ICSO 2016

International Conference on Space Optics

Biarritz, France

18–21 October 2016

Edited by Bruno Cugny, Nikos Karafolas and Zoran Sodnik

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES
esa
ICSO
International Conference on Space Optics
2016
Biarritz, France
18-21 October
www.icso2016.com

Benefits of time-frequency coding for quantum key distribution

J. Rödiger

N. Perlot

O. Benson

R. Freund

International Conference on Space Optics — ICSO 2016, edited by Bruno Cugny, Nikos Karafolas,
Zoran Sodnik, Proc. of SPIE Vol. 10562, 105623N · © 2016 ESA and CNES
CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2296180

BENEFITS OF TIME-FREQUENCY CODING FOR QUANTUM KEY DISTRIBUTION

J. Rödiger[1,2], N. Perlot[1], O. Benson[2], R. Freund[1]
[1]*Fraunhofer Heinrich Hertz Institute, Germany.* [2]*Humboldt-Universität zu Berlin, AG Nanooptik, Germany*

I. INTRODUCTION

Quantum key distribution (QKD), the first applicable quantum technology, is able to distribute a secret key to two parties. This key can then be used as a one-time-pad for absolutely secure communication. The first QKD protocol was the polarization based BB84 protocol proposed in [1]. Since then many QKD protocols have been proposed and investigated [2, 3].

Establishing a trusted node QKD network over satellites is a promising way of making quantum-secure communication ready to use for secret communication over large distances. For such a network a suitable QKD protocol is needed. Here we present a QKD protocol well suited for satellite QKD, the time-frequency (TF-) QKD protocol, and outline how a global QKD network could be implemented with satellites using today's technology.

The TF-QKD protocol in its discrete form was proposed by [4, 5] and is based on the time-frequency uncertainty relation and is a BB84-like QKD protocol with the two bases being realized by discrete modulations in time and frequency, namely the pulse position modulation (PPM) and frequency shift keying (FSK). With one photon per pulse, measuring in one of the bases increases the uncertainty in the other basis and thus deletes the information possibly encoded therein. An implementation of the TF-QKD protocol was reported in [6] and another implementation using entangled photons in [7]. Aspects concerning eavesdropping [8] and turbulence in free-space channels [9] were discussed. Furthermore, TF protocols using continuous instead of discrete variables are addressed by current research as well [10-14].

As will be shown, the TF-QKD protocol is well suited for free-space QKD and highly compatible with classical communication systems which makes TF-QKD a good choice for satellite-based QKD networks.

II. PRINCIPLE OF THE TIME-FREQUENCY QKD PROTOCOL

A. The BB84 protocol

We first recall the basic concept of the BB84 protocol which mostly applies to the TF protocol. In the BB84 protocol linear polarization of single photons is used to form two bases, each consisting of two symbols, which carry the information [1, 15, 16]. The two symbols of each base are represented by two orthogonal orientations of polarization, namely 0° and 90° for one basis and +45° and -45° for the other (Fig. 1).

The photons are prepared randomly in one of the two bases by a sender (Alice) and sent to a receiver (Bob) who measures the photons, again randomly, in one of the two bases. Due to the bases' properties, measuring in the wrong basis leads to a random outcome and deletes the sent information. After the transmission of single-photon pulses, Alice and Bob communicate over a classical channel which bases they have chosen and only keep the information from photons with coinciding bases. The result is called the sifted key. The fundamental idea of QKD relies on the fact that an Eavesdropper (Eve) also has to choose a measurement basis randomly (she cannot measure in both bases while still getting the full information possibly stored in each), leading to bit errors that will be propagated to Bob. Alice and Bob can detect those errors by comparing a fraction of the photons (which will then be discarded) and deduce Eves knowledge of the sifted key. If Eve's information on the sifted key is larger than Alice's and Bob's, the key distribution process needs to be canceled and redone. If Alice's and Bob's information is larger, they can use classical error-correction and privacy amplification to shorten the sifted key to a private and identical key. This key can be used for example as a one-time pad for absolute secure communication. For more details see [3].

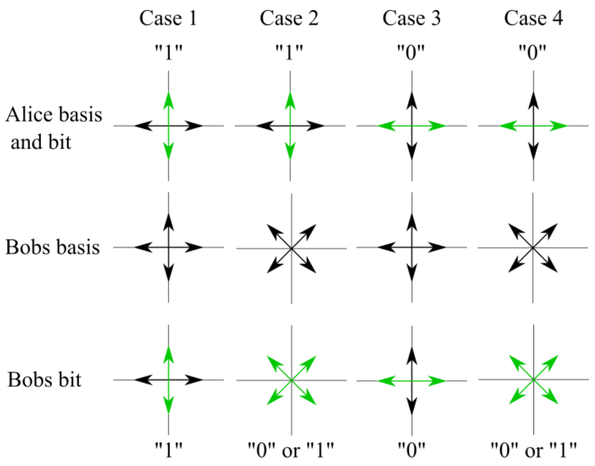
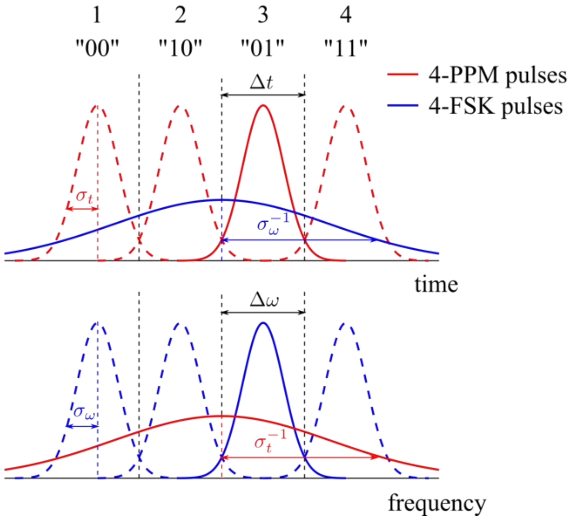


Fig. 1. In this example Alice sends four photons, all in the 0°/90° Basis. Bob changes his measurement basis randomly. He gets the correct symbol, when he is in the same basis as Alice and a random symbol, when he is not.

B. The time-frequency QKD protocol

For the TF-QKD protocol, the time-frequency uncertainty relation prevents Eve from getting the full information in both bases. *M*-PPM and *M*-FSK symbols represent the time and frequency bases, respectively. These two orthogonal modulations feature, in the time or frequency domain, *M* pulse slots, in which a single photon is sent or measured (Fig. 2 a)). Each PPM (FSK) pulse is represented by a symbol pulse in the time (frequency) domain carrying the information and a conjugated pulse in the frequency (time) domain, which contains no information at all. Although different pulse shapes can be used, we choose pulses with Gaussian shapes because they offer time-frequency symmetry and can be easily generated.



a)

	Pulse width	Pulse separation	Conjugated pulse width
Time	σ_t	$\Delta t = 2\sigma_t$	$\sigma_\omega^{-1} = M\sigma_t$
	25 ps	50 ps	100 ps
Freq.	σ_ω	$\Delta\omega = 2\sigma_\omega$	σ_t^{-1}
	10 GHz	20 GHz	40 GHz

b)

Fig. 2. a) Example of transmitted symbols in the time (red) and frequency (blue) bases. Each photon is represented by a pulse with either time or frequency information. Each pulse represents exactly one photon, thus they can be seen as the probability distribution of the photon being measured at a certain position in the time or in the frequency domain. The filter boundaries of Bob's measurement devices are marked as vertical dashed black lines. **b)** Possible values for pulse width and separation in both bases for $M = 4$ symbols per basis. Those pulse parameters can be implemented with today's technology.

To measure in one basis, a filter is needed which decreases the uncertainty in this basis while simultaneously increasing the uncertainty in the other. This is similar to the BB84 protocol where a wrong-basis measurement changes the polarization of a photon and hereby deletes its information.

Measuring in the wrong basis leads to a random result if the conjugated pulses are wide enough. For a good overlap between the symbol pulses and the conjugated pulses, the conjugated pulses shall be roughly M times wider than the slots. In addition, the symbol pulse should be as wide as the slots to prevent gaps between the pulses. Finally, assuming Fourier-limited pulses, the width of a pulse is inverted after its Fourier transform. . The parameters in Fig. 2 b) obey these three relationships and are a good compromise between available technology for time as well as for frequency filters. A conceptual difference in comparison to the BB84 protocol is the already mentioned possibility to use more than two symbols in each basis increasing the number of bits carried by each photon. In Fig. 2 the example of $M = 4$ symbols per basis is shown.

C. Setup

The advantage of the time frequency protocol is that it can be implemented mainly from off-the-shelf telecom components. This is especially true for a single-mode fiber (SMF) based setup, since many components are working with SMFs. A proposed setup is shown in Fig. 3.

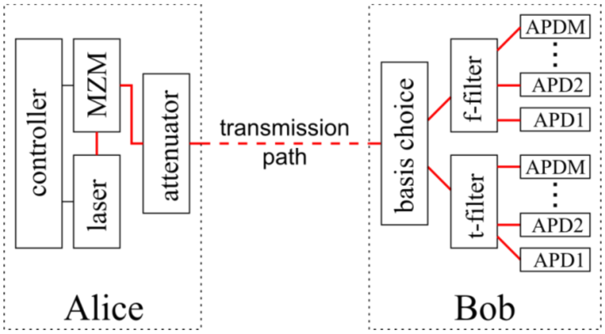


Fig. 3. Suggested implementation of the TF-QKD protocol. Mainly off-the-shelf telecom components are used in this implementation. The solid red lines represent single-mode fibers (SMF), the dashed red line represents the transmission path, which could be a fiber, the atmosphere, water or outer space. A tunable laser, a Mach-Zehnder modulator (MZM) to shape the pulses, a controller for steer the laser and the MZM and an attenuator to obtain single photon level are used for Alice's setup. A basis switch (for example a MZM with two usable outputs or a beamsplitter), frequency (f-) and time (t-) filters (for example cascaded standard demultiplexers and MZM) and a suitable number avalanche photo-detectors (APD) are used for Bob's setup. In Alice's part of the setup, a tunable laser (which will later be attenuated) creates photons with the desired central wavelength which are then shaped by a Mach-Zehnder modulator (MZM). Although lasers do not provide perfect single photons (there is some probability that multi-photon pulses occur) it is possible to still preserve security with the so called decoy state method [17-19].

Assuming Fourier-limited pulses, shaping them with the MZM in the time domain also shapes them in the frequency domain. Both the laser and the MZM must be controlled, for example by arbitrary-waveform generators operated with a computer. After forming the pulses, they need to be attenuated to single-photon level, typically between 0.1 and 0.5 photons per pulse.

The photons are now guided to Bob. Depending on the transmission path (which can be a fiber, the atmosphere, water or outer space) additional devices such as optical antennas for free-space communication, are needed. Note, that due to the quantum mechanical no-cloning theorem, single photons cannot be duplicated or amplified with retaining their states (quantum repeaters [20, 21] could someday be used as amplifiers for quantum communication but are far off from being market-ready). This implies that occurring losses in the transmission path and in Bob's setup decrease the key rate and thus limits the distance over which a key can be distributed [22, 23].

Bob firstly needs to guide the photons to either the time or the frequency basis. This can be done actively (for example by a MZM with two usable outputs) or passively (for example with a beam splitter). The next step is to respectively filter the photons in time or in frequency. As frequency filters, standard SMF demultiplexers can be used while MZMs can function as time filters (the MZMs only have two outputs and thus need to be cascaded for $M > 2$). Each filter output must then be terminated by a single-photon detector, e.g. an Avalanche photon diodes (APD). Depending on the available components, optical filtering can implemented differently. One superconducting nanowire single photon detector (SNSPD) [24, 25] could be used as the time and (for example with a prior dispersive element) as a frequency resolving detector. The SNSPDs need to be cooled with liquid helium which is technically challenging and expensive, but the number of detectors can be reduced significantly when a higher number M of symbols per basis is used. In addition, the dead time of SNSPDs is much shorter than the dead time of APDs.

III. SATELLITE QUANTUM COMMUNICATION WITH THE TF-QKD PROTOCOL

A. Compatibility with classical communication

The TF-QKD protocol has the following advantages:

- With the exception of single-photon detectors, the TF-QKD protocol can be implemented with off-the-shelf telecom components.
- 1550-nm photons can be used, which on the one hand offers a wide variety of high-end components from classical communication and on the other hand absorption in atmospheric channels is low..
- PPM is a common modulation for classical optical communication with satellites.
- Polarization is unused in TF-QKD (contrary to polarization-based BB84) and thus can be used for duplexing.
- With PPM and FSK, it is possible to use an arbitrarily large alphabet and thus to transmit more than 1 bit/photon.

TF-QKD is thus a good protocol candidate for satellite based QKD networks.

B. QKD links over satellite

As mentioned before QKD over fiber or ground-based free-space channels have a limited reach. Up to now, distances no larger than 307 km over fiber [22] and 144 km over free-space [23] have been demonstrated. QKD over satellites, however, offers a much larger coverage with an attenuation that scales quadratically (and not exponentially) with the distance.. Different issues regarding satellite QKD are discussed in the literature like for example in [26-29].

In principle all satellite orbits are suitable for establishing QKD-links. However, for higher altitude satellites like geostationary (GEO) satellites the high loss makes it very challenging to implement single-photon based communication. Thus in the following we will only consider low-earth-orbit (LEO) satellites with an altitude between 200 and 2000 km.

For the downlink, the receiving telescope on ground can be large provided that all the power can be coupled to the photodetector. For the uplink, the transmitting telescope aperture, and thus the antenna directivity, on ground may not be as large because the beam pointing is more challenging. This results in an asymmetry in the achievable secret key rate between up- and downlinks. If SMF receiver is used without adaptive optics, then up and downlinks are symmetrical and will provide the same key rate.

C. Satellite based QKD networks

Any QKD network needs to have some kind of nodes, firstly to overcome the distance limits of a few hundred kilometers and secondly to switch between different users that pair up to communicate secretly. Since untrusted-node networks (where Eve is allowed to have access to the nodes, without the security being corrupted, for example with the help of quantum repeaters [20, 21]) are not yet ready for use, trusted-node networks (where Eve is not allowed to have access to the nodes) are currently the only possibility to be used in QKD networks. Some examples of trusted-node satellite QKD networks are given in [30].

As an example, a trusted-node satellite QKD network is presented in the following using LEO satellites (see also Fig. 4). The loss of satellites with higher altitudes would be higher decreasing the secret key rate. Two parties called Bob and Charlie, which both have to be in the line of sight of the satellite at some point on its orbit, want to share a secret key. Therefor the satellite first shares a secret key B with Bob, when they have a line-of-sight link and later, when Charlie has a line-of-sight link with the satellite, they share a second secret key C of equal length. Both keys are then added modulo-wise and the resulting key AB is announced publicly. Both

Bob and Charlie can deduce the key of the respectively other party with help of their key and the key AB. Either key B or key C (both now known by Bob and Charlie) can now be used for secret one-time pad communication. A network of satellites could connect every point on earth surface, enabling worldwide quantum communication.

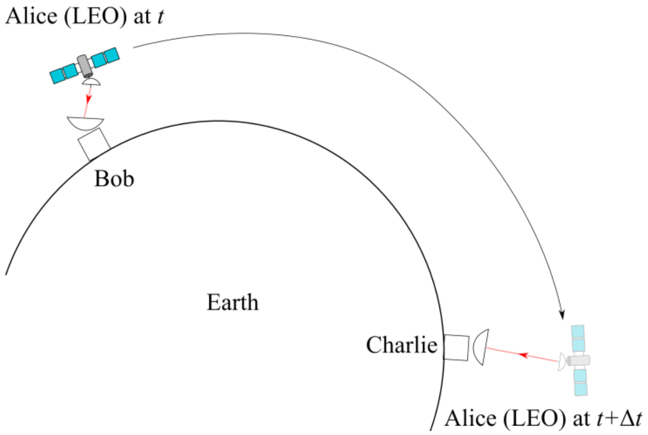


Fig. 4. An Example for satellite QKD is shown which enables absolute secure communication between Bob and Charlie. The satellite, representing Alice, first shares a secret key with Bob and later with Charlie. Bob and Charlie can deduce the key of each other with help from Alice who announces the modulo-wise added sum of Bob's and Charlie's key. Either Bob's or Charlie's key can be used for one-time-pad encrypted communication.

IV. CONCLUSION

The TF-QKD protocol is a promising candidate for being implemented in free-space QKD, especially satellite QKD. Such a scenario where LEO satellites are used as trusted nodes in a worldwide QKD network is presented. Using the TF-QKD protocol combined with the presented satellite based QKD network would be a promising method for distributing absolute secure keys worldwide, especially with respect to the compatibility with off-the-shelf technology.

REFERENCES

[1] H. Bennett Ch and G. Brassard, "Quantum cryptography: public key distribution and coin tossing int," in *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, 1984, pp. 175–9.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[4] Z. Chang-Hua, P. Chang-Xing, Q. Dong-Xiao, G. Jing-Liang, C. Nan, and Y. Yun-Hui, "A new quantum key distribution scheme based on frequency and time coding," *Chinese Physics Letters*, vol. 27, no. 9, p. 090301, 2010.

[5] S. Yelin and B. C. Wang, "Time-frequency bases for bb84 protocol," *arXiv preprint quant-ph/0309105*, 2003.

[6] M. Leifgen, R. Elschner, N. Perlot, C. Weinert, C. Schubert, and O. Benson, "Practical implementation and evaluation of a quantum-key-distribution scheme based on the time-frequency uncertainty," *Physical Review A*, vol. 92, no. 4, p. 042311, 2015.

[7] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," *Physical review letters*, vol. 98, no. 6, p. 060503, 2007.

[8] Y. Zhang, I. B. Djordjevic, and M. A. Neifeld, "Weak-coherent-state-based time-frequency quantum key distribution," *Journal of Modern Optics*, vol. 62, no. 20, pp. 1713–1721, 2015.

[9] X. Sun, I. B. Djordjevic, and M. A. Neifeld, "An adaptation method to improve secret key rates of time-frequency qkd in atmospheric turbulence channels," in *SPIE LASE*. International Society for Optics and Photonics, 2016, pp. 97390Z–97390Z.

[10] L. Zhang, C. Silberhorn, and I. A. Walmsley, "Secure quantum key distribution using continuous variables of single photons," *Physical review letters*, vol. 100, no. 11, p. 110504, 2008.

[11] B. Qi, “Quantum key distribution based on frequency-time coding: security and feasibility,” *arXiv preprint arXiv:1101.5995*, 2011.

[12] J. Nunn, L. Wright, C. Söller, L. Zhang, I. Walmsley, and B. Smith, “Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion,” *Optics express*, vol. 21, no. 13, pp. 15959–15973, 2013.

[13] Z. Zhang, J. Mower, D. Englund, F. N. Wong, and J. H. Shapiro, “Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry,” *Physical review letters*, vol. 112, no. 12, p. 120506, 2014.

[14] B. Qi, “Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation,” *Optics letters*, vol. 31, no. 18, pp. 2795–2797, 2006.

[15] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[16] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.

[17] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[18] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Physical Review Letters*, vol. 94, no. 23, p. 230504, 2005.

[19] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.

[20] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, “Quantum repeaters based on atomic ensembles and linear optics,” *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[21] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: the role of imperfect local operations in quantum communication,” *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[22] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photonics*, vol. 9, no. 3, pp. 163–168, 2015.

[23] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova *et al.*, “Quantum teleportation over 143 kilometres using active feed-forward,” *Nature*, vol. 489, no. 7415, pp. 269–273, 2012.

[24] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, “Superconducting nanowire single-photon detectors: physics and applications,” *Superconductor science and technology*, vol. 25, no. 6, p. 063001, 2012.

[25] E. A. Dauler, M. E. Grein, A. J. Kerman, F. Marsili, S. Miki, S. W. Nam, M. D. Shaw, H. Terai, V. B. Verma, and T. Yamashita, “Review of superconducting nanowire single-photon detector system design options and demonstrated performance,” *Optical Engineering*, vol. 53, no. 8, pp. 081907–081907, 2014.

[26] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein, “How to implement decoy-state quantum key distribution for a satellite uplink with 50-db channel loss,” *Physical Review A*, vol. 84, no. 6, p. 062326, 2011.

[27] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang *et al.*, “Direct and full-scale experimental verifications towards ground-satellite quantum key distribution,” *Nature Photonics*, vol. 7, no. 5, pp. 387–393, 2013.

[28] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, “Air-to-ground quantum communication,” *Nature Photonics*, vol. 7, no. 5, pp. 382–386, 2013.

[29] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, “Feasibility of satellite quantum key distribution,” *New Journal of Physics*, vol. 11, no. 4, p. 045017, 2009.

[30] D. Elser, S. Seel, F. Heine, D. Finocchiaro, R. Campo, A. Recchia, A. L. Pera, T. Länger, M. Peev, T. Scheidl, and R. Ursin, “Network architectures for space-optical quantum cryptography services,” in *Proc. International Conference on Space Optical Systems and Applications (ICSOS) 2012*, Ajaccio, Corsica, 2012, pp. Post–1.