# Quantum key distribution as a quantum machine learning task

**Marcelin Gallezot**
Thomas Decker, Sven F. Kerstan, Alessio Paesano, Anke Ginter, Wadim Wormsbecher

*JoS Quantum GmbH, c/o Techquartier, Platz der Einheit 2, 60327 Frankfurt am Main, Germany*

marcelin.gallezot@jos-quantum.de

We propose considering Quantum Key Distribution (QKD) protocols as a use case for Quantum Machine Learning (QML) algorithms. We define and investigate the QML task of optimizing eavesdropping attacks on the quantum circuit implementation of the BB84 protocol. QKD protocols are well understood, and solid security proofs exist enabling an easy evaluation of the QML model performance. The power of easy-to-implement QML techniques is shown by finding the explicit circuit for optimal individual attacks in a noise-free setting. For the noisy setting we find, to the best of our knowledge, a new cloning algorithm, which can outperform known cloning methods. Finally, we present a QML construction of a collective attack by using classical information from QKD post-processing within the QML algorithm.

## References

[1] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. LLoyd, Quantum machine learning, Nature 549, 195 (2017).

[2] C. H. Bennett, G. Brassard, Proceedings of the ieee international conference on computers, systems and signal processing (1984).

[3] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, Quantum circuit learning, Physical Review A 98 (2018)

## Figures

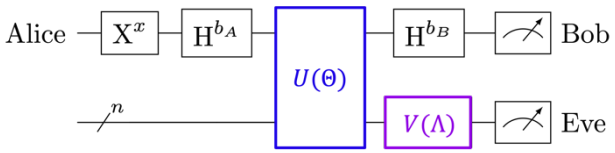


**Figure 1:** Quantum circuit representation of the BB84 protocol. The communication channel is represented by a qubit with Alice and Bob at each side. Eve has access to an ancillary system and can interact with the line.

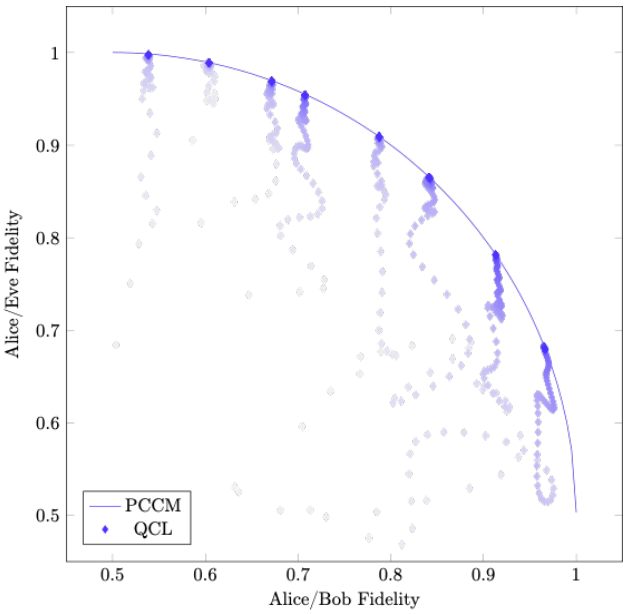


**Figure 2:** Comparison of the PCCM with the results of QCL. We conducted eight QCL training rounds with different parameters. Optimization results are marked by diamonds, colored according to the training step