Quantum cloning attack on equiangular spherical code QKD protocols

Karol Bartkiewicz[1], Karel Lemr[2], Antonín Černoch[3], Jan Soubusta[3], and Adam Miranowicz [1]

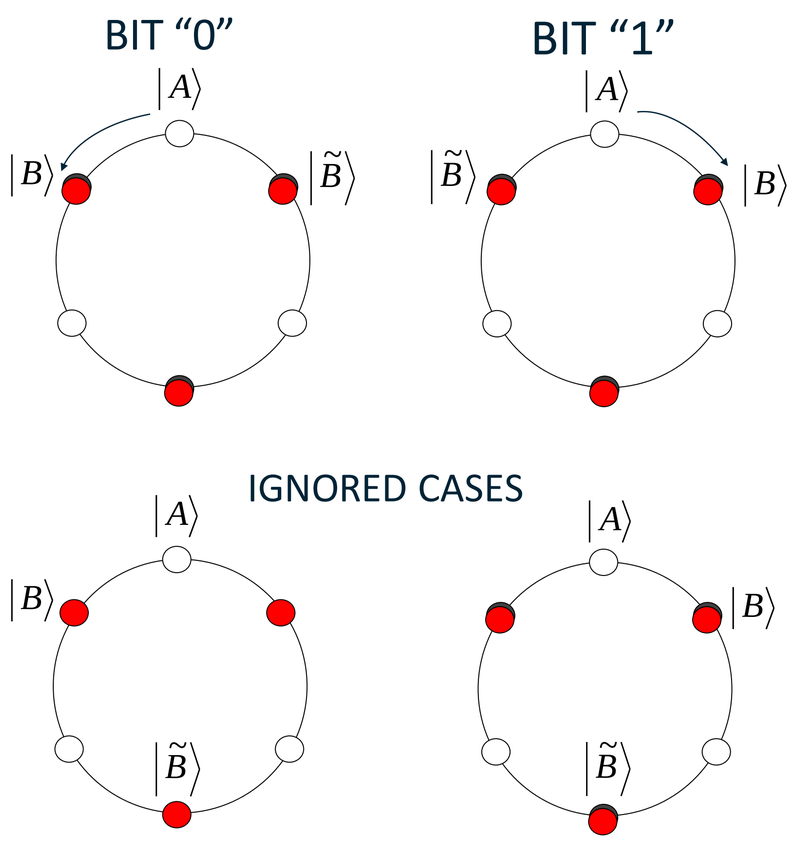
[1] Faculty of Physics, Adam Mickiewicz University, PL-61-614 Poznań, Poland
[2] RCPTM, Joint Laboratory of Optics of Palacky University and Institute of Physics of Academy of Sciences of the Czech Republic, Faculty of Science, Palacky University 17. listopadu 12, 771 46 Olomouc, Czech Republic
[3] Institute of Physics of Academy of Science of the Czech Republic, Joint Laboratory of Optics of PU and IP AS CR, 17. listopadu 12, 77207 Olomouc, Czech Republic

Abstract

We proposed a quantum cloning attack on the equiangular spherical code quantum key distribution (QKD) of Renes [1] and performed an experimental simulation of such attack. The spherical code QKD protocols provide improved tolerance of eavesdropping in comparison to their unbiased basis counterparts. We showed on the example of a trine-state variant of the QKD protocol (counterpart of the BB84 protocol [2] wchich was also attacked by us in a smilar way) that a cloning attack followed by a state estimation [3] procedure is a feasible eavesdropping strategy while assuming not exceptionally low losses (including the key bit error rates), which is the case for experimentally-feasible QKD networks (see [4]).

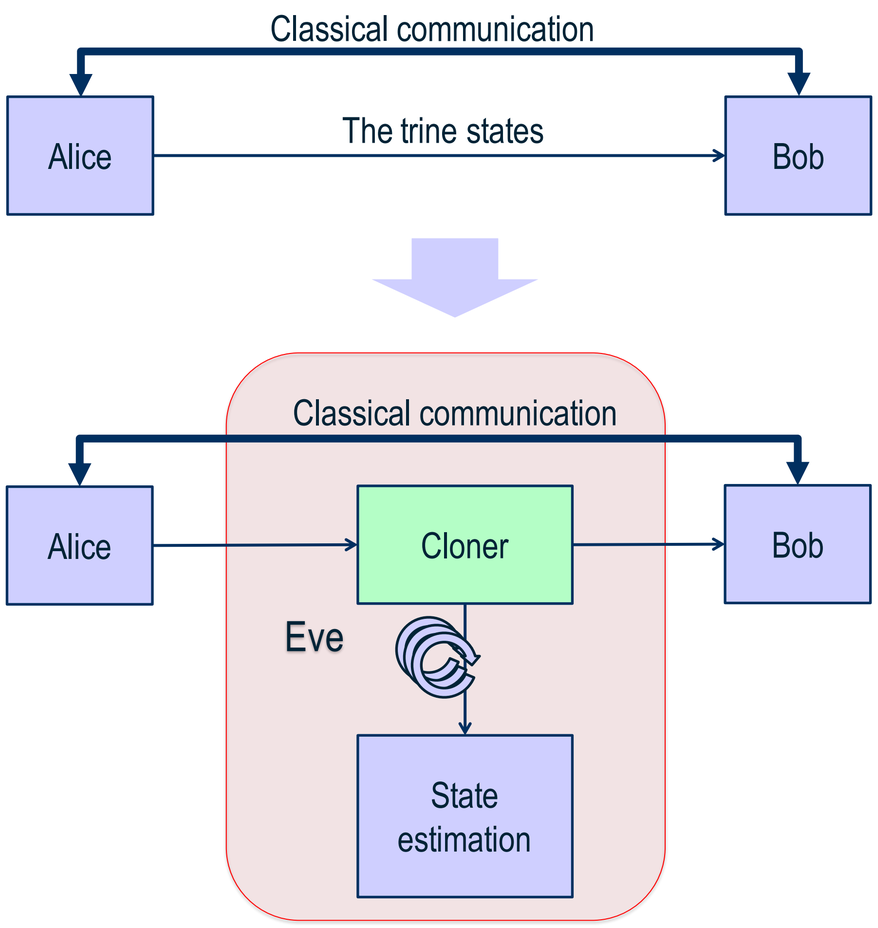
Our tunable optimal cloner prepares two asymmetric copies of a polarization-encoded trine state qubit for a fixed ratio of single-copy fidelities. In some cases the cloner provides two copies with the highest possible sum of single-copy fidelities.

Equiangular spherical code for equatorial qubits



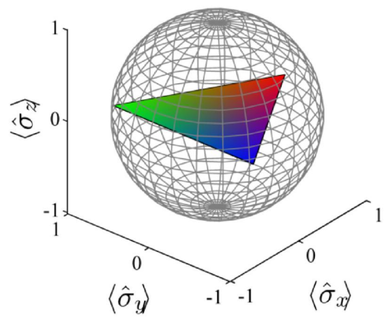
This protocol, as proposed by Renes [1], can be simply explained on the example of trine states on Bloch's sphere. Alice and Bob publicly agree beforehand to send one of the trine states marked by empty and solid dots, respectively. They also agree that the clockwise (anticlockwise) sequence of their states corresponds, e.g., to bit 1 (0). Bob publicly informs Alice what he has **not** measured. Alice ignores the inconclusive cases (and informs Bob about them). In the other two cases, Alice and Bob can calculate the same bit value.

Eavesdropping



Eve (the eavesdropper) first clones the qubit sent by Alice, then listens to the announcements made by Alice and Bob. Finally, she performs state estimation procedure on her clone.

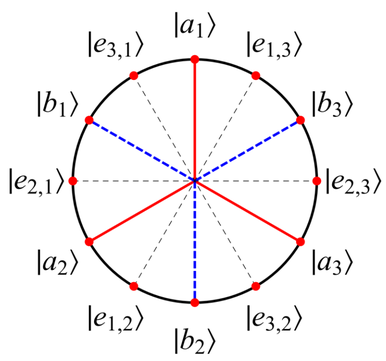
Optimal asymmetric 1 to 2 cloner



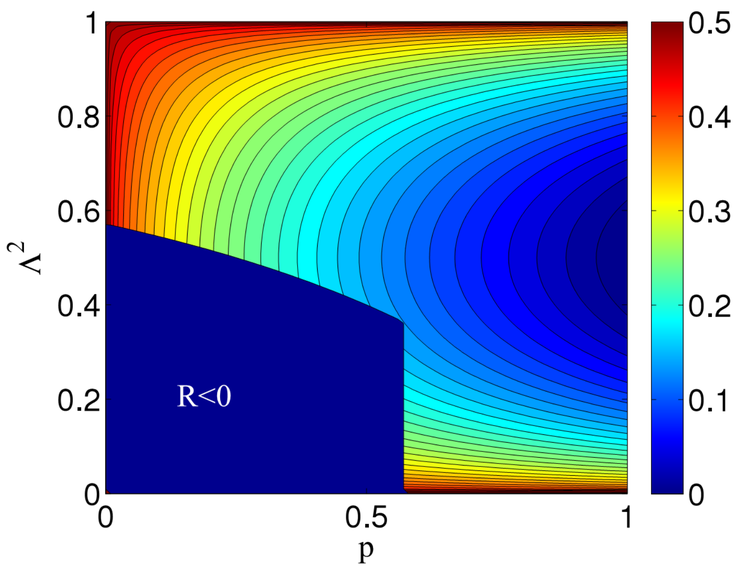
In the experiment we used the multipurpose cloning machine described in Ref. [5] set to clone the trine states (or the four BB84 states) in an optimal way (from Eave's point of view) for a fixed single-copy fidelity ratio (Eve's fidelity to Bobs fidelity, F_E/F_B).

State estimation procedure

Depending on the messages exchanged between Alice and Bob, Eve performs Helstrom measurement (see Ref. [3]) to check what state was sent by Alice. Then she makes the best guess about the bit value that is to be shared by Alice and Bob.



Security vs cloning attack



The fidelity of Bob's and Eve's clones is given as

$$F_B = \frac{1}{2}\left(1+\Lambda\sqrt{p\left(1-\Lambda^2\right)}\right),$$

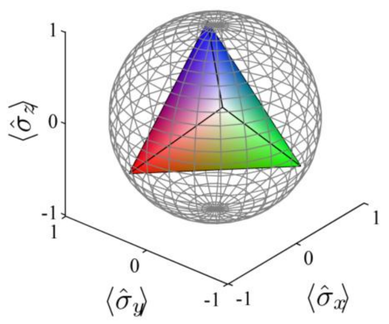
$$F_E = \frac{1}{2}\left(1+\Lambda\sqrt{(1-p)\left(1-\Lambda^2\right)}\right).$$

The figure on the left presents the results of our numerical simulations, i.e, bit error rate in sifted key achieved by Alice and Bob while being attacked by Eve. The attack is successful for secret key rate R<0 (the blue area).

- We performed the best cloning attack (for bitt error rate 13.65%) with success rate about 20%.
- The protocol was considered secure for error rate < 16.6% for the class of attacks descrbed in [1]).

Conclusions

The experimental results imply that cloning based eavesdropping could be feasible in the future. By using our quantum cloner followed by state estimation (based on publicly available information) Eve is able to eavesdrop as long as Alice and Bob accept 7dB losses and 13.65% bit error rate which is lower than the security bound given in [1] (for BB84 we get error rate of 14.9%). Moreover, our approach can be extended to the tetrahedron version of the spherical code QKD protocol (or the six-state protocol).



Acknowledgements

Czech Ministry of Education OPVK project CZ.1.07/2.3.00/20.0017, CZ.1.07/2.3.00/20.0058, Palacky Univ. IGA project PrF-2012-003 and Czech Acad. of Sciences project AVOZ10100522. Polish Ministry of Science and Higher Education under Grants No. 2619/B/H03/2010/38 and 3271/B/H03/2011/40.

References

[1] J. M. Renes, Phys. Rev. A **70**, 052314 (2004).
[2] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York, 1984), p. 175.
[3] A. Chefles, Contemp. Phys. **41**, 401 (2000); arXiv:quant-ph/0010114 (2000).
[4] T. Chen, J. Wang, H. Liang, W. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W. Cai, L. Ju, L. Chen, L. Wang, Y. Gao, K. Chen, C. Peng, Z. Chen, and J. Pan, Opt. Express **18**, 27217-27225 (2010).
[5] K. Lemr, K. Bartkiewicz, A. Cernoch, J. Soubusta, and A. Miranowicz, arXiv:1201.6234v1 [quant-ph] (2012).