Experimental Realization of a Quantum Zero-Knowledge Proof

Marta Irene Garcia Cid
Dileepsai Bodanapu, Alberto Gatto, Paolo Martelli, Vicente Martin and Laura Ortiz

Indra Sistemas S.A., 28108, Madrid, Spain
Universidad Politecnica de Madrid, 28660, Madrid, Spain
Cohaerentia S.r.l, 20133, Milano, Italy
Politecnico di Milano, 20133, Milano, Italy

migarcia@indra.es

An interactive quantum zero-knowledge protocol [1] is proposed and demonstrated in modified Quantum Key Distribution devices [2][3] executing two fundamental cases between a verifier and a prover who pre-share a secret. In the first case, all players are honest, while in the second case, one of the users is a malicious player. The acceptance or rejection of the proof is determined by the Quantum Bit Error Rate (QBER) where an increase around 25% is demonstrated in the second case over the case of honesty. Additional proofs have also been carried out for distances up to 60 km between verifier and prover. The security and robustness of the protocol has been analysed, demonstrating its completeness, soundness and zero-knowledge properties.

References

[1] S. Goldwasser, S. Micali and C. Rackoff. The knowledge complexity of interactive proof-systems, ACM, 2019
[2] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing, TCS (1), 7-11, 2014
[3] A. Gatto et al. A BB84 QKD field-trial in the Turin metropolitan area, PSC Conference, Vol. 2 OSA Technical Digest (OPG, 2021), paper Tu1A.

Figures

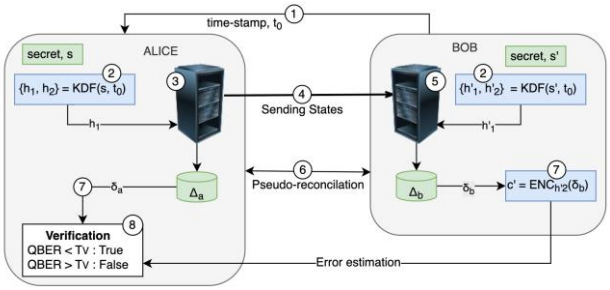

Figure 1: Quantum Zero Knowledge Protocol

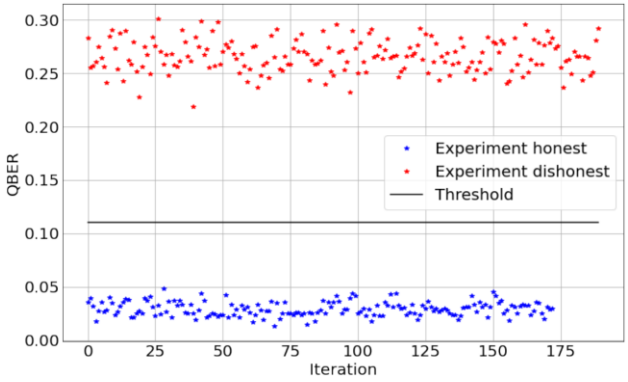

Figure 2: QBER Comparison between honest and dishonest cases

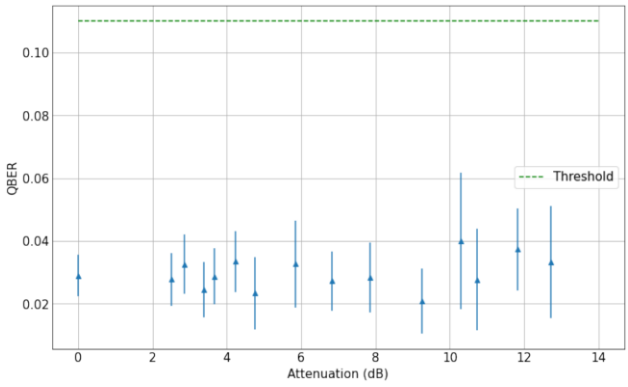

Figure 3: QBER versus link losses in the honest case