ARTICLE OPEN

Check for updates

Enhancing quantum cryptography with quantum dot single-photon sources

Mathieu Bozzio[1,5]✉, Michal Vyvlecka[1,5]✉, Michael Cosacchi[2], Cornelius Nawrath[3], Tim Seidelmann[2], Juan C. Loredo[1,4], Simone L. Portalupi[3], Vollrath M. Axt[2], Peter Michler[3] and Philip Walther[1,4]

Quantum cryptography harnesses quantum light, in particular single photons, to provide security guarantees that cannot be reached by classical means. For each cryptographic task, the security feature of interest is directly related to the photons' non-classical properties. Quantum dot-based single-photon sources are remarkable candidates, as they can in principle emit deterministically, with high brightness and low multiphoton contribution. Here, we show that these sources provide additional security benefits, thanks to the tunability of coherence in the emitted photon-number states. We identify the optimal optical pumping scheme for the main quantum-cryptographic primitives, and benchmark their performance with respect to Poisson-distributed sources such as attenuated laser states and down-conversion sources. In particular, we elaborate on the advantage of using phonon-assisted and two-photon excitation rather than resonant excitation for quantum key distribution and other primitives. The presented results will guide future developments in solid-state and quantum information science for photon sources that are tailored to quantum communication tasks.

npj Quantum Information (2022)8:104 ; https://doi.org/10.1038/s41534-022-00626-z

INTRODUCTION

With the rise of quantum algorithms capable of breaking modern encryption schemes, there follows a global response to search for stronger security levels[1–3]. While the security of most current schemes relies on the complexity of solving difficult mathematical problems, quantum-mechanical laws can provide security against adversaries endowed with unlimited computational power for some tasks[4,5]. This type of security, known as information-theoretic security, motivates research towards a quantum internet[6].

Modern communication networks rely on a handful of fundamental building blocks, known as cryptographic primitives[7,8]. These can be combined with one another to provide security in various applications such as message encryption, electronic voting, digital signatures, online banking, anonymous messaging, and software licensing, to name a few. In order to reach information-theoretic security through quantum primitives, information is typically encoded onto quantum properties of light, such as photonic path, time-bin, polarization, and photon number[5]. In the quantum realm, the uncertainty principle then ensures that any eavesdropper attempting to access quantum-encoded information, while unaware of the preparation basis, will alter the quantum states in a way that is detectable by the honest parties[4,9].

For such quantum primitives, it is expected that quantum dot-based single-photon sources (QDS) can excel by generating photons on-demand, with high brightness and low multiphoton contribution[10,11]. In fact, source brightness is crucial in achieving high-speed quantum communication[12,13], while low multiphoton contribution minimizes information leakage to a malicious eavesdropper[14]. In contrast to these on-demand single-photon sources, widely used Poisson-distributed sources (PDS), such as attenuated laser states[5] and spontaneous parametric down-conversion[15], suffer from a stringent trade-off between high brightness and low multiphoton emission. Despite elaborate countermeasures proposed to overcome this trade-off[16,17], the distance and rate of secure quantum communication can be increased using on-demand single-photon sources.

Some pioneering works have already implemented instances of quantum key distribution (QKD) employing QDS[18–25] or other single-photon sources[26,27], comparing their performance to PDS in terms of secret key rate. In these works, brightness and purity are the sole figures of merit used to establish a comparison, while the additional tuning capabilities of QDS and their role in quantum cryptography have not yet been investigated.

In this work, we explore features of QDS to enhance the performance and security of quantum-cryptographic primitives, with an emphasis on telecom wavelengths. We first optimize and compare the brightness and single-photon purity of three main optical pumping schemes, using realistic intra-cavity simulations of quantum dot dynamics. We then show how photon-number coherence generated from QDS, experimentally demonstrated in[28], can be erased or preserved to boost the performance of practical QKD, and match its fundamental security requirements[17,29]. We further explain how the field of mistrustful quantum cryptography[7,8], not yet implemented with QDS, can significantly benefit from this feature. Our findings are designed to bridge the gap between the quantum dot and quantum cryptography communities: we optimize and benchmark QDS optical pumping schemes for four main quantum cryptographic primitives, exploiting the combined advantage of brightness, single-photon purity, and photon-number coherence. The studied primitives include quantum key distribution (standard BB84, decoy and twin-field)[5,16,30,31], unforgeable quantum tokens[32–34],

[1]University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), University of Vienna, 1090 Vienna, Austria. [2]Theoretische Physik III, Universität Bayreuth, 95440 Bayreuth, Germany. [3]Institut für Halbleiteroptik und Funktionelle Grenzflächen (IHFG), Center for Integrated Quantum Science and Technology (IQST) and SCoPE, University of Stuttgart, 70569 Stuttgart, Germany. [4]Christian Doppler Laboratory for Photonic Quantum Computer, Faculty of Physics, University of Vienna, 1090 Vienna, Austria. [5]These authors contributed equally: Mathieu Bozzio, Michal Vyvlecka. ✉email: mathieu.bozzio@univie.ac.at; michal.vyvlecka@univie.ac.at

quantum strong coin flipping[35–37], and quantum bit commitment[38–40] under storage assumptions.

RESULTS

Comparison of pumping schemes

Solid-state single-photon sources can be excited under different optical pumping schemes, and we aim to provide a fair comparison of their performance for quantum cryptography. Using realistic intra-cavity simulations for GaAs-based QDS, we calculate the emitted photon-number occupations up to three photons for resonant excitation (RE), longitudinal phonon-assisted (LA) excitation and two-photon excitation (TPE). In Fig. 1, we then compare each scheme's brightness and single-photon purity, and estimate the full-width-at-half-maximum excitation pulse length which maximizes both properties (marked with black symbols).

RE schemes are based on resonant excitation of a two-level system[41–43]. The spectral degeneracy of the excitation laser and the emitted photons usually imposes separation based on polarization filtering, which may cause significant collection losses of around 50%[42,44]. Other methods, exploiting dichromatic pumping or trion recombination in asymmetric cavities however, can overcome such limitations[45,46]. Since RE exhibits Rabi oscillations of the excitonic state populations, its brightness and single-photon purity are susceptible to pump power fluctuations—thus presenting challenges for quantum network applications[47]. As we show in Fig. 1a, for a fixed RE π-pulse area, single-photon purity decreases with pulse length due to re-excitation processes, while brightness decreases as the emission statistics tend to a Poisson distribution[48,49].

The main limitations of RE may be overcome by using LA excitation schemes. Here, the pump energy is slightly higher than the relevant excitonic transition, and the fast emission of a longitudinal-acoustic (LA) phonon precedes the population of the excited state. Due to this additional incoherent step, Rabi oscillations vanish, and the purity of the emitted single photons becomes less sensitive to small pump power fluctuations[50]. Recently, it was shown that LA excitation can reach even smaller multiphoton components than its RE counterpart[51], while still enabling spectral filtering of the pump[52,53]. As regards to brightness, Fig. 1b displays an increase with pulse length, as was experimentally demonstrated in[52]. With longer pulses however, the peak intensity decreases for a fixed pulse area, thus lowering the efficiency of the phonon excitation process.

RE and LA multiphoton contributions can be greatly reduced by addressing the exciton-biexciton cascade through TPE schemes, usually employed to generate spectrally-separated entangled photon pairs. Here, the re-excitation probability scales quadratically with the pulse length, as opposed to linearly in the resonantly-driven RE scheme[49], which can reduce multiphoton emission by several orders of magnitude[54]. Moreover, TPE offers the possibility to overcome the collection efficiency limitations of RE: the spectral separation of the generated photons allows for frequency filtering of the pump laser[55], avoiding the polarisation filtering losses. We show in Fig. 1c that the brightness is low for short pulse lengths, due to a remaining overlap with the exciton transition, causing the biexciton level to be only partially populated. Although the emitted exciton polarization is random, which would limit the brightness to half the values of Fig. 1c, recent works have shown the possibility of deterministically preparing the exciton polarization with near-unit brightness by adding a stimulated biexciton excitation after the original two-photon excitation[56–58].

Photon-number coherence

We now discuss the presence of coherence in the photon-number basis, a usually disregarded feature of interest, under each excitation scheme. For PDS such as attenuated laser states, this quantity refers to a fixed phase relationship between the various Poisson-distributed number states. For QDS, this will materialize as a coherent superposition of vacuum, single and two-photon states.

In RE, it was experimentally demonstrated in[28] that the coherently-driven Rabi oscillations translate into emitted photon-number coherence: values of coherence purity as high as 96% for π-pulse areas were measured. On the other hand, this coherence can gradually vanish as the pump is detuned from resonance in LA schemes, along with the vanishing of Rabi oscillations[51]. Our quantum dot dynamics simulations support these findings: for the optimal pulse lengths of Fig. 1, the normalized off-diagonal density matrix elements of LA between the vacuum and single-photon components are around 10 times smaller than the RE ones. Accordingly, we will assume in this work that states emitted under RE are pure in photon-number basis,

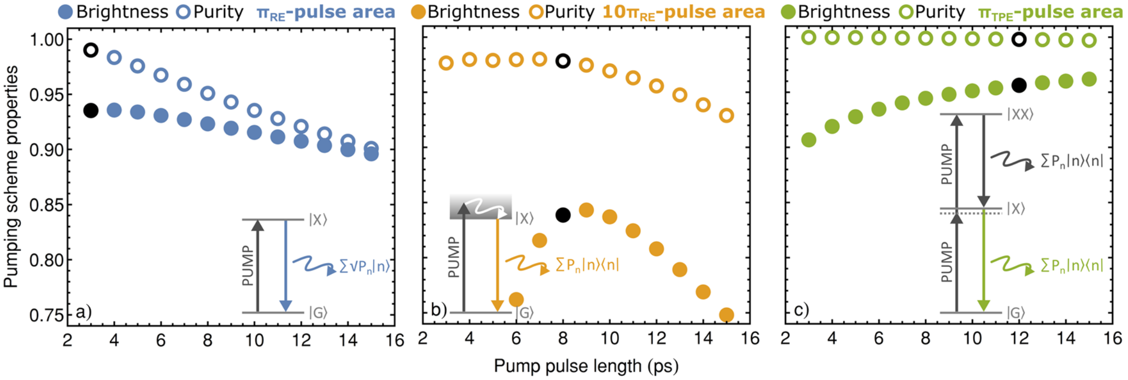

Fig. 1 Simulation of emission properties under different pumping schemes. Simulated brightness and single-photon purity for individual pumping schemes calculated from our numerical model (see Methods) for (**a**) resonant excitation (RE) between ground $|G\rangle$ and exciton $|X\rangle$ states, (**b**) longitudinal phonon-assisted excitation (LA) (**c**) two-photon excitation (TPE) between ground $|G\rangle$ and biexciton $|XX\rangle$ states. Insets show a schematic representation of each pumping scheme (the upper grey area in the LA sketch represents the vibrational quasi-continuum of the exciton state). Optimal FWHM pulse lengths are marked with black disks and circles, chosen pulse areas for maximum population inversion are π_{RE} for RE and π_{TPE} for TPE, while we choose $10\pi_{RE}$ for LA. Simulation parameters are: dot-cavity coupling $\hbar g = 50\,\mu$eV, radiative decay rate $\hbar\gamma = 0.66\,\mu$eV, cavity loss rate $\hbar\kappa = 379\,\mu$eV (yielding a Purcell factor of $P = 10$), initial system temperature $T = 4.2$K, electron confinement length 3 nm, and material properties typical for GaAs. Throughout the paper, we assume that photonic states are maximally pure in the photon-number basis for RE, i.e. expressed as $\sum_{n=0}^{\infty}\sqrt{p_n}|n\rangle$, while they are expressed as diagonal states for LA and TPE, i.e. as $\sum_{n=0}^{\infty} p_n|n\rangle\langle n|$.

while those emitted under LA present vanishing off-diagonal elements.

In TPE, our simulation results display off-diagonal elements around 20 times smaller than the RE ones. Although the biexciton level follows Rabi oscillations under resonant TPE[54,55], loss of coherence arises from a radiative decay between the biexciton to exciton state, which creates a timing jitter similar to the phonon-induced jitter in LA schemes. We will therefore also assume that states emitted under TPE present vanishing off-diagonal elements. Note that this assumption is expected to hold for the stimulated schemes discussed in[56–58], since the remaining jitter due to the biexciton transition is significantly larger than the jitter responsible for coherence erasure.

Practical sources and security

We now discuss the role of brightness, single-photon purity and photon-number coherence in quantum primitives involving two parties, exchanging a sequence of classical and quantum (photonic) messages that do not rely on quantum entanglement. Each of these primitives achieves a different functionality within quantum networks, and thus also requires its own security figure of merit.

The main efficiency limitations of PDS may be understood upon inspection of the generated state $\sum_{n=0}^{\infty} C_\mu(n)|n\rangle$, where the $P_\mu(n) = |C_\mu(n)|^2$ coefficients follow a Poisson distribution with average photon number μ, and $\{|n\rangle\}$ span the photon-number basis. Increasing the source brightness (i.e., increasing μ) comes at the cost of increasing the multiphoton components $n \geqslant 2$, which renders the respective quantum primitive vulnerable to attacks involving photon number splitting on lossy channels[14]. Thus, μ is typically kept very low in quantum-cryptographic implementations, in the range $\mu \sim 0.005$–0.5[5,32,35,39], which limits the communication rate. On the other hand, single-photon purity in QDS can be increased without an intrinsic penalty on the multiphoton component. Achieving higher QDS brightness is then ultimately a technological challenge, limited by the collection efficiency of the source[11,46], and not a fundamental limitation as in the case of PDS.

In contrast to their PDS counterparts, QDS have not yet been optimized to suit the security requirements of quantum primitives. Most importantly, a main assumption behind the implementation of decoy QKD and other primitives is that the global phase of PDS must be actively scrambled, to effectively destroy the coherence in the number basis[17,29]:

$$\sum_{n=0}^{\infty} C_\mu(n)|n\rangle \xrightarrow[\text{scrambling}]{\text{phase}} \sum_{n=0}^{\infty} P_\mu(n)|n\rangle\langle n|. \qquad (1)$$

Under this assumption, the adversary's cheating strategy is restricted to performing an attack conditioned on the photon-number content of each pulse. Many works rely on this feature to prove the security of quantum primitive implementations[5,16,31,32,35].

Achieving phase randomization with active phase modulation or laser gain switching imposes practical limitations of a few GHz on repetition rates[12,59]. These limitations, combined with the low values of μ required due to fundamental PDS source statistics, can bring effective communication rates down to a few MHz. Unwanted remnants of coherence in the number basis, furthermore, can be exploited for a large spectrum of attacks, using unambiguous state discrimination for instance[60,61]. In contrast, as discussed in this work, QDS can be excited in such a way that this coherence is intrinsically suppressed, thus circumventing the need for active phase scrambling. With demonstrated Purcell-enhanced photon lifetimes of tens of picoseconds[46,62] and source efficiencies now beyond the 50% level[46], QDS have the potential to enable secure communication rates of tens of GHz[13], i.e. around 3 orders of magnitude higher than effective PDS communication rates. This is not only true for QKD but for many quantum primitives as shown in the following sections.

Quantum key distribution

A few decades after the birth of quantum key distribution (QKD)[4], experimentalists started demonstrating that QDS with low collection efficiencies can already outperform PDS in terms of secret key rate[22–25]. We first show that, while this is true for standard QKD implemented without the decoy-state countermeasure, beating PDS with decoy states[16] requires much higher QDS collection efficiencies at an equal repetition rate. Our results, based on the optimal performance of pumping schemes in Fig. 1, are displayed in Fig. 2: without decoy states (*a*), QDS with collection efficiency 1% are enough to outperform PDS after 100 km, while infinite decoy schemes (*b*) require at least 30%. We should emphasize, however, that this benchmark must be scaled by a repetition rate factor for QDS which could achieve considerably higher repetition rates than phase-randomized PDS. Any state preparation losses, including modulator losses,

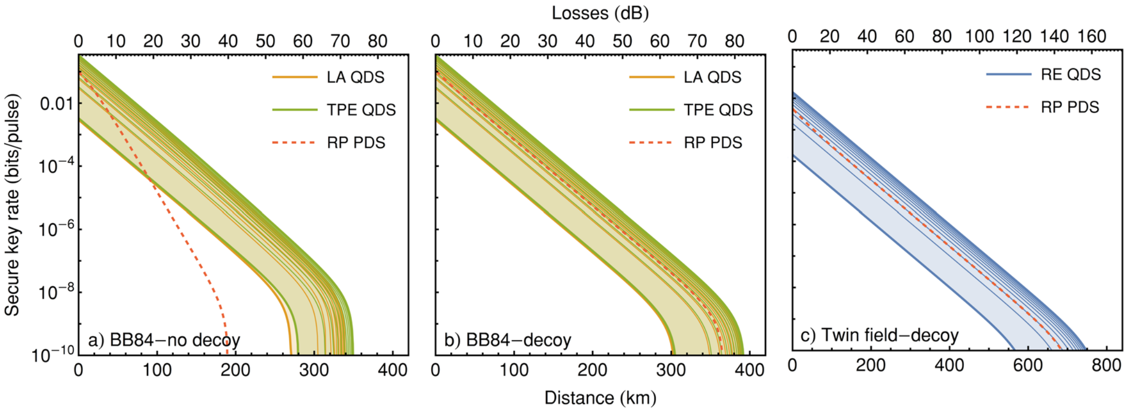

Fig. 2 Source comparison for three main QKD schemes. Simulated secret key rates using one-way classical post-processing[82,83] for (**a**) BB84 without decoy states, (**b**) BB84 with infinite decoy states, (**c**) twin-field with infinite decoy states. The continuum in each plot shows the attainable key rates for QDS ranging from 1 to 100% collection efficiencies, with intermediate curves showing steps of 10%. The dashed line indicates the optimal performance of randomized-phase (RP) PDS. For QDS, pulse lengths were chosen to simultaneously maximize the brightness and single-photon purities from Fig. 1: 3 ps for RE, 8 ps for LA, 12 ps for TPE. Chosen pulse areas: π_{RE} for RE, $10\pi_{\mathrm{RE}}$ for LA, π_{TPE} for TPE. photon-number populations $\{p_n\}$ up to $n = 3$ were inferred from the subsequent values of brightness and single-photon purity. Parameters for all plots are: $e = 2\%$ single photon error rate, 0.21 dB/km single mode telecom fiber losses, $Y_0 = 10^{-9}$ dark count probability, unit detection efficiency, and error-correcting code inefficiency $f = 1.2$.

can be absorbed in the QDS collection efficiency, and the resulting key rate inferred from Fig. 2. Comparisons can also be established using finite (and different) number of decoy intensities for QDS and PDS.

The optimal pumping scheme for QKD then follows from Eq. 1: the states' global phase must be uniformly randomized[17,29], which implies that standard and decoy-state QKD should only be implemented with LA and TPE. Any remaining photon-number coherence will lead to a decrease in the secure key rate, as shown in[29].

Twin-field QKD, on the other hand, requires two states, generated by Alice and Bob, to interfere on an untrusted party's beamsplitter[30,31]. This forces Alice and Bob to scramble the global phase of their states in an active manner (using a modulator for instance), such that they can record their original fixed phase encoding. We therefore argue that twin-field schemes must be implemented with RE QDS, in order to provide the two parties with a shared phase reference before the scrambling. We simulate the protocol performance of[31] under these conditions in Fig. 2c, assuming the implementation of decoy states. We note that performing TF-QKD with a perfect single photon source (RE π-pulse and unit single-photon purity) is impossible, since there is no accessible phase to encode the key information. However, by decreasing the pulse area a little below π, in the same manner as[28], it is possible to create a coherent superposition of vacuum and single-photon, thus providing an accessible phase to perform the protocol.

Our results are focused on QKD implemented with discrete degrees of freedom, such as polarization or time-bin. For completeness, we note the existence of QKD protocols optimized for continuous degrees of freedom of PDS, such as phase and amplitude[63]. These can actually compete with discrete-variable QKD over metropolitan distances, using simpler technology, but are sensitive to larger attenuations due to heavier post-selection and noise estimation techniques[64,65].

Quantum primitives beyond QKD

Quantum cryptography presents a broad spectrum of other primitives, many of which belong to the branch of mistrustful cryptography[7,8]: unlike in QKD, Alice and Bob are not collaborators, but adversaries wishing to compute a common function. Decoy-state methods are then more challenging to apply (although not impossible for all protocols), since Alice and Bob do not trust each other.

Remarkably, the desired security properties for such primitives can be very sensitive to photon-number coherence. In this instance, substituting PDS by appropriately optimized QDS can yield even more benefits than in QKD. To show this, we extend the practical security analyses of three mistrustful quantum primitives[32,35,38] to the QDS framework, and estimate the QDS collection efficiencies required to outperform PDS for the relevant security figures of merit. Our performance results are summarized in Table 1 for all primitives.

We display the performance of QDS and PDS for one example primitive in Fig. 3: unforgeable quantum tokens. This primitive allows a central authority to issue tokens, comprised of quantum states, whose unforgeability is intrinsically guaranteed by the no-cloning theorem, thus requiring no hardware assumptions. One famous application is quantum money, which, in its private-key form, can prevent banknote forgery[9], double-spending with credit cards[32,66] and guarantee features such as user privacy[34].

In Fig. 3a, we compare the noise tolerance of the quantum token scheme from[66] for PDS and QDS as a function of source efficiency. Noise tolerance indicates how much experimental error rate can be tolerated such that the unforgeability property holds, while source efficiency is the probability that a threshold single-photon detector will click in a lossless setting. Naturally, PDS reach a maximal noise tolerance for source efficiencies around 63%, corresponding to $\mu \approx 1$, before dropping again when the multi-photon contribution becomes too significant. For QDS, we notice a striking difference between schemes with coherence (RE) and those without (LA and TPE): the latters give an overhead of almost 2% on the noise tolerance with respect to RE at high source efficiencies. This difference is crucial in making implementations feasible, since boosting the fidelity of quantum state preparation and quantum storage by a few percent can be extremely challenging. These differences are also reflected in Fig. 3b, which identifies the collection efficiencies at which QDS can outperform the best PDS performance: while LA and TPE require 44% and 38%, respectively, RE must be pushed to 47% to beat PDS. For information purposes, we also select three state-of-the art experimental QDS, and show how they would perform in such a beyond-QKD protocol with their reported values of brightness and single-photon purity.

Figure 3c finally compares the performance of each source as a function of distance. Once again, the difference between LA/TPE and RE is significant due to the coherence feature. We notice here that the maximal distance for all sources is much shorter than in QKD schemes, since our selected quantum token scheme bears a maximal loss tolerance of 50%: above this limit, an adversary can clone the quantum token without introducing any errors[66].

Our work showcases the importance of engineering optical pumping schemes towards specific primitives. Table 1 displays non-trivial requirements for quantum strong coin flipping for instance: unlike with QKD and quantum tokens, QDS perform better at lower collection efficiencies, thus rendering state-of-the art QDS already capable of providing quantum advantage in such mistrustful primitives. Furthermore, the absence of photon number coherence in LA and TPE allow these schemes to reach quantum advantage over significantly longer distances than RE schemes: for the selected protocol from[35], these values read 86 km and 36 km for TPE and LA, respectively, vs. 25 km for RE.

DISCUSSION

We have estimated threshold collection efficiencies for which GaAs-based quantum-dot photon sources can outperform Poisson-distributed-based implementations in four main quantum-cryptographic primitives. The estimations include the combined effect of brightness, single-photon purity, and photon-number coherence. We have shown in particular that resonant excitation should be used for twin-field QKD, but not for decoy QKD and other quantum primitives due to the unwanted presence of photon-number coherence that violates practical security assumptions.

We believe that these results will provide a benchmark for future achievements in quantum dot cavity structures, especially at telecom wavelengths[13,67–69]. Although state-of-the-art dot-cavity simulation frameworks cannot account for all characteristics of quantum dots emitting in the telecom range, current telecom performance[13,70,71] shows good agreement with our 900nm framework: the brightness and purities are not strongly dependent on the emission wavelength. Furthermore, frequency conversion of 900nm photons to telecom photons can currently reach efficiencies up to 57%[72]. These extra losses can be absorbed in our collection efficiency quantity.

We wish to encourage future quantum key distribution experiments with optimal pumping schemes, taking into account the security assumptions provided by the quantum cryptography community. Finally, we hope to stimulate experiments that explore the full potential of quantum dot-based single-photon sources for other quantum network primitives like unforgeable tokens[32–34], coin flipping[35,36] and bit commitment[38–40]. We believe our analysis can be extended in future works to multipartite entanglement-based quantum network primitives, such as secret sharing[73] and anonymous messaging[74].

Table 1. QDS performance for the main quantum primitives.

				Zero distance		Distance		
Primitive	Description	Figure of merit	Optimal pumping	Threshold collection	QDS 100%/	Loss tolerance - km (dB)		
	Applications			*T*%	Max PDS	QDS *T*%	QDS 100%	PDS
Key distribution BB84 -no decoy	Alice and Bob wish to establish a secret key over a public channel.	Secret key rate	TPE	30	3.3	331 (70)	350 (74)	190 (40)
			LA	34	2.9	323 (68)	339 (71)	
	Message encryption, digital signatures, channel authentication.							
BB84 -decoy			TPE	33	3.1	375 (79)	393 (83)	366 (77)
			LA	37	2.6	375 (79)	390 (82)	
Twin field -decoy			RE	29	3.3	738 (155)	778 (163)	714 (150)
Unforgeable tokens	Alice issues a token to Bob, such that he may use it only once.	Noise tolerance	TPE	38	2.6	14 (3)	14 (3)	11 (2.3)
	Unforgeable money, license/copy protection, one-time programs.		LA	44	2.2	13.7 (2.9)	14 (3)	
			RE	47	2.0	12.9 (2.8)	14 (3)	
Coin flipping	Alice and Bob wish to remotely toss a fair coin, such that none of the two parties can bias	Quantum advantage (for bias)	TPE	49	N/A	100 (21)	86 (18)	N/A
			LA	16	N/A	73 (10)	36 (8)	
			RE	<24	N/A	<82 (17)	<25 (5)	
	The outcome towards their preferred value.							
	Multiparty computing, leader election/e-voting, secure online gaming.			for 1000 states and 1.5% honest abort		⚠ lower collections perform better than higher ones		
Bit commitment (under bounded storage)	Alice sends a bit to Bob, such that: (1) Alice cannot change the bit after committing to its value, (2) Bob cannot discover the value until she reveals it.	Security threshold	TPE	17	9.6	17.9 (3.9)	41.0 (9)	10.2 (2.2)
			LA	19	7.9	17.6 (3.9)	53.5 (11.8)	
	Multiparty computing, zero-knowledge proofs, verifiable secret sharing.							

A description of each primitive is provided, along with its main network applications, and our chosen security figure of merit. In each case, we summarize the various QDS pumping scheme performances and the threshold collection efficiencies T required to outperform PDS in a lossless setting. We then display the performance ratio of QDS with 100% collection over the best PDS at zero distance (note that this ratio has to be scaled for QDS achieving higher repetition rates than PDS). We then calculate the loss tolerance, both in terms of distance (in km) assuming single-mode telecom fiber losses of 0.21 dB/km, and in terms of absolute losses (in dB) for QDS reaching T% collection, QDS reaching 100% collection, and randomized-phase PDS.

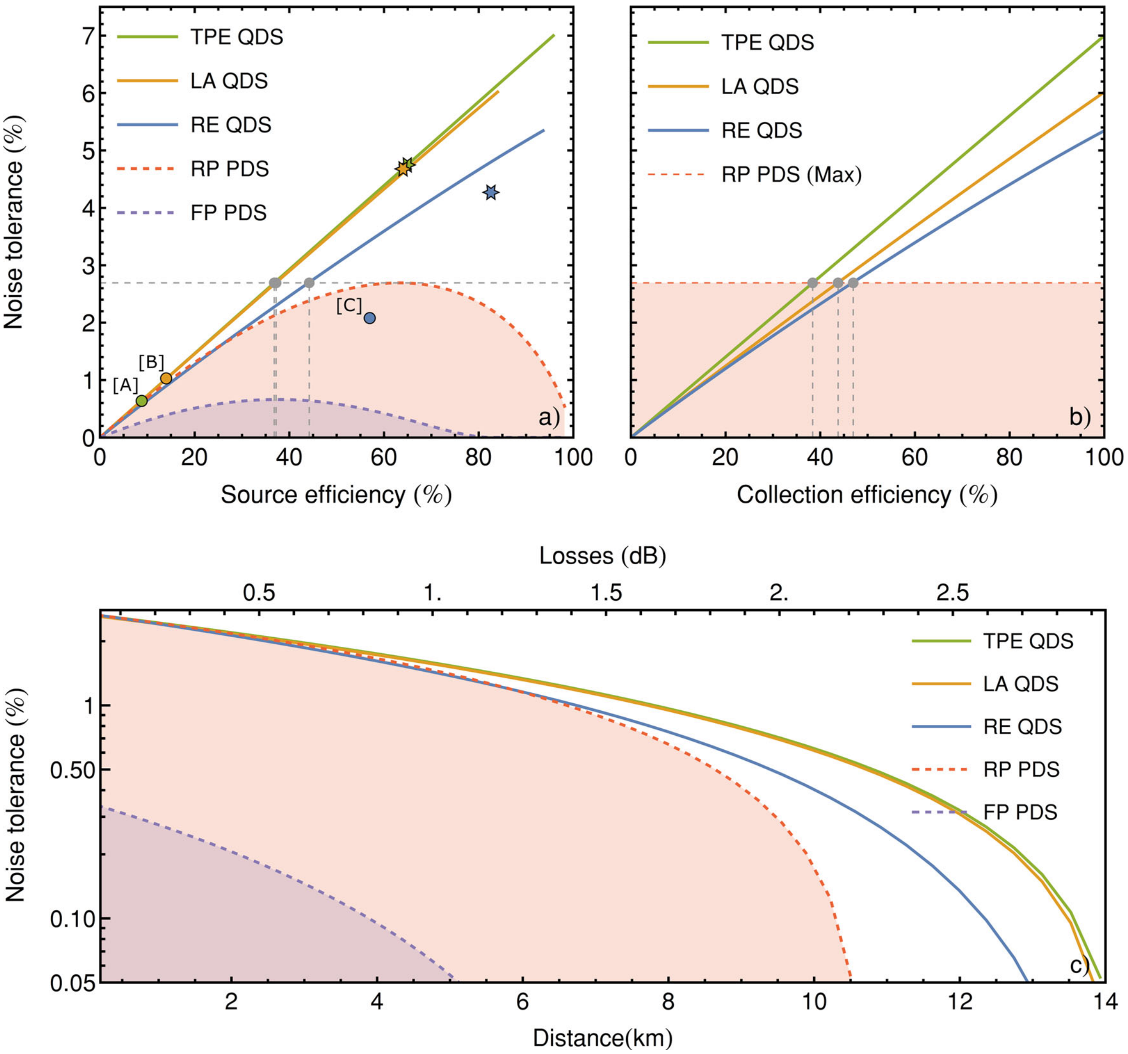

Fig. 3 Source comparison for unforgeable quantum tokens (quantum verification protocol from[66]). a Numerical noise tolerance as a function of source efficiency for RE, LA and TPE QDS, along with fixed-phase (FP) and randomized-phase (RP) PDS. Source efficiency is defined as $1-e^{-\mu}$ for PDS and $1-\sum_{n=0}^{\infty} p_n(1-\eta)^n$ for QDS, where η is the QDS collection efficiency. Photon-number populations $\{p_n\}$ emitted under different QDS excitation schemes were obtained from the brightness and single-photon purity results of Fig. 1, assuming the optimal pulse lengths marked in black. RE photonic states are assumed to be maximally pure in number basis, expressed as $\sum_{n=0}^{\infty} \sqrt{p_n}|n\rangle$, while LA states were expressed as diagonal states $\sum_{n=0}^{\infty} p_n|n\rangle\langle n|$. Colored circles indicate the performance of three state-of-the-art quantum dots, inferred from the experimental brightness and purity values reported in [A]=[84], [B]=[85], [C]=[46], corrected to unit detector efficiency. Stars indicate the potential of these quantum dots assuming the reported collection losses, but no setup losses. **b** Numerical noise tolerance as a function of QDS collection efficiency, compared to the best performance of PDS sources (dashed line). **c** Numerical noise tolerance plotted as a function of distance, assuming single mode telecom fiber losses of 0.21 dB/km. The QDS collection efficiencies were chosen as the intersection points from (**b**), also summarized in Table 1.

METHODS

Quantum dot dynamics

Our GaAs-based quantum dot, driven by a pulsed pump laser, is modelled either as a two- or a three-level system coupled to a single-mode microcavity in the Jaynes-Cummings manner. The interaction of the quantum dot with phonons is treated by the standard pure-dephasing Hamiltonian[75–78]. In this way, we solve for the dynamics of the dot-cavity system by employing a numerically exact path-integral formalism[79–81]. The detailed intra-cavity simulations, along with the derivation of the photon number populations, are presented in Supplementary Note 1.

Practical security analyses

Supplementary Notes 2 and 3 show how the collection efficiencies and state encodings are modelled, both in the presence and absence of photon number coherence, for PDS and QDS, respectively. Supplementary Note 4 provides some high-level descriptions of the four main quantum primitives, and displays all results justifying our claims. Supplementary Note 5 briefly introduces mathematical tools required to understand the security analyses, namely semidefinite programs and Choi's theorem on completely positive maps. Supplementary Notes 6 to 10 provide the practical security analyses of all protocols, and the extensions to account for the presence of coherence in the QDS framework.

DATA AVAILABILITY

The numerical data generated and analysed during the current study is available from the corresponding author upon reasonable request.

CODE AVAILABILITY

The code used during this study is available from the corresponding author upon reasonable request.

Received: 11 March 2022; Accepted: 23 August 2022;
Published online: 08 September 2022

REFERENCES

1. Gouzien, E. & Sangouard, N. Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory. *Phys. Rev. Lett.* **127**, 140503 (2021).
2. Martín-López, E. et al. Experimental realization of shor's quantum factoring algorithm using qubit recycling. *Nat. Photonics* **6**, 773–776 (2012).
3. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* **26**, 1484–1509 (1997).
4. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, vol. 1, 175–179 (Bangalore, 1984).
5. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
6. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. *Science* **362**, 6412 (2018).
7. Broadbent, A. & Schaffner, C. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography* **78**, 351–382 (2016).
8. Bozzio, M., Cavaillès, A., Diamanti, E., Kent, A. & Pitalúa-García, D. Multiphoton and side-channel attacks in mistrustful quantum cryptography. *PRX Quantum* **2**, 030338 (2021).
9. Wiesner, S. Conjugate coding. *ACM Sigact News* **15**, 78 (1983).
10. Michler, P. Quantum Dots for Quantum Information Technologies (Springer International Publishing, 2017).
11. Senellart, P., Solomon, G. & White, A. High-performance semiconductor quantum-dot single-photon sources. *Nat. Nanotechnol.* **12**, 1026–1039 (2017).
12. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
13. Anderson, M. et al. Gigahertz-clocked teleportation of time-bin qubits with a quantum dot in the telecommunication *c* band. *Phys. Rev. Appl.* **13**, 054052 (2020).
14. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330–1333 (2000).
15. Schneeloch, J. et al. Introduction to the absolute brightness and number statistics in spontaneous parametric down-conversion. *J. Opt.* **21**, 043501 (2019).
16. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
17. Lo, H.-K. & Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quantum Info. Comput.* **7**, 431–458 (2007).
18. Vajner, D. A., Rickert, L., Gao, T., Kaymazlar, K. & Heindel, T. Quantum communication using semiconductor quantum dots. *Adv. Quantum Technol.* **5**, 2100116 (2022).
19. Basset, F. B. et al. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **7**, 12 (2021).
20. Schimpf, C. et al. Quantum cryptography with highly entangled photons from semiconductor quantum dots. *Sci. Adv.* **7**, 16 (2021).
21. Takemoto, K. et al. Quantum key distribution over 120-km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci. Rep.* **5**, 14383 (2015).
22. Heindel, T. et al. Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New J. Phys.* **14**, 083001 (2012).
23. Collins, R. J. et al. Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source. *J. Appl. Phys.* **107**, 073102 (2010).
24. Intallura, P. et al. Quantum communication using single photons from a semiconductor quantum dot emitting at a telecommunication wavelength. *Journal of Optics A: Pure and Applied Optics* **11**, 5 (2009).
25. Waks, E. et al. Quantum cryptography with a photon turnstile. *Nature* **420**, 762 (2002).
26. Wang, Q. et al. Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source. *Phys. Rev. Lett.* **100**, 090501 (2008).
27. Murtaza, G. et al. Efficient room-temperature molecular single-photon sources for quantum key distribution. preprint at https://arxiv.org/abs/2202.12635 (2022).
28. Loredo, J. C. et al. Generation of non-classical light in a photon-number superposition. *Nat. Photonics* **13**, 803–808 (2019).
29. Cao, Z., Zhang, Z., Lo, H.-K. & Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phys.* **17**, 053014 (2015).
30. Wang, S. et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **16**, 154–161 (2022).
31. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
32. Bozzio, M. et al. Experimental investigation of practical unforgeable quantum money. *Npj Quantum Inf.* **4**, 5 (2018).
33. Guan, J.-Y. et al. Experimental preparation and verification of quantum money. *Phys. Rev. A* **97**, 032338 (2018).
34. Kent, A., Lowndes, D., Pitalúa-García, D. & Rarity, J. Practical quantum tokens without quantum memories and experimental tests. *Npj Quantum Inf.* **8**, 28 (2022).
35. Pappa, A. et al. Experimental plug and play quantum coin flipping. *Nat. Commun.* **5**, 3717 (2014).
36. Berlín, G. et al. Experimental loss-tolerant quantum coin flipping. *Nat. Commun.* **2**, 561 (2011).
37. Bozzio, M., Chabaud, U., Kerenidis, I. & Diamanti, E. Quantum weak coin flipping with a single photon. *Phys. Rev. A* **102**, 022414 (2020).
38. Ng, N. H. Y., Joshi, S. K., Chen Ming, C., Kurtsiefer, C. & Wehner, S. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Commun.* **3**, 1326 (2012).
39. Lunghi, T. et al. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.* **111**, 180504 (2013).
40. Liu, Y. et al. Experimental unconditionally secure bit commitment. *Phys. Rev. Lett.* **112**, 010504 (2014).
41. Uppu, R. et al. Scalable integrated single-photon source. *Sci. Adv.* **6**, eabc8268 (2020).
42. Somaschi, N. et al. Near-optimal single-photon sources in the solid state. *Nat. Photonics* **10**, 340–345 (2016).
43. He, Y.-M. et al. On-demand semiconductor single-photon source with near-unity indistinguishability. *Nat. Nanotechnol.* **8**, 213–217 (2013).
44. Arcari, M. et al. Near-unity coupling efficiency of a quantum emitter to a photonic crystal waveguide. *Phys. Rev. Lett.* **113**, 093603 (2014).
45. He, Y.-M. et al. Coherently driving a single quantum two-level system with dichromatic laser pulses. *Nat. Phys.* **15**, 941–946 (2019).
46. Tomm, N. et al. A bright and fast source of coherent single photons. *Nat. Nanotechnol.* **16**, 399–403 (2021).
47. Reindl, M. et al. Phonon-assisted two-photon interference from remote quantum emitters. *Nano Lett.* **17**, 4090–4095 (2017).
48. Fischer, K. A. et al. Pulsed rabi oscillations in quantum two-level systems: beyond the area theorem. *Quantum Sci. Technol.* **3**, 014006 (2017).
49. Hanschke, L. et al. Quantum dot single-photon sources with ultra-low multi-photon probability. *Npj Quantum Inf.* **4**, 43 (2018).
50. Lüker, S. & Reiter, D. E. A review on optical excitation of semiconductor quantum dots under the influence of phonons. *Semicond. Sci. Technol.* **34**, 063002 (2019).
51. Cosacchi, M., Ungar, F., Cygorek, M., Vagov, A. & Axt, V. M. Emission-frequency separated high quality single-photon sources enabled by phonons. *Phys. Rev. Lett.* **123**, 017403 (2019).
52. Thomas, S. E. et al. Bright polarized single-photon source based on a linear dipole. *Phys. Rev. Lett.* **126**, 233601 (2021).
53. Ding, X. et al. On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar. *Phys. Rev. Lett.* **116**, 020401 (2016).
54. Schweickert, L. et al. On-demand generation of background-free single photons from a solid-state source. *Appl. Phys. Lett.* **112**, 093106 (2018).
55. Müller, M., Bounouar, S., Jöns, K. D., Glässl, M. & Michler, P. On-demand generation of indistinguishable polarization-entangled photon pairs. *Nat. Photonics* **8**, 224 (2014).
56. Sbresny, F. et al. Stimulated generation of indistinguishable single photons from a quantum ladder system. *Phys. Rev. Lett.* **128**, 093603 (2022).
57. Wei, Y. et al. Tailoring solid-state single-photon sources with stimulated emissions. *Nat. Nanotechnol.* **17**, 470–476 (2022).
58. Yan, J. et al. Double-pulse generation of indistinguishable single photons with optically controlled polarization. *Nano Lett.* **22**, 1483–1490 (2022).
59. Kobayashi, T., Tomita, A. & Okamoto, A. Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser. *Phys. Rev. A* **90**, 032320 (2014).
60. Tang, Y.-L. et al. Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A* **88**, 022308 (2013).
61. Duvsek, M., Jahma, M. & Lütkenhaus, N. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A* **62**, 022306 (2000).
62. Liu, F. et al. High purcell factor generation of indistinguishable on-chip single photons. *Nat. Nanotechnol.* **13**, 835–840 (2018).
63. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
64. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378–381 (2013).

65. Valivarthi, R., Etcheverry, S., Aldama, J., Zwiehoff, F. & Pruneri, V. Plug-and-play continuous-variable quantum key distribution for metropolitan networks. *Opt. Express* **28**, 14547–14559 (2020).
66. Bozzio, M., Diamanti, E. & Grosshans, F. Semi-device-independent quantum money with coherent states. *Phys. Rev. A* **99**, 022336 (2019).
67. Kolatschek, S. et al. Bright purcell enhanced single-photon source in the telecom o-band based on a quantum dot in a circular bragg grating. *Nano Lett.* **21,18**, 7740–7745 (2021).
68. Nawrath, C. et al. Resonance fluorescence of single in(ga)as quantum dots emitting in the telecom c-band. *Appl. Phys. Lett.* **118**, 244002 (2021).
69. Takemoto, K., Takatsu, M., Hirose, S. & Yokoyama, N. An optical horn structure for single-photon source using quantum dots at telecommunication wavelength. *J. Appl. Phys.* **101**, 081720 (2007).
70. Sittig, R. et al. Thin-film InGaAs metamorphic buffer for telecom C-band InAs quantum dots and optical resonators on GaAs platform. *Nanophotonics* **11**, 1109–1116 (2022).
71. Miyazawa, T. et al. Single-photon emission at 1.5-μm from an inas/inp quantum dot with highly suppressed multi-photon emission probabilities. *Appl. Phys. Lett.* **109**, 132106 (2016).
72. van Leent, T. et al. Long-distance distribution of atom-photon entanglement at telecom wavelength. *Phys. Rev. Lett.* **124**, 010510 (2020).
73. Bell, B. A. et al. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **5**, 5480 (2014).
74. Unnikrishnan, A. et al. Anonymity for practical quantum networks. *Phys. Rev. Lett.* **122**, 240501 (2019).
75. Besombes, L., Kheng, K., Marsal, L. & Mariette, H. Acoustic phonon broadening mechanism in single quantum dot emission. *Phys. Rev. B* **63**, 155307 (2001).
76. Borri, P. et al. Ultralong dephasing time in InGaAs quantum dots. *Phys. Rev. Lett.* **87**, 157401 (2001).
77. Axt, V. M., Kuhn, T., Vagov, A. & Peeters, F. M. Phonon-induced pure dephasing in exciton-biexciton quantum dot systems driven by ultrafast laser pulse sequences. *Phys. Rev. B* **72**, 125309 (2005).
78. Reiter, D. E., Kuhn, T. & Axt, V. M. Distinctive characteristics of carrier-phonon interactions in optically driven semiconductor quantum dots. *Advances in Physics: X* **4**, 1655478 (2019).
79. Vagov, A., Croitoru, M. D., Glässl, M., Axt, V. M. & Kuhn, T. Real-time path integrals for quantum dots: Quantum dissipative dynamics with superohmic environment coupling. *Phys. Rev. B* **83**, 094303 (2011).
80. Cygorek, M., Barth, A. M., Ungar, F., Vagov, A. & Axt, V. M. Nonlinear cavity feeding and unconventional photon statistics in solid-state cavity QED revealed by many-level real-time path-integral calculations. *Phys. Rev. B* **96**, 201201(R) (2017).
81. Cosacchi, M. et al. Path-integral approach for nonequilibrium multitime correlation functions of open quantum systems coupled to Markovian and non-Markovian environments. *Phys. Rev. B* **98**, 125302 (2018).
82. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Info. Comput.* **4**, 325–360 (2004).
83. Kraus, B., Gisin, N. & Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **95**, 080501 (2005).
84. Wang, H. et al. On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability. *Phys. Rev. Lett.* **122**, 113602 (2019).
85. Ding, X. et al. On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar. *Phys. Rev. Lett.* **116**, 020401 (2016).

ACKNOWLEDGEMENTS

M.B., M.V, J.C.L. and P.W. acknowledge support from the European Commission through UNIQORN (no. 820474), the AFOSR via Q-TRUST (FA9550-21-1-0355), the Austrian Science Fund (FWF) through BeyondC (F7113) and Reseach Group (FG5), and from the Austrian Federal Ministry for Digital and Economic Affairs, the National Foundation for Research, Technology and Development and the Christian Doppler Research Association. M.C., T.S. and V.M.A. are grateful for funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under project No. 419036043. C.N., S.L.P. and P.M. gratefully acknowledge the funding by the German Federal Ministry of Education and Research (BMBF) via the project QR.X (16KISQ013) and the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 899814 (Qurope). The work reported in this paper was partially funded by Project No. EMPIR 20FUN05 SEQUME.

AUTHOR CONTRIBUTIONS

M.B., M.V., C.N., S.L.P., P.M. and P.W. conceived the project, and V.M.A, P.M and P.W supervised the project. M.B., M.V., M.C. and T.S. performed the theoretical calculations, security analyses, and numerical simulations. M.B., M.V. and M.C. wrote the manuscript, with input from C.N., T.S., J.C.L., S.L.P., V.M.A., P.M. and P.W.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-022-00626-z.

Correspondence and requests for materials should be addressed to Mathieu Bozzio or Michal Vyvlecka.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.