Quantum key distribution by phase flipping of coherent states of light

G. A. Barbosa\textsuperscript{1}, J. van de Graaf\textsuperscript{2}, P. Mateus\textsuperscript{3,4} and N. Paunković\textsuperscript{3,5}

\textsuperscript{1} QuantaSEC – Consulting, Projects and Research in Physical Cryptography Ltd., Brazil
\textsuperscript{2} Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, Brazil
\textsuperscript{3} Instituto de Telecomunicações, Portugal
\textsuperscript{4} Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa
\textsuperscript{5} (Dated: September 23, 2016)

In this paper we present quantum key distribution protocol that, instead of single qubits, uses 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 and the “collective attack”, we introduce two types of verification procedures, and analyse the protocol’s security using the Holevo bound.

PACS numbers: 03.67.-a, 03.67.Ac, 03.67.Dd

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 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. To meet such requirements, a protocol for distributing keys using coherent states of light was introduced in \[8\] (see also recent proposals \[10, 11\]). The use of 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. In addition to that, the protocol \[8\] 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 \[12\] and subsequently analysed in \[13\] (see also a recent scheme \[14\] 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 \[8\], and secure message transfer with single qubits \[12\], 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 \[12\] 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 \[15\], 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. 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 \$\|\$ or \[? \] . 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 \(H = \hbar \omega (\hat{a} \dagger \hat{a} + \frac{1}{2})\), 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:

\[
|\alpha\rangle = e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle,
\]

where \(\alpha = e^{i\varphi}|\alpha\rangle \in \mathbb{C} \setminus \{0\}\). Coherent states saturate Heisenberg relations for the position and the momentum operators \(\hat{x} = \sqrt{\frac{\hbar}{2\omega}}(\hat{a} + \hat{a}^\dagger)\) and \(\hat{p} = i\sqrt{\frac{\hbar}{2\omega}}(\hat{a} - \hat{a}^\dagger)\), 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 \[10\]).

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 \(\hat{R}(\varphi) = e^{-i n \varphi}\). Given light-pulse intensity \(\langle \hat{n} \rangle = |\alpha|^2\) and choosing a “reference value” \(\alpha\), one can define states:

\[
|\Psi(\varphi)\rangle = \hat{R}(\varphi)|\alpha\rangle = |e^{-i \varphi} \alpha\rangle.
\]

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:

\[
|\langle \Psi(\varphi)|\Psi(\varphi')\rangle|^2 = \exp[-4|\alpha|^2(\sin \frac{\Delta \varphi}{2})^2]
\]

\[
\xrightarrow{\Delta \varphi \to 0} \exp[-|\alpha|^2 \Delta \varphi^2]
\]

\[
= \exp[-\frac{(\varphi - \varphi')^2}{2\sigma^2}],
\]

with \(\sigma^2 = 1/(2|\alpha|^2) = 1/(2\langle \hat{n} \rangle)\). 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:

\[
|\langle \Psi(\varphi)|\Psi(\varphi')\rangle|^2 = \exp[-2|\alpha|^2(1 - \cos \Delta \varphi)]
\]

\[
\xrightarrow{|\Delta \varphi| = \pi} \exp[-4|\alpha|^2]
\]

\[
|\alpha|^2 \gg 1 \rightarrow 0.
\]

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 \(\mathcal{B}_k = \{|\Psi(\varphi_k)\rangle, |\Psi(\varphi^+_k)\rangle\}\), given by the angles \(\varphi_k = k \frac{\pi}{M}\) and \(\varphi^+_k = k \frac{\pi}{M} + \pi\), 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, \(|\Psi(\varphi^+_k)\rangle\), encodes bit value 1. Note that for each \(k\), there exists the corresponding \(\tilde{k} = k + M \mod 2M\), 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 [17], 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.

### III. THE PROTOCOL

We combine the ideas of secure key distribution with continuous variables presented in [8] with the secure message transmission scheme introduced in [12]. 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 \( \pi \)) 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 [12] 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 \( \mathcal{B}_k \) basis, i.e., is in state \(|\Psi(\varphi_{kj})\rangle\rangle_j \). [The pulses are distinguishable by the time or the place of emission (depending on weather 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 \(|\psi_k\rangle = \otimes_{j=1}^K |\Psi(\varphi_{kj})\rangle\rangle_j \) is given by a tensor product of \( K \) coherent pulses. (2) Each pulse \(|\Psi(\varphi_{kj})\rangle\rangle_j \) will be used to encode a single bit value of the key \( r \), by rotating its phase by \( \pi \), 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 \( \hat{\rho}_k = Tr_{k/k_j} |\psi\rangle\langle\psi| \) of the \( j \)-th light pulse are indeed the expected pure states \( \hat{R}(\varphi_{kj}) |\alpha\rangle \). 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 \(|\psi_e(r)\rangle\) 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
\[
|\psi_k\rangle = \bigotimes_{j=1}^{K} R(\varphi_{k_j}) |\alpha\rangle = \bigotimes_{j=1}^{K} e^{-i\varphi_{k_j}} |\alpha\rangle,
\]
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 $k'_j = \Box$ otherwise, and sends $v$ and $k'$ to Bob over the authenticated channel. Here, $\Box$ 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 $v_j = 0$, $\hat{R}(\varphi_{k'_j}) |\alpha\rangle$.
(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:
\[
|\psi'_k(r)\rangle = \bigotimes_{j=1}^{K'} R(r_j \pi) |\psi_k\rangle.
\]
(e) Bob sends $|\psi'_k(r)\rangle$ to Alice.
(f) Bob chooses a random bit string $w$ of size $K' = K/2$ and weight $K'' = K/4$, and sends it 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 $w_j = 0$, $\hat{R}(\varphi_{k_j}) |\alpha\rangle$.
(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 $B_0$.
\[
|\psi''(r')\rangle = \bigotimes_{j=1}^{K''} R(-\varphi_{k_j}) |\psi_k(r)\rangle = \bigotimes_{j=1}^{K''} e^{-ir_j \pi} |\alpha\rangle = \bigotimes_{j=1}^{K''} |r'_j\rangle.
\]
However, Eve could in principle use more sophisticated techniques to, (i) upon intercepting the state $|\psi_k\rangle$ learn the chosen bases $k$, and consequently decode the key $r$ or (ii) upon intercepting the encoded state $|\psi_k(r)\rangle$ “directly” learn the key $r$ (possibly by initially entangling 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 passing the mentioned verification technique). In next section, we prove that for adequately chosen numbers of bases $2M$ and pulses sent $K$, Eve cannot learn but a negligible part of the chosen bases $k$.

Regarding the “collective attack” (ii), the following additional verification could be introduced in order to prevent any entanglement between Eve and the pulses exchanged between Alice and Bob. In addition to the $K$ pulses prepared in pure coherent states $|\psi_k\rangle$, Alice prepares a certain number, say $E$, of maximally entangled pairs of coherent-light pulses $|\psi\rangle_{AB}$ (for entangled coherent states and their respective Bell inequalities, see the recent work [18–20]). She keeps the systems $A$ to herself, while sending the systems $B$ to Bob, randomly inserting them between the $K$ pure-state pulses $|\psi_k\rangle$. Half of the entangled pairs (again, randomly chosen among the total of $E$ pairs) Alice and Bob use to check the violation of a suitable Bell inequality by performing local measurements and classical communication over the mentioned (classical) authenticated channel. This way they prevent, because of the monogamy of entanglement, any additional correlations with Eve’s ancilla that might occur while transmitting pulses from Alice to Bob. The other half is used by Alice to check, upon receiving back from Bob all of the remaining pulses, and subsequently (over the authenticated channel) the values of keys $r_j$ used by Bob on the pulses from the entangled pairs, whether the states of those pairs are indeed $[\hat{I}_A \otimes \hat{R}_B(r_j,\pi)] |\psi\rangle_{AB}$.

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 [21]).

IV. SECURITY OF THE PROTOCOL

In the following, we show the security of $k$, Alice’s choice of bases. 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:

$$\hat{\rho}_B = \frac{1}{(2M)^K} \sum_{k_1,...,k_K=0}^{2M-1} \left[ \bigotimes_{j=1}^{K} |\Psi(\varphi_{k_j})\rangle\langle\Psi(\varphi_{k_j})| \right]$$

$$= \left( \hat{\rho} \right) \otimes K,$$

(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 $\hat{\rho}_B$:

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

(7)

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

$$H(k) = K \cdot \log M.$$

(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:

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

(9)
Indeed, numerical results for $S(\hat{\rho})$ confirm that the above criterion is satisfied even for modest values on photons per pulse (for the evaluation of the matrix elements of $\hat{\rho}$, see Appendix A). 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” $\alpha$). We see that after a steep increase, the curve reaches a plateau $S_{\text{max}}(\hat{\rho})$, showing that for big enough $M$ the above criterion (9) is satisfied. On Figure 2 we plot $S_{\text{max}}(\hat{\rho})$ 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 $S_{\text{max}}(\hat{\rho})$ confirming the above plot from Figure 2. Since any non-selective measurement increases the entropy, one has:

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

(10)

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 (A4)), 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 $\langle \hat{n} \rangle = |\alpha|^2 \ll M$.

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 \cite{32} requires for certain amount of a pre-shared secret key, our protocol does not (a feature shared with the protocol presented in \cite{12}). However, unlike the protocol from \cite{12}, 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 \cite{12}). 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 \(S_{\text{max}}(\hat{\rho})\), we confirmed the numerically observed logarithmic behaviour of its dependance on \(|\alpha|\), thereby ensuring the protocol’s security, by choosing sufficiently large \(M \gg \langle \hat{n} \rangle = |\alpha|^2\).

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 \cite{22}.

**ACKNOWLEDGMENTS**

PM and NP thank Antony Laverrier for fruitful discussions and for bringing us the attention to the recent work \cite{10,11}. This work was partially supported, by SQIG at Intituto de Telecomunicações, and the CV-Quantum and QbigD internal projects at IT funded by FCT PEst-OE/EEI/LA0008/2013 and UID/EEA/50008/2013.

**Appendix A: Calculation of the elements of \(\hat{\rho}_M\)**

From equation (4) for coherent states, one can obtain the following expression for \(\hat{\rho}\):

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

(A1)

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

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

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

(A2)

Finally, one gets

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

(A3)

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

\[
\rho_{n,n} = \frac{e^{-|\alpha|^2}|\alpha|^{2n}}{n!}
\]

(A4)

\[
\rho_{n,n+2l+1} = \frac{e^{-|\alpha|^2}|\alpha|^{2(n+l)+1} e^{-i(2l+1)\theta}}{M \sqrt{n!(n+2l+1)!}} \frac{e^{i(l+\frac{1}{2})\pi}}{e^{i(l+\frac{1}{2})\pi} - 1}.
\]
[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, Science 283, 2050 (1999) [http://www.sciencemag.org/content/283/5410/2050.full.pdf].
[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] G. A. Barbosa, Phys. Rev. A 68, 052307 (2003).
[9] G. A. Barbosa and J. Graaf, arXiv: 1406.1543 [cs.CR].
[10] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A 92, 062323 (2015).
[11] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, arXiv: 1510.08737v3 [quant-ph].
[12] G. M. Nikolopoulos, Phys. Rev. A 77, 032348 (2008).
[13] U. Seyfarth, G. M. Nikolopoulos, and G. Alber, Phys. Rev. A 85, 022342 (2012).
[14] C. Vlachou, J. Rodrigues, P. Mateus, N. Paunković, and A. Souto, International Journal of Quantum Information 13, 1550050 (2015).
[15] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences), 1st ed. (Cambridge University Press, 2004).
[16] W.-M. Zhang, D. H. Feng, and R. Gilmore, Rev. Mod. Phys. 62, 867 (1990).
[17] C. W. Helstrom, Quantum Detection and Estimation Theory (Academic Press, New York, 1976).
[18] X. Wang, B. C. Sanders, and S. hua Pan, Journal of Physics A: Mathematical and General 33, 7451 (2000).
[19] C.-Y. Park and H. Jeong, Phys. Rev. A 91, 042328 (2015).
[20] E. E. Hach, P. M. Alsing, and C. C. Gerry, Phys. Rev. A 93, 042104 (2016).
[21] Z. Xu, J. Zhou, R. Loura, A. Almeida, P. André, A. Pinto, P. Mateus, and N. Paunković, Phys. Rev. A 89, 052336 (2014).
[22] J. Rodrigues, P. Mateus, N. Paunković, and A. Souto, arXiv: 1407.8146 [quant-ph].