Pathways for Entanglement-Based Quantum Communication in the Face of High Noise

Xiao-Min Hu,[1,2] Chao Zhang,[1,2] Yu Guo,[1,2] Fang-Xiang Wang,[1,2] Wen-Bo Xing,[1,2] Cen-Xiao Huang,[1,2] Bi-Heng Liu,[1,2,*] Yun-Feng Huang,[1,2] Chuan-Feng Li,[1,2,†] Guang-Can Guo,[1,2] Xiaoqin Gao,[3,4,5,‡] Matej Pivoluska,[6,7,§] and Marcus Huber[8,3,‖]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, People's Republic of China*

[2]*CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China*

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

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

[5]*Department of Physics, University of Ottawa, Advanced Research Complex, 25 Templeton Street, K1N 6N5 Ottawa, Ontario, Canada*

[6]*Institute of Computer Science, Masaryk University, 602 00 Brno, Czech Republic*

[7]*Institute of Physics, Slovak Academy of Sciences, 845 11 Bratislava, Slovakia*

[8]*Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, 1020 Vienna, Austria*

(Received 29 December 2020; revised 25 June 2021; accepted 29 July 2021; published 10 September 2021)

Entanglement-based quantum communication offers an increased level of security in practical secret shared key distribution. One of the fundamental principles enabling this security—the fact that interfering with one photon will destroy entanglement and thus be detectable—is also the greatest obstacle. Random encounters of traveling photons, losses, and technical imperfections make noise an inevitable part of any quantum communication scheme, severely limiting distance, key rate, and environmental conditions in which quantum key distribution can be employed. Using photons entangled in their spatial degree of freedom, we show that the increased noise resistance of high-dimensional entanglement can indeed be harnessed for practical key distribution schemes. We perform quantum key distribution in eight entangled paths at various levels of environmental noise and show key rates that, even after error correction and privacy amplification, still exceed 1 bit per photon pair and furthermore certify a secure key at noise levels that would prohibit comparable qubit based schemes from working.

DOI: 10.1103/PhysRevLett.127.110505

Quantum key distribution (QKD) [1–5] is one of the most prominent and mature applications of quantum information theory. It can be used to establish a shared and private random bit string among two parties, that can subsequently be used to encrypt information [6]. There are different levels of security of quantum key distribution, depending on the assumptions placed on each of the devices used. The weakest form are the so-called prepare and measure protocols [1,7,8], which assume a trusted source of quantum states in possession of one of the parties, as well as perfectly characterized measurement devices for both parties. Although such assumptions about components of QKD implementation are often reasonable, they open up loopholes which the potential adversary can abuse to perform attacks on the implementation of the protocol [9,10]. The other extreme is given by so-called device independent quantum key distribution [11–15], where no assumptions are placed on any devices, except for the privacy of locally generated randomness. Such protocols provide a revolutionary paradigm shift in designing secure QKD protocols, but they remain largely impractical, because they require loophole-free Bell inequality violations, which can be obtained only in strict laboratory conditions [16–18]. In between these two extremal cases, there are plenty of scenarios with various levels of trust placed on the devices, which leads to very different practically achievable key rates [19–26]. Entanglement-based protocols belong to this last group as they typically assume the entanglement source is in the control of the adversary. This makes entanglement protocols secure against many attacks abusing source imperfections (e.g., photon splitting attack [27,28]), and possibly against prepare and measure protocols.

The physical principle ensuring security of quantum key distribution protocols can be intuitively understood from two fundamental facts about quantum physics. First of all, an unknown quantum state cannot be copied (no-cloning theorem [29–31]), and second, a state cannot undergo a measurement procedure without being influenced (projection postulate of quantum mechanics, see, e.g., [32]).

So when encoding information in individual quantum systems, it is impossible to intercept and learn information from them, without also revealing one's presence. While this principle enables classically unachievable levels of security, it also presents a serious challenge. Any interaction of these individual quantum systems with an environment, any background photons that are accidentally detected, and other imperfections in the devices will manifest as noise in the data. Such environmental noise cannot be distinguished from noise that would result from malicious activity. There are two big challenges of contemporary QKD stemming from noise [33]. First, QKD protocols cannot certify any shared key, if the noise level is above a certain threshold. Second, environmental noise significantly affects the achievable key rate of many protocols even in relatively low noise regimes. One of the big remaining challenges of QKD is therefore to design protocols which can tolerate large amounts of environmental noise and produce large amounts of key in moderate noise regimes. The potential way to solve both of these challenges by employing high-dimensional degrees of freedom of photons (see Ref. [34]) has been proposed as early as 20 years ago [35,36]. The idea of increased key rate is straightforward—one photon carrying information in d dimensional degree of freedom (called a *qudit*) can produce as much as $\log_2 d$ bits of randomness. Simultaneously, in theory, increasing the dimension d of used quantum systems also increases the amount of tolerable noise [37]. Practical demonstrations of high-dimensional QKD (HDQKD) followed much later. Prepare and measure protocols demonstrated that in low noise regimes one can indeed obtain increased key rates [38–46]. On the other hand entanglement-based HDQKD protocols were achieved only by employing additional assumptions about the distributed state [47], thus compromising the source independence of the protocol, or restricted measurements [48,49]. Additionally, none of the implementations show exceptionally high noise resistance. This is partially caused by the fact that with the increasing dimensions in the real experiment, one inevitably also increases the environmental noise (see Ref. [50]). Further, this increased noise takes an extra toll, as error correction requires more communication in higher dimensions.

In this Letter we present a first experimental demonstration of an entanglement-based HDQKD protocol, which does not impose any assumptions about the distributed state. This is possible thanks to several recent breakthroughs. It was recently shown [51] that high-dimensional entanglement, i.e., entanglement in multiple degrees of freedom, can exhibit an increased resistance to real physical noise compared with low-dimensional counterparts. This led to the proposal of a QKD protocol, simultaneously coding in multiple subspaces of high-dimensional states [50] (see also [52]), theoretically predicting the possibility of establishing a secure key in the presence of unprecedented noise levels. The last recent breakthrough is the development of experimental setups for the creation and manipulation of path entanglement [53], which allow implementation of true multioutcome measurements with high fidelity. Putting these ideas together, we implement the protocol introduced in [50] using eight-dimensional path entanglement and bilateral eight-outcome measurements. We show that even after postprocessing, the key rate exceeds 1 bit per coincidence, i.e., each detected pair establishes more key than would be possible to encode in even a perfect and noiseless qubit. Furthermore, we prepare an entire family of states by adding artificial noise to the experiment, fully exploring the achievable noise resistance of the protocol.

First, let us briefly review the high-dimensional entanglement-based QKD protocol developed in [50]. The protocol is composed of N rounds, in which the source distributes a $d \times d$ entangled state $\rho_{\mathrm{AB}} \in \mathcal{H}_A \otimes \mathcal{H}_B$ to two communicating parties, Alice and Bob. In the ideal case $\rho_{\mathrm{AB}} = |\phi_d^+\rangle\langle\phi_d^+|$, where $|\phi_d^+\rangle = (1/\sqrt{d}) \sum_{i=0}^{d-1} |ii\rangle$. Postulates of quantum mechanics guarantee that measuring this state by both Alice and Bob in the d-dimensional computational basis (called a *key basis*) leads to two $\log_2(d)N$-bit strings X and Y. These two strings are uniformly distributed, perfectly correlated and private; thus, they constitute a shared secret key. However, any real world implementation is necessarily imperfect, and thus the quality of the state ρ_{AB} needs to be assessed. Particularly, in randomly chosen rounds, Alice and Bob measure the state in a *test basis* which allows them to estimate the amount of key they can distill from their key basis measurement outcomes X and Y. This step is then followed by classical postprocessing. This is composed of *error correction*, in which differences between X and Y are corrected and *privacy amplification*, in which the final key—a shorter but uniformly distributed shared string—is obtained. We employ methods developed in [37], where the quality of data obtained in the d-dimensional key basis is assessed by measurements in a mutually unbiased basis [54]. The test rounds of the protocol are then used to assess the following error vector:

$$\vec{e}_t = (e_t^{(0)}, e_t^{(1)}, \ldots, e_t^{(d-1)}), \tag{1}$$

where $e_t^{(j)} = \sum_{i=0}^{d-1} \Pr(i, i+j \bmod d|\mathrm{test})$ is the probability that Alice obtained result i and Bob obtained result $i+j \bmod d$, when they were both measuring in their test basis. This error vector is used to bound the adversary's information in the asymptotic regime against collective attacks as $H(\vec{e}_t)$, where $H(\cdot)$ is the Shannon entropy function [37]. A similar error vector $\vec{e}_k$ can be defined for the measurements in the key basis. In turn, $H(\vec{e}_k)$ gives the amount of information Alice and Bob need to exchange in the error correction phase. Together, the asymptotic key rate per coincidence of a d-dimensional instance of the described entanglement-based protocol can be estimated as

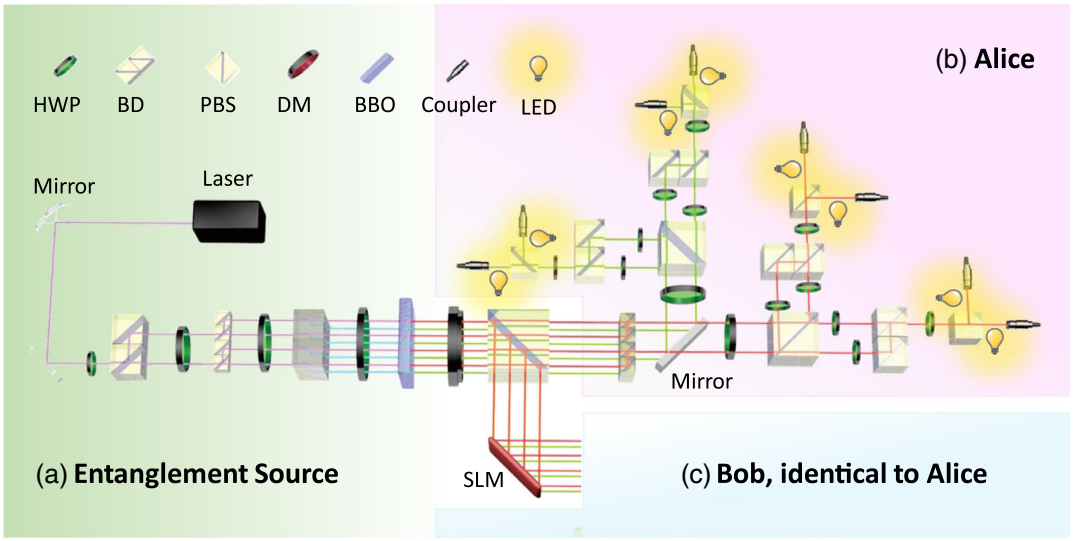

FIG. 1. Experimental setup. (a) Preparation of eight-dimensional entanglement: Eight parallel beams are obtained by eight equal divisions of the continuous-wave light (at 404 nm, the diameter is 0.6 mm), with the help of three half-wave plates (HWPs at 22.5°) and three BDs. Eight beams are assigned into eight two-layer paths, the upper layer and the lower layer represented by purple and blue colors, respectively, and labeled with "0," "1," …, "7." The distance between two neighboring paths is 2 mm. Another HWP at 22.5° is necessary for all beams to transmit with H polarization. Each beam that injects into a beta-barium-borate (BBO) crystal will generate infrared photon pairs called single and idler photons ($H^{\text{classic}}_{404\text{ nm}} \overset{\text{SPDC}}{\rightarrow} |H\rangle_{808\text{ nm}} \otimes |V\rangle_{808\text{ nm}}$) via the Type-II spontaneous parametric down conversion (SPDC) [55,56] (see the Supplemental Material [57]). Because of the eight beams pumping the BBO crystal being coherent, the photon pairs are generated in a coherent superposition in different paths. Hence an eight-dimensional path-based entangled target state $|\phi_8^+\rangle = 1/\sqrt{8}\sum_{i=0}^{7}|ii\rangle$ (at 808 nm), distributed in red layers and green layers, respectively, is prepared. When using only the upper layer, we get a four-dimensional target state $|\phi_4^+\rangle = 1/\sqrt{4}\sum_{i=0}^{3}|ii\rangle$. Similarly working with two paths ("0" and "1") only we get a two-dimensional target state $|\phi_2^+\rangle = 1/\sqrt{2}\sum_{i=0}^{1}|ii\rangle$. The remaining 404 nm beams are removed after the BBO crystal by a DM, and the photons pairs are separated by a PBS. H photons are sent to Alice, while V photons are sent to Bob after using a phase-only SLM to manipulate the phase of incident photons. (b),(c): Multioutcome measurements for Alice and Bob. Sixteen adjustable intensity light emitting diode light sources in front of 16 couplers are used to introduce noise on each detector. The conversion of projective measurements between computational basis and subspace Fourier-transform basis can be realized by changing the angles of HWPs (see the Supplemental Material [57]).

$$K_d \geq \log_2(d) - H(\vec{e}_k) - H(\vec{e}_t). \tag{2}$$

A key technique we use from [50] is the splitting of the d-dimensional Hilbert space into d/k mutually exclusive subspaces of size k leading to additional postselection—Alice and Bob keep the measurement outcomes, only if they obtained results in the same subspace. The key rate is obtained separately in each subspace, and the final key rate is obtained as an average of d/k observed key rates.

In our experiment, we thus aim at creating a maximally entangled state in all d dimensions using path entanglement. To fully explore the high-noise regime in a controlled manner, we shine ambient light on each detector.

To explore the interplay of global and subspace dimensions, we study three cases of global dimension, $d = 8$, $d = 4$, and $d = 2$, with subspace dimensions $k = 2$, 4, and 8. For preparing the eight-dimensional target state $|\phi_8^+\rangle$, encoded in the path degree of freedom, we use three half-wave plates (HWPs) at 22.5° together with three BDs. Eight parallel beams are distributed to eight paths with the same energy by dividing the pump light equally. The light is produced by a continuous-wave diode laser at 404 nm, as shown in Fig. 1(a). Remarkably, it is easy to prepare the four-dimensional target state $|\phi_4^+\rangle$ if we only consider the upper layer (marked red in Fig. 1). To compensate for the phase between Alice and Bob, a spatial light modulator (SLM) is added to implement an arbitrary phase on the vertically polarized light [53].

In our setup we use polarization to control the path degree of freedom in order to implement eight-outcome measurements required for the protocol. Note, however, that in principle, our multioutcome measurement technique can be generalized to higher dimensions effectively [53]. By changing the angles of HWPs placed in parts (b) and (c) of Fig. 1, Alice and Bob can switch between the projective measurements used in the protocol (see the Supplemental Material [57]). Because of current limitations on the parallelism of beams in the beam displacer (BD), the mutually unbiased basis in dimension 8 would not reach the desired fidelity, a fact that will in the future be mitigated by improvements in BD manufacturing. Nonetheless, we generalized the protocol to work with mutually unbiased

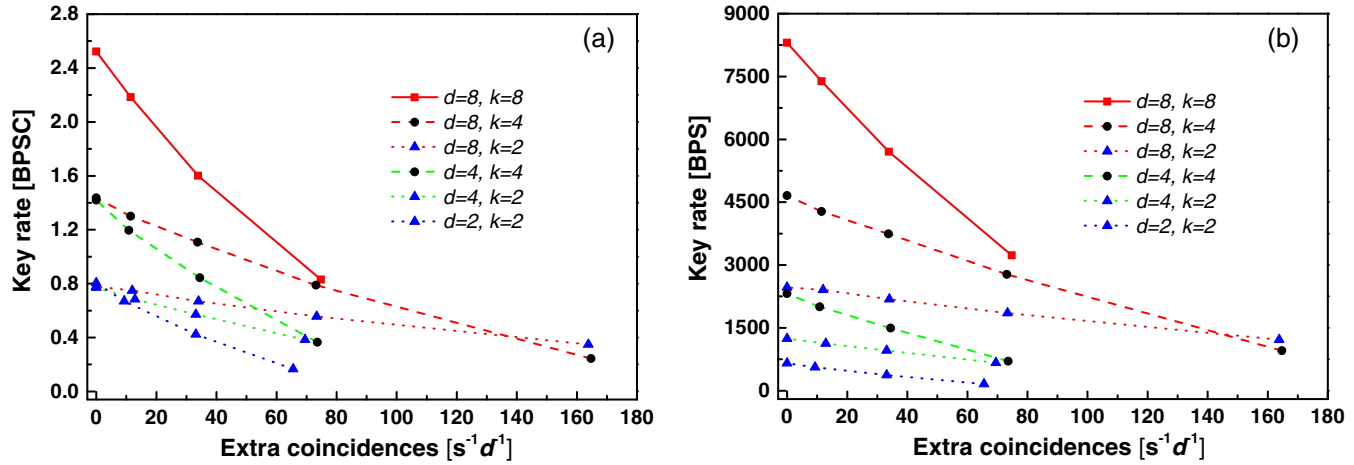

FIG. 2. The key rate of bits per subspace postselected coincidence (BPSC) (a), and of bits per second (BPS) (b) obtained in the eight-, four-, and two-(red, green, and blue)dimensional spaces. Noise is shown as average additional coincidences per second, divided by the local dimension (8, 4, and 2, respectively). The points (error bars are inside the symbols) represent the experimental values obtained by adding different levels of noise. The accurate experimental data are shown in Tables S6–S11 of the Supplemental Material [57].

subspace measurements with overlapping subspaces to certify security in eight dimensions, even without fully mutually unbiased measurements as described in the original protocol (see the Supplemental Material [57]). We record coincidences between all paths and compute both the secure key generated per selected photon pair (i.e., the average key rate per subspace postselected coincidence K_{BPSC}) and the resulting secure key per second ($K_{\mathrm{BPS}} = K_{\mathrm{BPSC}} \times \mathrm{TSCS}$, where TSCS is the total subspace coincidence per second). These results are plotted in Figs. 2(a) and 2(b). The key rate is computed from raw data by following the subspace protocol from Ref. [50] with key rate formula presented in Eq. (2) for different levels of physical noise, i.e., varying environmental conditions created by adding physical noise to the setup in a controlled fashion. This is achieved by putting independent noise sources in front of each optical coupler to introduce white noise, as shown in Figs. 1(b) and 1(c), respectively. These extra sources of noise lead to accidental coincidences in the data, which we use as a measure of physical environmental noise in the setup. Our noise parameter is described by the number of accidental coincidences added to the measurement data per second divided by the local dimension d, but it can be equivalently expressed by the value of parameter p in the experimental state

$$\rho_d = (1-p)\rho_d^{\mathrm{ent}} + p\frac{I_{d^2}}{d^2}, \tag{3}$$

where I_{d^2}/d^2 is the completely mixed state of a $d \times d$ dimensional quantum state, ρ_d^{ent} is the actual state our entanglement setup produces, and $p \in \{0, 0.025, 0.075, 0.15, 0.3\}$ (see the Supplemental Material [57]).

We perform six separate experiments, for eight, four, and two local paths (i.e., local dimensions) and subspace measurements in dimensions 2 and 4.

We observe that for low noise, we can obtain a much higher key rate K_{BPSC} by setting the subspace dimension k higher for the same global dimension d. However, with the noise increasing, using the subspaces with lower dimensions leads to stronger noise robustness. From the experimental results, we can see the key rate K_{BPSC} of $k = 4$ decreases rather fast compared with the cases with $k = 2$. Similar results are shown in subspaces with different dimensions when $d = 4$. Importantly, the robustness of the protocol also increases with the total dimension d. For example, the key rate K_{BPSC} of $k = 4$ decreases more slowly in $d = 8$ than in $d = 4$, and a similar observation can be made for $k = 2$.

One can notice that for all subspace sizes, K_{BPS} is effectively doubled when one compares $d = 8$ to $d = 4$ and $d = 2$. This occurs because doubling d also doubles the number of entangled pairs generated per second, as more beam paths are collected in detectors. TSCS therefore increases from ≈800 pairs per second in the case of $d = 2$ to ≈1600 pairs per second in the case of $d = 4$ and ≈3200 pairs per second in the case of $d = 8$ (see the Supplemental Material [57]). Note, however, that the increase of TSCS for higher dimensions can be expected also for fundamental reasons. Considering the damage threshold of nonlinear crystals (such as BBO) [58], the permitted maximal pump strength is proportional to the path dimension d, and one can, in principle, create more entangled pairs for higher d. This is because in path entanglement the crystal is pumped at multiple distinct locations and therefore heated more evenly.

The intricate relation between global and subspace dimension shows a clear pathway toward optimal usage of high-dimensional entanglement for quantum communication. While increasing the global dimension improves the achievable key rate and noise resistance simultaneously, it should be noted that it of course comes at the cost of increasing the number of detectors on each side. Another

interesting factor is the optimal subspace dimension, as it clearly shows that for low noise levels a high subspace dimension is optimal. On the other hand the noise resistance is achievable with decreasing subspace dimension as a function of noise. In experimental setups with constant signal to noise ratios this implies a single optimal subspace coding. In variable situations, such as complex quantum networks or free space communication it would seem prudent to consider an on-the-fly optimization of the subspace dimension to swiftly adapt to changing conditions. The particular scheme we use for creating spatial entanglement carries another distinct advantage for quantum communication. The fact that we coherently split the beam prior to pumping the crystal means that the pump laser is heating the crystal in a more distributed fashion, allowing for larger crystals and larger pump intensities before a limiting intensity is reached. This increases the potential number of entangled pairs per second and carries with it the potential to again increase the key rate by another physical mechanism. We also want to point out that there remains one significant pathway to improve the key rate by implementing more than two mutually unbiased basis (MUB) measurements in the test rounds. As shown in [37] using multiple MUB measurements should lead to an increase in both the amount of certified bits per round and noise resistance. However, we expect that high total dimension d and subspace size $k = 2$ will lead to the greatest noise resistance even in protocols using multiple MUB measurements. This is based on the following intuition: In high-noise regimes the distributed entangled state ρ can be expected to have a Schmidt number equal to 2 and thus measurements in subspaces of size 2 are best suited to fully utilize it in a QKD protocol.

In conclusion, by implementing the first entanglement-based, high-dimensional, and multioutcome QKD experiment, we were able to achieve key rates exceeding 1 bit of perfect key after error correction per photon pair. This significant increase even survived the artificial injection of additional accidentals through ambient light. By increasing the artificial noise, we were also able to demonstrate the superior noise resistance of subspace coding in high-dimensional systems and experimentally explore the intricate relationship between global dimension, subspace dimension, key rate, and noise. Our experiment proves the viability of high-dimensional coding for overcoming some of the most significant challenges of quantum communication and identifies novel pathways for noise resistant key distribution. Phase-stable distribution of path-based entangled states in real experimental conditions is a significant challenge that needs to be addressed before our approach can be used in practice. Path to orbital angular momentum conversion [59] or multicore fibers [60,61] could be the missing ingredient to take this proof of principle demonstration toward practical QKD implementation. Finally, the improved rate of entanglement distribution will be of interest to other entanglement-based applications beyond QKD.

This work was supported by the National Key Research and Development Program of China (No. 2017YFA0304100, No. 2016YFA0301300 and No. 2016YFA0301700), National Natural Science Foundation of China (Nos. 11774335, 11734015, 11874345, 11821404, 11904357), the Key Research Program of Frontier Sciences, CAS (No. QYZDY-SSW-SLH003), Science Foundation of the CAS (ZDRW-XH-2019-1), the Fundamental Research Funds for the Central Universities, USTC Tang Scholarship, Science and Technological Fund of Anhui Province for Outstanding Youth (2008085J02), Anhui Initiative in Quantum Information Technologies (Nos. AHY020100, AHY060300). X. G. acknowledges the support of Austrian Academy of Sciences (ÖAW) and Joint Centre for Extreme Photonics (JCEP). M. H. acknowledges funding from the Austrian Science Fund (FWF) through the STARTproject Y879-N27. M. P. acknowledges the support of Vedecká Grantová Agentúra MŠVVaŠ SR a SAV (VEGA) project 2/0136/19 and Grant Agency of Masaryk University (GAMU) project MUNI/G/1596/2019.

*bhliu@ustc.edu.cn
†cfli@ustc.edu.cn
‡xgao5@uottawa.ca
§pivoluskamatej@gmail.com
‖marcus.huber@univie.ac.at

[1] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014), theoretical Aspects of Quantum Cryptography–celebrating 30 years of BB84.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[4] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Adv. Opt. Photonics **12**, 1012 (2020).
[6] H. Delfs and H. Knebl, Symmetric-key cryptography, in *Introduction to Cryptography: Principles and Applications* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2015), pp. 11–48.
[7] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[8] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[10] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. Applied **10**, 064062 (2018).
[11] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[12] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
[13] C. A. Miller and Y. Shi, J. ACM **63**, 1 (2016).
[14] R. Arnon-Friedman, R. Renner, and T. Vidick, SIAM J. Comput. **48**, 181 (2019).
[15] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, Quantum Sci. Technol. **4**, 035011 (2019).
[16] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán *et al.*, Nature (London) **526**, 682 (2015).
[17] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).
[18] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán *et al.*, Phys. Rev. Lett. **115**, 250401 (2015).
[19] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[20] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).
[21] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).
[22] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[23] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).
[24] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **117**, 190501 (2016).
[25] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[26] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).
[27] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[28] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[29] J. L. Park, Found. Phys. **1**, 23 (1970).
[30] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[31] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, Cambridge, England, 2011).
[33] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Inf. **2**, 16025 (2016).
[34] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, Adv. Quantum Technol. **2**, 1900038 (2019).
[35] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[36] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[37] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301(R) (2010).
[38] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Sci. Rep. **3**, 2316 (2013).
[39] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, New J. Phys. **17**, 033033 (2015).
[40] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, Phys. Rev. A **96**, 022317 (2017).
[41] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, e1701491 (2017).
[42] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, Optica **4**, 1006 (2017).
[43] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, npj Quantum Inf. **3**, 25 (2017).
[44] D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, and L. K. Oxenløwe, Phys. Rev. Applied **11**, 064058 (2019).
[45] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, Quantum Sci. Technol. **4**, 035008 (2019).
[46] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, Phys. Rev. Applied **14**, 014051 (2020).
[47] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, New J. Phys. **17**, 022002 (2015).
[48] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, New J. Phys. **8**, 75 (2006).
[49] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Phys. Rev. A **88**, 032305 (2013).
[50] M. Doda, M. Huber, G. Murta, M. Pivoluska, M. Plesch, and C. Vlachou, Phys. Rev. Applied **15**, 034003 (2021).
[51] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Phys. Rev. X **9**, 041042 (2019).
[52] L. Dellantonio, A. S. Sørensen, and D. Bacco, Phys. Rev. A **98**, 062301 (2018).
[53] X.-M. Hu, W.-B. Xing, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, P. Erker, and M. Huber, Phys. Rev. Lett. **125**, 090503 (2020).
[54] I. Bengtsson, G. Adenier, C. A. Fuchs, and A. Y. Khrennikov, AIP Conf. Proc. **889**, 40 (2007).
[55] J. Schneeloch, S. H. Knarr, D. F. Bogorin, M. L. Levangie, C. C. Tison, R. Frank, G. A. Howland, M. L. Fanto, and P. M. Alsing, J. Opt. **21**, 043501 (2019).
[56] Z.-Y. J. Ou, *Multi-Photon Quantum Interference* (Springer, New York, 2007), Vol. 43.
[57] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.127.110505 for details about calculating key rate in $d = 8, k = 8$ case, multi-outcome measurements implementation, spontaneous parametric down-conversion process (SPDC) and multiphoton

noise. Further, supplemental material contains the description of noise loading and detailed experimental results.

[58] Y.-F. Huang, B.-H. Liu, L. Peng, Y.-H. Li, L. Li, C.-F. Li, and G.-C. Guo, Nat. Commun. **2**, 546 (2011).

[59] R. Fickler, R. Lapkiewicz, M. Huber, M. P. Lavery, M. J. Padgett, and A. Zeilinger, Nat. Commun. **5**, 4502 (2014).

[60] B. Da Lio, D. Cozzolino, N. Biagi, Y. Ding, K. Rottwitt, A. Zavatta, D. Bacco, and L. K. Oxenløwe, npj Quantum Inf. **7**, 63 (2021).

[61] X.-M. Hu, W.-B. Xing, B.-H. Liu, D.-Y. He, H. Cao, Y. Guo, C. Zhang, H. Zhang, Y.-F. Huang, C.-F. Li *et al.*, Optica **7**, 738 (2020).