Quantum key distribution by phase flipping of coherent states of light

G. A. Barbosa[1],[*] J. van de Graaf[2],[†] P. Mateus[3,4],[‡] and N. Paunković[3,4][§]

[1] *QuantaSEC – Consulting, Projects and Research in Physical Cryptography Ltd., Brazil*
[2] *Departamento de Ciência da Computação,*
Universidade Federal de Minas Gerais, Brazil
[3] *Instituto de Telecomunicações, Portugal*
[4] *Departamento de Matemática,*
Instituto Superior Técnico, Universidade de Lisboa
(Dated: November 14, 2018)

In this paper we present quantum key distribution protocol that, instead of single qubits, uses mesoscopic coherent states of light $|\alpha\rangle$ to encode bit values of a randomly generated key. Given the reference value $\alpha \in \mathbb{C}$, and a string of phase rotations each randomly taken from a set of $2M$ equidistant phases, Alice prepares a quantum state given by a product of coherent states of light, such that a complex phase of each pulse is rotated by the corresponding phase rotation. The encoding of i-th bit of the key $r = r_1 \ldots r_\ell$ is done by further performing phase rotation $r_i \pi$ (with $r_i = 0, 1$) on the i-th coherent state pulse. In order to protect the protocol against the man-in-the-middle attack, we introduce a verification procedure, and analyse the protocol's security using the Holevo bound. We also analyse the possibility of beam splitting-like and of collective attacks, showing the impossibility of the former and, in the case of our protocol, the inadequacy of the latter. While we cannot prove full perfect security against the most general attacks allowed by the laws of quantum mechanics, our protocol achieves faster quantum key distribution, over larger distances and with lower costs, than the single-photon counterparts, maintaining at least practical security against the current and the near future technologies.

I. INTRODUCTION

Quantum mechanics offers advantages when implementing data processing tasks in comparison to their classical counterparts. Arguably the most prominent one is the famous Shor algorithm for factoring numbers [1]. While a practical implementation of a working scalable quantum computer, despite considerable success in the last decade, is still out of reach of today's technology, quantum cryptographic systems can already be bought on the market today. Quantum cryptography started with an early work from 1969 by Wiesner, who introduced notions of quantum multiplexing and quantum money, though he only managed to publish his work more than a decade later, in 1983 [2]. Based on his ideas, Bennett and Brassard introduced their famous four-state BB84 protocol for key distribution [3]. The unconditional security of quantum key distribution (QKD) [4–7] is a consequence of the laws of physics, and as such is stronger than the computational security of classical counterparts, based on unproven mathematical conjectures.

The physical systems that encode the bit values in the BB84 QKD protocol are qubits – two-level quantum systems. So far, implementations of QKD protocols have (predominantly) used quantum optical systems. Thus, in the majority of such applications qubit states were naturally encoded in single-photon states (usually in polarisation). The use of single photons as carriers of qubits achieves theoretical perfect security, but has, nevertheless, a few drawbacks regarding single-photon detectors which are, at the present stage of technology: (i) relatively expensive, and (ii) too slow to facilitate the amount of information exchanged by today's average consumers. At the current technology stage commercial telecommunication detectors may operate at rates of 40GHz (e.g., ref. [8]) or above while commercial single-photon detectors are still struggling below 50MHz (see for example [9]) due to the need to quench the avalanche of a high numbers of electrons. Even laboratory superconducting nanowire detector devices operate at rates below 1 GHz as they need time for thermal dissipation after each excitation. Radical changes may appear in the technological horizon but this is way beyond the subject of this paper.

To meet such requirements, various different protocols for distributing keys using coherent states of light were studies in [10–19]. While the protocols based on coherent states do achieve levels of security of single-photon QKD [20], to obtain the optimal key rates, one requires low average photon numbers [21], i.e., they too suffer from the above

[*] geraldoabarbosa@gmail.com

[†] jvdg@dcc.ufmg.br

[‡] pmat@math.tecnico.ulisboa.pt

[§] npaunkov@math.tecnico.ulisboa.pt

mentioned weaknesses. The use of mesoscopic coherent states indeed solves the above two problems (i) and (ii): multi-photon detectors (for average numbers of $10^2 - 10^4$ photons per pulse) need to be much less sensitive, and are thus less expensive, and can count many more pulses per unit time. Instead of quadrature measurements the protocol presented in this paper only utilises phase encoding and detection in M-ry levels according to [12, 16]. In addition to that, the protocol [12, 16] uses a finite pre-shared secret key, constantly updating along its execution the shared randomness to achieve secure information transfer.

Recently, a secure public key encryption scheme based on single-qubit rotations was presented in [22] and subsequently analysed in [23] (see also a recent scheme [24] based on quantum walks). Nevertheless, its standard optical applications using single-photon polarisation as a realisation of a qubit suffers from the same deficiencies as the above mentioned realisations of QKD. In this paper, based on the ideas of key distribution with continuous variables [12, 16], and secure message transfer with single qubits [22], we present a version of a key distribution scheme in which bit values are encoded in (multi-photon) coherent states of light. Note that, unlike the protocol presented in [22] which uses (single-photon) qubits, in our protocol states which encode single bit values are now from an infinitely-dimensional Hilbert space, and could thus, in principle, carry an unlimited amount of classical information. This makes the argument for the protocol's security, based on the Holevo theorem, rather non-trivial in our case (for the proof of the Holevo theorem, see for example [25], Section 12.1.1, and the references therein). The main result of our paper is that such argument is indeed satisfied even for the particular infinitely-dimensional quantum states: given an ensemble $\hat{\rho}$ of particular coherent states used by Alice in our protocol, the amount of information carried by a single pulse is finite, bounded from above by the finite value of von Neumann entropy $S(\hat{\rho})$; this way, the protocol is secure against Eve's attempt to learn Alice's choice of bases k, and thus subsequently read out Bob's encrypted key (for details, see Section IV). Note that once authentication for the users is established, the system does not demand a pre-sharing of keys to start the distribution stage, in contrast with [12] or [16]. Therefore, no courier is ever needed to refresh keys. Coherent states with mesoscopic number of photons are much easier to construct and lead to a much faster key distribution system than single-photon QKD systems. These are also relevant results that allow for a renewal of bit-to-bit encryption protocols.

The paper is organised as follows. In the next section, we introduce basic properties of coherent states of light. In Section III, we present the protocol. In the subsequent Section IV, we analyse the protocol's security. Finally, in the last section, we present conclusions and some possible future lines of research.

II. COHERENT STATES OF LIGHT

For simplicity, we consider only single-mode states of light, given by the annihilation operator $\hat{a}$. The ground state $|0\rangle$ of the Hamiltonian $\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})$, also called the *vacuum*, determines the orthonormal basis $\{|n\rangle = \frac{1}{\sqrt{n!}}\hat{a}^n|0\rangle | n \in \mathbb{N}_0\}$, called the *number basis*. Coherent states are given by the following expression:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{1}$$

where $\alpha = e^{i\varphi}|\alpha| \in \mathbb{C} \setminus \{0\}$. Coherent states saturate Heisenberg relations for the position and the momentum operators $\hat{x} = \sqrt{\frac{m\omega\hbar}{2}}(\hat{a}^\dagger + \hat{a})$ and $\hat{p} = i\sqrt{\frac{\hbar}{2m\omega}}(\hat{a}^\dagger - \hat{a})$, i.e., $\Delta\hat{x}\Delta\hat{p} = \hbar/2$. Moreover, the expectation values $\langle\hat{x}\rangle$ and $\langle\hat{p}\rangle$ for coherent states obey position and momentum equations of motion of a classical harmonic oscillator. Therefore, they are considered to be the most "classical" quantum states (for more details on coherent states, see for example a comprehensive review [26]).

One can introduce the so-called number operator $\hat{n} = \hat{a}^\dagger\hat{a} = \sum_{n=0}^{\infty} n|n\rangle\langle n|$ which counts the photon-number. For coherent states $|\alpha\rangle$ the average photon-number, i.e., its intensity, is $\langle\hat{n}\rangle = |\alpha|^2$. Moreover, the number operator is generator for the phase-rotation operator $\hat{R}(\varphi) = e^{-i\hat{n}\varphi}$. Given light-pulse intensity $\langle\hat{n}\rangle = |\alpha|^2$ and choosing a "reference value" α, one can define states:

$$|\Psi(\varphi)\rangle = \hat{R}(\varphi)|\alpha\rangle = \left|e^{-i\varphi}\alpha\right\rangle. \tag{2}$$

For each two angles $\varphi \neq \varphi'$, the corresponding states $|\Psi(\varphi)\rangle$ and $|\Psi(\varphi')\rangle$ have a non-zero overlap. In the limit $\Delta\varphi \to 0$, we have:

$$\begin{aligned}
|\langle\Psi(\varphi)|\Psi(\varphi')\rangle|^2 &= \exp[-4|\alpha|^2(\sin\tfrac{\Delta\varphi}{2})^2] \\
&\xrightarrow{\Delta\varphi \to 0} \exp[-|\alpha|^2\Delta\varphi^2] \\
&= \exp[-\tfrac{(\varphi-\varphi')^2}{2\sigma_\alpha^2}],
\end{aligned}$$

with $\sigma_\alpha^2 = 1/(2|\alpha|^2) = 1/(2\langle \hat{n} \rangle)$. On the other hand, for $|\Delta\varphi| = |\varphi - \varphi'| = \pi$, even for modest values of the average number of photons, the two states become quasi-orthogonal:

$$| \langle \Psi(\varphi)|\Psi(\varphi') \rangle |^2 \quad = \quad \exp[-2|\alpha|^2(1 - \cos\Delta\varphi)]$$
$$\xrightarrow{|\Delta\varphi|=\pi} \exp[-4|\alpha|^2]$$
$$\xrightarrow{|\alpha|^2 \gg 1} 0.$$

Thus, each two states $|\Psi(\varphi)\rangle$ and $|\Psi(\varphi + \pi)\rangle$ form a (quasi-orthogonal) basis. In our protocol, we will consider $2M$ discrete bases $\mathcal{B}_k = \{|\Psi(\varphi_k)\rangle, |\Psi(\varphi_k^\perp)\rangle\}$, given by the angles $\varphi_k = k\frac{\pi}{M}$ and $\varphi_k^\perp = k\frac{\pi}{M} + \pi$, with $k = 0, 1, \ldots 2M - 1$ and $M \in \mathbb{N}$. As quantum states are used to encode bit values 0 and 1, we will consider bases $\mathcal{B}_k$ to be ordered, such that the first vector $|\Psi(\varphi_k)\rangle$ encodes bit value 0, and the second, $|\Psi(\varphi_k^\perp)\rangle$, encodes bit value 1. Note that for each k, there exists the corresponding $\tilde{k} = k + M \pmod{2M}$, such that the two bases $\mathcal{B}_k$ and $\mathcal{B}_{\tilde{k}}$ consist of the same two states, encoding the opposite bit values. The "reference" basis $\mathcal{B}_0$ we will call the *computational basis*, with $|0\rangle = |\Psi(0)\rangle = |\alpha\rangle$ and $|1\rangle = |\Psi(\pi)\rangle = |e^{-i\pi}\alpha\rangle$. Finally, we will use the term "measurement in a (computational) basis" in a sense of "performing the optimal state discrimination between the two basis states ($|\Psi(0)\rangle$ and $|\Psi(1)\rangle$)". According to the Helstrom bound [27], the minimum probability of making an error in ambiguously inferring between two pure states $|\psi\rangle$ and $|\phi\rangle$ is $P_e = \frac{1}{2}(1 - \sqrt{1 - |\langle\psi|\phi\rangle|^2})$, which for two quasi-orthogonal states from $\mathcal{B}_k$ gives effectively perfect discrimination. Optimal discrimination between quasi-orthogonal coherent states in experiments is customary and can be efficiently performed in the lab (see for example the M-ry phase encoding procedure or amplitude encoding scheme [28–30]).

III. THE PROTOCOL

We combine the ideas of secure key distribution with continuous variables presented in [12, 16] with the secure message transmission scheme introduced in [22]. From a high level point of view, the latter scheme is as follows: Alice prepares a quantum system consisting of qubits, whose orientations are chosen at random but known to Alice, and sends it to Bob. He encodes his bits by doing nothing for a 0, and applying a phase flip (rotation of π) for a 1, and then returns the system to Alice. Since she prepared the system she knows how to measure each qubit and can retrieve the bit encoded. Our protocol follows the same overall idea, but instead of using qubits (two-dimensional quantum systems), we use coherent states of light pulses to encode the bit values.

The functionality presented in [22] is that of secure message transmission from Alice to Bob. However, we prefer to cast our techniques as a key distribution scheme, with the obvious option of using the resulting key r as input to an additional One-Time Pad encryption round. Note that this modification does not change the underlying physics; it merely adds an additional round over the classical channel. And it offers more flexibility since the resulting key can be used to send a message from Alice to Bob, from Bob to Alice, or for message authentication. The reason for preferring key distribution over message transmission is that if the input for the protocol is a random string, then several kinds of post-processing techniques (such as privacy amplification) are permitted, whereas if the input is a plaintext message then post-processing must not degrade the message. Also, an abort when information has leaked will be too late in the latter case.

Before giving more details about the quantum part, observe that Alice and Bob also dispose of a classical communication channel, more precisely a *public authenticated channel*. By this we mean a broadcast channel which does not provide privacy (i.e., anyone can listen to a conversation), but does provide message and source authentication – Eve cannot tamper with a message sent by Alice or Bob. Note that the existence of such a channel is a standard assumption in most quantum key distribution, including BB84 [3].

As explained above, the quantum part of the protocol consists of three steps: (1) Alice sends to Bob K distinguishable pulses of coherent light, such that each pulse $j = 1 \ldots K$ encodes the bit value 0 in the $\mathcal{B}_{k_j}$ basis, i.e., is in state $|\Psi(\varphi_{k_j})\rangle_j$. [The pulses are distinguishable by the time or the place of emission (depending on wether they are produced sequentially in time by a single laser, or in parallel, by a number of different lasers), denoted by the label j of the kets (i.e., each light pulse is from a different Hilbert space $\mathcal{H}_j$).] This way, Alice produces a multi-photon quantum system whose state $|\psi_k\rangle = \otimes_{j=1}^K |\Psi(\varphi_{k_j})\rangle_j$ is given by a tensor product of K coherent pulses. (2) Each pulse $|\Psi(\varphi_{k_j})\rangle_j$ will be used to encode a single bit value of the key r, by rotating its phase by π, in case $r_j = 1$, and doing nothing in case $r_j = 0$. (3) Alice rotates back each pulse to its computational basis and reads bit string r. In other words, our protocol can be interpreted as a quantum one-time pad generalisation in which, instead of two distinguishable classical/orthogonal/basis states, Alice chooses between $2M$ partially distinguishable quantum bases.

Now, the simplest way for a malicious Eve to eavesdrop the communication is a full man-in-the-middle attack: she intercepts Alice's quantum state $|\psi_k\rangle$ and keeps it stored in a stable quantum memory (say, a delay device such as an optical fibre pool), while sending her own state $|\psi_e\rangle$ to Bob, which the latter will use to encode his key r. Now Eve, upon intercepting Bob's state $|\psi_e(r)\rangle$ encoded with her own e, can easily decode it to learn r, and forward it to Alice encoded in the state $|\psi_k(r)\rangle$.

The above attack can be easily avoided by a simple verification technique: when she sends the quantum state $|\psi_k\rangle$, Alice also provides Bob, through the authenticated channel, with a certain number (say, $K/2$) of randomly chosen bases k_j of k, thus allowing Bob to check if the partial states $\hat{\rho}_{k_j} = \mathrm{Tr}_{k \backslash k_j} |\psi\rangle\langle\psi|$ of the j-th light pulse are indeed the expected pure states $\hat{R}(\varphi_{k_j})|\alpha\rangle$. This explains the inclusion of Steps 2b and 2c in Protocol 1 below. This verification technique should also be applied at the end of Step 2, with the roles reversed, to avoid Eve tampering with the state $|\psi_k(r)\rangle$ sent from Bob to Alice. This corresponds to Steps 2f and 3a below.

This verification technique is fairly standard in quantum cryptography (used for example in famous quantum key distribution schemes). It severely restricts Eve's class of attacks. For example, she cannot split coherent-light pulses, keeping one part with her, as this change of state would be easy to spot by measuring the average photon number). So Bob and Alice must receive the intended states $|\psi_k\rangle$ and $|\psi_k(r)\rangle$, at the beginning of Steps 2 and 3, respectively. Eve can only correlate her ancilla systems (on which she can subsequently perform measurements) with $|\psi_k\rangle$ and $|\psi_k(r)\rangle$, respectively.

This leads to the following protocol.

Protocol 1 (QKD by phase flip)

Setup:

- $\langle\hat{n}\rangle = |\alpha|^2$: expected photon number

- $2M$: number of possible bases

- K : initial number of pulses

- $k = (k_1, \ldots, k_K)$, where each $k_j \in \{0, \ldots, 2M - 1\}$: Alice's choice of bases

- $r = (r_1, \ldots, r'_K)$, where each $r_j \in \{0, 1\}$: Bob's choice of key bits

Step 1. *Preparation of the quantum state*

(a) For $1 \leq j \leq K$, Alice chooses uniformly at random $k_j \in \{0, \ldots, 2M - 1\}$, forming his choice of bases $k = (k_1, \ldots, k_K)$.

(b) Alice prepares the corresponding quantum state

$$|\psi_k\rangle = \bigotimes_{j=1}^{K} \left[\hat{R}(\varphi_{k_j})|\alpha\rangle_j \right] = \bigotimes_{j=1}^{K} \left| e^{-i\varphi_{k_j}}\alpha \right\rangle_j \tag{3}$$

and sends it to Bob.

Step 2. *Encoding the random key r*

(a) Bob receives $|\psi_k\rangle$ and informs Alice of that fact.

(b) Alice chooses a random bit string v of size K and weight $K' = K/2$ (i.e., a string with equal number of zeros and ones). Then she computes k', where $k'_j = k_j$ if $v_j = 0$, and $k'_j = \square$ otherwise, and sends v and k' to Bob over the authenticated channel. Here, $\square$ represents a default value different from any possible value of k_j, indicating that the pulses for which $v_j = 1$ will not be used in the Bob's verification procedure (the following Step 2 (c)).

(c) Bob receives v, k' and verifies that for j with $v_j = 0$, $\hat{\rho}_{k'_j}$ equals the pure state $\hat{R}(\varphi_{k'_j})|\alpha\rangle_j$.

(d) Let $|\psi'_k\rangle$ denote the quantum state received by Bob in which positions with $v_i = 0$ have been traced out. Bob generates a random string r of size $K/2$, the key, and encrypts it as follows:

$$|\psi'_k(r)\rangle = \left[\bigotimes_{j=1}^{K'} \hat{R}(r_j\pi) \right] |\psi_k\rangle. \tag{4}$$

(e) Bob sends $|\psi'_k(r)\rangle$ to Alice.

(f) Bob chooses a random bit string w of size $K' = K/2$ and weight $K'' = K/4$. Then he computes r', where $r'_j = r_j$ if $w_j = 0$, and $r'_j = \square$ otherwise, and sends w and r' to Alice over the authenticated channel. He computes the final key r which is obtained from r by concatenating all the bit positions r_i for which $w_i = 1$.

Step 3. *Decoding the random key r*

(a) Alice receives $|\psi'_k\rangle$ and uses her choice of bases k to verify that for j with $w_j = 0$, $\hat{\rho}_{k_j}$ equals the pure state $\hat{R}(\varphi_{k_j} + r_j\pi)|\alpha\rangle_j$.

(b) Then she uses the remaining positions, i.e. with $w_j = 1$, to determine r of size K'' encoded in quantum states of the computational basis $\mathcal{B}_0$:

$$
\begin{aligned}
|\psi''(r)\rangle &= \left[\bigotimes_{j=1}^{K''} \hat{R}(-\varphi_{k_j})\right] |\psi_k(r)\rangle \\
&= \bigotimes_{j=1}^{K''} \left|e^{-ir_j\pi}\alpha\right\rangle_j \\
&= \bigotimes_{j=1}^{K''} |r_j\rangle_j.
\end{aligned}
\tag{5}
$$

Note that, in order to perform state verification in Step 2c, Bob has to store $|\psi_k\rangle$ in a stable quantum memory, while waiting for Alice to send him the needed classical information, during Step 2b. The existence of long-term stable quantum memories is currently still a matter of considerable technological limitations, which might seem to undermine the security of current implementation of our protocol. However, while indeed the lack of quantum memories prevents the implementation of the verification procedure, it also prevents Eve from performing the man-in-the-middle attack, the very reason for the need for verification. In other words, as long as stable quantum memories are out of the reach of the technology, Eve would not be able to perform the attack which would require the verification procedure, and consequently the protocol security would not be compromised by this fact. It is an interesting question, though, to analyse the case of Eve and Bob having realistic, noisy memories, but of a different quality – say, Eve is a wealthy corporation/agency that wants to breach the privacy of ordinary everyday consumers who cannot afford the expensive cutting-edge technology. While indeed interesting and relevant, such analysis exceeds the scope of this paper (for the analysis of the effects of realistic noisy memories on the security on a two-state quantum bit-commitment protocol, see [31]).

IV. SECURITY OF THE PROTOCOL

In the following, we analyse in more detail the protocol's security against attacks in which Eve intercepts pulses sent by Alice, performs measurements on them and forwards the pulses to Bob, or just entangles her ancillas with the pulses and measures the pulses returned by Bob after Step 2, as well as against the beam splitting attack. First, we show the security of k, Alice's choice of bases: upon intercepting the state $|\psi_k\rangle$, Eve cannot learn the chosen bases k, and consequently she cannot decode the key r. Note that from the point of view of Eve, who does not know k, the mixed state $\hat{\rho}_B$ of an array of K pulses of coherent light sent by Alice is:

$$
\begin{aligned}
\hat{\rho}_B &= \frac{1}{(2M)^K} \sum_{k_1,\ldots k_K=0}^{2M-1} \left[\bigotimes_{j=1}^{K} |\Psi(\varphi_{k_j})\rangle\langle\Psi(\varphi_{k_j})|\right] \\
&= (\hat{\rho})^{\otimes K},
\end{aligned}
\tag{6}
$$

where $\hat{\rho} = \frac{1}{2M}\sum_{k=0}^{2M-1} |\Psi(\varphi_k)\rangle\langle\Psi(\varphi_k)|$. The summation over k_j implies the lack of knowledge of Eve on the basis used among the possible bases. Note that both $\hat{\rho}_B$ and $\hat{\rho}$ are implicitly functions of M and $\langle\hat{n}\rangle = |\alpha|^2$. The Holevo Theorem says that upon performing an arbitrary POVM on $|\psi_k\rangle$, the mutual information $I(k : e)$ between k and Eve's inference e is bounded by the von Neumann entropy $S(\hat{\rho}_B)$ of the state $\hat{\rho}_B$:

$$
I(k : e) \leq S(\hat{\rho}_B) = K \cdot S(\hat{\rho}).
\tag{7}
$$

On the other hand, the Shannon entropy $H(k)$ of k is:

$$H(k) = K \cdot \log M. \tag{8}$$

In other words, in order not to allow Eve to learn more than a negligible part of k, the following equation has to be satisfied:

$$S(\hat{\rho}) \ll \log M. \tag{9}$$

From equation (1) for coherent states, one can obtain the following expression for $\hat{\rho}$:

$$\hat{\rho} = \frac{1}{2M} \sum_{k=0}^{2M-1} |\Psi(\varphi_k)\rangle\langle\Psi(\varphi_k)| \tag{10}$$

$$= \frac{e^{-|\alpha|^2}}{2M} \sum_{n,n'=0}^{+\infty} \frac{(\alpha)^n (\alpha^*)^{n'}}{\sqrt{n!n'!}} J(n,n';M)|n\rangle\langle n'|,$$

where $J(n,n';M) = \sum_{k=0}^{2M-1} e^{ik(n'-n)\frac{\pi}{2M}} = \sum_{k=0}^{2M-1} q^k$ and $q = e^{i(n'-n)\frac{\pi}{2M}}$. For $q \neq 1$ (i.e., $n \neq n'$), we have:

$$J(n,n';M) = \begin{cases} 2M, & \text{if } n'-n = 0 \\ 0, & \text{if } n'-n = 2l, l \in \mathbb{Z} \setminus \{0\} \\ -\dfrac{2}{e^{i\frac{2l+1}{2M}\pi} - 1}, & \text{if } n'-n = 2l+1, l \in \mathbb{Z} \setminus \{0\}. \end{cases} \tag{11}$$

Finally, one gets

$$\hat{\rho} = \sum_{n \in \mathbb{N}_0} \rho_{n,n} |n\rangle\langle n| + \sum_{n \in \mathbb{N}_0} \rho_{n,n+2l+1} |n\rangle\langle n+2l+1|, \tag{12}$$

with the matrix elements given by ($\alpha = |\alpha|e^{i\theta}$):

$$\rho_{n,n} = \frac{e^{-|\alpha|^2}|\alpha|^{2n}}{n!} \tag{13}$$

$$\rho_{n,n+2l+1} = \frac{e^{-|\alpha|^2}|\alpha|^{2(n+l)+1}}{M\sqrt{n!(n+2l+1)!}} \cdot \frac{e^{-i(2l+1)\theta}}{e^{(l+\frac{1}{2})\frac{\pi}{m}} - 1}.$$

Numerical results for $S(\hat{\rho})$ confirm that the above criterion (9) is satisfied even for modest values on photons per pulse. On Figure 1 we present $S(\hat{\rho})$ as a function of M, for $\langle \hat{n}\rangle = |\alpha|^2 = 200$ (note that due to the symmetry, the von Neumann entropy is not a function of the phase of the "reference value" α). We see that after a steep increase, the curve reaches a plateau $S_{max}(\hat{\rho})$, showing that for big enough M the above criterion (9) is satisfied. On Figure 2 we plot $S_{max}(\hat{\rho})$ for $\langle \hat{n}\rangle = |\alpha|^2 = 8, \ldots, 200$ showing that the security criterion (9) is satisfied for a wide range of photon-numbers.

Moreover, one can give an upper bound to $S_{max}(\hat{\rho})$ confirming the above plot from Figure 2. Since any non-selective measurement increases the entropy, one has:

$$S(\hat{\rho}) \leq S\left(\sum_n |n\rangle\langle n|\hat{\rho}|n\rangle\langle n| \right) = H(\{p_n^{(\hat{n})}\}), \tag{14}$$

where $p_n^{(\hat{n})} = \langle n|\hat{\rho}|n\rangle$ is the probability to find n photons in the pulse. The results of the measurement of the number operator $\hat{n}$ obey the Poisson distribution (the diagonal elements of $\hat{\rho}$, see (13)), for which the Shannon entropy's leading term in the large-$|\alpha|$ asymptotic expansion is precisely of the order of $\ln |\alpha|$. Thus, in order to satisfy the security criterion (9), one must have $\langle \hat{n}\rangle = |\alpha|^2 \ll M$.

One might consider an analogous to the beam-splitting attack used in the case of single-photon key-distribution cryptography: Eve can try to split the coherent pulse sent from Alice, send one of its parts to Bob, and keep the rest with her. Unlike the single-photon case, where the signals are weak (precisely in order to minimise the probability of multi-photon emissions), in our case of genuine multi-photon coherent pulses, one can measure photon-number as well. Indeed, since the average photon number is given by $\langle \hat{n}\rangle = |\alpha|^2$, this is precisely what Bob does in Step 2 (c): "verifies that for j with $v_j = 0$, $\hat{\rho}_{k'_j}$ equals the pure state $\hat{R}(\varphi_{k'_j})|\alpha\rangle_j$" (obviously, verifying that the state is given by a complex number $e^{-i\varphi_{k'_j}}\alpha_j$ goes beyond just checking its absolute value $|\alpha_j|^2$).

In realistic implementations, the photon losses during the emission, transmission and detection, as well as due to imperfect detectors, lead to an effective decrease of the mean photon-number $|\alpha|^2$. Nevertheless, the users of the devices, Alice and Bob, do have the knowledge of the original laser intensity and overall efficiency of the fibre and detectors used, provided by the lab/company that have assembled and maintain the network (much as any user is provided by the essential specifications of a product needed for it to be properly used). This way, Bob can in advance anticipate the losses of an untempered network, and detect eavesdropping through additional losses.

One of the common attacks widely considered regarding quantum key distribution protocols is the so-called collective attack. Such attacks, designed for the BB84-like key distribution, is not really applicable in our case. In BB84 (and similar protocols), upon exchanging quantum systems and performing the measurements, Alice and Bob exchange classical information over the public network that allows them to extract the key. The collective attacks are the attacks in which Eve intercepts quantum communication from Alice to Bob, entangles her ancilla qubits to those sent by Alice, resends the intercepted qubits to Bob, and waits to perform the measurement(s) on her ancillas only upon learning the subsequently exchanged classical information. But in our protocol, no classical information is exchanged between Alice and Bob regarding the pulses used for extracting the key, apart from the trivial information on the success of the final measurement performed by Alice, so this type of attack is not applicable in our case.

Eve could in principle use more sophisticated techniques to, upon intercepting the encoded state $|\psi_k(r)\rangle$, "directly" learn the key r. For instance, she could initially entangle her ancilla with the pulses sent by Alice in such a way to preserve the classical correlations between the bases k and the quantum states $|\psi_k\rangle$, thus succeeding to pass the protocol's verification procedure, and finally perform a joint coherent measurement on the pulses returned by Bob to Alice. As noted at the end of the previous section, showing the protocol's security against general coherent attacks under realistic effects of noise and measurement errors exceeds the scope of this paper. Following the ideas of device-independent quantum cryptography [32], one could introduce an additional verification based on the violation of a Bell-like inequality and on entanglement monogamy, which could in principle allow Alice and Bob to detect
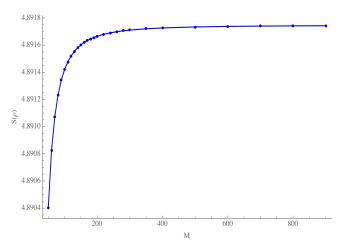

Figure 1. (color online) The plot of $S(\hat{\rho})$ as a function of M for $\langle \hat{n} \rangle = |\alpha|^2 = 200$.
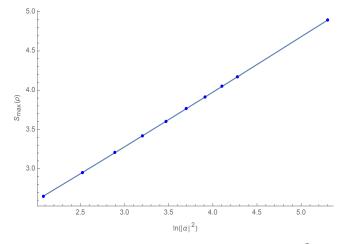

Figure 2. (color online) The logarithmic plot of $S_{max}(\hat{\rho})$ as a function of $\ln(|\alpha|^2)$, for $\langle \hat{n} \rangle = |\alpha|^2 = 8, \ldots, 200$.

arbitrary weak tampering by Eve. Nevertheless, mesoscopic continuous variable entangled states are far beyond today's technology.

Furthermore, one should keep in mind that the proposed system can work in long haul channels where several amplification stages are used (see Section V of [33]). Tapping techniques that could be used by Eve based on single photons cannot work through optical amplifiers, due to the non-cloning theorem. Finally, the mesoscopic signals also demand some bandwidth separation from other channels whenever a same optical fiber is used to avoid signal "talking" from the intense modes with the mesoscopic one.

V. CONCLUSIONS

In this paper, we have presented a quantum key distribution protocol that uses coherent states of light to encode single-bit values, and analysed its security. The protocol is based on the interplay between the quantum noise and the information acquired by Eve (given by the Holevo's theorem): whenever the laser signals are strong enough so that the noise over signal ratio $\langle(\Delta\hat{n})^2\rangle/\langle\hat{n}\rangle^2$ goes to zero, the signal can be seen as a classical signal and can be perfectly copied. In the opposite case, if the shot noise is high enough, no measurement will produce identical results on similarly prepared signals. This is the physical protection behind this communication – the attacker cannot distinguish between the signals sent from Bob to Alice in the public communication stage. This establishes the basic condition for the application of Holevo's theorem.

Moreover, while the protocol introduced in [12, 16] requires for certain amount of a pre-shared secret key, our protocol does not (a feature shared with the protocol presented in [22]). However, unlike the protocol from [22], which is based on single-qubit rotations, our protocol is not constrained by the need of slow and expensive detectors, characteristic for applications that encode bit values in single-photon states. Finally, the "Holevo argument" is rather non-trivial in our case, as single bit values are encoded in states from an infinitely-dimensional Hilbert space (and not in 2-dimensional qubit states, as is the case of [22]). We confirmed numerically that for a huge range of the average photon-number per pulse, the maximal amount of information that can be transmitted by a single pulse of coherent light, as a function of M, saturates to a finite value. Moreover, by giving the upper bound to the von Neumann entropy $S_{max}(\hat{\rho})$, we confirmed the numerically observed logarithmic behaviour of its dependance on $|\alpha|$, thereby ensuring the protocol's security, by choosing sufficiently large $M \gg \langle\hat{n}\rangle = |\alpha|^2$. We also showed that the protocol is secure against a beam-splitting attacks, and that the analog of the collective attack is not applicable to the case of our protocol.

It should be emphasized that the presented protocol is a fast protocol due to the light intensities involved, the fast detectors utilized (telecomm type) and the lower associated cost. The presented protocol is not a single photon based protocol neither depend on short distances under losses to operate as usual in the BB84 kind of protocols. Also the objective is not to present any substitutive for BB84 or the single photon family but just to present a practical and fast system for many applications that demand long range, lower cost and fast speeds.

The main direction of the future work would be to analyse quantitatively the protocol's security level as a function of security parameters M and $\langle\hat{n}\rangle = |\alpha|^2$ against concrete attacks (single-qubit measurements only, etc.). One can also study other cryptographic protocols with continuous variables based on the public key encryption scheme used in this article. For example, it is possible to straightforwardly use coherent states instead of two-dimensional states of qubits to achieve more robust oblivious transfer protocol presented in [34].

ACKNOWLEDGMENTS

[1] P. Shor, SIAM J. Comput. **26**, 1484 (1997).
[2] S. Wiesner, SIGACT News **15**, 78 (1983).
[3] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984) pp. 175–179.
[4] H. K. Lo and H. Chau, **283**, 2050 (1999).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[6] D. Mayers, J. ACM **48**, 351 (2001).

[7] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[8] *Highspeed detectors*, Newport Corporation, California, USA (2016), url = http://www.lightwavestore.com/ product_datasheet/OTI-Rx-015C_pdf1.pdf.

[9] *Single photon detectors*, Thor Labs, New Jersey, USA (2016), url = https://www.thorlabs.com/ newgrouppage9.cfm? objectgroup_id=5255&pn=SPCM20A/M.

[10] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).

[11] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[12] G. A. Barbosa, Phys. Rev. A **68**, 052307 (2003).

[13] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[14] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Phys. Rev. A **76**, 052323 (2007).

[15] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nature Photonics **7**.

[16] G. A. Barbosa and J. van de Graaf, Brazilian Journal of Information Security and Cryptography **2**, 16 (2015).

[17] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A **92**, 062323 (2015).

[18] D. Huang, P. Huang, D. Lin, and G. Zeng, Scientific Reports **6**.

[19] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, arXiv: 1510.08737v3 [quant-ph].

[20] A. Leverrier, arXiv: 1701.03393 [quant-ph].

[21] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).

[22] G. M. Nikolopoulos, Phys. Rev. A **77**, 032348 (2008).

[23] U. Seyfarth, G. M. Nikolopoulos, and G. Alber, Phys. Rev. A **85**, 022342 (2012).

[24] C. Vlachou, J. Rodrigues, P. Mateus, N. Paunković, and A. Souto, International Journal of Quantum Information **13**, 1550050 (2015).

[25] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)*, 1st ed. (Cambridge University Press, 2004).

[26] W.-M. Zhang, D. H. Feng, and R. Gilmore, Rev. Mod. Phys. **62**, 867 (1990).

[27] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[28] E. Corndorf, G. Barbosa, C. Liang, H. P. Yuen, and P. Kumar, Opt. Lett. **28**, 2040 (2003).

[29] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, Phys. Rev. A **71**, 062326 (2005).

[30] O. Hirota, K. Ohhata, M. Honda, S. Akutsu, Y. Doi, K. Harasawa, and K. Yamashita, "Experiments of 10 gbit/sec quantum stream cipher applicable to optical ethernet and optical satellite link," (2009).

[31] R. Loura, A. J. Almeida, P. S. André, A. N. Pinto, P. Mateus, and N. Paunković, Phys. Rev. A. **89**, 052336 (2014).

[32] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[33] G. A. Barbosa, Phys. Rev. A **71**, 062333 (2005).

[34] J. Rodrigues, P. Mateus, N. Paunković, and A. Souto, Journal of Physics A: Mathematical and Theoretical **50**, 205301 (2017).