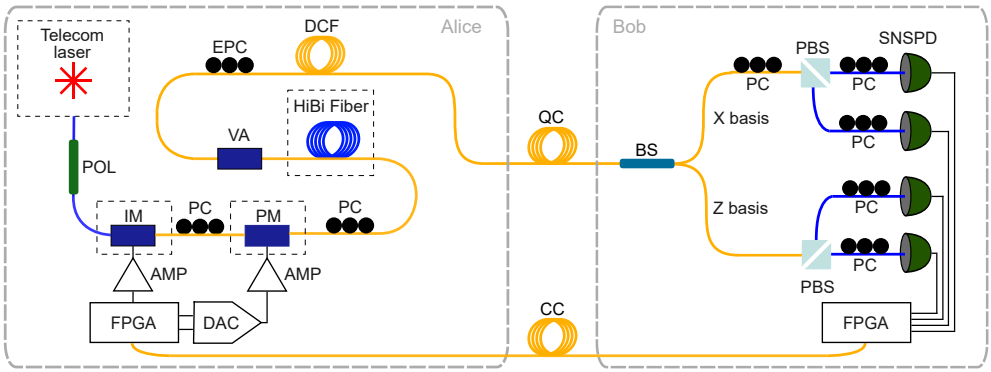
Performance and security of 5 GHz repetition rate polarization-based Quantum Key Distribution

F. Grünenfelder, A. Boaron, D. Rusca, A. Martin and H. Zbinden
Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland
arXiv:2007.15447 (2020)

ABSTRACT

We implement 5 GHz clocked polarization-based simplified BB84 protocol. Secret keys can be distributed over 151.5 km of standard telecom fiber at a rate of 54.5 kbps. The high clock frequency might give rise to correlations between the pulses. We characterize the correlations in decoy intensity, polarization and in the phase between the pulses and discuss their impact on the security of the protocol.

IMPLEMENTATION



Alice uses a phase modulator (PM) together with highly birefringent fiber (HiBi Fiber) to prepare the three polarization states of the simplified BB84 protocol [1].

An intensity modulator (IM) is employed to prepare the decoy states. We use an electronic polarization controller (EPC) to compensate for polarization drift in the quantum channel (QC).

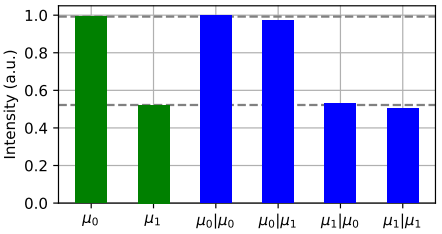
Bob uses in-house made superconducting nanowire single-photon detectors (SNSPDs) to distinguish the polarization states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$.

SECRET KEY RATE

Fiber length (km)	Attenuation (dB)	Sifted key rate (kbps)	ϕ_Z (%)	Q_Z (%)	SKR (kbps)
101.0	20.2	2320.2	3.67	1.93	392.7
151.5	30.3	330.0	3.50	1.88	54.5

Measured secret key rate (SKR) and corresponding experimental parameters. The quantum channel consists of standard single-mode fiber. The parameter ϕ_Z is the phase error rate and Q_Z is the QBER Z. The given rates are averages over ten privacy amplification blocks.

CORRELATION IN THE DECOY STATES



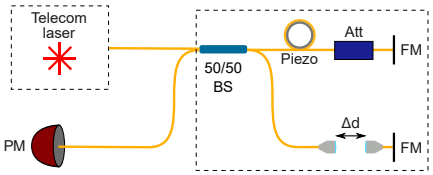
In our implementation, we use the one-decoy protocol in the finite key regime [2]. We measured the mean intensity of the signal state (μ_0) and of the decoy state (μ_1) at Alice's output. We determined the mean intensity of the signal and decoy states as a function of the previous state. The intensity varies up to 3% depending on which state was sent before.

DEGREE OF PHASE CORRELATION

Phase randomization between pulses is a neccessity for the decoy method [2]. The probability of creating a pulse with the same phase as its predecessor is bounded by

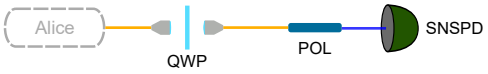
$$p_c^* = \max_{\Delta d} \frac{V_{\text{pulsed}}(\Delta d)}{V_{\text{CW}}(\Delta d)} = 0.0019,$$

where V_{pulsed} is the visibility in gain-switched mode and V_{CW} is the visibility in continous wave mode.



Setup to measure degree of phase correlation.

CORRELATION IN THE POLARIZATION STATES

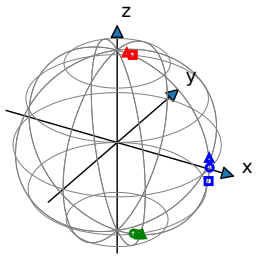


Setup to measure the polarization correlation:
A rotatable quarter-wave pate together with a polarizer is used to determine the polarization [3].

In an ideal implementation, Alice would prepare the states $|0\rangle$ and $|1\rangle$ in the Z basis and $|+\rangle$ in the X basis. In a real implementation she prepares states of the form

$$|\psi_{j|k}\rangle = \cos\frac{\theta_{j|k}}{2}|0\rangle + \sin\frac{\theta_{j|k}}{2}|1\rangle.$$

We measured the angles $\theta_{j|k}$. The state $|\psi_{0|k}\rangle$ is marked in red, $|\psi_{1|k}\rangle$ in green and $|\psi_{+|k}\rangle$ in blue. The index k is the value of the previous state. The triangles mark states where $k = 0$, the squares mark states where $k = 1$ and the circles mark states where $k = +$.



Measured polarization states.

CONCLUSION

- We realized a 5 GHz clocked BB84 implementation and reached a SKR of 54.5 kbps at 150 km of standard single mode fiber.
- We characterized the relevant parameters connected to potential security loopholes.
- Further research has to be done on the impact of the three types of correlation in terms of security.

REFERENCES

[1] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Physical Review A 90 (2014), 10.1103/physreva.90.052314
[2] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, Applied Physics Letters 112, 171104 (2018).
[3] B. Schaefer, E. Collett, R. Smyth, D. Barrett, and B. Fraher, American Journal of Physics 75, 163 (2007)

Contact : fadri.gruenenfelder@unige.ch

QSIT Quantum Science and Technology
National Centre of Competence in Research
UNIVERSITÉ DE GENÈVE