Performance analysis of a low-cost, low-complexity, free-space QKD scheme based on the B92 protocol

Matteo Canale, Davide Bacco, Simon Calimani, Francesco Renna
Nicola Laurenti, Giuseppe Vallone, Paolo Villoresi
Department of Information Engineering, University of Padua, via G. Gradenigo, 6/b, 35131 Padova, Italy.
E-mail: {canalema, calimani, frarenna, nil, vallone, villoresi}@dei.unipd.it

We present the performance results of *QuAKE (Quantum Advanced Key Exchanger)*, a QKD scheme over a free-space quantum channel based on an implementation of the B92 protocol [1].

I. Quantum transmission and physical layer

A. Transmission protocol

The transmitter (Alice) uses two infrared (850 nm) attenuated diode lasers to send the bits 0 and 1, encoded in the vertical $|\updownarrow\rangle$ and $+45^\circ$ linear $|\swarrow\nearrow\rangle$ polarization of the photons, respectively. A 808 nm laser beam is also used along for synchronization. The receiver (Bob) uses a dichroic mirror (DM) to separate the information qubits from the synchronization signal: the latter is reflected and detected by an avalanche photodiode, whereas the qubits, trasmitted by the DM, impinge on a 50/50 beam splitter (BS). On either output of the BS, a polarizer and a single photon avalanche photodiode (SPAD) detect the -45° linear $\langle\nwarrow\searrow|$ or horizontal $\langle\leftrightarrow|$ polarization photons respectively. Each click of either SPAD corresponds to the reception of a sifted 0 or 1, respectively. The frequency of the bit trasmission is 2.5 MHz. Precisely, Alice repeatedly uses a 800ns slot to send two bits: in the first 200ns of the slot she sends the synchronization beam; after the synchro-laser, she waits 200ns and then sends the two bits separated by 200ns.

B. Channel losses

The measured sifted key rate results in $R_{\mathrm{sift}} = 23.8\,\mathrm{kb/s}$, which combined with the B92 protocol efficiency ($\eta = 1/4$) yields an estimated total loss along the source/channel/detector chain $\alpha = R_{\mathrm{sift}}/(\eta R_{\mathrm{raw}}) = 3.82 \cdot 10^{-2}$.

C. Attack model

We consider selective individual attacks, where Eve measures each photon independently with probability $0 < q < 1$, using either basis, ($\langle\leftrightarrow|, \langle\updownarrow|$) or ($\langle\swarrow|, \langle\nwarrow|$), randomly chosen. In the *intercept and resend (IS)* attack [2], each measured bit is resent with the same encoding as used by Alice, thus increasing the error rate at Bob. In the *unambiguous state discrimination (USD)* attack [3] only the 0's that are measured with the ($\langle\swarrow|, \langle\nwarrow|$) basis and the 1's that are measured with the ($\langle\leftrightarrow|, \langle\updownarrow|$) basis are retransmitted to Bob, thereby introducing further losses at the legitimate receiver.

II. Key processing over the public channel

A. Channel estimation

The channel losses and quantum bit error rate (QBER) are evaluated from the sifted key in each round of the key sharing protocol. The loss estimate is the ratio of sifted to raw bits, whereas the QBER is estimated by disclosing $N_{\mathrm{qber}} = 10^3$ bits of the sifted key, randomly chosen, over the public channel. The estimate variance allows to reliably detect combined eavesdropping attacks of the two types described in Section I-C whenever the eavesdropping probability for each photon is $q > 0.246$.

B. Key reconciliation

Key reconciliation is performed by means of the Winnow scheme [4], with parameters optimized according to the estimated QBER, so that a target reconciled bit error rate (BER) of 10^{-5} is attained with the least possible information revealed. As an example, for QBER $= 3\,\%$, we choose 4 iterations with increasing block sizes $8, 32, 128, 512$, respectively.

C. Privacy amplification

Privacy amplification is guaranteed by hashing with full rank Toeplitz random binary matrices [5], with size $N_{\mathrm{sec}} \times N_{\mathrm{sift}}$, where N_{sift} is the length of the reconciled key, and N_{sec} the length of the secure key. On making use of the upper bound provided in [6] and the binomial distribution of the bit sequence disclosed to the eavesdropper, the information leaked to Eve in each round can be bounded below 1 bit per each key round. We set $N_{\mathrm{sift}} - N_{\mathrm{rev}} - N_{\mathrm{sec}} = 90$ bit, where N_{rev} is the amount of information revealed in the discussion for reconciliation.

D. Authentication of the public channel

The discussion over the public channel is equipped with unconditionally secure authentication. The concatenation of all messages transmitted by a terminal in a protocol round is hashed by means of a keyed function to a 100 bit tag, which is then XORed with a *one time pad*. The hash function is chosen from the Stinson ε-almost strongly universal$_2$ class [7], with a 1255 bit key, and is renewed every 25 rounds. The hashing key and one time pad require 250 secure bits per round, that are taken from the previously generated keys, thus lowering the *net key rate*.

III. System performance and secure key rates

The measured key rates are summarized in the table below.

raw key rate	$R_{\mathrm{raw}} = 2.5\,\mathrm{Mb/s}$
average estimated loss	$\alpha = 3.82\,\%$
sifted key rate	$R_{\mathrm{sift}} = 23.8\,\mathrm{kb/s}$
average estimated QBER	$\varepsilon = 2.96\,\%$
undetected eavesdropping rate	$q \leq 0.246$
secure key rate	$R_{\mathrm{sec}} = 11.1\,\mathrm{kb/s}$
eavesdropping leakage rate	$R_{\mathrm{leak}} \leq 4.7\,\mathrm{b/s}$
net key rate	$R_{\mathrm{net}} = 9.94\,\mathrm{kb/s}$

References

[1] C. H. Bennett, *Phys. Rev. Lett.*, **68**, 3121 (1992)
[2] B. Huttner *et al.*, *Phys. Rev. A* **51**, 1863 (1995)
[3] M. Dušek *et al.*, *Phys. Rev. A* **62**, 022306 (2000)
[4] W. T. Buttler *et al.*, *Phys. Rev. A* **67**, 052303 (2003)
[5] C.-H. Fung *et al.*, *Phys. Rev. A* **81**, 012318 (2010)
[6] C. H. Bennett *et al.*, *IEEE Trans. Inf. Th.*, **41**, 1915 (1995)
[7] D. R. Stinson, *Designs, Codes and Cryptography* **4**, 369 (1994)