Scheme for practical server-client COW-QKD based on auto-compensated fiber interferometer

I. H. López Grande*[1] and M. A. Larotonda †[1]

[1]DEILAP, CITEDEF (Instituto de Investigaciones Científicas y Técnicas para la Defensa), Buenos Aires, Argentina

Massive and global implementation of QKD systems demands fast and simple schemes for secret key distribution. Protocols like COW-QKD [1] and DPSR-QKD [2] were proposed pursuing this aim. Server-client [3] schemes also fulfill another desirable property of practical QK, which is to hold large resources in a "server-side" while the "client" technical requirements are kept to the minimum.
We present an experimental proposal for COW-QKD scheme based on a plug & play setup and an auto-compensated fiber interferometer. The scheme is presented on a server-client fashion with all the delicate and expensive components in the server side (laser, detector and interferometer) while the client side comprises only an intensity modulator and a Faraday mirror. The scheme is intended to generate secure cryptographic key at high rates in a simple way. We explore two alternatives for the server's experimental setup; in one case using a Faraday-Michelson interferometer (FMI) configuration and in the other employing a Polarization-Beam-Splitter based Mach-Zehnder (MZI) interferometer. Each setup and its distinctive features are briefly described below and will be discussed in the presentation.

The proposed experimental setup implements the COW-QKD [1] protocol with time-bin encoding. It requires to prepare and measure two data states: $|0\rangle$ and $|1\rangle$ and a decoy state: $|+\rangle$, using the standard qubit notation. The two alternatives presented for the server scheme are shown in figure 1. In the Faraday-Michelson version, Bob emits intense laser pulses at a fixed rate R. The light source is a commercial $1550\,nm$ DFB pigtailed laser diode, externally modulated with an electro-absorbption modulator. At Bob's side the light pulses enter a path-unbalanced Faraday-Michelson interferometer via a circulator, thus creating a temporal pulse pattern. The temporal unbalance between fiber paths is chosen half the period $1/R$: this doubles the original pulse frequency at the FMI output. At Alice side she encodes the three states needed [shown at the bottom of figure 1.a)] to perform the protocol by selectively blocking the incoming pulses with an intensity modulator. At the end of the fiber a Faraday mirror reflects the pulses back to Bob while suppressing all birefringence effects. Finally using fixed attenuation Alice attains the optimal mean photon number per pulse required for the security of the protocol. Bob detects the states prepared by Alice in two bases. The data detection line (DL) consists in a single photon detection module (SPDM) detecting the arrival time of the incoming pulses which encode the states $|0\rangle$ an $|1\rangle$. For the monitoring line (ML) the pulses re-enter the FMI. There, half of the light of the decoy states interferes constructively and exit the beam splitter throughout the line connected to the circulator and is detected by a SPDM. If an eavesdropper intends to obtain information from the data basis states he or she will necessarily break the coherence of decoy pulses. The effect will be a decrease in the count rate of the monitoring line. At the monitoring detector, interference can be evaluated differently depending on the arrival time of the detected photons. On one side interference occurs between pulses that pass once through each of the arms of the FMI. This is "intra-bit" interference; in this case paths are automatically balanced and light exits through the desired output of the beam splitter if an untampered decoy pulse has been measured. In contrast, "across-the bit" interference, which arises from two consecutive laser pulses (one passing two times through the long path and the other going twice through the short one) will be recombined with an arbitrary phase depending on the path difference, hence requiring some kind of stabilization procedure to assure the correct measure of coherence between subsequent laser pulses. This is achieved by tuning the laser wavelength by slightly changing its pump current. The coherence between pulses is broken when sophisticated coherent attacks are performed over several pulses.

The second proposal for the server setup consists in an unbalanced Mach-Zehnder fiber interferometer composed by two PBS and polarization maintaining fibers [Fig. 1.b)]. The light pattern prepared by Bob at

*ignaciolopezgrande@gmail.com.ar
†mlarotonda@citedef.gob.ar

the output of the interferometer is in the state: $\frac{1}{\sqrt{2}}(|0H\rangle + |1V\rangle)$. The way Alice encodes quantum states and the detection in the data basis is the same as above (time-bin coding), however for the detection in the monitoring line Bob uses both outputs of a PBS. A 22.5° inline Faraday rotator adds the non-reciprocity between output and input of the server stage, necessary to obtain interference *intra* and *inter* bits. Decoy pulses passing one time through each MZI arm will exit the interferometer at a particular time and with polarization orthogonal to light interfering by passing two times by the same MZI arm (coherence "across-the-bit" separation). When coherence between interfering pulses is broken the photon rate of the polarizations measured in the monitoring line will differ from the expected.

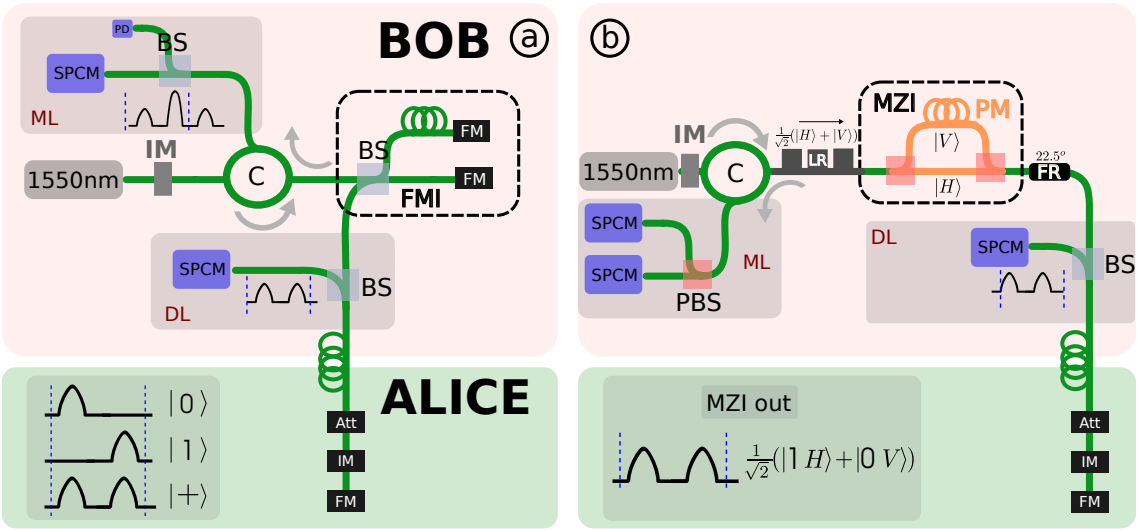

Figure 1: *The two alternatives for autocompensated COW-QKD are shown. a) The Michelson-Faraday version. b) The polarizing beam-splitter Mach-Zehnder interferometer based version. ML (monitoring Line),DL (detection line),FMI (Faraday mirror interferometer),MZI (Mach-Zehnder interferometer),FR (Faraday Rotator),FM (Faraday mirror),IM (intensity modulator).*

References

[1] Damien Stucki, Claudio Barreiro, Sylvain Fasel, Jean-Daniel Gautier, Olivier Gay, Nicolas Gisin, Rob Thew, Yann Thoma, Patrick Trinkler, Fabien Vannel, Hugo Zbinden,**"High speed coherent one-way quantum key distribution prototype"**, *Optics Express,* ***17****, p. 13326 (2009)*,

[2] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto, **"Differential Phase Shift Quantum Key Distribution"**. *Phys. Rev. Lett.* ***89****, 037902 (2002)*

[3] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R.W. Nock, J. Munns, D. Bonneau, P. Jiang, H.W. Li, A. Laing, J.G. Rarity, A.O. Niskanen, M.G. Thompson, and J.L. O'Brien, **"Reference-Frame-Independent Quantum-Key-Distribution Server with a Telecom Tether for an On-Chip Client"**. *Phys. Rev. Lett.* ***112****, 130501 (2014)*,