Editors' Suggestion

Overcoming noise limitations in quantum key distribution with quantum privacy amplification

Philipp Sohr,[1,2,3,4,*] Sebastian Ecker,[1,3,4] Lukas Bulla,[1,3,4] Martin Bohmann,[1,3,4] and Rupert Ursin[1,3,4]

[1] *Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, Vienna 1090, Austria*

[2] *Atominstitut, Technische Universität Wien, Vienna 1020, Austria*

[3] *Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, Boltzmanngasse 5, Vienna 1090, Austria*

[4] *Quantum Technology Laboratories GmbH, Clemens-Holzmeister-straße 6/6, Vienna 1100, Austria*

(Received 8 February 2024; revised 4 June 2024; accepted 17 July 2024; published 21 August 2024)

High-quality, distributed quantum entanglement is the distinctive resource for quantum communication and forms the foundation for the unequaled level of security that can be assured in quantum key distribution. While the entanglement provider does not need to be trusted, the secure key rate drops to zero if the entanglement used is too noisy. In this paper, we show experimentally that QPA is able to increase the secure key rate achievable with QKD by improving the quality of distributed entanglement, thus increasing the quantum advantage in QKD. Beyond that, we show that QPA enables key generation at noise levels that previously prevented key generation. These remarkable results were only made possible by the efficient implementation exploiting hyperentanglement in the polarization and energy-time degrees of freedom. We provide a detailed characterization of the gain in secure key rate achieved in our proof-of-principle experiment at different noise levels. The results are paramount for the implementation of a global quantum network linking quantum processors and ensuring future-proof data security.

DOI: 10.1103/PhysRevApplied.22.024059

I. INTRODUCTION

Quantum key distribution (QKD) allows two communication parties, Alice and Bob, to generate a cryptographic key at a distance, even in the presence of a technologically unbounded adversary [1,2]. The distinctive feature of QKD is the security based on physical principles [3,4]. Since the security of QKD can be proven without making assumptions on the adversary whatsoever, the security is not threatened by technological progress of the adversary.

Quantum entanglement is one of the outstanding physical phenomena used as a resource for quantum information processing tasks. By measuring entangled photon pairs at distant locations, identical randomness is generated at these locations, which is exclusively shared by two parties [5,6].

In fact, these characteristic properties of entanglement are precisely those that are essential for the distribution of a symmetric cryptographic key [7]. Entanglement-based QKD protocols such as E91 [8] and BBM92 [9] make use of these properties. As long as Alice and Bob share pure entangled states, the monogamy of entanglement guarantees privacy of the resulting randomness [10,11]. In the absence of errors caused by environmental noise, adversarial interaction or device imperfections, a perfectly secure key would be shared between Alice and Bob already after sifting of the measured data. However, entanglement cannot be generated remotely by local operations and classical communication (LOCC), but it has to be generated in one place to be then distributed to the communication parties. Inevitable interaction with the environment during distribution as well as eavesdropping attempts reduce the purity, leaving Alice and Bob with noisy, mixed entangled states. As a result, Alice and Bob share nonperfect correlations after measurement and sifting. By analyzing the measurement data, it is possible to monitor the correlations resulting from entanglement and thereby detect any eavesdropping attempts [9]. Due to this unique feature of identifying eavesdropping attempts, Alice and Bob do not need to trust the entanglement provider. It is therefore conceivable that not only the quantum channel but also the source of the entangled photons is under the control of a malicious third party.

Whenever Alice and Bob discover an eavesdropping attempt, they take appropriate measures to assure the security of distributed keys. In classical postprocessing, the

*Contact author: philipp.sohr@qtlabs.at

 © 2024 American Physical Society

security of the distributed key is increased at the cost of the length of the key. If the entanglement is too noisy, whether due to cheating by the entanglement provider or interaction with the environment during transmission, the secure key length is reduced to zero [12,13]. But even if this noise threshold is exceeded, it is still possible to generate a secure key with QKD by improving the quantum resources before the classical postprocessing.

One approach to increase the noise resistance [14] is high-dimensional (high-dim) QKD, that uses high-dim entanglement as an advanced quantum resource [15–17]. With increasing dimension, the background noise is more and more diluted, leading to a higher signal-to-noise ratio and an increased noise threshold [18,19]. While high-dim entanglement is readily produced in experiment, the measurements required for high-dim QKD are involved [20–22]. Another approach is entanglement distillation [23], which can improve the shared entanglement by LOCC at the cost of the number of qubit pairs. In the context of QKD, as shown in Fig. 1, entanglement distillation is known as quantum privacy amplification (QPA) [24]. In the original QPA proposal, two photon pairs that are sufficiently [25] but not maximally entangled were used to output a single photon pair closer to a maximally entangled state. However, implementations of a two-copy scheme are faced with two major problems: (i) the impossibility of implementing a deterministic controlled NOT (CNOT) operation between two independent photons with passive linear optics [26–29] and finite resources and (ii) the low probability of simultaneous transmission of two photon pairs. Recently, it has been shown that single-copy entanglement distillation can leverage the entanglement of different degrees of freedom (DOF) of a single photon pair to overcome these challenges [30,31]. Similarly to high-dim entanglement, hyperentanglement is readily produced in spontaneous parametric down-conversion (SPDC) [32,33] and with other photon-pair generation techniques [34,35]. However, while the exploitation of high-dim entanglement for QKD requires sophisticated measurements, QKD in conjunction with QPA, in contrast, is performed with common qubit measurements. Notably, the deterministic realization of the CNOT gate between two DOF of the same photon, as shown in Fig. 1, is possible with linear optics [36,37]. The polarization (pol) and energy-time (*e*-*t*) DOF employed by the work presented in Ref. [30] are known for their robustness as quantum information carriers and have been successfully distributed over free space [20,38–40] and long-haul optical fiber links [41–43], making them an ideal choice for future applications. It has been demonstrated, that single-copy entanglement distillation can improve the Bell-state fidelity for a wide range of noisy input states [30]. For three single noise levels and using the less practical spatial encoding, a potential advantage of a single-copy distillation experiment has been shown [31]. However, it remains to be shown that the effects of the increased entanglement quality outweigh the reduced number of entangled qubit pairs, resulting in an actual advantage of QPA for QKD.

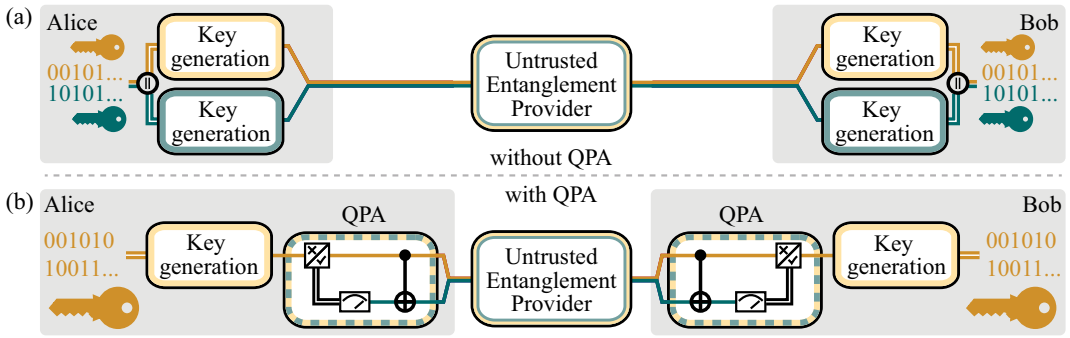

FIG. 1. Schematic of entanglement distribution for QKD with and without quantum privacy amplification (QPA). Alice and Bob are provided with hyperentangled states by an untrusted, potentially malicious party that controls both the entanglement source and the quantum channel. The two degrees of freedom (DOF) are indicated by the yellow and turquoise colors, respectively. In scenario (a), a separate key is generated independently from each degree of freedom first. Then, the two keys are concatenated, which increases the total key rate. However, the distributed entanglement could be noisy and mixed, either due to an eavesdropping attempt by the entanglement provider or due to interaction with the environment during distribution. This reduces the secure key rate and as soon as the noise threshold of the employed QKD protocol is reached, the secure key rate drops to zero, i.e., no secure key can be generated. With QPA as shown in scenario (b), the noise threshold can be increased and a key can be generated in noise ranges that are not accessible in scenario (a). Alice and Bob each perform a controlled NOT gate between the DOF of their received photon. They project the target DOF (turquoise) onto the computational basis. If their measurement results agree, they keep the photon pair. Otherwise, they discard the photon pair. The entanglement in the remaining DOF is used as a resource to generate a key. With the quantum resources enhanced by QPA, it is possible to raise the noise threshold and achieve key rates in the one remaining DOF that are higher than the concatenated key rate without QPA.

Here, we report on the experimental demonstration of QPA with hyperentanglement in the field-tested polarization and energy-time degrees of freedom. We compare the sum of the key rates extracted from both DOF before QPA with the key rate extracted from the polarization DOF after QPA, see Fig. 1. We show that the implementation of QPA not only increases the overall key rate, but also enables QKD with noisy entanglement in cases where this would no longer be possible with classical postprocessing alone. To fully explore this process, we intentionally generate noisy entanglement in a finely controlled manner by mixing two Bell states in the polarization DOF and three Bell states in the energy-time DOF. We systematically assemble a range of noise contributions into a map to precisely show the performance of our setup under various conditions.

II. EXPERIMENT

We generate hyperentangled photon pairs in an SPDC process. A Franson-type interferometer, as shown in Fig. 2, projects the energy-time DOF to a two-dimensional path DOF, such that a polarizing beam splitter (PBS) can act as a CNOT gate flipping the path of the photon depending on the polarization. Postselection on the path modes after the Franson-type interferometer completes QPA. The performance of the setup is quantified by local projective measurements, both before and after the interferometer.

In our table-top experiment, we had full control over the source of entangled photons as well as over the noisy channel. The high-quality polarization entanglement is generated by carefully tuning the polarizing Sagnac interferometer [44,45] to maximize the overlap of the biphoton modes resulting from the bidirectional pumping of the ppKTP crystal. The energy-time entanglement [46] arises naturally by pumping the crystal with a narrow-band continuous-wave laser. While it is known that the generation time of the single photons of a pair must be the same due to the conservation of energy, the absolute generation time of a pair cannot be predicted. All generation times within the coherence time of the laser are coherently superimposed. By the Franson-type interferometer [47], this high-dimensional entanglement is projected on a two-dimensional path DOF, namely the short (S) and the long (L) paths of the interferometer, each with a delay $t_{S_{A/B}}$ and $t_{L_{A/B}}$, respectively. The phase of the energy-time Bell

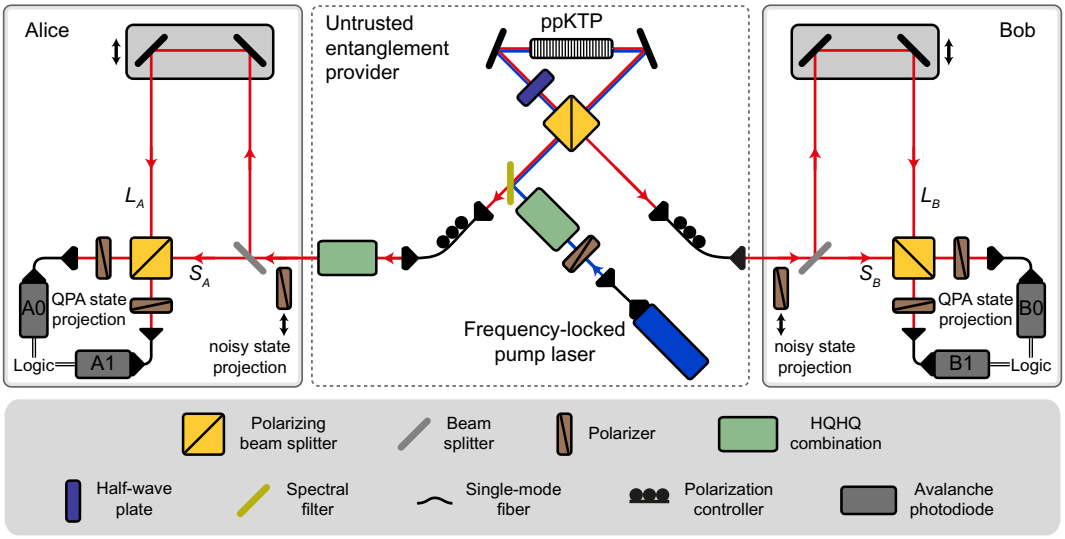

FIG. 2. Experimental setup scheme of quantum privacy amplification. Pairs of single photons hyperentangled in the polarization and the energy-time degree of freedom (DOF) are created in a spontaneous parametric down-conversion (SPDC) process by bidirectional pumping of a periodically poled potassium titanyl phosphate (ppKTP) crystal in a Sagnac-type source with a 405-nm narrow-bandwidth continuous-wave laser. The single photons are coupled to a single-mode fiber and distributed to Alice and Bob. Combinations of two quarter- and two half-wave plates (HQHQ) are used to tune the state generated at the source as well as to create mixtures of Bell states. To perform the QPA step, both Alice and Bob are equipped with an imbalanced Mach-Zehnder interferometer each with a polarizing beam splitter (PBS) at the output, constituting a Franson-type interferometer. Each PBS acts as deterministic controlled NOT gate between the polarization DOF and the energy-time (path) DOF of one and the same photon. The translation stages in the long arm are used both to adjust the phase of the energy-time Bell state, and to counteract length changes of the interferometer arms due to mechanical influences and temperature drifts in the laboratory. The single photons are detected by fiber-coupled avalanche photodiodes. The measurements for key estimation are performed with polarization filters after and optionally also before the interferometer. In the energy-time DOF, this projective measurement corresponds to the identification of the detector that detected a photon. For the sake of clarity, auxiliary systems such as the stabilization of the Franson interferometer are omitted in this figure. A more detailed scheme can be found in Fig. 2 of Ref. [30].

state is tuned by carefully adjusting the length imbalance of one of the Mach-Zehnder interferometers on the order of the wavelength, see Fig. 2. As a result, we obtain a hyperentangled state Φ^+, that is close to a ϕ^+ Bell state in both DOF

$$\left|\Phi^+\right\rangle = \frac{1}{2}\left[\left(|H,H\rangle + |V,V\rangle\right) \otimes \left(|t_S,t_S\rangle + |t_L,t_L\rangle\right)\right]. \quad (1)$$

The mixed state in the polarization DOF is generated with a combination of wave plates acting on one photon of a pair. The wave plates are adjusted in a way that their combination causes a tunable rotation about the y axis on the Bloch sphere $\left(R_y(\theta) \otimes \mathbb{1}\right)$. By time averaging over the settings for $\pm\theta$, the Bell state ψ^- is mixed to the originally prepared ϕ^+ state. In the energy-time DOF, the mixed state is generated by increasing the coincidence window for accepting coincidences in the postprocessing. By including the noninterfering background of the Franson interference, an equal admixture of the Bell states ψ^+ and ψ^- to the originally prepared ϕ^+ state is achieved (for details see Appendix of Ref. [30]).

The heart of the QPA setup (Fig. 2) are the two PBSs acting as bilateral CNOT between the DOF of one and the same photon. The coincidence events are accepted if either detectors A0 and B0 or detectors A1 and B1 registered a photon, otherwise, they are discarded.

The ratio between the accepted coincidences C_{pass} and the total coincidences C_{tot} is defined as the yield of the QPA process $y = C_{\text{pass}}/C_{\text{tot}}$. In contrast to the originally proposed two-copy QPA [24], which is limited to a maximal yield of 0.5, since one photon pair was always consumed independent of the quality of the input states, the yield of the single-copy QPA presented here approaches 1. Even though the fidelity with respect to a Bell state can be increased with such a setup, with a yield up to one [30], it is not obvious, that this manifests a benefit for QKD.

To estimate a lower bound on the key rate, we measure in the two linear mutually unbiased bases, i.e., the computational basis $\{|H\rangle, |V\rangle\}$ in the polarization DOF and $\{|t_S\rangle, |t_L\rangle\}$ in the energy-time DOF as well as the superposition bases $\left\{\left(|H\rangle \pm |V\rangle\right)/\sqrt{2}\right\}$ and $\left\{\left(|t_S\rangle \pm |t_L\rangle\right)/\sqrt{2}\right\}$, respectively. The noisy entanglement, introduced by the admixture of Bell states, is recognized as erroneous detection events in the experiment N_{err}. The noise is quantified by the quantum bit error rate (QBER), which is defined as the quotient of the number of erroneous detection events and the total number of events, $e = N_{\text{err}}/N$. With this at hand, we compute a lower bound of the secure key rate k in the asymptotic limit of infinite key length with the Devetak-Winter formula [48]

$$k\left(e_z, e_x\right) \geq \max\left(0, 1 - h_2(e_z) - h_2(e_x)\right), \quad (2)$$

where $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy. Before the QPA step, both DOF of the hyperentangled state can, in principle, be used to generate a secure key as depicted in Fig. 1. The secure key rate before the QPA k_{noisy} is the sum of the secure key rate in each DOF,

$$k_{\text{noisy}} = k\left(e_z^{\text{pol}}, e_x^{\text{pol}}\right) + \frac{k\left(e_z^{e\text{-}t}, e_x^{e\text{-}t}\right)}{2}. \quad (3)$$

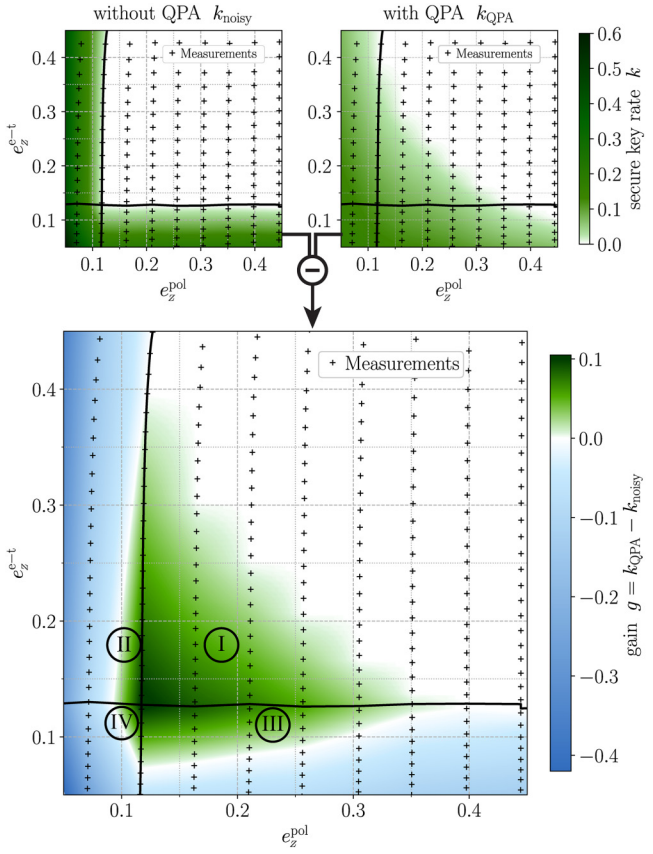

FIG. 3. Advantage in the secure key rate by QPA mapped for various noise levels in each DOF separately. The measurement points indicated by the markers (not all are shown for readability; the error bars are smaller than the markers) span a grid of the QBER in the z basis in both DOF. In the two top plots, the color, that results from a linear interpolation between the measurement points, indicates the secure key rate before and after the QPA step. Both heatmaps share the same colorbar. The thick black lines indicate the QBER threshold, which is about 11% in the polarization DOF and slightly higher in the energy-time DOF due to the noise composition. Comparing the two heatmaps, it is already clearly visible that the area of the positive key rate with QPA extends over the limits of the key rate without QPA. Even clearer becomes the advantage of QPA in the bottom heatmap displaying the QPA gain in the secure key rate. The region of positive gain reaches down to 9.1% QBER in the polarization DOF and 7.2% QBER in the energy-time DOF up to 40% QBER in either DOF. We reach a maximum gain of 0.105. Not only is it possible to generate a key where it was not possible before (I), but also can the key rate be improved in regions where key generation was possible in one DOF (II), (III) and even in both DOF (IV) before.

After QPA, the QBER in the polarization DOF $\check{e}^{\mathrm{pol}}_{x/z}$ has changed and the yield y has to be taken into account, so that the key rate after QPA k_{QPA} computes as

$$k_{\mathrm{QPA}} = y * \frac{k\left(\check{e}^{\mathrm{pol}}_{z}, \check{e}^{\mathrm{pol}}_{x}\right)}{2}. \tag{4}$$

The factor $1/2$ in Eqs. (3) and (4) reflects the 50% loss due to the Franson interferometer. As a measure for the performance of the protocol, we define the gain g in secure key rate as the difference between the sum of the key rate after QPA and the two key rates using noisy entanglement

$$g = k_{\mathrm{QPA}} - k_{\mathrm{noisy}}. \tag{5}$$

III. RESULTS

We obtained a true advantage by increasing the noise threshold of QKD with our QPA experiment, indicated by the positive gain shown in Fig. 3. The region of positive gain can be divided into three parts. Firstly, the regions (II) and (III), where the noise threshold was exceeded in one DOF, but secure key generation was still possible in the other DOF before the QPA step. In these regions the application of QPA increased the secure key rate. Region (III) is larger than region (II) due to the 50% loss introduced by the implementation of the Franson interferometer to utilize the energy-time entanglement. Secondly, in a small domain (IV) the noise was close to the threshold in both DOF before the QPA. With QPA, we increased the secure key rate in this region even though both DOF contributed to the total pre-QPA secure key rate. Thirdly, in the largest part of the region of positive gain (I), we generated a secure key rate facing a noise level that prevented key generation before. This shows that QPA can increase the noise threshold of QKD, enabling a positive secure key rate where this was not possible before. Negative gains are obtained if high-quality entanglement is provided at least in one of the two DOFs. While the maximal gains will always be found along the noise thresholds, the amplitude and spread of negative gain can be reduced by improving the implementation of QPA.

IV. DISCUSSION AND CONCLUSIONS

With this work, we demonstrate experimentally that QPA boosts the quantum advantage of QKD. Provided with noisy quantum resources, Alice and Bob usually process their classical records of the quantum measurements to obtain identical, secret keys. However, once the noise threshold of the employed protocol is reached, the secure key length reduces to zero, rendering QKD impossible with the provided resources. We show that QPA can improve the quality of the quantum resources, such that the post-QPA key rate exceeds the total pre-QPA key rate close to and beyond the noise threshold of QKD. This pioneering demonstration was only made possible by the increased efficiency of the single-copy scheme harnessing hyperentanglement in the polarization and the energy-time DOF. Not only does the hyperentanglement enable an implementation of a deterministic CNOT gate with linear optics without ancillary photons, but also is the efficiency increased since each QPA step requires the distribution of only one photon pair. As a consequence of the latter, our QPA method has quadratic advantage in both the creation and the transmission probability of the photon pairs compared to two-copy schemes. This advantage is particularly relevant in high-loss regimes such as long-distance links. The constant 2-dB loss introduced by the Franson interferometer can be avoided by active switching [49]. The dense grid of measurement points for various noise levels in both DOF subspaces independently does allow a thorough assessment of the implemented QPA scheme's performance. The resulting map of the advantage of QPA is not only of great importance for implementation purposes, but also for further focused research. The most remarkable finding of this work is that QPA can increase the noise threshold, enabling QKD in hitherto inaccessible noise regimes. While the noise threshold can also be raised with high-dim QKD, QKD supported by QPA works with qubit measurements that are easier to implement and the QPA module can even be retrofitted in deployed QKD systems. Combining the noise advantages of high-dim QKD with our QPA method promises robustness to various types of noise. We have demonstrated the capabilities of QPA to counteract a noise factorizing in the DOF subspaces. Isotropic noise in the joint state space of different DOF such as noise caused by background light or detector dark counts can be diluted by embedding the polarization state in a high-dimensional state space, such as the energy-time state space [14]. The results of this work are of great importance for implementations of QKD, a technology that is currently emerging from fundamental research toward commercial application. As such, our results will contribute significantly to the advent of a robust global QKD network providing secure communication and forming the basis of the quantum internet. In the future, implementations of QPA could be extended to further DOF, given that an efficient CNOT gate can be performed between them. Using entanglement in additional DOF could enable more QPA steps with a single photon pair, further increasing the advantage of QPA. In particular, this would allow to counteract arbitrary subspace noise [23]. Finally, it remains open to demonstrate the advantage of QPA in an in-field test with real noise as well as the combination with high-dim QKD schemes.

ACKNOWLEDGMENTS

We acknowledge funding from the Austrian Science Fund (FWF) through the START Project No. Y879-N27

and from the European Unions Horizon 2020 programme Grant Agreement No. 857156 (OpenQKD).

P.S., S.E., and R.U. conceived the project; P.S., S.E., and L.B. designed and developed the experiment under the guidance of M.B. and R.U.; P.S. and S.E. evaluated the experimental data; P.S. wrote the first draft of the manuscript; all authors discussed the results, contributed to writing and reviewed the manuscript; M.B. and R.U. supervised the project.

The experimental data and the analysis will be provided upon reasonable request.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[2] R. Renner and R. Wolf, Quantum advantage in cryptography, AIAA J. **61**, 1895 (2023).

[3] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A **72**, 012332 (2005).

[4] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (2022).

[5] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[6] A. Zeilinger, A foundational principle for quantum mechanics, Found. Phys. **29**, 631 (1999).

[7] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a precondition for secure quantum key distribution, Phys. Rev. Lett. **92**, 217903 (2004).

[8] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[9] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem, Phys. Rev. Lett. **68**, 557 (1992).

[10] M. Koashi and A. Winter, Monogamy of quantum entanglement and other correlations, Phys. Rev. A **69**, 022309 (2004).

[11] J. Barrett, A. Kent, and S. Pironio, Maximally nonlocal and monogamous quantum correlations, Phys. Rev. Lett. **97**, 170409 (2006).

[12] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, Generalized privacy amplification, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[13] R. Renner and R. König, in *Theory of Cryptography*, Lecture Notes in Computer Science, edited by J. Kilian (Springer, Berlin, Heidelberg, 2005), p. 407.

[14] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Overcoming noise in entanglement distribution, Phys. Rev. X **9**, 041042 (2019).

[15] M. Erhard, M. Krenn, and A. Zeilinger, Advances in high-dimensional quantum entanglement, Nat. Rev. Phys. **2**, 365 (2020).

[16] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, High-dimensional quantum communication: Benefits, progress, and future challenges, Adv. Quantum Technol. **2**, 1900038 (2019).

[17] X.-M. Hu, C. Zhang, Y. Guo, F.-X. Wang, W.-B. Xing, C.-X. Huang, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, X. Gao, M. Pivoluska, and M. Huber, Pathways for entanglement-based quantum communication in the face of high noise, Phys. Rev. Lett. **127**, 110505 (2021).

[18] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Phys. Rev. A **82**, 030301(R) (2010).

[19] A. Ferenczi and N. Lütkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, Phys. Rev. A **85**, 052310 (2012).

[20] L. Bulla, K. Hjorth, O. Kohout, J. Lang, S. Ecker, S. P. Neumann, J. Bittermann, R. Kindler, M. Huber, M. Bohmann, R. Ursin, and M. Pivoluska, Distribution of genuine high-dimensional entanglement over 10.2 km of noisy metropolitan atmosphere, Phys. Rev. A **107**, L050402 (2023).

[21] L. Bulla, M. Pivoluska, K. Hjorth, O. Kohout, J. Lang, S. Ecker, S. P. Neumann, J. Bittermann, R. Kindler, M. Huber, M. Bohmann, and R. Ursin, Nonlocal temporal interferometry for highly resilient free-space quantum communication, Phys. Rev. X **13**, 021001 (2023).

[22] A. Bergmayr, F. Kanitschar, M. Pivoluska, and M. Huber, How to harness high-dimensional temporal entanglement, using limited interferometry setups, arXiv:2308.04422.

[23] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of noisy entanglement and faithful teleportation via noisy channels, Phys. Rev. Lett. **76**, 722 (1996).

[24] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noisy channels, Phys. Rev. Lett. **77**, 2818 (1996).

[25] M. Horodecki, P. Horodecki, and R. Horodecki, Distillability of inseparable quantum systems, arXiv:quant-ph/9607009.

[26] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Demonstration of an all-optical quantum controlled-NOT gate, Nature **426**, 264 (2003).

[27] T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson, Experimental controlled-NOT logic gate for single photons in the coincidence basis, Phys. Rev. A **68**, 032316 (2003).

[28] S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger, Realization of a photonic controlled-NOT gate sufficient for quantum computation, Phys. Rev. Lett. **93**, 020504 (2004).

[29] Z. Zhao, A.-N. Zhang, Y.-A. Chen, H. Zhang, J.-F. Du, T. Yang, and J.-W. Pan, Experimental demonstration of a nondestructive controlled-NOT quantum gate for two independent photon qubits, Phys. Rev. Lett. **94**, 030501 (2005).

[30] S. Ecker, P. Sohr, L. Bulla, M. Huber, M. Bohmann, and R. Ursin, Experimental single-copy entanglement distillation, Phys. Rev. Lett. **127**, 040506 (2021).

[31] X.-M. Hu, C.-X. Huang, Y.-B. Sheng, L. Zhou, B.-H. Liu, Y. Guo, C. Zhang, W.-B. Xing, Y.-F. Huang, C.-F. Li, and G.-C. Guo, Long-distance entanglement purification for quantum communication, Phys. Rev. Lett. **126**, 010503 (2021).

[32] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Generation of hyperentangled photon pairs, Phys. Rev. Lett. **95**, 260501 (2005).
[33] P. G. Kwiat, Hyper-entangled states, J. Mod. Opt. **44**, 2173 (1997).
[34] M. Prilmüller, T. Huber, M. Müller, P. Michler, G. Weihs, and A. Predojević, Hyperentanglement of photons emitted by a quantum dot, Phys. Rev. Lett. **121**, 110503 (2018).
[35] C. Reimer, S. Sciara, P. Roztocki, M. Islam, L. Romero Cortés, Y. Zhang, B. Fischer, S. Loranger, R. Kashyap, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, W. J. Munro, J. Azaña, M. Kues, and R. Morandotti, High-dimensional one-way quantum processing implemented on d-level cluster states, Nat. Phys. **15**, 148 (2019).
[36] M. Fiorentino and F. N. C. Wong, Deterministic controlled-NOT gate for single-photon two-qubit quantum logic, Phys. Rev. Lett. **93**, 070502 (2004).
[37] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Beating the channel capacity limit for linear photonic superdense coding, Nat. Phys. **4**, 282 (2008).
[38] J. Yin, *et al.*, Satellite-based entanglement distribution over 1200 kilometers, Science **356**, 1140 (2017).
[39] F. Steinlechner, S. Ecker, M. Fink, B. Liu, J. Bavaresco, M. Huber, T. Scheidl, and R. Ursin, Distribution of high-dimensional entanglement via an intra-city free-space link, Nat. Commun. **8**, 15971 (2017).
[40] J. Jin, J.-P. Bourgoin, R. Tannous, S. Agne, C. J. Pugh, K. B. Kuntz, B. L. Higgins, and T. Jennewein, Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel, Opt. Express **27**, 37214 (2019).
[41] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, Entanglement distribution over a 96-km-long submarine optical fiber, Proc. Natl. Acad. Sci. **116**, 6684 (2019).
[42] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Distribution of time-bin entangled qubits over 50 km of optical fiber, Phys. Rev. Lett. **93**, 180502 (2004).
[43] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, and R. Ursin, Continuous entanglement distribution over a transnational 248 km fiber link, Nat. Commun. **13**, 6134 (2022).
[44] T. Kim, M. Fiorentino, and F. N. C. Wong, Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer, Phys. Rev. A **73**, 012316 (2006).
[45] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, A wavelength-tunable fiber-coupled source of narrowband entangled photons, Opt. Express **15**, 15377 (2007).
[46] A. Martin, T. Guerreiro, A. Tiranov, S. Designolle, F. Fröwis, N. Brunner, M. Huber, and N. Gisin, Quantifying photonic high-dimensional entanglement, Phys. Rev. Lett. **118**, 110501 (2017).
[47] J. D. Franson, Bell inequality for position and time, Phys. Rev. Lett. **62**, 2205 (1989).
[48] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A: Math. Phys. Eng. Sci. **461**, 207 (2005).
[49] F. Vedovato, C. Agnesi, M. Tomasin, M. Avesani, J.-Å. Larsson, G. Vallone, and P. Villoresi, Postselection-loophole-free Bell violation with genuine time-bin entanglement, Phys. Rev. Lett. **121**, 190401 (2018).