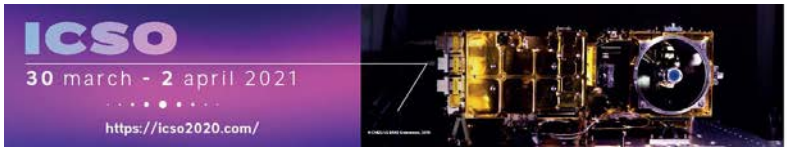
International Conference on Space Optics—ICSO 2020

Virtual Conference

30 March–2 April 2021

Edited by Bruno Cugny, Zoran Sodnik, and Nikos Karafolas



Photon-efficient quantum key distribution using multiqubit time-bin encoding

International Conference on Space Optics — ICSO 2020, edited by Bruno Cugny, Zoran Sodnik, Nikos Karafolas, Proc. of SPIE Vol. 11852, 118525J · © 2021 ESA and CNES
CCC code: 0277-786X/21/$21 · doi: 10.1117/12.2599962

Photon-efficient quantum key distribution using multiqubit time-bin encoding

Michał Jachura[a], Marcin Jarzyna[a], Marcin Pawłowski[b], and Konrad Banaszek[a,c]

[a]Centre for Quantum Optical Technologies, Centre of New Technologies,University of Warsaw, Banacha 2c, 02-097 Warszawa, Poland
[b]International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland
[c]Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warszawa, Poland

ABSTRACT

A method for photon-efficient quantum key distribution (QKD) is proposed and analyzed theoretically. The technique is based on nested encoding of multiple logical qubits into the discretized temporal degree of freedom of a single photon. The states of individual logical qubits are measured using a cascade of interferometric stages followed by time-resolved photon counting. The method may be useful in implementations of entanglement-based QKD protocols whose performance is limited by the brightness of onboard sources of nonclassical light, based e.g. on spontaneous parametric down-conversion. Numerical optimization taking into account the presence of background noise indicates the potential of multiqubit encoding for a nearly tenfold increase of the attainable key rate for entanglement-based LEO satellite QKD systems.

Keywords: Optical communication, photon counting, quantum entanglement

1. INTRODUCTION

Quantum key distribution (QKD) over satellite-to-ground optical links provides a way to establish a secure key for cryptographic purposes between two or more sites without deploying costly terrestrial network infrastructure.[1] Furthermore, entanglement-based QKD protocols allow legitimate users to treat the satellite as an untrusted node by verifying quantum correlations between photons emitted from an onboard source of non-classical light. Inherently low brightness of such sources[2,3] combined with substantial propagation losses makes it of paramount importance to use efficiently the photon flux reaching the receive terminals.[4,5] In this paper we present and analyze theoretically a method to extract multiple secret key bits from detection of individual photon pairs using qubit-based QKD protocols, such as E91[6] or BBM92.[7] The essential advantage of qubit-based QKD protocols is thorough theoretical understanding of their security.[8]

The method presented here is based on scalable encoding of m logical qubits into a single photon prepared as a superposition of 2^m time slots. Quantum states of individual qubits can be read out using a cascade of interferometric stages in a manner analogous to the recently proposed receiver for photon-efficient classical communication with BPSK signals.[9,10] As increasing the number of logical qubits encoded in one photon may augment the detrimental effects of broadband background optical radiation on the detected quantum correlations, we use a simple model to identify the optimal operating point determined by the attenuation of the satellite-to-ground optical channels and the background noise strength. Based on the parameters of the MICIUS mission,[11,12] numerical results indicate the potential of multiqubit encoding for a nearly tenfold increase of the attainable key rate for entanglement-based LEO satellite QKD systems.

Further author information: (Send correspondence to K.B.)
M.Jach.: E-mail: m.jachura@cent.uw.edu.pl, Telephone: +48 22 55 43 793
M.Jarz.: E-mail: m.jarzyna@cent.uw.edu.pl, Telephone: +48 22 55 43 751
M.P.: E-mail: marcin.pawlowski@ug.edu.pl, Telephone: +48 58 523 51 78
K.B.: E-mail: k.banaszek@uw.edu.pl, Telephone: +48 22 55 43 750

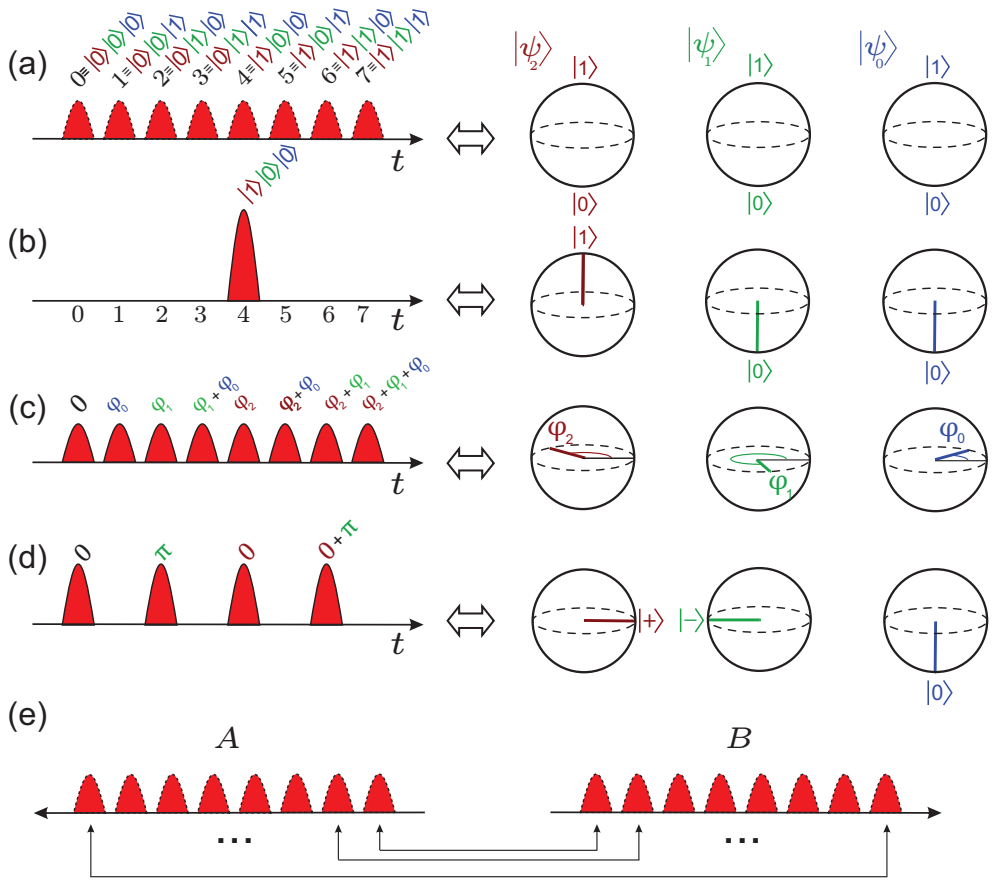


Figure 1. Encoding of multiple logical qubits into a single photon prepared as a superposition of temporal slots. (a) The slot number written in the binary representation specifies the basis states of individual qubits. (b) The presence of a photon in a single temporal slot corresponds to a product of qubit basis states. (c) An equally weighted superposition of a photon across all the slots with a hierarchy of relative phases is isomorphic to a product of equatorial states $\big(|0\rangle + e^{i\varphi_j}|1\rangle\big)/\sqrt{2}$. (d) An example of a combination of a product state and two equatorial states $|\pm\rangle = \big(|0\rangle \pm |1\rangle\big)/\sqrt{2}$. (e) A pair of photons, labeled with A and B, prepared in an entangled state with one-to-one correlations between individual temporal slots.

This paper is organized as follows. Sec. 2 describes the concept of multiqubit encoding. The scalable optical receiver in the form of a cascade of interferometric stages decoding the qubit states is presented in Sec. 3. Implementation of a multiqubit QKD protocol in the presence of background noise is modelled in Sec. 4 and optimized in Sec. 5. Finally, Sec. 6 concludes the paper.

2. MULTIQUBIT ENCODING

The principle of multiqubit encoding is shown schematically in Fig. 1(a). Suppose that a single photon occupies one of 2^m temporal slots. The kth temporal slot, where $k = 0, 1, \ldots, 2^m - 1$, corresponds to a combination of basis states $|0\rangle$ or $|1\rangle$ for each one of m logical qubits. The states of individual qubits are specified by digits in a binary string representing the integer k, as exemplified in Fig. 1(b). This mapping is naturally extended to superposition states. In particular, logical qubits prepared in equatorial states $\big(|0\rangle + e^{i\varphi_j}|1\rangle\big)/\sqrt{2}$ that are equally weighted superpositions of $|0\rangle$ and $|1\rangle$ correspond to the photon uniformly distributed across all 2^m slots. The phases φ_j of the equatorial states define a hierarchy of relative phases between temporal slots depicted in Fig. 1(c). As illustrated in Fig. 1(d), a combination of basis states and equatorial states, the latter taken for concreteness as $|\pm\rangle = \big(|0\rangle \pm |1\rangle\big)/\sqrt{2}$, is represented by the photon occupying only some of the temporal slots.

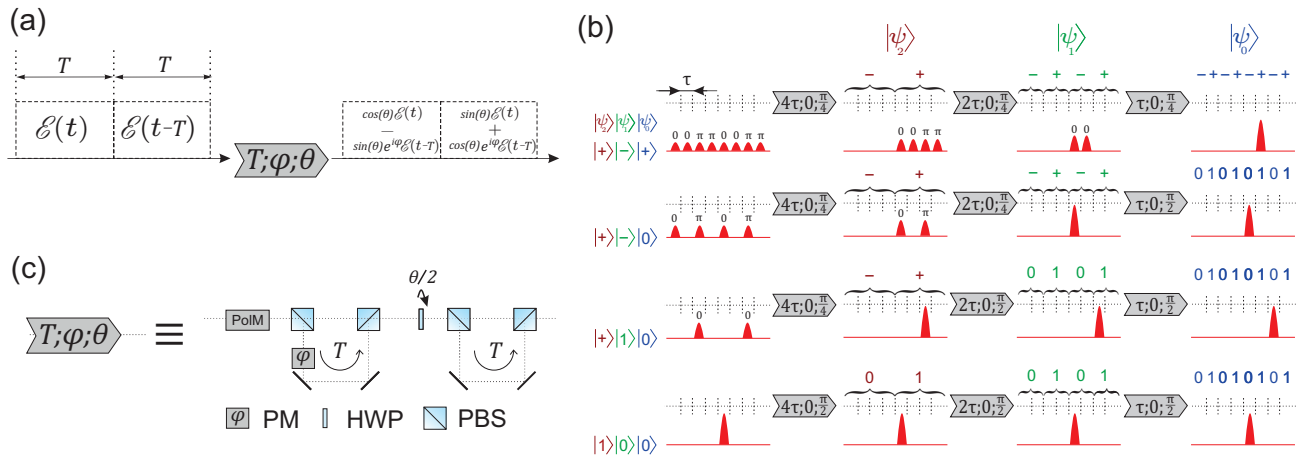


Figure 2. (a) An interferometric stage acting as a beam splitter combining the optical field in two adjacent time intervals of duration T. The parameters φ and θ determine the field transformation realized by the beam splitter. (b) Transformation introduced by a cascade of interferometric stages. With a suitable choice of beam splitter parameters, orthogonal pairs of states of logical qubits are bijectively mapped onto the temporal position of the photon at the output of the cascade. (c) Implementation of an interferometric stage based on polarization switching and polarization-dependent delay lines. PM, phase modulator; HWP, half-wave plate; PBS, polarizing beam splitter.

The above encoding is generalized in a straightforward manner to pairs of photons, labelled in Fig. 1(e) with indices A and B. Suppose that the two photons are generated in a quantum mechanical pure state such that the temporal locations of individual photons across all the 2^m slots are totally random, but they are perfectly correlated up to single slots. Such a state is formally equivalent to a set of m qubit pairs, each pair prepared in a maximally entangled state $|\Psi_+\rangle = \big(|0\rangle|0\rangle + |1\rangle|1\rangle\big)/\sqrt{2}$. In order to utilize this resource for a qubit-based QKD protocol, one needs a receiver implementing projection of individual logical qubits onto superposition states.

3. SCALABLE RECEIVER

The basic idea of the scalable receiver is to read out the states of individual logical qubits using a cascade of interferometric stages.[13] As depicted in Fig. 2(a), each stage acts as a beam splitter in the temporal domain, combining the optical field in pairs of adjacent time intervals. At the output of the cascade shown in Fig. 2(b), detecting the photon in a given temporal slot corresponds to projecting each of the logical qubits onto one of the two states constituting the measurement basis for that qubit. Importantly, the measurement basis can be selected independently for each of the logical qubits by an appropriate choice of the phase and the splitting ratio of the corresponding stage.

A possible realization of an interferometric module based on polarization switching, polarization-dependent delay lines, and birefringent elements is shown in Fig. 2(c). Unless adaptive optics is used in the receive telescope, the interferometers need to tolerate wavefront distortions introduced by atmospheric turbulence. Spatially multi-mode delay-line interferometers have been demonstrated in the context of space-to-ground optical communication links using the DPSK format[14] as well as time-bin qubit QKD over free-space channels.[15,16]

4. BACKGROUND NOISE

In practice, the number of logical qubits that can be usefully encoded into the temporal degree of freedom of single photons is limited by the effects of background radiation. Consider a model where the source produces entangled photon pairs at a rate R_{source} and the acceptance bandwidth of the spectral filter at the receiver entrance is adjusted in line with the slot rate, i.e. inversely with the slot duration. If broadband background radiation contributes to the incoming optical signal, the amount of noise allowed in by the filter can be then

treated as independent of the slot duration. Let n_b denote the mean number of background photons per slot. Further analysis will be carried out in the regime $n_b \ll 1$, typical for space communication systems operated at optical frequencies.

Let the power transmission of the optical channels from the source to each of the ground stations be equal and given by $\eta \ll 1$. This parameter can incorporate also the signal attenuation introduced by the transmit and receive optics as well as the non-unit efficiency of photodetectors. Further, let p_{pair} be the probability of generating a photon pair within a frame of 2^m slots. The leading-order contributions to the event rate R_{event} originate from coincidences between pairs of signal photons, $\eta^2 R_{\text{source}}$, coincidences between signal and background photons, $2{\cdot}2^m n_b{\cdot}\eta{\cdot}R_{\text{source}}$, coincidences between pairs of background photons, $(2^m n_b)^2{\cdot}p_{\text{pair}}^{-1}{\cdot}R_{\text{source}}$, and coincidences triggered by double photon pairs, $2 \cdot \eta^2 \cdot p_{\text{pair}} \cdot R_{\text{source}}$. Altogether this gives:

$$R_{\text{event}} = \eta^2[1 + 2 \cdot 2^m n_b/\eta + (2^m n_b/\eta)^2 \cdot p_{\text{pair}}^{-1} + 2p_{\text{pair}}]R_{\text{source}}. \tag{1}$$

Assuming symmetric collective attacks and ideal one-way postprocessing, the asymptotic key rate for qubit-based QKD protocols considered here reads:[8]

$$R_{\text{key}} = R_{\text{event}} \cdot m \cdot [1 - 2\mathsf{H}(\text{QBER})], \tag{2}$$

where $\mathsf{H}(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function and QBER stands for the quantum bit error rate. In the scenario under consideration, coincidences occurring between signal and background photons as well as those produced by pairs of background photons generate errors with the probability 50%. Furthermore, non-ideal optical interference in the receiver stages can be described[10] by a visibility parameter $V \leq 100\%$. If the logical qubits are measured in equatorial bases, a coincidence between two signal photons will also contribute to the QBER with the probability $(1 - V^2)/2$. Finally, double pairs produce 50% error probability if photons from different pairs are detected, and $(1 - V^2)/2$ error probability if photons from the same pair make it to the receiver, which yields the average error probability in this case equal to $\frac{1}{4}(2 - V^2)$. Consequently one has:

$$\text{QBER} = \frac{\frac{1}{2}[2 \cdot \eta \cdot 2^m n_b + (2^m n_b)^2 \cdot p_{\text{pair}}^{-1}] + \frac{1}{2}(1 - V^2)\eta^2 + \frac{1}{4}(2 - V^2) \cdot 2 \cdot \eta^2 \cdot p_{\text{pair}}}{\eta^2 + 2 \cdot \eta \cdot 2^m n_b + (2^m n_b)^2 \cdot p_{\text{pair}}^{-1} + 2 \cdot \eta^2 \cdot p_{\text{pair}}}. \tag{3}$$

Note that the channel transmission η and the background noise strength n_b enter the above expression through the ratio n_b/η. In order to ensure a positive key rate one needs $\mathsf{H}(\text{QBER}) < 1/2$, which translates to a very good approximation into a 11% threshold for the QBER at which quantum key distribution becomes impossible.

5. OPTIMIZATION

Further analysis will assume that the pair production rate R_{source} is independent of the slot duration. A useful performance metric is the amount of the cryptographic key per one detected signal photon pair, given by the ratio $R_{\text{key}}/(\eta^2 R_{\text{source}})$. This quantity depends on the ratio n_b/η, the pair probability p_{pair}, the visibility V of the interferometric modules in the receiver, as well as the number m of logical qubits encoded in one photon. Fig. 3(a-c) depicts the result of optimizing the ratio $R_{\text{key}}/(\eta^2 R_{\text{source}})$ over an integer m as a function of n_b/η for visibilities $V = 100\%$, 99%, and 98% and the pair generation probability $p_{\text{pair}} = 10^{-2}$. It is seen that with a diminishing noise contribution the benefit of multiqubit encoding becomes more substantial. As seen in Fig. 3(d-f), the optimal QBER stays at low single-digit percents which corresponds to high key contents per logical qubit. Non-unit visibility in the interferometric receiver has rather substantial effect on the attainable key rate.

Fig. 4 shows the actual key rate for the source brightness $R_{\text{source}} = 5.6 \cdot 10^6$ pairs/s as a function of the channel transmission η and the background noise strength n_b for the interference visibilities $V = 100\%$, 99%, and 98%. Regions corresponding to a given optimal number m^* of logical qubits are separated with white solid lines. The symbols "+" and "x" indicate respectively the best- and the worst-case operating conditions of the MICIUS mission[11,12] assuming that the time-bandwidth area selected by the receiver filter is equal to ten. It is seen that up to tenfold improvement in the key rate is possible, but this requires nearly ideal operation of the interferometric receiver.

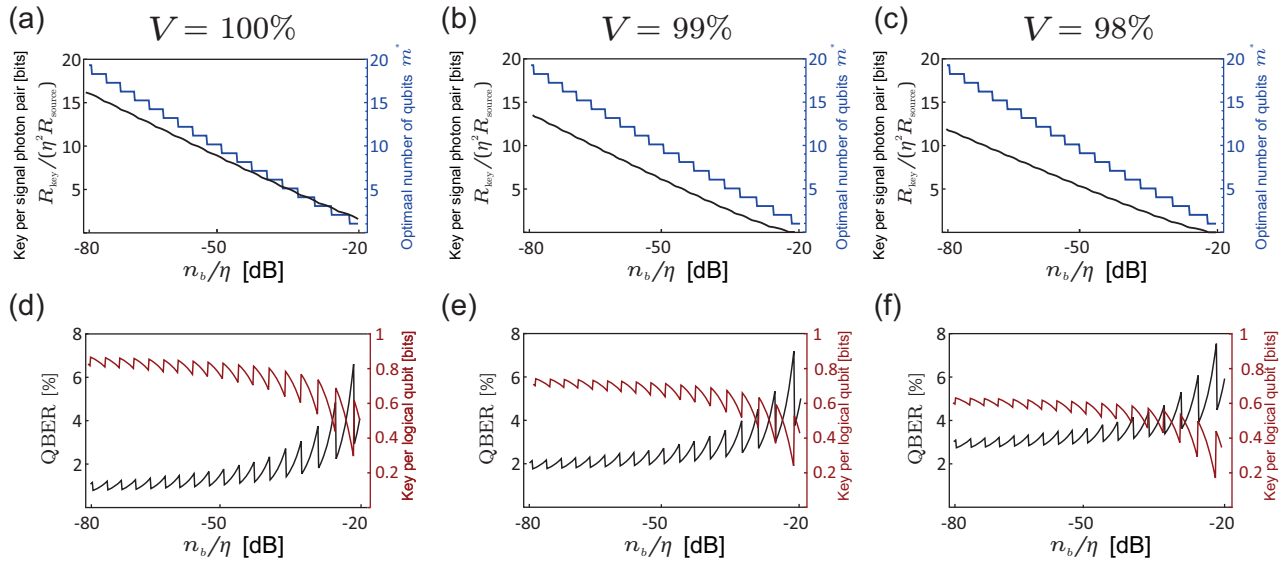


Figure 3. The key rate per one detected signal photon pair for the interference visibilities (a) $V = 100\%$; (b) $V = 99\%$; (c) $V = 98\%$ shown along with the optimal number of logical qubits m^* as a function of the ratio n_b/η which specifies the relative probability of detecting a background photon within one slot with respect to detecting a signal photon. The probability of producing a photon pair within one frame is $p_{\text{pair}} = 10^{-2}$. (d-f) The quantum bit error rate QBER for the optimal m^* and the resulting key amount in bits per one logical qubit.

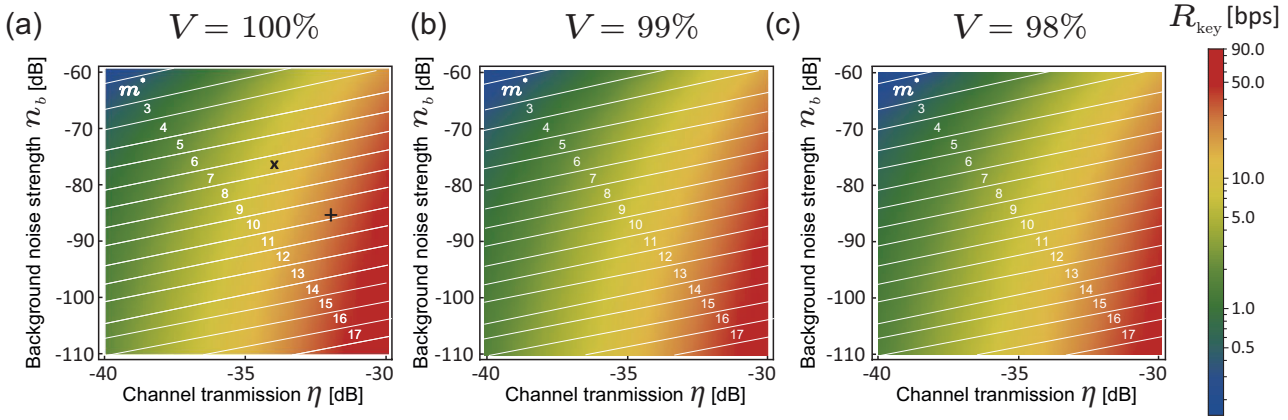


Figure 4. The key rate in bits per second for the source brightness $R_{\text{source}} = 5.6 \cdot 10^6$ pairs/s as a function of the optical channel transmission η and the background noise strength n_b for the interferometric visibility of the receiver stages: (a) $V = 100\%$; (b) $V = 99\%$; (c) $V = 98\%$. White lines separate regions corresponding to a given optimal number m^* of logical qubits. The symbols "+" and "x" indicate respectively the best- and the worst-case operating conditions of the MICIUS mission assuming that the time-bandwidth area selected by the receiver filter is equal to ten.

6. CONCLUSIONS

Scalable multiqubit time-bin encoding offers a method to boost the key rate in QKD scenarios limited by the brightness of sources of entangled photon pairs. Importantly, the key security can be analyzed using the well established theory developed for qubit-based protocols. It should be noted that this approach to security analysis makes rather conservative assumptions regarding eavesdropping strategies that can be pursued by the adversary. Further increase in key rates may be achieved by implementing QKD protocols designed for higher-dimensional discrete systems.[17–19]

Close attention needs to be paid to the design of entangled photon pair sources to ensure high production rates and good quality of quantum correlations.[20–23] The source characteristics should be matched by signal filtering at the receiver entrance to reduce as much as possible the contribution of background noise without substantial attenuation of the signal photon flux. Performance trade-offs inherent to conventional time-frequency filters[24] could be in principle relaxed by currently explored techniques for nonlinear coherent filtering.[25]

ACKNOWLEDGMENTS

This work is a part of the projects "Quantum Optical Technologies" and "International Centre for Theory of Quantum Technologies" carried out within the International Research Agendas programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund.

REFERENCES

[1] Bedington, R., Arrazola, J. M., and Ling, A., "Progress in satellite quantum key distribution," *npj Quantum Information* **3**(1), 30 (2017).

[2] Steinlechner, F., Trojek, P., Jofre, M., Weier, H., Perez, D., Jennewein, T., Ursin, R., Rarity, J., Mitchell, M. W., Torres, J. P., Weinfurter, H., and Pruneri, V., "A high-brightness source of polarization-entangled photons optimized for applications in free space," *Opt. Express* **20**(9), 9640–9649 (2012).

[3] Jachura, M., Karpiński, M., Radzewicz, C., and Banaszek, K., "High-visibility nonclassical interference of photon pairs generated in a multimode nonlinear waveguide," *Opt. Express* **22**(7), 8624–8632 (2014).

[4] Zhong, T., Zhou, H., Horansky, R. D., Lee, C., Verma, V. B., Lita, A. E., Restelli, A., Bienfang, J. C., Mirin, R. P., Gerrits, T., Nam, S. W., Marsili, F., Shaw, M. D., Zhang, Z., Wang, L., Englund, D., Wornell, G. W., Shapiro, J. H., and Wong, F. N. C., "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," *New Journal of Physics* **17**(2), 022002 (2015).

[5] Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., and Gauthier, D. J., "Provably secure and high-rate quantum key distribution with time-bin qudits," *Science Advances* **3**(11), e1701491 (2017).

[6] Ekert, A. K., "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, 661–663 (1991).

[7] Bennett, C. H., Brassard, G., and Mermin, N. D., "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.* **68**, 557–559 (Feb 1992).

[8] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M., "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, 1301–1350 (2009).

[9] Banaszek, K. and Jachura, M., "Structured optical receivers for efficient deep-space communication," in [*Proceedings of the IEEE International Conference on Satellite Optical Systems and Applications (ICSOS)*], 34–37 (2017).

[10] Zwoliński, W., Jarzyna, M., Kunz, L., Jachura, M., and Banaszek, K., "Photon-efficient communication based on BPSK modulation with multistage interferometric receivers," in [*46th European Conference on Optical Communication (ECOC 2020)*], We2F–5 (2020).

[11] Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., Li, G.-B., Lu, Q.-M., Gong, Y.-H., Xu, Y., Li, S.-L., Li, F.-Z., Yin, Y.-Y., Jiang, Z.-Q., Li, M., Jia, J.-J., Ren, G., He, D., Zhou, Y.-L., Zhang, X.-X., Wang, N., Chang, X., Zhu, Z.-C., Liu, N.-L., Chen, Y.-A., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y., and Pan, J.-W., "Satellite-based entanglement distribution over 1200 kilometers," *Science* **356**(6343), 1140–1144 (2017).

[12] Yin, J., Li, Y.-H., Liao, S.-K., Yang, M., Cao, Y., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, S.-L., Shu, R., Huang, Y.-M., Deng, L., Li, L., Zhang, Q., Liu, N.-L., Chen, Y.-A., Lu, C.-Y., Wang, X.-B., Xu, F., Wang, J.-Y., Peng, C.-Z., Ekert, A. K., and Pan, J.-W., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature* **582**(7813), 501–505 (2020).

[13] Jachura, M., Jarzyna, M., Pawłowski, M., and Banaszek, K., "Scalable interferometric receiver for photon-efficient quantum communication," in [*OSA Quantum 2.0 Conference*], QTh5A.3 (2020).

[14] Sodnik, Z. and Sans, M., "Extending EDRS to laser communication from space to ground," in [*International Conference on Space Optical Systems and Applications (ICSOS)*], (2012).

[15] Jin, J., Agne, S., Bourgoin, J.-P., Zhang, Y., Lütkenhaus, N., and Jennewein, T., "Demonstration of analyzers for multimode photonic time-bin qubits," *Phys. Rev. A* **97**(4), 043847 (2018).

[16] Cahall, C., Islam, N. T., Gauthier, D. J., and Kim, J., "Multimode time-delay interferometer for free-space quantum communication," *Phys. Rev. Applied* **13**, 024047 (2020).

[17] Cerf, N. J., Bourennane, M., Karlsson, A., and Gisin, N., "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.* **88**, 127902 (2002).

[18] Huber, M. and Pawłowski, M., "Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement," *Phys. Rev. A* **88**, 032309 (2013).

[19] Niu, M. Y., Xu, F., Shapiro, J. H., and Furrer, F., "Finite-key analysis for time-energy high-dimensional quantum key distribution," *Phys. Rev. A* **94**, 052323 (2016).

[20] U'Ren, A. B., Banaszek, K., and Walmsley, I. A., "Photon engineering for quantum information processing," *Quantum Info. Comput.* **3**(7), 480–502 (2003).

[21] Kolenderski, P., Wasilewski, W., and Banaszek, K., "Modeling and optimization of photon pair sources based on spontaneous parametric down-conversion," *Phys. Rev. A* **80**, 013811 (2009).

[22] Torres, J. P., Banaszek, K., and Walmsley, I., "Engineering nonlinear optic sources of photonic entanglement," *Progress in Optics* **56**, 227–331, Elsevier (2011).

[23] Anwar, A., Perumangatt, C., Steinlechner, F., Jennewein, T., and Ling, A., "Entangled photon-pair sources based on three-wave mixing in bulk crystals," arXiv:2007.15364 (2020).

[24] Raymer, M. G. and Banaszek, K., "Time-frequency optical filtering: efficiency vs. temporal-mode discrimination in incoherent and coherent implementations," *Opt. Express* **28**(22), 32819–32836 (2020).

[25] Brecht, B., Reddy, D. V., Silberhorn, C., and Raymer, M. G., "Photon temporal modes: A complete framework for quantum information science," *Phys. Rev. X* **5**(4), 041017 (2015).