Experimental realization of equiangular three state quantum key distribution

Matteo Schiavon, Giuseppe Vallone, and Paolo Villoresi
Dipartimento di Ingegneria dell'Informazione, Università di Padova, via Venezia 15, 35131 Padova

(Dated: April 28, 2016)

Quantum key distribution using three states in equiangular configuration combines a security threshold comparable with the one of the Bennett-Brassard 1984 protocol with a lower requirement of resources at the receiver. It also allows to estimate the quantum bit error rate (QBER) without the need to reveal part of the key. This makes it suitable for applications where the resources available at the receiver are limited. We implement an entanglement-based version of this protocol and evaluate its performance, both in the asymptotic limit of infinite key and in the case of finite key. We obtain an asymptotic secure key rate of more than 10 kbit/s with a mean QBER of 1.6%, and a fraction of secure bits larger than 25% for a block size of 10^6 bits.

Quantum key distribution (QKD) is a cryptographic technique allowing two parties, commonly referred to as Alice and Bob, to exchange a cryptographic key at the application layer. Unlike other key distribution schemes, whose security is based on some assumptions on the complexity of some numerical problems, QKD security is based on the laws of quantum mechanics, that prevent the extraction of information from a state without perturbing it. The first QKD protocol has been proposed by Bennett and Brassard in 1984 (BB84) [1], and uses four states from two mutually unbiased bases. In 1992, Bennett showed that two non-orthogonal states are sufficient for QKD (B92 protocol) [2], however this scheme suffers from a strong dependence on channel losses, that could be exploited by an attacker to extract information about the key [3]. Loss independent unconditional security can be restored by adding a third state to the protocol.

The optimal three-state QKD protocol has been proposed by Phoenix, Barnett and Chefles in 2000 (PBC00) [4] and uses three states forming an equilateral triangle in the X-Z plane of the Bloch sphere, as shown in Figure 1. Each of the three possible couple of states, $S_1 = \{|\psi_1\rangle, |\psi_2\rangle\}$, $S_2 = \{|\psi_2\rangle, |\psi_3\rangle\}$, and $\{|\psi_3\rangle, |\psi_1\rangle\}$, can be thought as a different implementation of the B92 protocol, rotated of 120° in the X-Z plane of the Bloch sphere. For each set S_i, the first state corresponds to bit 0 and the second to bit 1. The PBC00 consists in a random choice, with probability $\frac{1}{3}$, of the B92 implementation to use for each exchanged qubit. Practically, Alice randomly chooses one of the three states $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$, with probability $\frac{1}{3}$ each, and sends it to Bob, who measures it with the POVM $\{\frac{2}{3}|\psi_1^\perp\rangle\langle\psi_1^\perp|, \frac{2}{3}|\psi_2^\perp\rangle\langle\psi_2^\perp|, \frac{2}{3}|\psi_3^\perp\rangle\langle\psi_3^\perp|\}$, where $|\psi_i^\perp\rangle$ is the orthogonal of $|\psi_i\rangle$. Alice and Bob record i and j if, respectively, they send $|\psi_i\rangle$ and measure $|\psi_j^\perp\rangle$. Since each state belongs to two different sets, and has bit value 0 for one set and 1 for the other one, Alice can choose the set by assigning to each exchanged qubit its value, by using a quantum random number generator (QRNG). Then, she communicates the set used for each qubit to Bob, who can thus discriminate between conclusive and inconclusive events like in the B92. Since the choice of the set is posterior to the detection of the qubits, the attacker cannot extract information by increasing the losses and performing the unambiguous state discrimination (USD) attack, thus improving the security of the protocol with respect to the B92. The PBC00, indeed, is asymptotically secure for a bit error rate of up to 9.81% [5] and has recently shown to be secure also in the case of finite key [6], by using the finite-key analysis framework introduced by Scarani and Renner [7] and

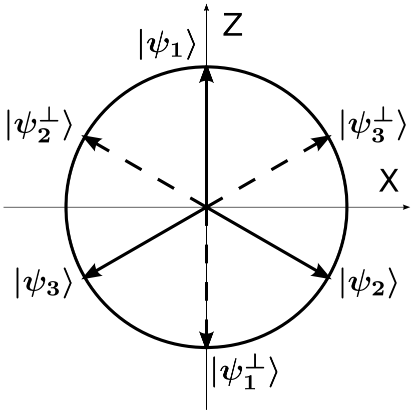

FIG. 1. States used in the PBC00 protocol. They lie in the X-Z plane of the Bloch sphere. Each couple of states, $S_1 = \{|\psi_1\rangle, |\psi_2\rangle\}$, $S_2 = \{|\psi_2\rangle, |\psi_3\rangle\}$, and $S_3 = \{|\psi_3\rangle, |\psi_1\rangle\}$, corresponds to a different implementation of a B92 protocol, each rotated of 120°.

the post-selection technique [8]. The symmetry of the protocol can also be exploited to use the number of inconclusive events to estimate the bit error rate, thus allowing to use all conclusive events for key generation. This feature has been first reported by Renes in 2004 [9] and the version of the PBC00 implementing this feature is therefore marked as R04.

In this work, we aim to present our recent results [10] about the experimental realization of an entanglement-based version of the R04 protocol, using the polarization degree of freedom. The setup used for the experiment is shown in Figure 2. A polarization singlet state is generated by an interferometric source of entangled photons in a Sagnac configuration. The two photons are then sent into Alice's and Bob's measurement apparatuses. The use of polarization singlet state allows the use of an identical apparatus for Alice and Bob, thus greatly simplifying the protocol with respect to the original proposal. The choice of the state to send is therefore made by Alice's measurement apparatus: each detector Ai at her side has $\frac{1}{3}$ probability of clicking, and heralds the presence of a photon with polarization $|\psi_i\rangle$ at Bob's side. This corresponds to the random choice of one of the three $|\psi_i\rangle$ with probability $\frac{1}{3}$. The measurement apparatus uses only passive optical devices, thus providing a much higher long term stability than the interferometric setup proposed by Phoenix *et al.* [4]. The detection uses three single-photon avalanche photodiodes (SPADs) for both Alice and Bob.

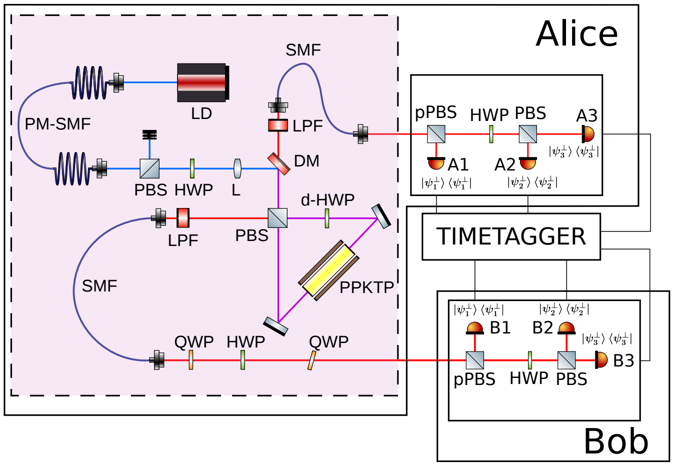
Alice
SMF
LD
PM-SMF
LPF
DM
PBS
HWP
L
d-HWP
LPF
PBS
SMF
PPKTP
QWP
HWP
QWP
pPBS
HWP
PBS
A3
A1
A2
$|\psi_1^\perp\rangle\langle\psi_1^\perp|$
$|\psi_2^\perp\rangle\langle\psi_2^\perp|$
$|\psi_3^\perp\rangle\langle\psi_3^\perp|$
TIMETAGGER
$|\psi_1^\perp\rangle\langle\psi_1^\perp|$
$|\psi_2^\perp\rangle\langle\psi_2^\perp|$
$|\psi_3^\perp\rangle\langle\psi_3^\perp|$
B1
B2
B3
pPBS
HWP
PBS
Bob

FIG. 2. Setup used for the experimental demonstration of the R04 protocol. A polarization singlet state is produced by a Sagnac interferometer. The two photons are then sent to Alice's and Bob's measurement apparatuses, consisting of a passive optical network and three single photon detectors each. The source is considered to be safe at Alice's side.

We show the analysis of a sample run of the experimental apparatus for about two hours of continuous acquisition. It consists in the exchange of $2 \cdot 10^8$ qubits, at a mean rate of 29 kHz.

We evaluate the efficiency of the protocol by estimating the fraction r of conclusive qubits leading to a secret key bit (secret fraction). In the asymptotic limit of infinitely long key, this fraction is given by

$$r = 1 - f_{EC} h(Q) - h\left(\frac{5}{4}Q\right),$$

where Q is the quantum bit error rate (QBER) and the term $f_{EC} = 1.1$ is an estimate of the efficiency of the error correction protocol. The QBER is calculated from the fraction of inconclusive events I as $Q = \frac{1-2I}{1-I}$. To give insight of the behaviour of the system, we have divided the acquired data into 90 blocks of about 80 s each, with a mean number of $1.1 \cdot 10^6$ conclusive bits per block. We evaluate the QBER and the asymptotic secure key rate for each block, obtaining the results shown in Figure 3. We estimate the fraction of correlated multi-photon events to be $\sim 1.5 \cdot 10^{-5}$, thus the information an attacker could obtain using the photon number splitting (PNS) attack is negligible.

Since in the real world the number of exchanged symbols is always finite, it is necessary to take into account also finite-size effect in the evaluation of the performance of a QKD protocol. In finite key analysis, the need to limit the probability of failure of the protocol leads to a further reduction in the secret fraction. Its upper bound, called security parameter, determines the fraction of bits that are wasted in every step of classical post-processing and is decided during the definition of the protocol. We restrict first to collective attacks, i.e. separate attacks on different qubits, applying the framework of Scarani and Renner [7], then we extend our evaluation to the most general attacks, using the post-selection technique [8]. In both cases, we take $4 \cdot 10^{-10}$ as security parameter. The results of the finite key analysis on the sample data are shown in Figure 4, where the fraction of secure bits in a single post-processing

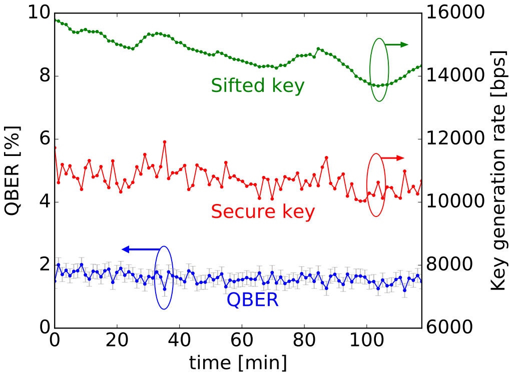

FIG. 3. Results of the sample run of the experimental setup. For each block, the QBER (blue) is calculated from the fraction of inconclusive events, and both the rate of conclusive events (green) and the secret key rate (red) are given.

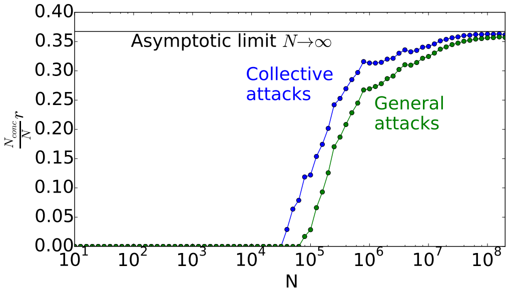

FIG. 4. Finite key analysis of the R04 protocol for collective (blue) and general attacks (green). The security parameter for both collective and general attacks is $4 \cdot 10^{-10}$.

block is plotted as a function of the block size N. This analysis gives an evaluation of the necessary trade-off between the block size and the fraction of secure bits in a block, a key parameter in the design of an implementation of the protocol.

Our work demonstrates the experimental feasibility of equiangular three state QKD and gives an early evaluation of its performance, with some design information that can be useful for its future implementation in a real key exchange scenario. The peculiarities of this protocol, i.e. the passive optics receiver requiring only three detectors and the error estimation from inconclusive results, make it interesting for those applications where the resources at the receiver are limited, but the guarantee of unconditional security independently from the loss level is still required. The recent advancements in integrated optics and single photon detectors make it feasible the integration of the whole receiver in a single chip. This protocol could find interesting applications in the emerging fields of embedded devices and drones, characterized by strict constraints in their available resources.

[1] C. H. Bennett and G. Brassard in *Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York), p. 175.

[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[3] K. Tamaki and N, Lütkenhaus, Phys. Rev. A **69**, 032316 (2004).

[4] S. Phoenix, S. Barnett, and A. Chefles, J. Mod. Opt. **47**, 507 (2000).

[5] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).

[6] M. Mafu, K. Garapo, and F. Petruccione, Phys. Rev. A **90**, 032308 (2014).

[7] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

[8] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).

[9] J. M. Renes, Phys. Rev. A **70**, 052314 (2004).

[10] M. Schiavon, G. Vallone, P. Villoresi, arXiv:*1603.07605* (2016).