A frequency-coded QKD scheme with an extension to qu-quarts

J. Bonetti and S. M. Hernandez
Instituto Balseiro, Av. Bustillo km 9.500, Bariloche (R8402AGP), Argentina

D. F. Grosz
Instituto Balseiro, Av. Bustillo km 9.500, Bariloche (R8402AGP), Argentina and Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina

We propose a novel scheme to implement the BB84 quantum key distribution (QKD) protocol in optical fibers based on a quantum frequency-translation (QFT) process. Unlike conventional QKD systems, which rely on photon polarization/phase to encode qubits, our proposal utilizes photons of different frequencies. Qubits are thus expected to reach longer propagation distances due to the photon frequency state being more robust against mechanical and/or thermal fluctuations of the transmitting medium. Finally, we put forth an extension to a security-enhanced four-character-alphabet (qu-quarts) QKD scheme.

I. INTRODUCTION

Quantum cryptography is amongst the most promising applications of quantum mechanics [1], since it enables privacy and inherently secure communication. Due to its simplicity, the BB84 protocol [2] is the most well-known single-particle QKD scheme and many BB84 experiments have been successfully carried out along optical fiber channels [4–6]. However, unwanted effects that corrupt qubits [1] hinder reaching long propagation distances. For instance, birefringence may change photon polarization [6] and mechanical and/or thermal fluctuations may modify its phase [5], seriously limiting quantum-communication efficiency. A very clever solution to tackle these problems relies on encoding qubits by means of their frequency [6–11]. That is, instead of using two orthogonal polarization or phase states, utilizing two different frequencies. This scheme involves at least two advantages: on the one hand, a photon traveling through an optical fiber is more likely to experience polarization and/or phase changes than changes in its frequency (in general, the latter are caused by design), rendering this type of encoding more stable; on the other hand, the possibility of augmenting the dimension of the encoding space presents itself naturally, as more than two frequencies can be used to implement QKD schemes based on qubits [12].

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 of them exhibits maximal uncertainty when measured in the other (e.g., 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 [13] (qu-quarts) based QKD. We propose to generate the aforementioned frequency-coded qubits relying on a special Four-Wave Mixing (FWM) process known as Quantum Frequency Translation (QFT), or Bragg Scattering (BS) [13–16]. It consists of a dual-pump configuration FWM (at frequencies \(w_{p1}\) and \(w_{p2}\), with a small signal at \(w_s\) (see Fig. 1). Interaction between these three frequencies in a nonlinear medium with third-order susceptibility \(\chi^{(3)}\) [17] produces an idler signal at \(w_{s2} = w_{p2} - w_{p1} + w_s\). From a quantum mechanical perspective, this process consists of two photon annihilations, one at \(w_{s2}\) and another at \(w_{s1}\), and the simultaneously creation of two photon at \(w_{p1}\) and \(w_{p2}\). The opposite process (creations at \(w_{p2}\) and \(w_{s1}\) and annihilations at \(w_{p1}\) and \(w_{s2}\)) is also allowed in this configuration. Although there are many other possible processes (other creation-annihilation combinations that conserve energy and number of photons, e.g., phase conjugation and modulation instability), they can be neglected if we assume, as we will, that this is the only frequency combination that also satisfies the phase-matching condition \([16]\) \(k_{p1} + k_{s2} = k_{p2} + k_s\). Each photon annihilation at \(w_{s1}\) involves a photon creation in \(w_{s2}\) and vice versa, so the quantity of photons at \(w_{s1}\) or \(w_{s2}\) remains constant. When the phase-matching condition is perfectly satisfied, all \(n\) photons in the small signal at \(w_s\) are annihilated, and \(n\) photons at the idler \(w_{s2}\) are created. The propagation distance at which this occurs is called the frequency-translation length (\(\lambda_{\text{FT}}\)).

If we consider the total QFT, starting with a single photon of frequency \(w_{s1}\) at \(z = 0\) as the initial state, for instance, and obtaining a single photon of frequency \(w_{s2}\) at \(z = \lambda_{\text{FT}}\) as the final state (see Fig. 1), a straightforward quantum interpretation of the described FWM process allows us to describe the single-photon QFT process by the photon frequency quantum state \(|\psi\rangle = \mu |w_{s1}\rangle + \nu |w_{s2}\rangle\), where \(|\mu|^2\) and \(|\nu|^2\) are the probabilities to find the photon at frequencies \(w_{s1}\) and \(w_{s2}\), respectively. If the propagation distance is \(\lambda_{\text{FT}}\) the photon will have a defined frequency \(w_{s2}\) with probability one, i.e., the frequency translation is complete. Between 0 and \(\lambda_{\text{FT}},\)
II. 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. [13]. 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

$$\frac{d}{dz} |\psi\rangle = i\hat{H} |\psi\rangle,$$

where the Hamiltonian is [13]

$$\hat{H} = \delta (\hat{a}_s \hat{a}^\dagger_s - \hat{a}_s \hat{a}^\dagger_s) + \kappa (\hat{a}^\dagger_s \hat{a}_{s+2} + \hat{a}^\dagger_{s-2} \hat{a}_s),$$

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

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

where $$\gamma$$ is the fiber nonlinear coefficient and $$P_1, P_2$$ are the pump powers. The phase mismatch $$\delta$$ is given by

$$\delta = \frac{\beta_{p2} - \beta_{p1} + \beta_{s1} - \beta_{s2} + \gamma (P_1 - P_2)}{2},$$

where $$\beta_{p1, p2, s1, s2}$$ are the propagation constants at each frequency. We choose pump powers such that the process has a perfect phase-matching condition ($$\delta = 0$$).

By replacing the photon frequency state $$|\psi\rangle = \mu |w_{s1}\rangle + \nu |w_{s2}\rangle$$ in Eq. 11 and solving for $$\delta = 0$$, we obtain

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

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

$$\lambda_{FT} = \frac{\pi}{2\kappa}.$$ 

Figure 8 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 sources (SFS1 and SFS2) of frequencies $$w_{s1}$$ and $$w_{s2}$$. By optimally switching, she chooses randomly the path that the photon will take. In one of these paths, the photon is sent without changing its frequency state (i.e., Alice uses the base $$\psi$$). The other path, instead, involves a half-QFT process on the photon and the frequency state changes to a maximally uncertain one (i.e., Alice uses the base $$\phi$$) when measured in the $$\psi$$ base. Bob also has an optical switch to choose the measurement base. If they choose the same base, the photon reaches Bob’s single-photon detectors (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 whether the bit value was). If they select opposite bases, the photon arrives at the SPD in a maximally uncertain frequency state (i.e., with respect to the measurement base $$\psi$$) and Bob measures one frequency or the other with the same probability; since this reading provides no information it will eventually be discarded by the QKD protocol.

It is important to mention that the proposed QKD scheme is realizable using currently available technologies. Recently, frequency translation of single-photons was proven successful in a photonic crystal fiber [10] (PCF). Also, single-photon sources are available.

III. EXTENSION TO QU-QUARTS QKD

Another significant advantage of frequency encoding is the possibility of having single-photon quantum states represented in a Hilbert space of dimension greater than 2. This fact can be exploited to encode qudits [12] (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 (i.e., 4 different signal frequencies) by a QFT process similar to that shown in the previous section. In Fig. 4, we show the proposed scheme. There we define the qu-quart region, a spectral band which includes the four signal frequencies $$w_{s1}, w_{s2}, w_{s3}$$ and $$w_{s4}$$. Alice has four SPS at these frequencies, which she uses to produce four different keys.

To show how this configuration works, let us consider the following example: If Alice launches a photon of frequency $$w$$ at the input end of the fiber several QFT processes can occur. The interaction among the photon and pumps 1 and 2 yields two possible results: the photon either "jumps" to $$w + \delta w$$ or it jumps to $$w - \delta w$$. The photon can also interact in a QFT with pumps 2 and 3. In this case, the photon can jump to $$w \pm 3 \delta w$$. The interaction with pumps 1 and 3 can also occur, and in this case jumps to $$w \pm 4 \delta w$$ are possible. However, if properly designed, the qu-quart region limits all the possibile jumps to just a few ones. Ideally, the qu-quart region dispersion will be such that the four signal frequencies are perfectly phase-matched among them but highly phase-mismatched with any frequency external to this region. In practice, this may be achieved by means of a dispersion-flattened fiber or a PCF whose dispersion profile is constant in the qu-quart region and changes abruptly in the boundaries. Jumps outside the qu-quart region are thus forbidden and the only possible QFT processes are the ones shown in Fig. 4. Note that the reason for including pump 3 is to enable the jump between $$w_{s1}$$ and
w_{s4}; furthermore, pump 3 power matches that of pump 1, thus making all frequency jumps to be governed by the same nonlinear coefficient κ.

III.1. Derivation of the Hamiltonian for the qu-quarts scheme

To have a precise physical description of the qu-quarts scheme, we derive the Hamiltonian (see, Eq. 1) for this configuration, which takes into account all possible interactions. To begin with, we analyze the propagation of the classical electromagnetic field in the nonlinear optical fiber by means of the Nonlinear Schrödinger Equation [17]

$$i \frac{\partial A}{\partial z} = \beta A - \gamma |A|^2 A,$$

(3)

where $A$ is the complex envelope of the electrical field normalized such that $|A|^2$ is the optical power in Watts, $\beta$ is a linear operator such that $\beta e^{-iw_0 t} = -\beta(w)e^{-iw_0 t}$, with $\beta(w)$ the dispersion profile of the fiber, and $\gamma$ the fiber nonlinear coefficient. We propose the solution

$$A = \sum_{m=1}^{3} A_{pm} + \sum_{m=1}^{4} A_{sm},$$

where

$$A_{pm} = \sqrt{T_m} e^{iw_{pm} z - i k_{pm} t}, \quad k_{pm} = \beta(w_{pm}) - \gamma P_m + \sum_{n=1}^{3} 2 \gamma P_n,$$

$$A_{sm} = A_{sm}(z) e^{ik_{sm} z - i w_{sm} t}, \quad k_{sm} = \beta(w_{sm}) + \sum_{n=1}^{3} 2 \gamma P_n,$$

$A_{pm}$ correspond to the pumps (under the usual undepleted-pump approximation) and $A_{sm}$ are small signals located in the qu-quart region. By replacing into Eq. (3) and retaining only the phase-matched QFT processes, we obtain

$$i \frac{\partial A_{sm}}{\partial z} = -\kappa (A_{s(m-1)} + A_{s(m+1)}),$$

(4)

for $m = 1, 2, 3, 4$, with $A_{s5} = A_{s1}$ and $A_{s0} = A_{s4}$, where $P_1 = P_3$.

We quantize the variables $A_{sm}$ by proposing the correspondence with quantum operators $\hat{A}_{sm} = \sqrt{\hbar w_0 / T} \hat{a}_{sm}$, where $\hat{a}_{sm}$ is an annihilation operator, $T$ an arbitrary time of measurement and $w_0 = (w_{s1} + w_{s2} + w_{s3} + w_{s4}) / 4$. Creation operators satisfy the commutation relation $[\hat{a}_{sm}, \hat{a}_{sm}^\dagger] = \delta_{sm}$, and they conform the number operators $\hat{N}_{sm} = \hat{a}_{sm}^\dagger \hat{a}_{sm}$, which might be interpreted as the photon quantity at frequency $w_{sm}$ during the time interval $T$. By defining the intensity operator $I_{sm} = \hat{A}_{sm}^\dagger \hat{A}_{sm}$, we recover the classical relation

$$\langle \hat{I}_{sm} \rangle = \frac{\hbar w_0}{T} \langle \hat{N}_{sm} \rangle,$$

where we assume that the qu-quart region bandwidth $(w_{s4} - w_{s1})$ is negligible with respect to $w_0$. If this were not the case, a straightforward correction can be made by considering a frequency-dependent $\gamma$ (i.e., self-steepening); for the sake of clarity, we keep the simpler approximate form. We look for a Hamiltonian so that the correspondence principle is satisfied, i.e., the mean values of $\hat{A}_{sm}$ evolve according to the classical Eq. (4)

$$i \frac{\partial \langle \hat{A}_{sm} \rangle}{\partial z} = -\kappa \left( \langle \hat{A}_{s(m-1)} \rangle + \langle \hat{A}_{s(m+1)} \rangle \right),$$

that is tantamount to say

$$\left[ \hat{A}_{sm}, \hat{H} \right] = \kappa \left( \hat{A}_{s(m-1)} + \hat{A}_{s(m+1)} \right),$$

Then, we propose the following Hamiltonian

$$\hat{H} = \kappa \frac{T}{\hbar w_0} \sum_{\mu=1}^{4} \left( \hat{A}_{s(\mu-1)}^\dagger \hat{A}_{s(\mu+1)} + \hat{A}_{s(\mu-1)}^\dagger \hat{A}_{s(\mu+1)} \right),$$

FIG. 2. Single-photon QFT (pumps are not showed).

FIG. 3. BB84 implementation via QFT. NLF stands for nonlinear fiber.
which can be easily verified by keeping in mind the commutation relations $[A_{sm}, A_{m'n}] = i\hbar w_0 / T \delta_{mn}$. Finally, $\hat{H}$ can be expressed in terms of creation and annihilation operators as

$$\hat{H} = \kappa \sum_{\mu=1}^{4} (\hat{a}_{\mu}^\dagger \hat{a}_{\mu(-1)} + \hat{a}_{\mu(-1)}^\dagger \hat{a}_{\mu}) \quad (5)$$

III.2. Single-photon propagation

The quantum state of the complex envelope of the electric field in the qu-quart region is represented by the linear combination of four-dimensional Fock states $|n_1, n_2, n_3, n_4\rangle$ where $n_{sm}$ is the number of photons at the mode $w_{sm}$. We are interested in having a single-photon at the input-end of the fiber with initial state being either $|w_{s1}\rangle = |1, 0, 0, 0\rangle$, $|w_{s2}\rangle = |0, 1, 0, 0\rangle$, $|w_{s3}\rangle = |0, 0, 1, 0\rangle$ or $|w_{s4}\rangle = |0, 0, 0, 1\rangle$. We may express the evolution of these states after any given propagated distance as

$$|\psi(z)\rangle = \mu(z) |w_{s1}\rangle + \nu(z) |w_{s2}\rangle + \rho(z) |w_{s3}\rangle + \varphi(z) |w_{s4}\rangle \quad (\text{and obtain precise solutions using the circular relations } |w_{s5}\rangle = |w_{s1}\rangle \text{ and } |w_{s0}\rangle = |w_{s4}\rangle)$$

together with the fact that $\hat{H} |w_{sm}\rangle = \kappa \left( |w_{s(m+1)}\rangle + |w_{s(m-1)}\rangle \right)$. Then the quantum state of the electric field $|\psi\rangle$ can be interpreted as the quantum state of the single-photon, where $|\mu|^2$, $|\nu|^2$, $|\rho|^2$ and $|\varphi|^2$ are the probabilities of measuring its corresponding frequency.

Using Eq. (1) we obtain

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

whose solution can be expressed as
III.3. BB84 with qu-quarts

The scheme is similar to that of the qubit scenario (Fig. 3) but with four SPD (at frequencies $\omega_{1s}$, $\omega_{2s}$, $\omega_{3s}$, and $\omega_{4s}$) instead of two. The bases for the qu-quarts scheme are obtained in the same way as before. The $\psi$ basis is used when Alice sends a single-photon directly as it is emitted from the SPS. However, to use the $\phi$ basis, Alice propagates the photon through a $\lambda_{FT}$/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. (6) and are given by

$$
\begin{align*}
\phi_1 &= \frac{1}{2} (|\psi_1\rangle + i|\psi_2\rangle - |\psi_3\rangle + i|\psi_4\rangle), \\
\phi_2 &= \frac{1}{2} (i|\psi_1\rangle + |\psi_2\rangle + |\psi_3\rangle - |\psi_4\rangle), \\
\phi_3 &= \frac{1}{2} (-|\psi_1\rangle + i|\psi_2\rangle + |\psi_3\rangle + i|\psi_4\rangle), \\
\phi_4 &= \frac{1}{2} (i|\psi_1\rangle - |\psi_2\rangle + |\psi_3\rangle + |\psi_4\rangle).
\end{align*}
$$

As in the qubits scheme, Bob choses the basis in which he reads the qu-quarts by deciding whether to propagate the photon (\phi) or not (\psi) through another $\lambda_{FT}$/2-long fiber before measuring its frequency. If Alice and Bob choose the same $\psi$ basis, Bob will measure a photon at a different frequency than that of the photon prepared by Alice (Fig. 5). This poses no problem in the practical implementation of the protocol, as the frequency measured by Bob is uniquely determined by the frequency sent by Alice.

Security advantages of a qu-quarts BB84 protocol have already been studied (15). 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 chose the $\psi$ basis, this intercept does not produce an error in the communication. However, if they use the $\phi$ 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, in average, 50% of detectable errors; meanwhile for qu-quarts it accounts for 75% of errors. As such, for qubits the Bit Error (BE) introduced by the eavesdropper is 1/4, meanwhile for qu-quarts the Quart Error (QE) is 3/8. This simple calculation shows that detection of eavesdropping is easier in the qu-quarts scheme.

IV. 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 current 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. Detailed calculations to cope with various design considerations were provided and an original extension of the scheme to qu-quarts was presented, expanding the available character space and providing enhanced security.

[1] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. Reviews of modern physics, 74(1):145, 2002.
[2] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. 1984.
[3] Mark Fox. Quantum optics: an introduction, volume 15. OUP Oxford, 2006.
[4] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. Nature Photonics, 9(3):163–168, 2015.
[5] Philip A Hiskett, Danna Rosenberg, Charles G Peterson, Richard J Hughes, S Nam, AE Lita, AJ Miller, and JE Nordholt. Long-distance quantum key distribution in optical fibre. New Journal of Physics, 8(9):193, 2006.
[6] Naoto Namekata, Shigehiko Mori, and Shuichiro Inoue. Quantum key distribution over an installed multimode optical fiber local. Optics express, 13(25):9961–9969, 2005.
[7] Nicolas Gisin. Statistics of polarization dependent losses. Optics communications, 114(5-6):399–405, 1995.
[8] Dirk Bouwmeester, Artur Ekert, Anton Zeilinger, et al. The physics of quantum information, volume 3. Springer, Berlin, 2000.
[9] Matthieu Bloch, Steven W McLaughlin, Jean-Marc Merolla, and Frédéric Patois. Frequency-coded quantum key distribution. Optics letters, 32(3):301–303, 2007.
[10] Ildar M Gabdulhakov and Oleg 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, pages 1–5. IEEE, 2017.
[11] EH Huntington and TC Ralph. Components for optical qubits encoded in sideband modes. Physical Review A, 69(4):042318, 2004.
[12] KR Rohit and Talabattulla Srinivas. High dimensional quantum key distribution: Bb84 protocol using qudits. In International Conference on Fibre Optics and Photonics, pages Th3A–77. Optical Society of America, 2016.
[13] IH Bechmann-Pasquinucci and Wolfgang Tittel. Quantum cryptography using larger alphabets. Physical Review A, 61(6):062308, 2000.
[14] Prem Kumar. Quantum frequency conversion. Optics letters, 15(24):1476–1478, 1990.
[15] CJ McKinzie, JD Harvey, S Radic, and MG Raymer. Translation of quantum states by four-wave mixing in fibers. Optics
[16] HJ McGuinness, MG Raymer, CJ McKinstrie, and S Radic. Quantum frequency translation of single-photon states in a photonic crystal fiber. *Physical review letters*, 105(9):093604, 2010.

[17] Govind P Agrawal. *Nonlinear fiber optics*. Academic press, 2007.

[18] HJ McGuinness, MG Raymer, and CJ McKinstrie. Theory of quantum frequency translation of light in optical fiber: application to interference of two photons of different color. *Optics express*, 19(19):17876–17907, 2011.

[19] Leonard Mandel and Emil Wolf. *Optical coherence and quantum optics*. Cambridge university press, 1995.