ÓPTICA PURA Y APLICADA
www.sedoptica.es

Type: RESEARCH PAPER
Section: Quantum and Non-Linear Optics

Quantum key distribution via frequency translation in a nonlinear optical fiber

Distribución cuántica de claves via translación de frecuencia en fibras ópticas no lineales

J. Bonetti[1], S. M. Hernandez[1*,2], D. F. Grosz[1,2]

1. Grupo de Comunicaciones Ópticas, Depto. de Ingeniería en Telecomunicaciones, Instituto Balseiro, Comisión Nacional de Energía Atómica, Río Negro 8400, Argentinan

2. Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), CABA 1425, Argentina

(*)E-mail: shernandez@ib.edu.ar

Received: 15/11/2022 Accepted: 16/05/2023
DOI: 10.7149/OPA.56.2.51118

ABSTRACT:

We propose a simple and original implementation of the BB84 quantum key distribution protocol via a quantum frequency-translation process in a nonlinear optical fiber. Unlike most conventional quantum key distribution implementations, which rely on the photon polarization/phase, encoding quantum information in the photon frequency state is inherently more stable against mechanical and/or thermal fluctuations over transmission media such as optical fibers. We also show the proposed scheme to be naturally expandable to larger character sets, and demonstrate a straightforward extension to a four-character alphabet (qu-quarts), providing enhanced security for quantum key distribution applications.

Key words: quantum key distribution, quantum frequency translation, BB84

RESUMEN:

Proponemos una aplicación simple y original del proceso de translación cuántica de frecuencias en una fibra no lineal a un protocolo BB84 de distribución cuántica de claves. A diferencia de la mayoría de las implementaciones de la distribución cuántica de claves, que utilizan la fase o la polarización de los fotones, codificar la información cuántica en el estado de frecuencia del fotón es inherentemente más estable frente a fluctuaciones ya sea mecánicas o térmicas sobre medios de transmisión como las fibras ópticas. También mostramos que el esquema propuesto puede escalar naturalmente a alfabetos más grandes, en particular demostramos la extensión a un alfabeto de 4 símbolos, proporcionando mayor seguridad a aplicaciones de distribución cuántica de claves.

Palabras clave: distribución cuántica de claves, translación cuántica de frecuencias, BB84

REFERENCES AND LINKS / REFERENCIAS Y ENLACES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of modern physics **74**(1), 145 (2002).

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing." Theor. Comput. Sci. **560**(P1), 7–11 (2014).

[3] M. Fox, Quantum optics: an introduction, vol. 15 (OUP Oxford, 2006).

[4] 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 **9**(3), 163–168 (2015).

[5] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. Lita, A. Miller, and J. Nordholt, "Long-distance quantum key distribution in optical fibre," New Journal of Physics **8**(9), 193 (2006).

[6] N. Namekata, S. Mori, and S. Inoue, "Quantum key distribution over an installed multimode optical fiber local," Optics express **13**(25), 9961–9969 (2005).

[7] 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," Physical Review Letters **93**(18), 180,502 (2004).

[8] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," Applied Physics Letters **112**(17), 171,108 (2018).

[9] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, "Efficient time-bin encoding for practical high-dimensional quantum key distribution," Physical Review Applied **14**(1), 014,051 (2020).

[10] N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, and D. J. Gauthier, "Robust and stable delay interferometers with application to d-dimensional time-frequency quantum key distribution," Physical Review Applied **7**(4), 044,010 (2017).

[11] 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 **21**(13), 15,959–15,973 (2013).

[12] N. Gisin, "Statistics of polarization dependent losses," Optics communications **114**(5-6), 399–405 (1995).

[13] D. Bouwmeester, A. Ekert, A. Zeilinger, et al., The physics of quantum information, vol. 3 (Springer, Berlin, 2000).

[14] M. Bloch, S. W. McLaughlin, J.-M. Merolla, and F. Patois, "Frequency-coded quantum key distribution," Optics letters **32**(3), 301–303 (2007).

[15] I. M. Gabdulhakov and O. G. Morozov, "Frequency coded quantum key distribution channel based on photon amplitude-phase modulation," in Systems of Signal Synchronization, Generating and Processing in Telecommunications (SINKHROINFO), 2017, pp. 1–5 (IEEE, 2017).

[16] K. Rohit and T. Srinivas, "High Dimensional Quantum Key Distribution: BB84 Protocol using qudits," in International Conference on Fibre Optics and Photonics, pp. Th3A–77 (Optical Society of America, 2016).

[17] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," Physical Review A **61**(6), 062,308 (2000).

[18] P. Kumar, "Quantum frequency conversion," Optics letters **15**(24), 1476–1478 (1990).

[19] C. McKinstrie, J. Harvey, S. Radic, and M. Raymer, "Translation of quantum states by four-wave mixing in fibers," Optics Express **13**(22), 9131–9142 (2005).

[20] H. McGuinness, M. Raymer, C. McKinstrie, and S. Radic, "Quantum frequency translation of single-photon states in a photonic crystal fiber," Physical review letters **105**(9), 093,604 (2010).

[21] G. P. Agrawal, Nonlinear fiber optics (Academic press, 2007).

[22] A. S. Clark, S. Shahnia, M. J. Collins, C. Xiong, and B. J. Eggleton, "High-efficiency frequency conversion in the single-photon regime," Optics letters **38**(6), 947–949 (2013).

[23] J. B. Christensen, J. G. Koefoed, B. A. Bell, C. J. McKinstrie, and K. Rottwitt, "Shape-preserving and unidirectional frequency conversion by four-wave mixing," Opt. Express **26**(13), 17,145–17,157 (2018).

[24] H. McGuinness, M. Raymer, and C. McKinstrie, "Theory of quantum frequency translation of light in optical fiber: application to interference of two photons of different color," Optics express **19**(19), 17,876–17,907 (2011).

[25] F. Honz, N. Vokić, P. Walther, H. Hübel, and B. Schrenk, "Polarization-Encoded BB84 QKD Transmitter Sourced by a SiGe Light Emitter," in Optical Fiber Communication Conference, p. M1l.5 (Optical Society of America, 2023).

[26] D. Ribezzo, M. Zahidy, A. Petitjean, G. Lemmi, C. D. Lazzari, I. Vagniluca, E. Conca, A. Tosi, T. Occhipinti, F. S. Cataliotti, L. K. Oxenløwe, A. Xuereb, D. Bacco, and A. Zavatta, "QKD protocol over 100 km long submarine optical fiber assisted by a system-in-package fast-gated InGaAs single photon detector," in Optical Fiber Communication Conference, p. M2l.4 (Optical Society of America, 2023).

[27] U. Sinha, S. Sahoo, A. Singh, K. Joarder, R. Chatterjee, and S. Chakraborti, "Single-photon sources," Optics and Photonics News **30**(9), 32–39 (2019).

[28] S. Thomas and P. Senellart, "The race for the ideal single-photon source is on," Nature Nanotechnology **16**(4),

367–368 (2021).

[29] R. Uppu, F. Pedersen, Y. Wang, C. Olesen, C. Papon, X. Zhou, L. Midolo, S. Scholz, A. Wieck, A. Ludwig, et al., "Scalable integrated single-photon source," Science Advances **6**(50), eabc8268 (2020).

[30] I. Aharonovich, D. Englund, and M. Toth, "Solid-state single-photon emitters," Nature Photonics **10**(10), 631–641 (2016).

[31] N. Somaschi, V. Giesz, L. De Santis, J. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Anton, J. Demory, et al., "Near-optimal single-photon sources in the solid state," Nature Photonics **10**(5), 340–345 (2016).

[32] W. Barnes, G. Björk, J. Gérard, P. Jonsson, J. Wasey, P. Worthing, and V. Zwiller, "Solid-state single photon sources: light collection strategies," The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics **18**(2), 197–210 (2002).

[33] J. C. Loredo, N. A. Zakaria, N. Somaschi, C. Anton, L. De Santis, V. Giesz, T. Grange, M. A. Broome, O. Gazzano, G. Coppola, et al., "Scalable performance in solid-state single-photon sources," Optica **3**(4), 433–440 (2016).

[34] A. Khalid, K. Chung, R. Rajasekharan, D. W. Lau, T. J. Karle, B. C. Gibson, and S. Tomljenovic-Hanic, "Lifetime reduction and enhanced emission of single photon color centers in nanodiamond via surrounding refractive index modification," Scientific reports **5**(1), 1–12 (2015).

[35] I. A. Khramtsov, M. Agio, and D. Y. Fedyanin, "Dynamics of single-photon emission from electrically pumped color centers," Physical Review Applied **8**(2), 024,031 (2017).

[36] B. J. Hausmann, T. M. Babinec, J. T. Choy, J. S. Hodges, S. Hong, I. Bulu, A. Yacoby, M. D. Lukin, and M. Lončar, "Single-color centers implanted in diamond nanostructures," New Journal of Physics **13**(4), 045,004 (2011).

[37] D. Le Sage, L. M. Pham, N. Bar-Gill, C. Belthangady, M. D. Lukin, A. Yacoby, and R. L. Walsworth, "Efficient photon detection from color centers in a diamond optical waveguide," Physical Review B **85**(12), 121,202 (2012).

[38] P. Michler, Quantum dots for quantum information technologies, vol. 237 (Springer, 2017).

[39] S. Hepp, M. Jetter, S. L. Portalupi, and P. Michler, "Semiconductor quantum dots for integrated quantum photonics," Advanced Quantum Technologies **2**(9), 1900,020 (2019).

[40] R. S. Daveau, K. C. Balram, T. Pregnolato, J. Liu, E. H. Lee, J. D. Song, V. Verma, R. Mirin, S. W. Nam, L. Midolo, et al., "Efficient fiber-coupled single-photon source based on quantum dots in a photonic-crystal waveguide," Optica **4**(2), 178–184 (2017).

[41] P. Lodahl, S. Mahmoodian, and S. Stobbe, "Interfacing single photons and single quantum dots with photonic nanostructures," Reviews of Modern Physics **87**(2), 347 (2015).

[42] C. Spinnler, M. C. Löbl, L. Zhai, G. N. Nguyen, A. Javadi, J. Ritzmann, L. Midolo, P. Lodahl, A. D. Wieck, A. Ludwig, et al., "Single-Photon Radiative Auger Emission from a Quantum Dot," in CLEO: QELS_Fundamental Science, pp. FW2Q–7 (Optical Society of America, 2021).

[43] J. Bonetti, N. Linale, and D. Grosz, "Heralded single-photon sources based on 2D-decorated nanowires," Physics Letters A **432**, 128,018 (2022).

[44] H. Mulvad, S. Abokhamis Mousavi, V. Zuba, L. Xu, H. Sakr, T. Bradley, J. Hayes, G. Jasion, E. Numkam Fokoua, A. Taranta, et al., "Kilowatt-average-power single-mode laser light transmission over kilometre-scale hollow-core fibre," Nature Photonics **16**(6), 448–453 (2022).

1. Introduction

Quantum cryptography is among the most promising applications of quantum mechanics [1] as it enables privacy and inherently secure communication. Due to its simplicity, the BB84 protocol [2, 3] is the most well-known single-particle quantum key distribution (QKD) scheme and many BB84 experiments have been successfully carried out over optical fiber channels [4–6]. Although the first proposals encoded qubits in the polarization-state or phase of single photons, several novel schemes have been developed such as time-bin QKD [7–9] and time-frequency QKD [10, 11]. However, unwanted effects that corrupt qubits [1] hinder reaching longer propagation distances. For instance, birefringence changes the photon polarization [12] and mechanical and/or thermal fluctuations may modify its phase [13], limiting quantum-communication efficiency. To circumvent these impairments, encoding qubits by means of their frequency state offers a natural solution [11, 14, 15]. In this paper, we put forth

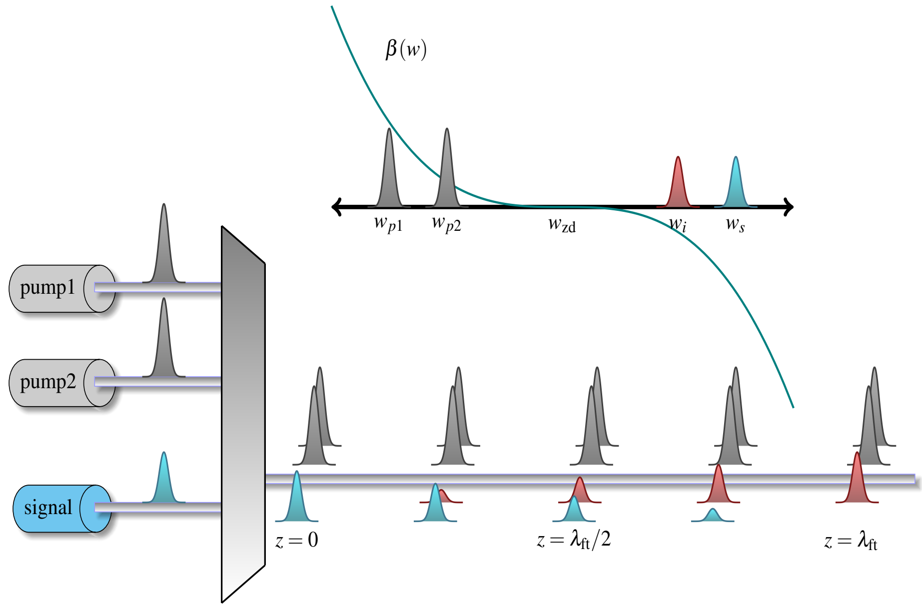

Fig. 1. Frequency conversion by Bragg scattering. Two strong pumps and a small signal are launched into a λ_{ft}-length fiber. At the output end of the fiber the signal frequency shifts from w_s to w_i.

a simple scheme relying on an efficient Quantum Frequency Translation (QFT) process in a nonlinear optical fiber that generates genuine frequency states; furthermore, the proposed scheme is shown to be naturally expandable to higher-dimensional alphabets, as more than two frequencies can be readily used to implement qudits-based QKD [16].

We should mention that a few other schemes have been proposed to perform frequency-coded QKD. For instance, in Ref. [11], time-frequency conversion is used to produce high-dimensional alphabets, but their scheme is essentially different in that entangled photons must be produced and distributed to both ends of the communication link. On the other hand, in the paper by Bloch et al. ([14]), electro-optical devices are conveniently used but the theoretical limit for the generation efficiency is lower than that of the QFT process proposed in this paper. Further, frequency encoding by means of electro-optical devices does not lend itself to a straightforward extension to higher-dimensional alphabets, as we will show it can be done with the scheme presented in this paper.

In the standard BB84 protocol [2] keys are distributed using qubits prepared in one of two bases, such that an absolutely certain quantum state measured in one base exhibits maximal uncertainty when measured in the other (e.g., a base of two orthogonal polarization states versus the same base rotated by $\pi/4$.) To begin with, we will illustrate our proposal by applying it to the standard BB84 protocol, i.e., by frequency coding qubits, and then we will move to the more involved case of quantum quarts (qu-quarts) QKD [17]. We propose to generate the aforementioned frequency-coded qubits relying on a special Four-Wave Mixing (FWM) process known as Quantum Frequency Translation or Bragg Scattering (BS) [18–20]. BS follows from the interaction of a dual-pump configuration (at frequencies w_{p1} and w_{p2}), with a small signal at w_s (see Fig. 1). Four-wave mixing in a nonlinear medium with third-order susceptibility $\chi^{(3)}$ [21], such as a nonlinear optical fiber, generates an idler signal at $w_i = w_{p1} - w_{p2} + w_s$. From a quantum mechanical perspective, this process produces the annihilation of two photons, one at w_{p1} and another at w_s, and the simultaneous creation of two photons at w_{p2} and w_i. Note that the opposite process (creation at w_{p1} and w_s, and annihilation at w_{p2} and w_i) is also allowed in a BS configuration. Although there are many other possible processes (other creation-annihilation combinations that conserve both the energy and the number of photons such as, e.g., phase conjugation and modulation instability,) these can be neglected if we assume, as we will, that the BS process is the only one that also satisfies the phase-matching condition $k_{p1} + k_s = k_{p2} + k_i$ [20]. Each photon annihilation at w_s involves a photon creation at w_i and vice versa, so the quantity of photons at w_s or w_i remains constant. When the phase-matching condition is satisfied, all n photons in the small signal at w_s are annihilated and n photons at the idler w_i are created. The propagation distance at which this occurs is called the *frequency-translation length*, λ_{ft}.

We now consider the complete QFT process, starting with a single photon of frequency w_s at $z = 0$ and ending

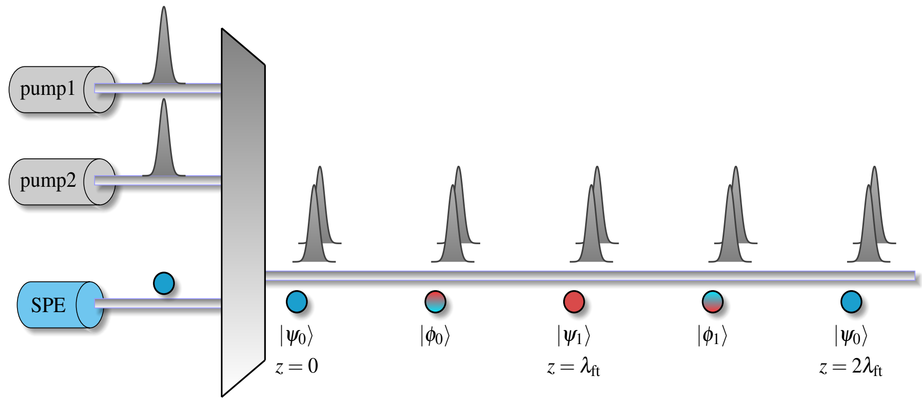

Fig. 2. Frequency translation of a single photon by a Bragg-scattering process. After a propagation of λ_{ft} length, the photon frequency is changed from w_s to w_i, or vice versa. At shorter propagated lengths the photon frequency is uncertain.

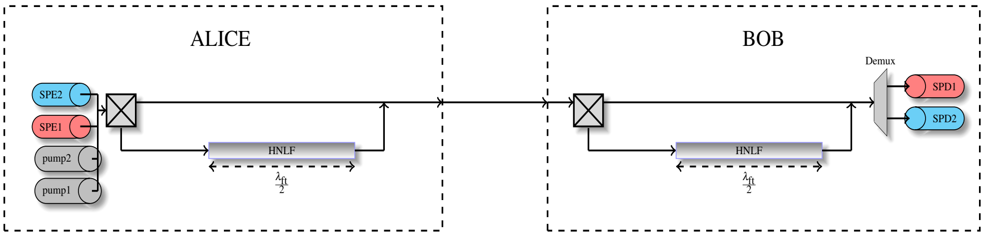

Fig. 3. Schematic implementation of the BB84 protocol by means of a BS quantum frequency-translation process. Alice randomly chooses to transmit the single-photon state with or without a half-length frequency translation. Bob, in turn, receives the transmitted photon and randomly performs another half-frequency translation. HNLF stands for high-nonlinear fiber. SPE: single-photon emitter. SPD: single-photon detector.

with a single photon of frequency w_i at $z = \lambda_{\mathrm{ft}}$ (see Fig. 2). A straightforward quantum interpretation of the described FWM interaction allows us to describe the single-photon QFT process by the photon frequency quantum state $|\psi\rangle = \mu\,|w_s\rangle + \nu\,|w_i\rangle$, where $|\mu|^2$ and $|\nu|^2$ are the probabilities of finding the photon at frequencies w_s and w_i, respectively. If the propagation distance is λ_{ft} the photon will have a defined frequency w_i with probability one, i.e., the frequency translation is complete. Between 0 and λ_{ft}, however, the photon frequency is a quantum superposition of both frequencies w_s and w_i. In fact, as it will be demonstrated in the next section, $|\mu|^2 = |\nu|^2 = 0.5$ at $\lambda_{\mathrm{ft}}/2$ and thus the photon frequency is maximally uncertain. We call this distance the *half-translation length*, $\lambda_{\mathrm{ft}}/2$.

The four states labeled in Fig. 2 ($|\psi_0\rangle$, $|\psi_1\rangle$, $|\phi_0\rangle$ and $|\phi_1\rangle$) are readily suited to be used as the standard BB84 protocol qubits, where we name the orthogonal bases ψ and ϕ. To produce and read qubits in the ϕ base we may propagate a photon through a $\lambda_{\mathrm{ft}}/2$-long QFT system. Alice and Bob decide which base they use by either applying or not applying this *half-translation* to the photon. When they use different bases Bob receives a maximally frequency-uncertain photon, like in a standard BB84 scheme.

It is worth mentioning that the frequency translation of a single photon with a high conversion efficiency of 98 percent has been demonstrated [22], and very recent work (see, e.g., Ref. [23]) demonstrated an enhanced phase-matching condition of the Bragg-scattering process along with suppression of spurious FWM processes, allowing for a 'clean' frequency conversion. These works point at the feasibility of QFT schemes through a Bragg scattering process.

2. Quantitative description of the qubits-based scheme

A quantum mechanical analysis of the QFT process in optical fibers has been presented in the work of McGuinness et al. [24]. Treating the pumps as classical fields and the signals as quantum fields, the single-photon frequency state can be described by the equation of motion

$$\frac{\partial}{\partial z}\left|\Psi\right\rangle = i\hat{H}\left|\Psi\right\rangle, \tag{1}$$

where the Hamiltonian is [19]

$$\hat{H} = \delta\left(\hat{a}_s^\dagger \hat{a}_s - \hat{a}_i^\dagger \hat{a}_i\right) + \kappa\left(\hat{a}_s^\dagger \hat{a}_i + \hat{a}_i^\dagger \hat{a}_s\right), \tag{2}$$

$\hat{a}^\dagger$ and $\hat{a}$ are the creation and annihilation operators, respectively, and κ is the *effective nonlinearity* defined as

$$\kappa = 2\gamma\sqrt{P_1 P_2}, \tag{3}$$

where γ is the fiber nonlinear coefficient and $P_{1,2}$ are the pump powers. The phase mismatch δ is given by

$$\delta = \frac{\beta(w_{p2}) - \beta(w_{p1}) + \beta(w_i) - \beta(w_s) + \gamma(P_1 - P_2)}{2}, \tag{4}$$

where $\beta(w)$ are the propagation constants at each frequency determined by the chromatic dispersion profile of the nonlinear fiber. We choose pump powers such that the process satisfies a perfect phase-matching condition ($\delta = 0$). This is done by setting $P_1 = P_2 = P$ and the frequency configuration of Fig. 1, centered at the zero-dispersion frequency w_{zd}, where $\beta(w_{p1}) = -\beta(w_i)$ and $\beta(w_{p2}) = -\beta(w_s)$.

By replacing the photon frequency state $\left|\Psi\right\rangle = \mu\left|w_s\right\rangle + \nu\left|w_i\right\rangle$ into Eq. (1) and solving for $\delta = 0$, we obtain

$$\begin{pmatrix} \mu(z) \\ \nu(z) \end{pmatrix} = \begin{pmatrix} \cos(\kappa z) & i\sin(\kappa z) \\ i\sin(\kappa z) & \cos(\kappa z) \end{pmatrix}\begin{pmatrix} \mu(0) \\ \nu(0) \end{pmatrix}. \tag{5}$$

This shows that the QFT process has a periodic behavior, toggling the probability of finding the photon in one of the two frequencies. Thus, the frequency-translation length can be easily obtained as

$$\lambda_{\mathrm{ft}} = \frac{\pi}{2\kappa}. \tag{6}$$

Figure 3 shows schematically how to implement the BB84 protocol by the QFT method. Bit values (1 and 0) are coded in the photon frequency. Alice has two single-photon emmiters (SPE1 and SPE2) of frequencies w_s and w_i, respectively. By optical switching, she randomly chooses the path taken by the photon. In one of these paths, the photon is transmitted with no change in its frequency state (i.e., Alice uses the base ψ.) The other path, instead, involves a half-QFT process and the photon frequency changes to a maximally uncertain state when measured in the ψ base. Bob also has an optical switch allowing him to choose the measurement base. If they choose the same base, the photon reaches Bob's single-photon detector (SPD) with a perfectly certain frequency state (i.e., $|\mu|^2 = 1$ and $|\nu|^2 = 0$, or $|\mu|^2 = 0$ and $|\nu|^2 = 1$, depending on the bit value.) If they select opposite bases, the photon arrives at the SPD in a maximally uncertain frequency state (with respect to the measurement base ψ) and Bob measures one frequency or the other with the same probability; this measured bit will be discarded in the key-sifting stage of the QKD protocol.

The proposal in Fig. 3 presents the same practical complications of any other BB84 scheme. The main challenge for its implementation lies on finding suitable SPEs and SPDs operating as closely as possible as single-photon devices. However, recent experiments show that novel *all-silicon* devices, such as SiGe light emitters [25] and InGaAs single-photon detectors [26], are enabling practical commercial BB84 system implementations. In addition, advances in single-photon sources [27–29], such as solid-state photon emitters [30–33], color-center SPSs [34–37], and quantum dots [38–42] are paving the way towards the ideal *on-demand* photon source. However, the BB84 based on a QFT process also exhibits particular challenges. On the one hand, the requirement of a HNLF with a nonlinear coefficient significantly higher than that of a single-mode fiber ($\gamma \gg 1.2$/W-km). Such high nonlinearity enables the usage of low-power pumps and still obtain a high effective nonlinearity κ, and a short frequency-translation length λ_{ft}. This HNLF can be implemented, for instance, with a graphene-oxide decorated nanowire exhibiting a fiber nonlinear coefficient of $\gamma = 10^5$/W-km [43] which would produce a $\lambda_{\mathrm{ft}} \simeq 8$ mm for a 0 dBW pump. On the other hand, if the communication channel is assumed to be a fiber, several detrimental effects have to be considered. For instance, the nonlinear interaction between the pumps and the signal must be reduced by reducing the pump power as explained before. Chromatic dispersion must be also compensated in the receiver side as frequency-dependent phase effects seriously affect the perfect phase-matching condition assumed in this scheme. At this point, we have to mention a promising technology that has the potential to make QFT-based BB84 easily implementable: the hollow-core fiber [44]. This kind of fiber, which is currently attracting the attention of the entire optical-communications community, exhibits a negligible nonlinear coefficient and chromatic dispersion, together

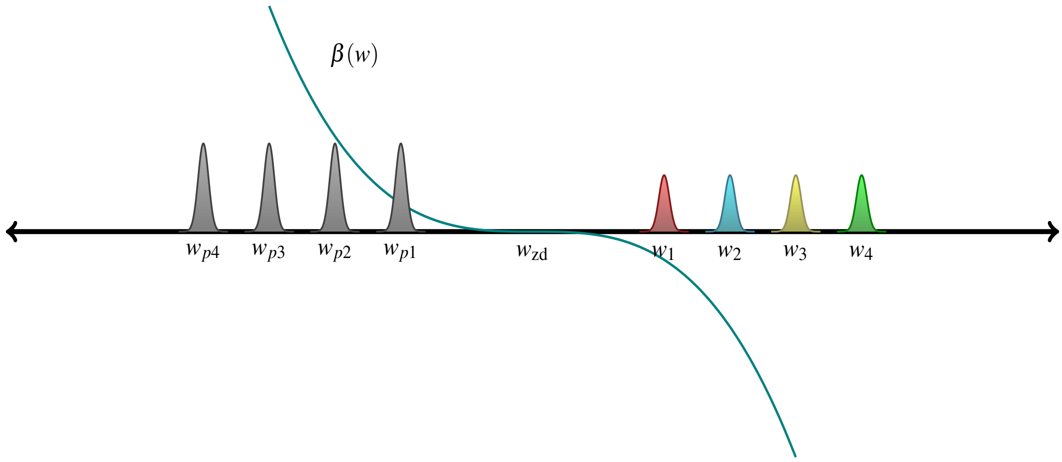

Fig. 4. Frequency configuration for the qu-quarts QKD scheme. It is a combination of six perfect phase-matched Bragg-scattering processes.

with a low attenuation comparable to that of a standard single-mode fiber.

3. Extension to qu-quarts

A significant advantage of our proposal lies in the possibility of having single-photon quantum states represented in a Hilbert space of greater dimensions. This fact can be exploited to encode qudits [16] (instead of qubits) in each photon. In particular, we put forth an original configuration to produce single-photon states belonging to a four-dimensional Hilbert space by a QFT process similar to the one described in the previous section. Note that the encoding of qudits in a conventional time-bin QKD scheme would require faster SPEs in order to reduce the time occupied by each bin. In this sense, the QFT-based QKD enables the parallelization of several low-speed SPEs, centered at different frequencies, in a similar way to wavelength-division multiplexing (WDM) systems to achieve an enhanced qubit rate.

In Fig. 4 we show the proposed scheme. This configuration is a superposition of six different frequency-translation processes described by the hamiltonian

$$\hat{H} = \kappa \sum_{\substack{j,k=1 \\ j\neq k}}^{4} \hat{a}_j^\dagger \hat{a}_k + \hat{a}_k^\dagger \hat{a}_j. \tag{7}$$

This original arrangement allows for the creation of four maximally uncertain photon states, starting from a single photon of well-defined frequency. In similar fashion as with qubits, we propose the quantum state

$$|\Psi\rangle = \mu\,|w_1\rangle + \nu\,|w_2\rangle + \rho\,|w_3\rangle + \varphi\,|w_4\rangle \tag{8}$$

for the single photon, where $|\mu|^2$, $|\nu|^2$, $|\rho|^2$ and $|\varphi|^2$ are the probabilities of measuring its corresponding frequency. By solving Eq. 1 with this hamiltonian we obtain the single-photon propagation,

$$\frac{d}{dz}\begin{pmatrix} \mu \\ \nu \\ \rho \\ \varphi \end{pmatrix} = i\kappa \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \\ \rho \\ \varphi \end{pmatrix}. \tag{9}$$

The proposed qu-quarts scheme is similar to that of the qubit scenario (Fig. 3) but with four SPEs and SPDs (at frequencies w_1, w_2, w_3 and w_4) instead of two. Bases are obtained in the same way as before. The ψ basis is used when Alice sends a single-photon directly as it is emitted from the SPE. However, to use the ϕ basis, Alice propagates the photon through a $\lambda_{\mathrm{ft}}/2$-long nonlinear fiber before sending it. In Fig. 5 we show the bases for the qu-quarts QKD. They can be easily derived from Eq. 9 and are given by

$$|\phi_1\rangle = \frac{1}{2}\left(|\psi_1\rangle - |\psi_2\rangle - |\psi_3\rangle - |\psi_4\rangle\right), \tag{10}$$

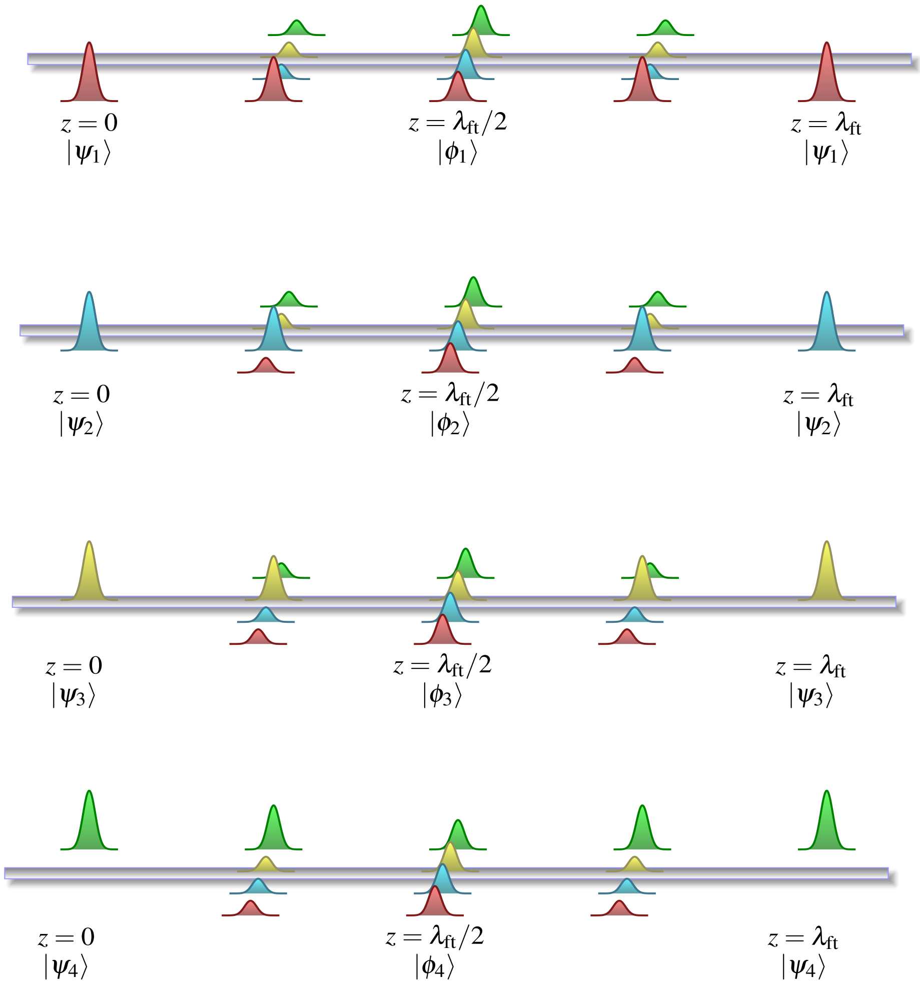

Fig. 5. Bases for the qu-quarts BB84 protocol.

$$|\phi_2\rangle = \frac{1}{2}\left(-|\psi_1\rangle + |\psi_2\rangle - |\psi_3\rangle - |\psi_4\rangle\right), \tag{11}$$

$$|\phi_3\rangle = \frac{1}{2}\left(-|\psi_1\rangle - |\psi_2\rangle + |\psi_3\rangle - |\psi_4\rangle\right), \tag{12}$$

$$|\phi_4\rangle = \frac{1}{2}\left(-|\psi_1\rangle - |\psi_2\rangle - |\psi_3\rangle + |\psi_4\rangle\right), \tag{13}$$

where $|\psi_i\rangle = |w_i\rangle$ stands for the computational basis. As in the qubits scheme, Bob chooses the basis in which he reads the qu-quarts by deciding whether to propagate the photon (ϕ) or not (ψ) through another $\lambda_{\mathrm{ft}}/2$-long fiber before measuring its frequency.

Security advantages of a qu-quarts BB84 protocol have already been discussed [17]. As a very simple proof of the security enhancement, an analysis of the intercept-resend attack can be performed. This simple eavesdropping technique consists in reading the frequency of the photon sent by Alice and resending Bob another photon at the measured frequency. If Alice and Bob choose the ψ basis, this intercept does not produce an error in the communication. However, if they use the ϕ basis, then Bob receives a photon of a maximally uncertain frequency. As such, the result of Bob's measurement is completely uncertain and this introduces errors in the communication that can be used to detect the presence of the eavesdropper. For qubits this uncertain measurement produces, on average, 50% of detectable errors; for qu-quarts, on the other hand, it accounts for 75% of errors. As such, the Bit Error (BE) introduced by the eavesdropper is $1/4$ for qubits and $3/8$ for qu-quarts. This simple calculation shows that detection of eavesdropping is easier in the qu-quarts scheme.

4. Conclusions

We proposed an original implementation of the BB84 quantum key distribution protocol, based on the frequency uncertainty of single photons in a quantum frequency-translation process in optical fibers. The scheme is expected to be more robust than most conventional BB84 implementations as the frequency of the photon, as opposed to its polarization/phase, is not affected by mechanical and/or thermal fluctuations of the transmitting medium. The scheme offers the possibility of naturally augmenting the encoding space, and an original extension to qu-quarts was presented, providing enhanced security against eavesdropping.

