna@jku.at

†These authors contributed equally.

temperatures below 10 K and using the resonant two-photon-excitation (TPE) condition.[20,21] One of the drawbacks of the very low working temperatures is that they are difficult to achieve in satellites, where strong payload restrictions have to be met. Starting from about 30 K, cryocoolers for lower temperatures become exceedingly bulkier than higher temperature models.[22] Regarding TPE and, in general, resonant excitation schemes, their main limitation is represented by random charge capture in the QD, normally resulting in a significant drop of the time fraction β, in which the QD is optically active (also known as blinking).[23,24] For the generation of single photons via strictly resonant excitation, blinking has been successfully suppressed by embedding QDs into charge-tunable devices,[25] which allows the charge state of a QD to be deterministically controlled.[26,27] The question whether blinking can be suppressed under TPE is not trivial, since—different from single photon resonant excitation—TPE requires excitation powers about 50 times larger, which can produce free carriers in the continuum via two-photon absorption in the barrier material. Although two-photon absorption by a QD in a diode structure has been observed via photocurrent measurements,[28] the usefulness of charge-tunable devices in the context of entangled-photon-pair generation with the TPE method has not been tested.

Here, we investigate the optical properties of GaAs QDs embedded in a p-i-n tunnel diode at a temperature of at least 20 K, demonstrate blinking-free emission of entangled photon pairs under TPE, and use these photons to successfully implement the BBM92 QKD protocol[6] under these conditions. The key generation happens between two buildings, connected by a 350-m long single-mode fiber inside the campus of the Johannes Kepler University.

Varying the voltage applied to the diode within a certain window allows for fine-tuning of the emission wavelength in a range of about 0.2 nm, while keeping the blinking-free emission intact. These structures can therefore be vital for applications in quantum networks,[3] where a precise matching of the wavelengths of multiple emitters becomes important,[29,30] and the transmission rate scales with β^2.[24]

2 GaAs Quantum Dots in a Diode Structure at a Temperature of 20 K

The GaAs QDs in a p-i-n diode structure, as shown in Fig. 1(a), were grown by molecular beam epitaxy. The first functional element is a distributed Bragg reflector, consisting of six pairs of $Al_{0.95}Ga_{0.05}As$ and $Al_{0.20}Ga_{0.80}As$ layers with 65.2 and 56.6 nm thicknesses, respectively. The n-doped region is formed by a 95-nm-thick $Al_{0.15}Ga_{0.85}As$ layer with a Si concentration of 10^{18} cm^{-3}. A combination of layers (15 nm $Al_{0.15}Ga_{0.85}As$ plus 8 nm $Al_{0.33}Ga_{0.67}As$) acts as tunnel barrier between the n-layer and the QDs, which are obtained via the local Al droplet etching technique[14] and covered by the 268-nm-thick $Al_{0.33}Ga_{0.67}As$ intrinsic region. A 65-nm thick layer of $Al_{0.15}Ga_{0.85}As$ doped with 5×10^{18} cm^{-3} carbon atoms forms the p-region. Layers of 5-nm $Al_{0.15}Ga_{0.85}As$ and 10-nm GaAs, each doped with 10^{19} cm^{-3} carbon, cap the structure to form a conductive surface and to protect the active region from oxidation. A DC voltage V_P is applied to the p-contact with respect to the grounded n-contact (see the Supplementary Material for details about the electrical contacts). A solid immersion lens on top of the structure enhances the overall extraction efficiency to about 3%.

The sample containing the GaAs QDs is fixed with silver glue on the cold-finger of a He flow cryostat and cooled to a temperature of 20 K. The temperature is measured with a calibrated silicon diode placed under the cold-finger, so we estimate that the actual sample temperature could be up to 5 K higher. One individual QD is optically excited by a focused pulsed laser with a repetition rate of 80 MHz and the laser energy E_P tuned to half of the biexciton (XX) energy, as depicted in the inset of Fig. 1(a). This resonant TPE scheme is the same as used in previous experiments.[15,16,18] Figure 1(b) shows the microphotoluminescence spectra of a QD when adjusting E_P at the working point $V_{P,0} = 0.3$ V, used for the further measurements, and then sweeping V_P from 0 to 1.5 V. The inset shows the corresponding diode current. In the voltage range of about 0.15 to 0.35 V, the QD is in its charge neutral configuration, and only the biexciton (XX) and the exciton (X) transition lines are visible. For higher voltages, a single electron tunnels into the QD so the negative trion (X^-) is addressed via phonon-assisted excitation. Figure 1(b) shows the spectrum at $V_{P,0}$, with the XX excited at the π-pulse. At this voltage, the autocorrelation function $g^{(2)}$ for a time span of 100 μs and a time-bin of 1 μs was recorded, depicted as the red data points in Fig. 1(d). In this case, the time-bin is much larger than the excitation period of 12.5 ns, so the antibunching from the single-photon emission becomes invisible. The $g^{(2)}$ is one for all time delays, which indicates the complete absence of blinking, i.e., an on-time fraction of $\beta = 1/g^{(2)}(0) = 1.00(2)$.[23] The black dashed line indicates the $g^{(2)}$ typically measured for previously used GaAs QDs without diodes, resulting in $\beta \approx 0.3$.

It is interesting to note that the diode provides a window for V_P of about 0.1 V, in which the QDs can be operated without blinking. This offers a tuning range for the central emission wavelengths of about 0.2 nm, as depicted for a different, but representative, QD in Fig. 1(e). The blue-dashed line indicates the case of $\beta = 1$, corresponding to no blinking. The same tuning range was also observed for temperatures well below 20 K.

3 Characterization of the Entangled Photon Pairs

The QDs of the diode sample used here exhibit an average FSS of about 6 μeV. Average values below 4 μeV are regularly achieved for nanoholes created at a substrate temperature of 600°C,[17,31] while a slightly higher temperature (about 610°C) was used here to possibly improve the crystal quality. Instead of resorting to strain tuning to bring the FSS of one individual QD to zero,[15] the stochastic distribution of the FSS among all QDs on the sample can be used to find a QD with a suitably low FSS for the given use case. To estimate the FSS required for a serviceable QBER in a BBM92 QKD arrangement, we first model the 2-qubit density matrix in polarization space[32] as

$$\rho_M(S, T_{1,X}, k) = \frac{k}{2}\begin{pmatrix} 1 & 0 & 0 & z^* \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ z & 0 & 0 & 1 \end{pmatrix} + \frac{1-k}{4} I^{(4)},$$

$$z = \frac{1+ix}{1+x^2}, \quad x = \frac{ST_{1,X}}{\hbar}, \tag{1}$$

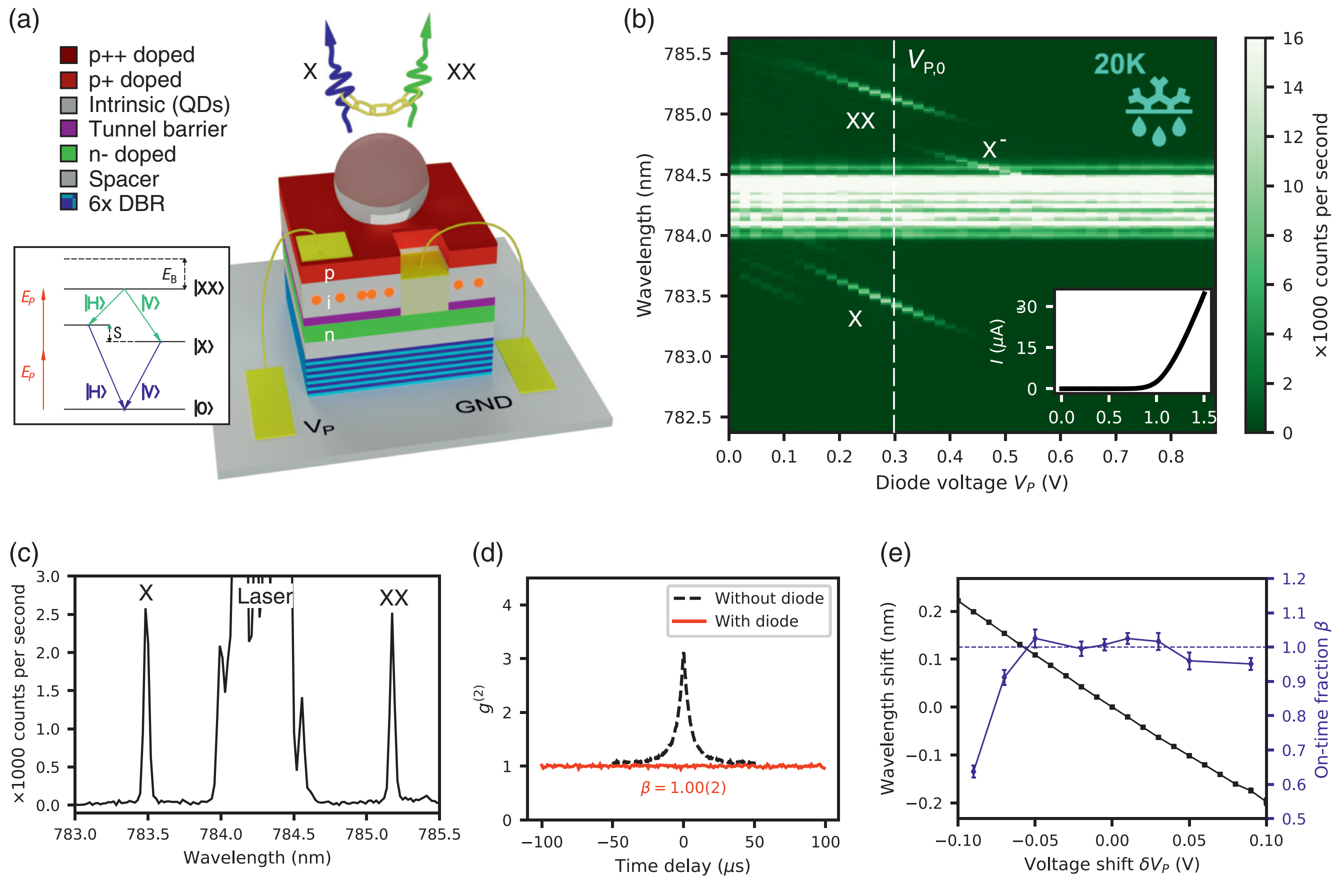

Fig. 1 Photoluminescence properties of GaAs QDs in a p-i-n diode structure at a temperature of 20 K, excited by resonant TPE. (a) p-i-n diode structure with a tunnel barrier between the n-doped and the intrinsic regions. The inset shows the principle of TPE, with E_P the laser energy, E_B the biexciton (XX) binding energy, and S the exciton (X) FSS. (b) Emission spectra at TPE conditions when sweeping the diode voltage V_P in forward bias. The inset shows the diode current I over V_P. The white-dashed line indicates $V_{\mathrm{P},0} = 0.3$ V, at which the diode is operated during the QKD experiment. (c) Emission at $V_\mathrm{P} = V_{\mathrm{P},0}$. (d) Second-order correlation function $g^{(2)}$ of the X signal with a time-bin of 1 μs at $V_\mathrm{P} = V_{\mathrm{P},0}$. The $g^{(2)}$ is shown for the QD in the diode structure (red), indicating an on-time fraction of $\beta = 1.00(2)$ and a QD without diode (black, dashed) with a typical value of $\beta \approx 0.3$. (e) Wavelength shift and β for different deviations $\delta V_\mathrm{P} = V_\mathrm{P} - V_{\mathrm{P},0}$. The blue-dashed line indicates a value of β corresponding to no blinking.

where S is the magnitude of the FSS, $T_{1,\mathrm{X}}$ is the X lifetime, k is the purity parameter, and $I^{(4)}$ is the 4×4 identity matrix. For the estimation of the required S, we set $T_{1,\mathrm{X}}$ to the typically observed value of 230 ps and $k = 1$. In this model, possible dephasing mechanisms other than state rotation induced by the FSS are neglected. From ρ_M, we calculate the expected QBER via

$$q(\rho_\mathrm{M}) = \frac{1}{2}\sum_{i=1}^{4} \langle O_i|\rho_\mathrm{M}|O_i|\rangle, \tag{2}$$

where $O_i \in \{H_\mathrm{A}V_\mathrm{B}, V_\mathrm{A}H_\mathrm{B}, D_\mathrm{A}A_\mathrm{B}, A_\mathrm{A}D_\mathrm{B}\}$ are the 2-qubit measurement bases between Alice (A) and Bob (B), in which a measured coincidence corresponds to a false key bit. After a brief scanning, we chose a QD with an FSS of $S = 0.96(9)$ μeV, for which we calculate a minimum QBER of 2.7%. In practice, a slightly higher QBER is to be expected due to additional dephasing processes.[15,32]

The XX and the X photons generated by TPE are filtered out individually and coupled into single mode fibers. Figure 2(a) shows the spectra of the XX and X emission lines merged at a 50:50 fiber beam splitter, of which one output is sent to the spectrometer. (The slightly lower XX signal intensity stems from the higher distance from the objective to the fiber collimator compared to the X signal, resulting in a lower coupling efficiency.)

Before performing the QKD experiment, a characterization of the single-photon emission characteristics and the polarization entanglement between the XX and the X photons is performed, as those properties primarily determine the QBER during the key generation process. The most important quantities are summarized in Table 1 and compared to the values for a different QD (in the same diode structure), measured at 5 K. Figure 2(b) shows a coincidence histogram of an autocorrelation measurement for both the XX and the X signals. Using a time-bin of 2 ns, the results are $g^{(2)}_\mathrm{XX}(0) = 0.034(4)$

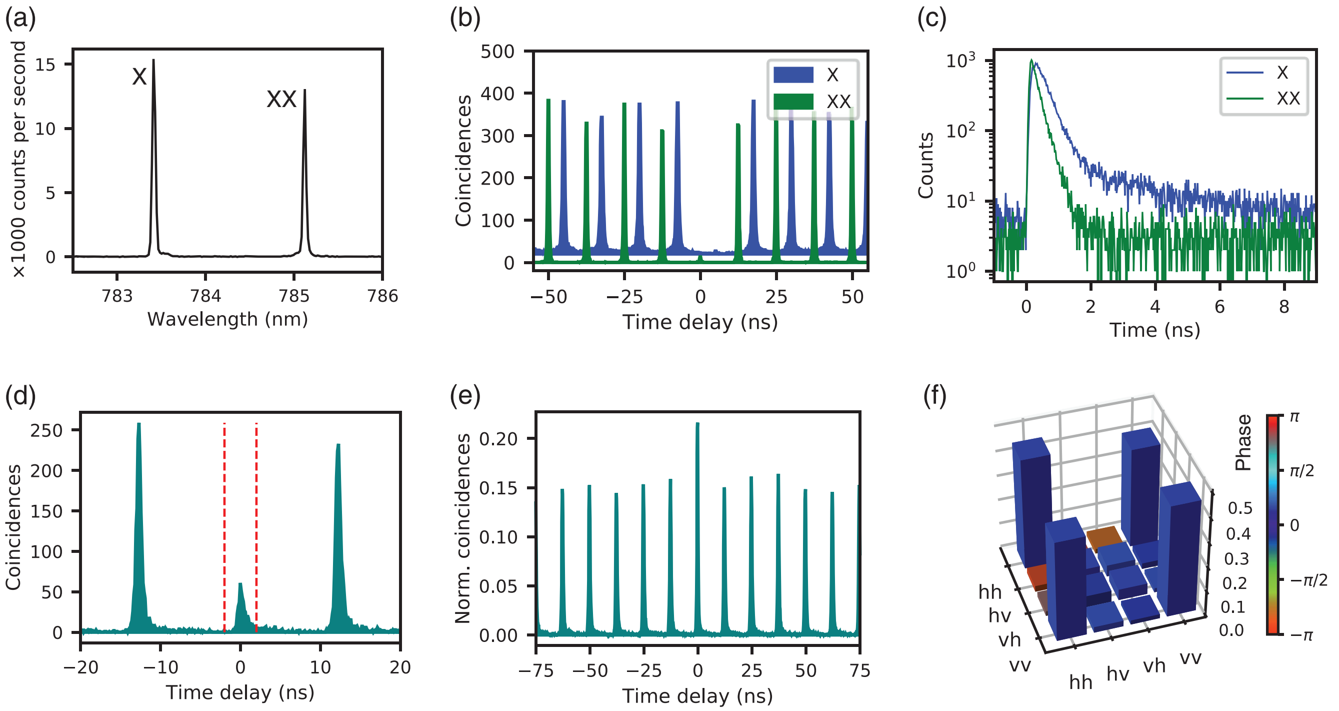

Fig. 2 Emission properties relevant for the polarization entanglement, measured at a temperature of 20 K. (a) Spectra of the individually filtered XX and X emission lines combined at a 50:50 fiber beam splitter. (b) Single-photon emission characteristics of the XX and X signals observed by detecting coincidences in a Hanbury–Brown–Twiss arrangement. The histogram for the X emission is shifted horizontally and vertically to facilitate reading. (c) Decay dynamics of the XX and X signals. The X signal exhibits a slow secondary decay channel, which is not present at temperatures lower than 10 K. (d) Examples among the 36 recorded coincidence histograms between the XX and X detections, corresponding to a measurement in the HV basis. The red-dashed lines indicate the time-bin of 2 ns, in which the coincidences are summed up to calculate the peak areas. (e) Unpolarized coincidence measurement between the XX and X photons. The excess coincidences at zero time delay stem from a nonunity photon-pair generation probability. (f) Density matrix of the two-photon polarization entangled state of the XX and X photons, recorded by full state tomography.

Table 1 Summarized emitter performance for two representative QDs in a diode structure excited by TPE, measured at temperatures of 5 K and 20 K, respectively.

	5 K		20 K	
Temperature	X	XX	X	XX
$g^{(2)}(0)$	0.017(4)	0.011(3)	0.020(3)	0.034(4)
Lifetime (ps)	238(3)	116(2)	252(9)	72(3)
Pair generation efficiency	0.91(2)		0.87(2)	
FSS (μeV)	1.13(7)		0.96(9)	
Calculated concurrence[a]	0.905		0.900	
Measured concurrence	0.904(3)		0.713(8)	
Calculated fidelity to $\vert\phi^+\rangle$[a]	0.959		0.960	
Measured fidelity to $\vert\phi^+\rangle$	0.975(1)		0.925(2)	

[a] Only considering expectation values of measured $g^{(2)}$, X lifetime, and FSS.[32]

and $g_X^{(2)}(0) = 0.020(3)$, which are comparable to previously measured values using the same optical arrangement at a temperature of 5 K (see Table 1), but with a slightly higher value for the XX signal. Compared to data acquired at 5 K, one can observe a broadening of the peaks belonging to the X signal. Inspecting the lifetime traces, which are shown for both the XX and X in Fig. 1(c), it becomes evident that this broadening stems from a slow decay channel of the X, which overlays with the monoexponential decay from the bright X to the ground state usually observed at 5 K (see the Supplementary Material for lifetime- and cross-correlation measurements at 5 K). A convoluted fit results in an X lifetime of $T_{1,\mathrm{X}} = 252(9)$ ps, with the caveat that this value is slightly overestimated due to the presence of the slow decay channel. The XX lifetime is measured as $T_{1,\mathrm{XX}} = 72(3)$ ps, which is significantly lower than the 120 ps typically observed at 5 K.

A full state tomography[33] is performed to determine the degree of entanglement between the XX and X photons. Figure 2(d) shows an example among the 36 recorded XX/X coincidence histograms, corresponding to a measurement in the HV basis. The red-dashed lines indicate the time-bin of 2 ns, in which the coincidences are summed up and compared with the average side peak area. The coincidences originating from the slow X decay channel (the "tail" on the right side of the peaks), which are partially excluded by this time-bin, account for about 9% of the total coincidences per excitation cycle. Figure 2(e) shows the weighted sum of the histograms corresponding to the measurement bases HH, VV, HV, and VH (where H is the horizontal, and V is the vertical polarization), normalized by their respective average side peak areas. From this histogram, a photon pair generation probability per excitation pulse of $\epsilon = 0.87(2)$ is calculated (see the Supplementary Material for details), which is marginally lower than the value of 0.91(2) observed at 5 K.

From the 36 correlation histograms, the 2-qubit density matrix in polarization space is calculated and depicted in Fig. 2(f). The maximum likelihood estimator used during this process is adapted for the dynamics of the QD light emission (see the Supplementary Material). The derived concurrence is 0.713(8), and the maximum fidelity to a Bell state is 0.925(5), which show a significant drop compared to the values obtained at 5 K. (We use the fidelity definition for mixed states[34] throughout this work.) We find that ρ at a temperature of 20 K can be approximated via Eq. (1) as $\rho = \rho_{\mathrm{M}}(S, T_{1,\mathrm{X}}, 1 - \overline{g} - \zeta)$, with $\overline{g} = [g^{(2)}_{\mathrm{XX}}(0) + g^{(2)}_{\mathrm{X}}(0)]/2$ the average $g^{(2)}(0)$ and $\zeta \approx 0.1$. The physical origin of the entanglement degrading effects, their temperature dependency, and their connection to the slow X decay channel appearing in the lifetime traces shown in Fig. 1(c) are subject of further investigation, as they could shed light on the changing dynamics of quasiparticles in GaAs QDs at higher temperatures.

The expected QBER of 7.45% calculated from ρ by Eq. (2) is still below the theoretical upper limit of 11% holding for the BBM92 protocol[6,8] and therefore suitable for performing QKD, as long as a sufficient amount of key bits are collected to mitigate finite key effects.[35]

4 Quantum Key Distribution with Entangled Photons

The XX and X photons in their individual single mode fibers are distributed to Alice and Bob, as shown in Fig. 3(a). The infrastructure is identical to the one used in a previous QKD experiment.[16] After an initial synchronization and polarization correction routine, the key generation is performed overnight for a total duration of about 8 h. The observed QBER, shown in Fig. 3(b), was evaluated periodically for 10% of the key bits (which were then discarded) and has an average value of 8.42%. The red-dashed line indicates the theoretical upper limit for the BBM92 protocol,[8] after which no finite key can be extracted from the raw key anymore.

The QBER shows a minimum of 6.15%, which is even lower than the 7.45% estimated from ρ, shown in Fig. 2(f). This discrepancy probably arises from the way in which the time-synchronization between Alice and Bob is maintained.

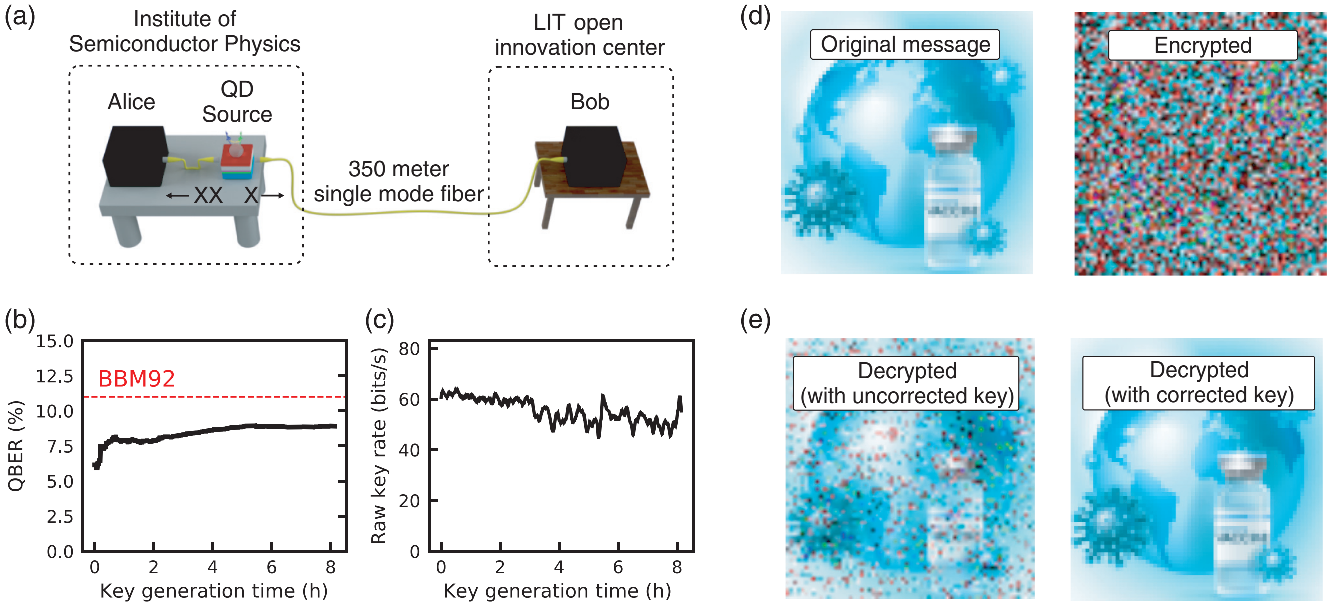

Fig. 3 Key generation in the BBM92 protocol over a time span of about 8 h and entanglement-based QKD. (a) QKD arrangement. Alice and the photon source are situated on an optical table, and Bob is placed in a movable box on a table in another building and connected with the source via a 350-m long single mode fiber. (b) QBER during the key generation with an average of 8.42%. The red-dashed line marks the maximum allowed QBER for BBM92 in the infinite key regime. (c) Raw key rate (after key sifting) with an average of 54.8 bits/s. (d) Encryption of a bitmap with the dimensions of 67 × 70 pixels and a color-depth of 4 bits, resulting in a total size of about 2.4 kilobytes. The encryption with Alice's key yields a scrambled message ready to be sent over a public channel. (e) Decryption at Bob's site when using an uncorrected key (left) and a corrected key (right).

To dynamically adjust the relative time delay between the arrival times of the XX and X photons at Alice and Bob, respectively, a peak in the continuously measured cross-correlation function is tracked. All photons around the peak maximum in a time window of 2 ns are used for key generation. We found that a shift of the center of this time-bin by 0.5 ns (about the time-resolution of our single photon detectors) can already change the QBER by around 2%, because a higher contribution of photons stemming from the slow X decay channel, shown in Fig. 2(c), decreases the entanglement (see the Supplementary Material for details). The time window during the key generation was therefore probably shifted with respect to the one used for calculating ρ. These findings are not only interesting for a better understanding of the underlying mechanisms degrading the entanglement at higher temperatures, but also indicate that with careful choice of the time window (within the limits of the detector resolution and clock synchronization among the communicating parties) a compromise between QBER and efficiency during the key generation process can be made.

We attribute the changing QBER over the course of the measurement to the following factors. The FSS changed from the initial 0.96(9) to 1.35(11) μeV over the course of the QKD measurements, which can add about 2% to the QBER due to an accelerated phase rotation process leading to a decreased fidelity to the ideal Bell state on average.[32] A changing FSS was never noticed before in these kinds of samples. A possible origin could be a changing strain state in the silver glue used to stick the sample on the chip carrier. The second contribution to a rising QBER could be a varying ambient temperature that affects the polarization rotation exerted by the fibers, which then leads to a larger deviation from the $|\phi^+\rangle$ Bell state, for which our QKD setup is designed. After the initial polarization correction, no active correction was performed during the 8 h of key generation.

Figure 3(c) shows the raw key generation rate after key sifting. A change in raw key rate over time occurs due to a slight drift of the cryostat relative to the objective, leading to a decreasing excitation and collection efficiency. We counter this effect by an automatized movement of the X/Y position of the cryostat via linear stages to optimize the average detector count rates, should they fall below a certain threshold. The average raw key rate over the full time span is found to be 54.8 bits/s. A total of 807,348 raw key bits were generated, corresponding to a duty cycle of about 50%. For the remaining 50% of time, the QKD system was blocked by the steps of compensating the drifts of the optics, key sifting, and QBER estimation, which were all performed sequentially to facilitate software and hardware error diagnosis. By parallelization of those steps, the duty cycle can be brought to 100%, as long as the data processing can keep up with the photon detection rate.

As the system presented here operates with an average QBER of 8.42% and therefore relatively close to the theoretical upper limit, the error correction and subsequent privacy amplification steps have to be chosen carefully to maximize the efficiency while leaking a minimum of information to a potential eavesdropper on the public channel. For this purpose, we adopt the security analysis recently employed for the Micius satellite QKD system,[10,35] where the setting is basically identical to our QKD system. This analysis addresses the effects of the estimated QBER in combination with a finite key length and adjusts the required key compression accordingly (see the Supplementary Material for details), leaving us with a total of 20,649 secure key bits after error correction.

The generated key is used to encrypt a bitmap with a size of 18,760 bits (about 2.4 kilobytes) [see Fig. 3(d)], using a one-time-pad procedure. The decryption is depicted in Fig. 3(e) for the cases when the raw/corrected key pair was used (left/right).

5 Discussion and Conclusion

In this work, we have demonstrated a blinking-free source of polarization-entangled photon pairs based on a GaAs QD operated at a temperature of at least 20 K. The intrinsically low FSS, owing to the local Al droplet etching technique,[14] together with the employed p-i-n diode allows us to generate an uninterrupted stream of photon pairs with a fidelity to the $|\phi^+\rangle$ Bell state of 0.925(2) when using the pulsed two-photon-excitation scheme.[20,21] The device also allows the fine-tuning of the emission wavelength within a range of 0.2 nm while keeping the blinking-free operation intact, which is favorable for interconnecting multiple sources to quantum networks.[3,4,24,30]

The source was used to demonstrate QKD via the BBM92 protocol[6] between two parties in two different buildings of the Johannes Kepler University, connected via a 350-m long underground single mode fiber. The average QBER was 8.42%. From the initial 807,348 key bits, a total of 20,649 error-free and privacy-amplified key bits could be distilled, using a state-of-the-art security analysis in the finite key regime.[35]

Comparing the decay dynamics of the biexciton and exciton states at temperatures of 20 K and 5 K allows us to identify a secondary slow decay channel of the exciton as the major entanglement degrading mechanism. While the physical origin of this observation and the elaboration of possible solutions will require further investigations, we find that the QBER during QKD can be optimized by a mild time filtering (see the Supplementary Material). This work makes us optimistic that combining electrical control with advanced photonic processing[36,37] and strain-tuning platforms[15,38] will lead to nearly ideal sources of entangled photon pairs that can be operated in demanding environments.

Acknowledgments

Christian Schimpf is a recipient of a DOC fellowship of the Austrian Academy of Sciences at the Institute of Semiconductor Physics at Johannes Kepler University, Linz, Austria. We thank C. Diskus for providing the Rb clocks used for QKD, M. Reindl and L. Costadedoi for their assistance in the optics laboratory, and K. Schweighofer for his contribution to the numerical optimization. Further, we thank P. Walther, M. Vyvlecka, and M. Bozzio for the continuous and fruitful discussion. This work was financially supported by the Austrian Science Fund (FWF) via the Research Group FG5, P 29603, P 30459, I 4320, I 4380, I 3762, the European Union's Horizon 2020 research and innovation program under Grant Agreements No. 899814 (Qurope) and No. 871130 (Ascent+), the Linz Institute of Technology (LIT), and the LIT Secure and Correct Systems Lab, supported by the State of Upper Austria. The authors declare no conflict of interest.

References

1. S. Pirandola et al., "Advances in quantum cryptography," *Adv. Opt. Photonics* **12**(4), 1012–1236 (2020).
2. X. Ma and J.-W. Pan, "Security of quantum key distribution with realistic devices," *Rev. Mod. Phys.* **92**(2), 025002 (2020).

3. N. Gisin and R. Thew, "Quantum communication," *Nat. Photonics* **1**(3), 165–171 (2007).
4. H. J. Kimble, "The quantum internet," *Nature* **453**(7198), 1023–1030 (2008).
5. A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**(6), 661–663 (1991).
6. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.* **68**(5), 557–559 (1992).
7. A. Acín et al., "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.* **98**(23), 230501 (2007).
8. N. Gisin et al., "Quantum cryptography," *Rev. Mod. Phys.* **74**(1), 145–195 (2002).
9. S. Wengerowsky et al., "Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre," *NPJ Quantum Inf.* **6**(1), 5 (2020).
10. J. Yin et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature* **582**(7813), 501–505 (2020).
11. X.-Y. Pan et al., "Temperature insensitive type II quasi-phase-matched spontaneous parametric downconversion," *Appl. Phys. Lett.* **119**(2), 021107 (2021).
12. J. Schneeloch et al., "Introduction to the absolute brightness and number statistics in spontaneous parametric down-conversion," *J. Opt.* **21**(4), 043501 (2019).
13. O. Benson et al., "Regulated and entangled photons from a single quantum dot," *Phys. Rev. Lett.* **84**(11), 2513–2516 (2000).
14. M. Gurioli et al., "Droplet epitaxy of semiconductor nanostructures for quantum photonic devices," *Nat. Mater.* **18**(8), 799–810 (2019).
15. D. Huber et al., "Strain-tunable GaAs quantum dot: a nearly dephasing-free source of entangled photon pairs on demand," *Phys. Rev. Lett.* **121**(3), 033902 (2018).
16. C. Schimpf et al., "Quantum cryptography with highly entangled photons from semiconductor quantum dots," *Sci. Adv.* **7**(16), aebe8905 (2021).
17. Y. H. Huo, A. Rastelli, and O. G. Schmidt, "Ultra-small excitonic fine structure splitting in highly symmetric quantum dots on GaAs (001) substrate," *Appl. Phys. Lett.* **102**(15), 152105 (2013).
18. L. Schweickert et al., "On-demand generation of background-free single photons from a solid-state source," *Appl. Phys. Lett.* **112**(9), 093106 (2018).
19. F. Basso Basset et al., "Quantum key distribution with entangled photons generated on demand by a quantum dot," *Sci. Adv.* **7**(12), eabe6379 (2021).
20. R. Hafenbrak et al., "Triggered polarization-entangled photon pairs from a single quantum dot up to 30 K," *New J. Phys.* **9**(9), 315 (2007).
21. M. Müller et al., "On-demand generation of indistinguishable polarization-entangled photon pairs," *Nat. Photonics* **8**(3), 224–228 (2014).
22. K. D. Timmerhaus and R. Reed, *Cryogenic Engineering*, Springer (2007).
23. J. P. Jahn et al., "An artificial Rb atom in a semiconductor with lifetime-limited linewidth," *Phys. Rev. B* **92**(24), 245439 (2015).
24. K. D. Jöns et al., "Two-photon interference from two blinking quantum emitters," *Phys. Rev. B* **96**(7), 075430 (2017).
25. R. J. Warburton et al., "Optical emission from a charge-tunable quantum ring," *Nature* **405**(6789), 926–929 (2000).
26. L. Zhai et al., "Low-noise GaAs quantum dots for quantum photonics," *Nat. Commun.* **11**(1), 4745 (2020).
27. N. Somaschi et al., "Near-optimal single-photon sources in the solid state," *Nat. Photonics* **10**(5), 340–345 (2016).
28. S. Stufler et al., "Two-photon Rabi oscillations in a single $In_xGa_{1-x}As$ GaAs quantum dot," *Phys. Rev. B* **73**(12), 125304 (2006).
29. V. Giesz et al., "Cavity-enhanced two-photon interference using remote quantum dot sources," *Phys. Rev. B* **92**(16), 161302 (2015).
30. M. Reindl et al., "Phonon-assisted two-photon interference from remote quantum emitters," *Nano Lett.* **17**(7), 4090–4095 (2017).
31. R. Keil et al., "Solid-state ensemble of highly entangled photon sources at rubidium atomic transitions," *Nat. Commun.* **8**(1), 15501 (2017).
32. A. J. Hudson et al., "Coherence of an entangled exciton-photon state," *Phys. Rev. Lett.* **99**(26), 266802 (2007).
33. D. F. V. James et al., "Measurement of qubits," *Phys. Rev. A* **64**(5), 052312 (2001).
34. R. Jozsa, "Fidelity for mixed quantum states," *J. Mod. Opt.* **41**(12), 2315–2323 (1994).
35. C. C. W. Lim et al., "Security analysis of quantum key distribution with small block length and its application to quantum space communications," *Phys. Rev. Lett.* **126**(10), 100501 (2021).
36. J. Liu et al., "A solid-state source of strongly entangled photon pairs with high brightness and indistinguishability," *Nat. Nanotechnol.* **14**(6), 586–593 (2019).
37. H. Wang et al., "On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability," *Phys. Rev. Lett.* **122**(11), 113602 (2019).
38. R. Trotta et al., "Energy-tunable sources of entangled photons: a viable concept for solid-state-based quantum relays," *Phys. Rev. Lett.* **114**(15), 150502 (2015).
39. J. Martinez-Mateo et al., "Demystifying the information reconciliation protocol cascade," *Quantum Inf. Comput.* **15**(5–6), 453–477 (2015).
40. Z. Yuan et al., "10-Mb/s quantum key distribution," *J. Lightwave Technol.* **36**(16), 3427–3433 (2018).

Christian Schimpf's academic career started in 2012 with the beginning of his physics studies at the Johannes Kepler University Linz, Austria, where he is currently in the later stage of his PhD studies. His research focus lies on semiconductor quantum dots, with emphasis on the generation of non-classical light for quantum optics and applications in the context of quantum communication.

Santanu Manna received his PhD in physics from Indian Institute of Technology Kharagpur, India, in 2014. He is currently a university assistant in the Institute of Semiconductor and Solid State Physics, Johannes Kepler University Linz, Austria. His research interest lies in the epitaxial growth by molecular beam epitaxy, device fabrication and measurements on III–V semiconductor based quantum devices like single/entangled photon emitters, quantum cascade laser based frequency comb and THz emitters.

Saimon F. Covre da Silva: Biography is not available.

Maximilian Aigner is a master student in the Department of Semiconductor and Solid State Physics at the Johannes Kepler University Linz, Austria. His research is focused on quantum dot based quantum optics, especially on entanglement related experiments.

Armando Rastelli is professor of semiconductor physics since 2012 and corresponding member of the Austrian Academy of Sciences since 2019. His main current focus is on the optimization of GaAs quantum dots as quantum light sources and their post-growth control via microstructured piezoelectric actuators for applications in photonic quantum science and technologies. He is coauthor of more than 230 peer-reviewed papers and has given 100 invited talks on the research activities of his group.