optica

Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder: supplementary material

COSTANTINO AGNESI[1,2,†], MARCO AVESANI[1,†], LUCA CALDERARO[1,2,†], ANDREA STANCO[1], GIULIO FOLETTO[1], MUJTABA ZAHIDY[1], ALESSIA SCRIMINICH[1], FRANCESCO VEDOVATO[1,2], GIUSEPPE VALLONE[1,2,3], AND PAOLO VILLORESI[1,2,*]

[1] *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy*
[2] *Istituto Nazionale di Fisica Nucleare (INFN) – sezione di Padova, Italy*
[3] *Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, 35131 Padova, Italy*
[†] *These authors contributed equally to this work.*
[*] *Corresponding author: paolo.villoresi@dei.unipd.it*

Published 2 April 2020

This document provides supplementary information to "Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder," https://doi.org/10.1364/OPTICA.381013. It includes additional information on the Intensity Modulator used for decoy-state preparation. Furthermore, additional simulations of Finite-Key security analysis are included.

1. EXTENDED DATA ON THE INTENSITY MODULATION

In our source the SoC also sets the intensity level of each pulse by exploiting the intensity modulator (see Fig. 1 of the main text). The used protocol requires the preparation of two intensity levels, that we set to $\mu_1 \approx 0.8$ and $\mu_2 \approx 0.28$ photons per pulse. This modulation, like the polarization modulation, does not present any significant or detrimental temporal drift during the experimental QKD runs.

As an example, we show in Fig. S1 the trend of both the intensity levels as a function of the acquisition time (one second of integration for each point) for the first left-point of the data presented in Fig. 4 of the main text. The two intensity levels are distributed around the expected values, and the standard deviations of the two temporal series are $\sigma_{\mu_1} = 0.007$ and $\sigma_{\mu_2} = 0.004$ photons per pulse, which are comparable with the expected statistical fluctuations due to the Poissonian nature of the registered counts.

In Fig. S2 we show, for the same dataset, the plot of the ratio μ_1/μ_2 of the intensity levels and the relative histogram. The mean value of the ratio (represented by the dotted lines) is 2.858 ± 0.002, which is compatible with the expected value of $0.8/0.28 \approx 2.857$ and the standard deviation $\sigma_{\mu 1/\mu 2}$ is 0.032. The shaded area around the mean value of the ratio in the upper panel on the right represents the expected fluctuations (at 3σ) due to the Poissonian statistics of the registered counts.

The acquisition shown in Fig. S1 and Fig. S2 is representative of all the data appearing in Fig. 4 of the main text, for which the acquisitions lasted for a variable time (in order to achieve a sufficient statistics).

2. FINITE-KEY SIMULATIONS

In addition to the Secure Key Rate (SKR) analysis of the main text, which includes finite-key corrections for the four acquisitions with lower losses, we present here some simulations of the performance of the system for longer acquisition time. The input parameters of the model are the same that generate the solid lines in Fig. 4 of the main text, in particular, the security parameters for the secrecy analysis and for confirmation of correctness are respectively $\epsilon_{\text{sec}} = 10^{-10}$ and $\epsilon_{\text{conf}} = 10^{-15}$.

In the simulation of Fig. S3, we fix the duration of the acquisition to one of four different values (90 seconds, 10 minutes, 1 hour and 6 hours) and we compute the expected SKR including the finite-key corrections and for the range of channel losses that we sampled in the experiment.

We also calculate the size of the sifted key that would be attained in such conditions. We note that our system is stable for

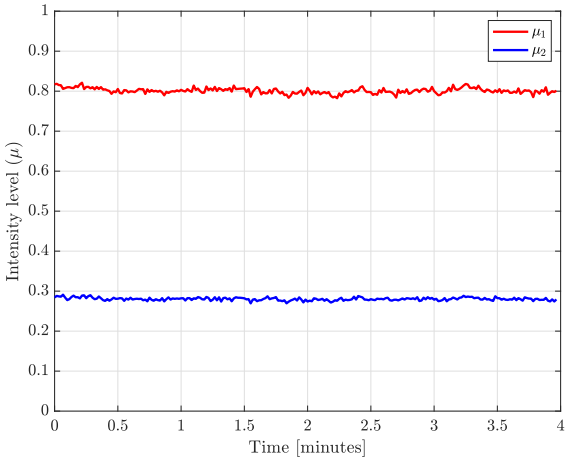

Fig. S1. Example of the intensity modulation obtained during a QKD run. Intensity levels as a function of time during the acquisition.

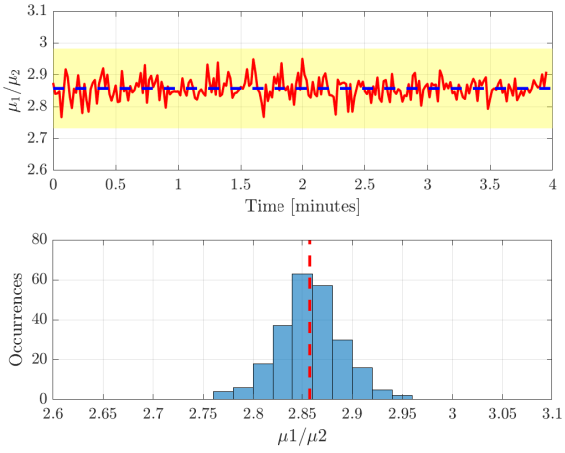

Fig. S2. Ratio μ_1/μ_2 as a function of time during acquisition and relative histogram. The dotted lines represent the mean value of the ratio, which is 2.858 ± 0.002. The shaded area in yellow represents the expected statistical fluctuations.

at least 6 hours, as shown by Fig. 3 of the main text. Therefore it can produce a secret key at about 38 dB of channel losses even including finite-key corrections (see red curve in Fig. S3).

In Fig. S4, we show simulations in which the size of the sifted key is fixed and time is a free parameter. If we target a sifted key size of $4.3 \cdot 10^7$ bits, the system is able to produce a secret key with 6 hours of operation at about 38 dB of channel losses (see red curve in Fig. S4).

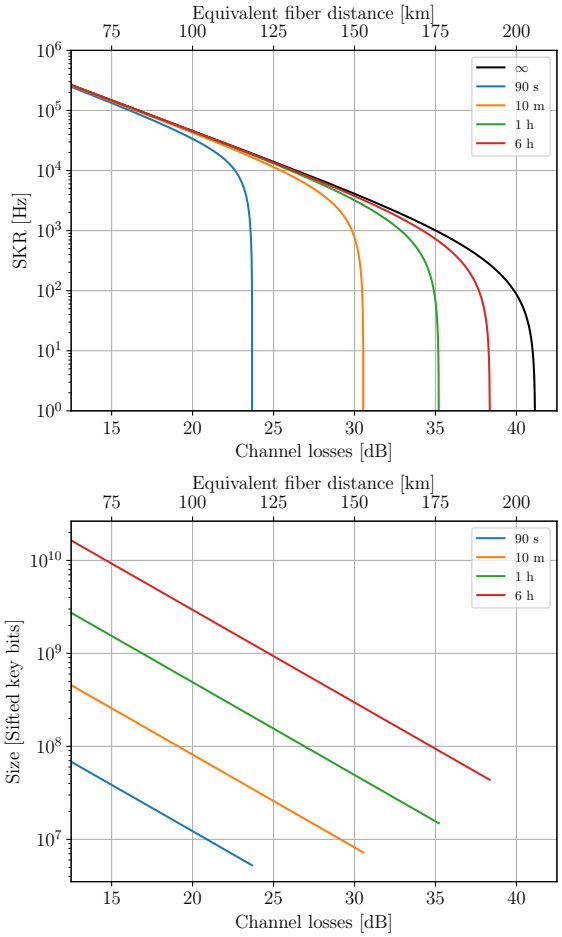

Fig. S3. Finite-key simulation using the same physical parameters of the experiment (Fig. 4 of the main text) but different acquisition time. (top) SKR as function of channel losses; the black curve shows the SKR in the asymptotic limit, the others include finite-key corrections. (bottom) Size of the attainable sifted key; only the points that can generate a secure key are shown. The conversion to equivalent fiber distance is based on SMF28 loss of 0.2 dB/km.

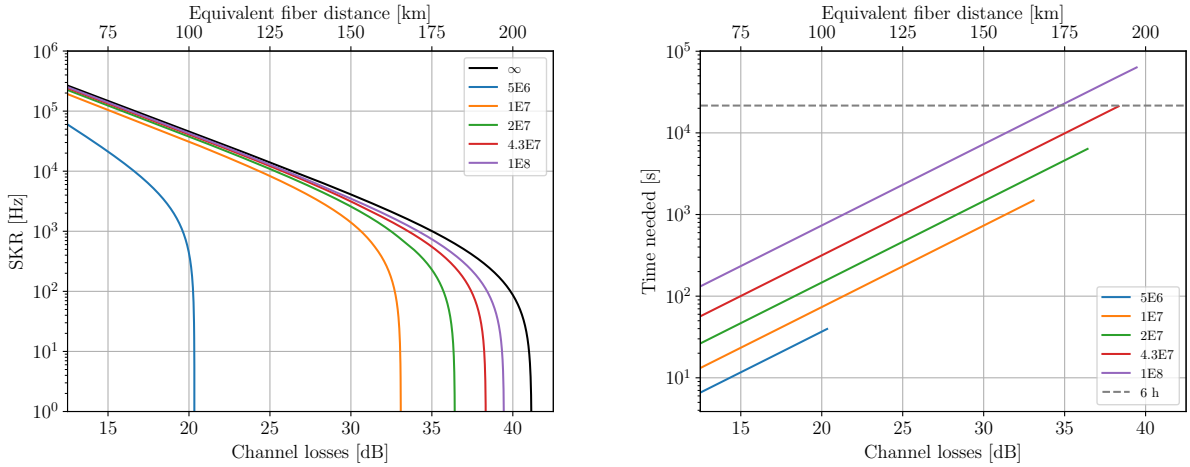

Fig. S4. Finite-key simulation using the same physical parameters of the experiment (Fig. 4 of the main text) but fixing the sifted key length. (left) SKR as function of channel losses; the black curve shows the SKR in the asymptotic limit, the others include finite-key corrections. (right) Time needed to produce the sifted key of required size; only the points that can generate a secure key are shown. The conversion to equivalent fiber distance is based on SMF28 loss of 0.2 dB/km.