Quantum Cryptography and Security

Quantum Key Distribution

Paolo Lapo Cerni
paololapo.cerni/at/studenti.unipd.it
University of Padua

20th December 2023

---

1 Introduction

One of the most effective practical applications in quantum cryptography and security is the *quantum key distribution*, in which a cryptographic key is securely distributed between Alice and Bob. In 1984, Bennett and Brassard proposed the so-called BB84 scheme [1], a theoretical proposal designed to work with true single-photons.
Such experimental setups are still unavailable for practical implementation and weak coherent laser pulses are used instead. However, pulsed lasers have a critical drawback: a non-negligible fraction of the emitted pulses contain more than one photon, making them vulnerable to the so-called *photon number splitting* (PNS) attack. During the communication between Alice and Bob, the eavesdropper (Eve) can perform a quantum non-demolition measurement (QND) on each of the quantum systems and measure the number of photons without disturbing any quantum states [2]. In case of a n-photon state (with $n > 1$), Eve could store in a quantum memory $n - 1$ of those, introducing no errors and undetected by the authorized partners.
Moreover, most of the security analysis classically done on the QKD protocols has been obtained in the asymptotic regime, i.e. considering infinitely long keys. In the finite-key scenario, Alice and Bob have to consider also the sampling problem of inferring the QBER on the $\mathbb{Z}$ basis from measurements on $\mathbb{X}$, and the fluctuations of the estimated quantities (statistics of the measurements) due to the finite realizations of the experiments.
In this report, we will introduce and analyze a *3-states 1-decoy* QKD protocol, evaluating the security of the obtained keys in the finite scenario. Such methods provide robust protocols to overcome the limitations of the multi-photon events and the finite keys.

2 Methods and analysis

Decoy state protocol

A laser generates a coherent state that can be written as:

$$|\alpha\rangle = \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} e^{-\mu/2} |n\rangle$$

where μ is the laser intensity and $|n\rangle$ the eigenstate of the number operator N.
In general, the emitted state can be described as the ensemble of Fock states $|n\rangle$ at fixed $\mu = |\alpha|^2$:

$$\rho = \sum_{n=0}^{+\infty} P_\mu(n) |n\rangle \langle n|$$

with $P_\mu(n)$ the probability of n events from the Poissonian distribution.
As briefly described, weak coherent pulses are vulnerable to the PNS attack. However, Alice and Bob can use the so-called *decoy method* to statistically analyze the probabilities of detection on Bob's side to detect a possible attack and estimate the security of the obtained key. This report will analyze the implementation of a *3-states 1-decoy efficient BB84* as described by Rusca et al. [3].

In this protocol, Alice and Bob agree on two orthogonal bases $\mathbb{Z}$ (key basis, $\{|H\rangle, |V\rangle\}$) and $\mathbb{X}$ (check basis, $\{|D\rangle, |A\rangle\}$). Therefore, for each laser pulse, Alice randomly chooses the transmitter basis with asymmetric probability P_Z and $P_X = 1 - P_Z$ such that $P_Z \gg P_X$. In our experimental implementation $P_Z^{(A)} \approx 0.9$ and $P_X^{(A)} \approx 0.1$. The protocol is called *3-states* because Alice uses only the set of states $\{|H\rangle, |V\rangle, |D\rangle\}$, so the state $|A\rangle$ is unused in emission.
Moreover, in a *1-decoy* setup, Alice randomly chooses both the basis $a_i \in \{\mathbb{Z}, \mathbb{X}\}$ and the pulse intensity $k \in \mathcal{K} = \{\mu_1, \mu_2\}$. In our case, $\mu_1 = 0.6$ ($P_{\mu_1} = 0.7$) and $\mu_2 = 0.1818$ ($P_{\mu_2} = 0.3$). Note that $\mu_1 > \mu_2$.
The basis selection probabilities at the receiver are instead equal: $P_Z^{(B)} \approx 0.5$ and $P_X^{(B)} \approx 0.5$. thus, Bob chooses his basis b_i and records the output of the measurement.

Then, the authorized parties have to sift the key by communicating their choices over the public channel. In so doing they define the sets $X_k = \{i : a_i = b_i = \mathbb{X}, k \in \mathcal{K}\}$ and $Z_k = \{i : a_i = b_i = \mathbb{Z}, k \in \mathcal{K}\}$ as the pairs state for which they used the same basis for a given intensity k. In so doing, they obtain the final raw key of size $n_Z = \sum_k n_{Z,k}$ with $n_{Z,k}$ the cardinality of the corresponding set, namely $n_{Z,k} = |Z_k|$. Note that n_Z can be considered a fixed parameter since you can run the key generator protocol until it reaches a chosen value (in this report we will consider $n_Z = 10^6$).
Alice and Bob can now compute the number of bits errors for each intensity $m_{Z,k}$. The total QBER in the $\mathbb{Z}$ basis will be the ratio m_Z/n_Z, where $m_Z = \sum_k m_{Z,k}$.
One can trivially define also $n_{X,k}$, n_X, $m_{X,k}$, and m_X.
Note that the number of events and the error rates can be written also in terms of Bob's detection given that Alice sent a n-photon state, $n_Z = \sum_{n=0}^{\infty} s_{Z,n}$ and $m_Z = \sum_{n=0}^{\infty} v_{Z,n}$.

Security estimation

Given the secrecy and correctness parameters ϵ_{sec} and ϵ_{cor}, one can prove that the secret key length for a finite-key analysis can be bounded by:

$$l = s_{Z,0}^l + s_{Z,1}^l(1 - h_2(\phi_Z^u)) - \lambda_{EC} - a\log_2(b/\epsilon_{sec}) - \log_2(2/\epsilon_{cor}).$$

where $s_{Z,0}^l$ and $s_{Z,1}^l$ are the lower bounds for the vacuum events and the single photon events (namely $s_{Z,0}$, $s_{Z,1}$) in the key basis, ϕ_Z^u is the upper bound of the phase error rate ϕ_Z, and λ_{EC} is the number of bits disclosed in the information reconciliation stage.
The parameters a and b depend on the security analysis taken into account (see Lim et al. [4]). In the case of a 1-decoy protocol, Rusca et al. [3] propose $a = 6$ and $b = 19$.

Considering the finite scenario described in [3], the first correction to do is to evaluate the difference between our observed quantity x and the corresponding asymptotic case x^*, due to the experimental fluctuations. The Hoeffding's inequality for independent variables [5] states that, with probability $1 - 2\epsilon$, holds:

$$|x^* - x| \leq \delta(x, \epsilon) \quad \text{with} \quad \delta(x, \epsilon) = \sqrt{x\log(1/\epsilon)/2}$$

Thus, we can then define:

$$n^{\pm}_{Z,k} := \frac{e^k}{p_k}(n_{Z,k} \pm \delta(n_Z, \epsilon_1)) \quad , \quad m^{\pm}_{Z,k} := \frac{e^k}{p_k}(m_{Z,k} \pm \delta(m_Z, \epsilon_2)) \qquad \forall k \in \mathcal{K}$$

Since the vacuum events $s_{Z,0}$ carry no information, neither for Bob nor for Eve, one can upper bound their contribution as:

$$s_{Z,0} \leq s^u_{Z,0} := 2(m_Z + \delta(n_Z, \epsilon_1))$$

Given the total probability to send a n-phton state $\tau_n = \sum_{k\in\mathcal{K}} p_k e^{-k} k^n/n!$ and assuming $\mu_1 > \mu_2$, one can also prove that:

$$s_{Z,0} \geq s^l_{Z,0} := \frac{\tau_0}{\mu_1 - \mu_2}\left(\mu_1 n^-_{Z,mu_2} - \mu_2 n^+_{Z,\mu_1}\right)$$
$$s_{Z,1} \geq s^l_{Z,1} := \frac{\tau_1\mu_1}{\mu_2(\mu_1 - \mu_2)}\left(n^-_{Z,\mu_2} - \frac{\mu_2^2}{\mu_1^2} n^+_{Z,\mu_1} - \frac{(\mu_1^2 - \mu_2^2)s^u_{Z,0}}{\mu_1^2\tau_0}\right)$$

Similarly, one can upper bound the number of bit errors in the $\mathbb{X}$ basis due to the single-photons:

$$v_{X,1} \leq v^u_{X,1} = \frac{\tau_1}{\mu_1 - \mu_2}\left(m^+_{X,\mu_1} - m^-_{X,\mu_2}\right)$$

and upper bound the phase error rate in the $\mathbb{Z}$ basis by the formula:

$$\phi_Z \leq \phi^u_X := \frac{v^u_{X,1}}{s^l_{X,1}} + \gamma(\epsilon_{sec}, \frac{v^u_{X,1}}{s^l_{X,1}}, s^l_{Z,1}, s^l_{X,1})$$

where

$$\gamma(a,b,c,d) := \sqrt{\frac{(c+d)(1-b)b}{cd\log 2}\log_2\left(\frac{c+d}{cd(1-b)b}\frac{21^2}{a^2}\right)}$$

As suggested by Lim et al. [4], we consider the disclosed bits during the error correction stage $\lambda_{EC} = f_{EC}h_2(\varepsilon_{obs})$ with f_{EC} set to be equal to 1.16 and ε_{obs} the average of the observed error rates in the key basis. Moreover, we set $\epsilon_1 = \epsilon_2 := \epsilon$, $\epsilon_{sec} = 19\epsilon = 10^{-9}$, and $\epsilon_{cor} = 10^{-15}$ [3].

Finally, we define the secret key rate SKR as the ratio between the secret key length and the total number of pulses N_{tot} sent to obtain the key, multiplied by the repetition rate of the source R:

$$\text{SKR} = \frac{l}{N_{\text{tot}}}R$$

We will consider $R = 1$.

Experimental realization

In this subsection, we will briefly introduce the experimental setup used to generate the data. A more complete and detailed description of a similar setup can be found in Agnesi et al. [6] and in Avesani et al. [7].
The transmitter (Alice) generates optical pulses (of $30 - 40$ps) via a gain-switched distributed feedback laser. With short pulses, you can better time-tag them and filter out the background noise.

Then, an intensity modulator (based on a *Sagnac interferometer* with a 70/30 beam splitter) sets each pulse to one of the two intensities chosen for the decoy method, maintaining the polarization. The polarization of the light is then modulated by the iPOGNAC, a modulator based on inline Lithium Niobate ($LiNbO_3$). With such apparatus, you can generate the four BB84 states.
Finally, Alice employs an attenuator and a filter.
The communication requires a single-mode fiber that introduces an unknown time dependency, while the measurements are based on single-photon detectors (SPAD). Bob uses only one detector instead of four, by time multiplexing the signals and using a polarization controller (APC).
A time-to-digital converter with a resolution of 81ps sends the data to the computers.

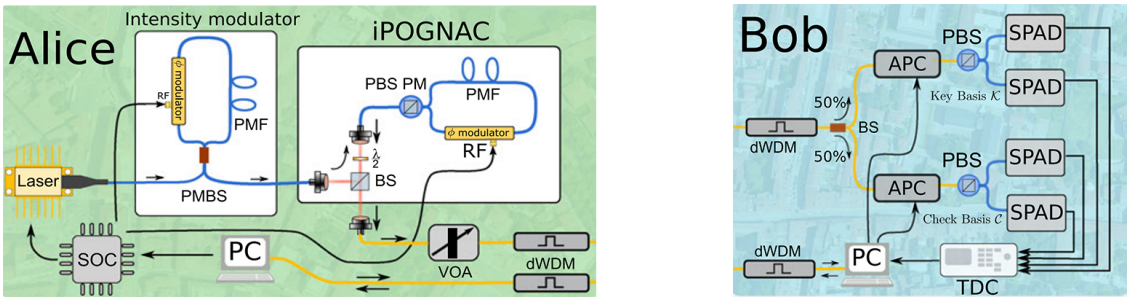

Figure 1. Setups of the authenticated parties. Schema from [7].

3 Results

The experimental data were organized into sets of 6000 pulses with time information about how long it took to collect those sets. Thus, we know the time used to generate each raw key [1].
Firstly, we can plot the time needed to process each block and the time used to generate a key of length $n_Z = 10^6$ (figure 2). As we can see the profile of the histograms is approximately Gaussian.

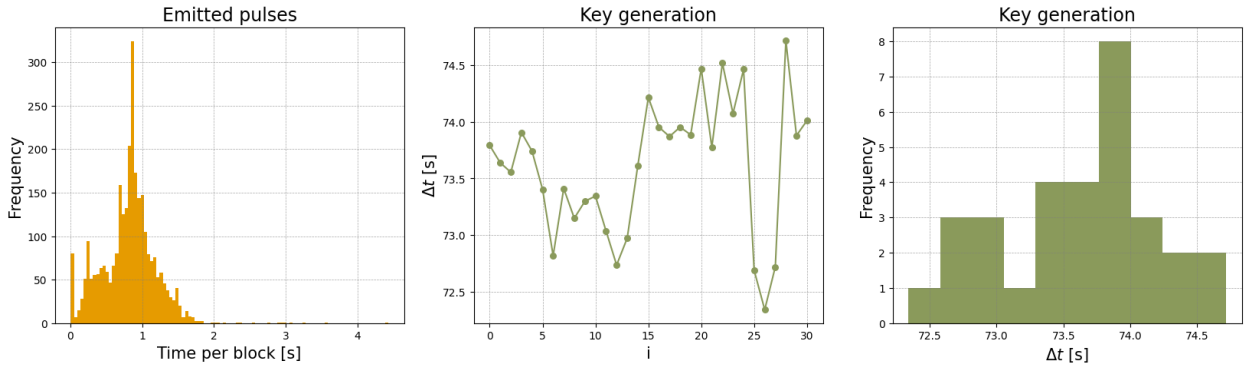

Figure 2. Distribution of the time needed to process a block (on the left) and to produce a key (on the right).

[1] This is not exactly true because we are interrupting the key generation when n_Z reaches the threshold and discarding the following bits of the last block used.

Then, we can analyze the QBER in the two bases and plot it as a function of the key number (i.e. the index of the obtained key) and the runtime (i.e. the time needed to the pulses used to generate the key). The magnitude of the QBER varies between 1% and 2%.
When plotted against the key number, the QBER follows a trend (figure 4, on the left) that is not related to the key generation time (figure 2, at the center). This could be related to some changes in the experimental apparatus that should be further investigated.
The QBER as a function of execution time also seems to follow a trend, but a precise analysis would require an estimate of the error in those values and more degrees of freedom (i.e. more realizations of the experiment).

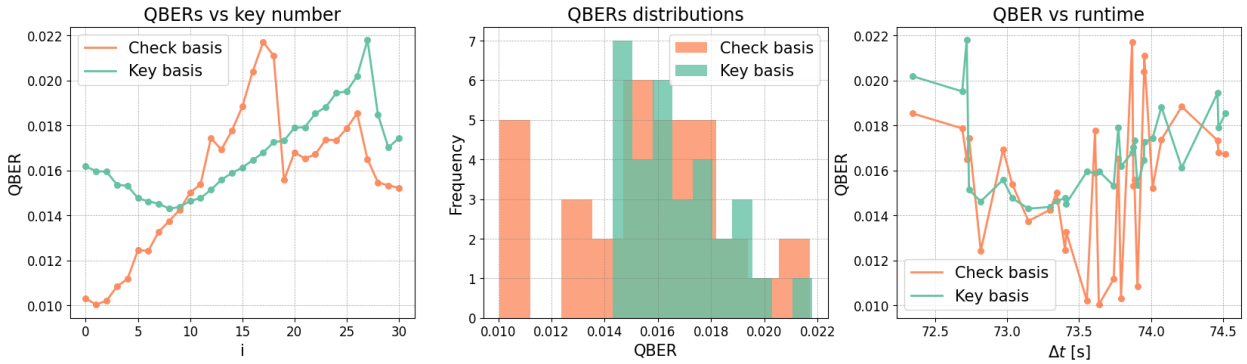

Figure 3. QBER analysis.

Finally, we can evaluate the SKR and plot it against both the key number and the execution time. Of course, the results are related to the one of the QBER analysis. The mean SKR is 0.086, while the standard deviation is 0.018.

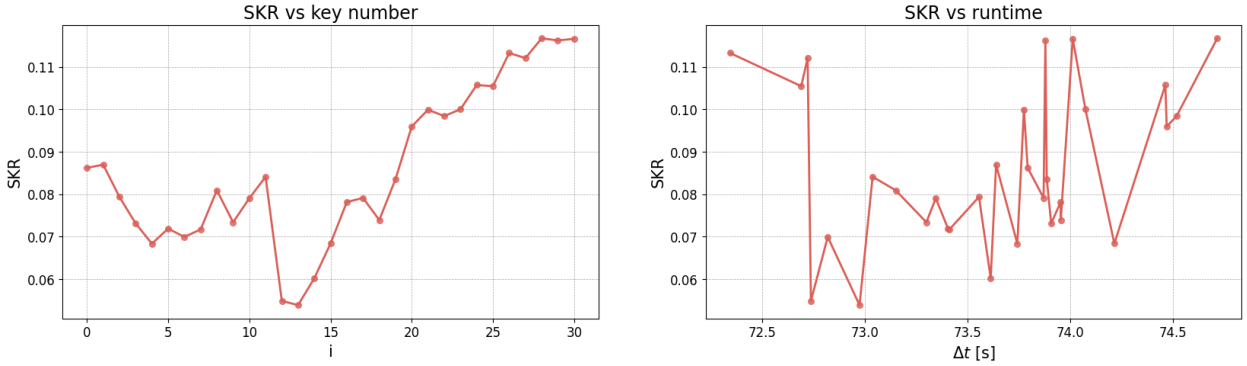

Figure 4. SKR analysis.

It is important to note that the estimate of $s^l_{Z,0}$ happens to be negative (un-physical). In such situation we fixed $s^l_{Z,0} = 0$. This seems to be related to the chosen block size, probably because the specific bounds proposed by Rusca et al. [3] were designed and tested for blocks of greater sizes.

4 Conclusions

In this report, we briefly introduced two problems of the practical implementation of the QKD protocols: the multi-photon events of the emitted laser pulses and the finite size of the obtained keys. We implemented a 3-states 1-decoy protocol to evaluate the secret key rate using realistic security parameters and a block length of 10^6 bits.
We noticed that the performance of the protocol seems to be correlated with the key number rather than the execution time as if the experimental setup changed over time.
On average, we obtain a SKR of 8.6%.

References

[1] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8, New York, 1984.

[2] AA Gaidash, VI Egorov, and AV Gleim. Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. In *Journal of Physics: Conference Series*, volume 735, page 012072. IOP Publishing, 2016.

[3] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden. Finite-key analysis for the 1-decoy state qkd protocol. *Applied Physics Letters*, 112(17), 2018.

[4] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Physical Review A*, 89(2):022307, 2014.

[5] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[6] Costantino Agnesi, Marco Avesani, Andrea Stanco, Paolo Villoresi, and Giuseppe Vallone. All-fiber self-compensating polarization encoder for quantum key distribution. *Optics letters*, 44(10):2398–2401, 2019.

[7] Marco Avesani, Luca Calderaro, Giulio Foletto, Costantino Agnesi, Francesco Picciariello, Francesco BL Santagiustina, Alessia Scriminich, Andrea Stanco, Francesco Vedovato, Mujtaba Zahidy, et al. Resource-effective quantum key distribution: a field trial in padua city center. *Optics letters*, 46(12):2848–2851, 2021.