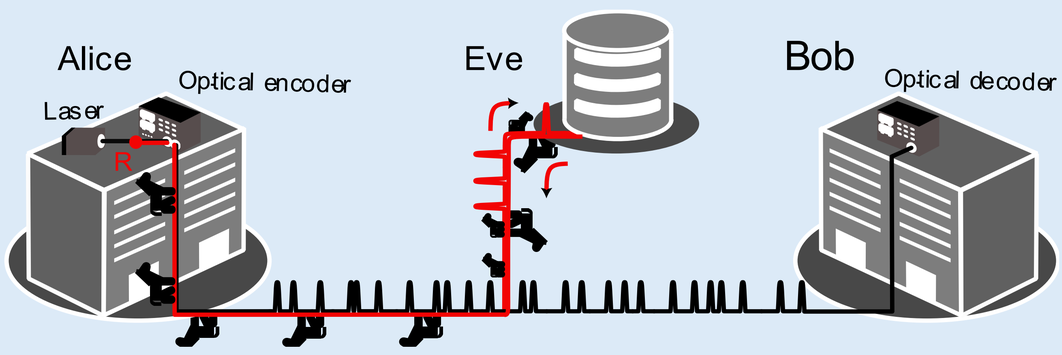
Postprocessing of Trojan-Horse Back-Reflections in High-Dimensional Time-Bin QKD

Beatriz Lopes da Costa[1,2,3,4], Christopher Spiess[1], Karolina Dziwulska[1], Karin Burger[1], Carlos Andres Melo Luna[1], and Fabian Steinlechner[1,5]

[1]Fraunhofer Institute for Applied Optics and Precision Engineering, Albert-Einstein-Strasse 7, 07745 Jena, Germany
[2]Instituto Superior Técnico, Universidade de Lisboa
[3]Physics of Information and Quantum Technologies Group, Centro de Física e Engenharia de Materiais Avançados (CeFEMA)
[4]PQI – Portuguese Quantum Insitute
[5]Friedrich Schiller University Jena, Abbe Center of Photonics, Albert-Einstein-Strasse 7, 07745 Jena, Germany

Introduction

- Quantum key distribution (QKD) enables the establishment of shared secret keys between distant parties by leveraging fundamental principles of quantum mechanics [1].
- In Trojan-horse attacks Eve injects bright light into the quantum channel and takes advantage of unwanted reflections within the QKD transceiver. [2,3]

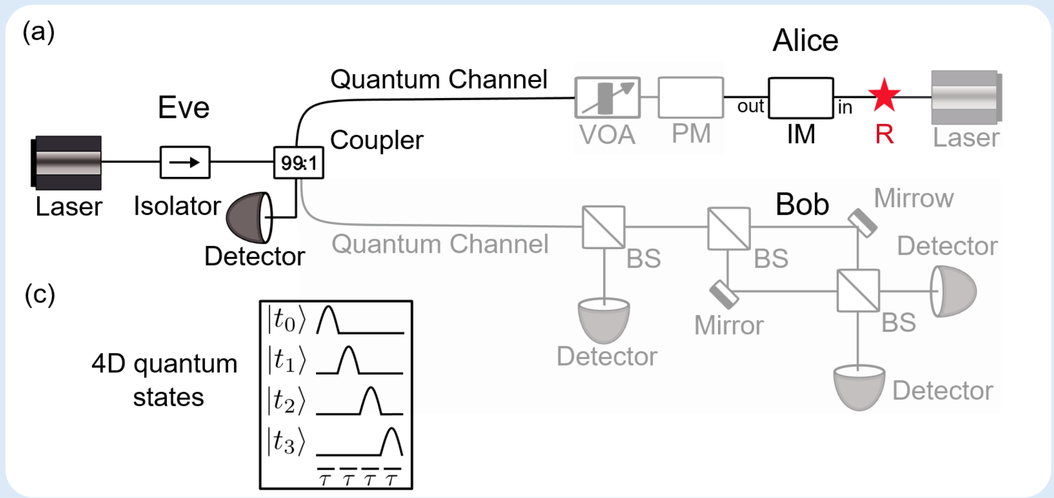


Implementation

- Reflection points located between the laser and the intensity modulator (IM).
- The reflection point's position determines the times at which the probe light returns to the IM for the second time.
- We define the normalized round-trip time

$$\nu = \frac{2Ln}{c\tau},$$

that quantifies the time that the probe-light takes between its two passes through the IM, in bin-width units τ .



- Three distinct classes of back-reflections:

1. Probe light that arrives at the IM outside its transmission window on both passes.
2. Probe light that arrives at the IM inside its transmission window on one pass.
3. Probe light that arrives at the IM inside its transmission window on both passes.

Post-processing

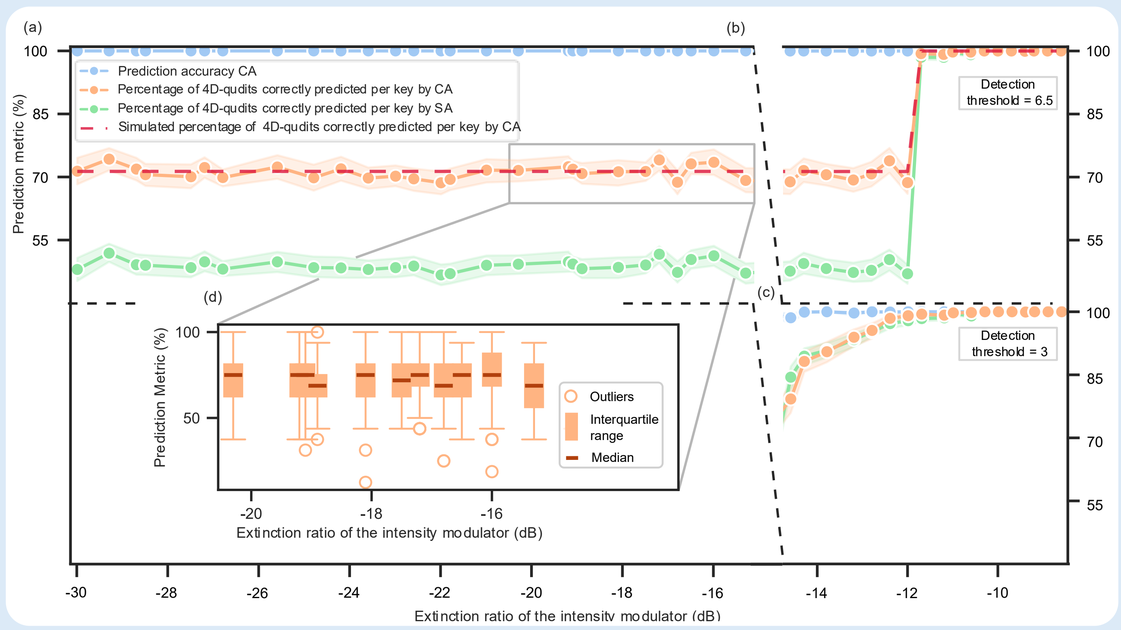
- We developed two processing algorithm:
  - Single-cycle algorithm (SA);
  - Correlation-assisted algorithm (CA).
- We analyze their performance using the Prediction Ratio (PR) and the Prediction Accuracy (PA).

$$\mathrm{PR}(\%) = \frac{\text{Number of qudits correctly predicted}}{\text{Number of qudits sent}}$$

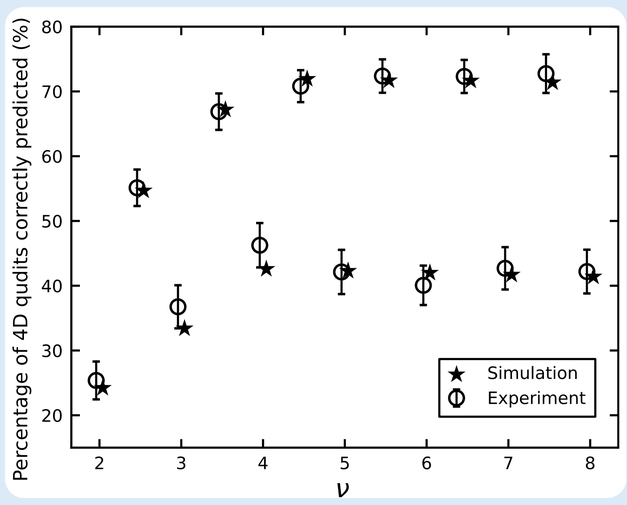
$$\mathrm{PA}(\%) = \frac{\text{Number of qudits correctly predicted}}{\text{Number of qudits predicted}}$$

Results

Fixed $\nu = 8.5$, different extinction ratios (ERs)

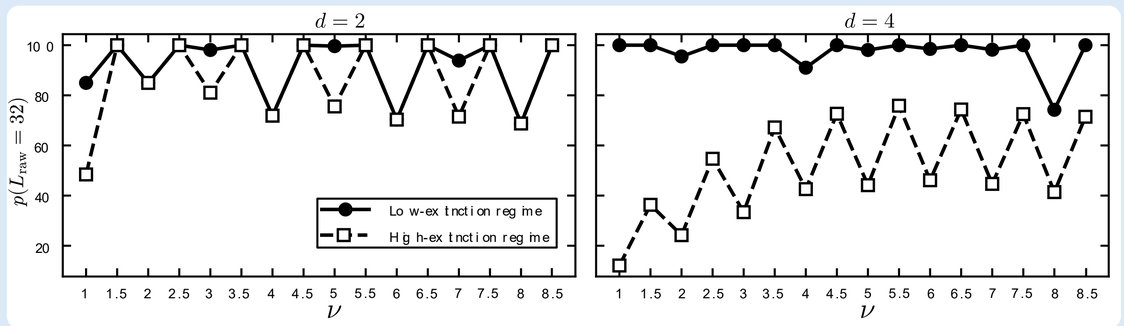


Different ν's, fixed extinction ratio (ER)



- The CA benefits significantly from exploiting correlations in the probe signal
- Experimental results agree well with the simulation
- ν has a significant impact on Eve's ability to guess the qudit sequence

Generalization to other dimensions



- The fraction of correctly recovered bits per sifted key is lower for d = 4 than for d = 2 in the high-extinction regime.

Conclusions

- We have provided an open-access simulator that accounts the hardware-specific parameters to allow for system-specific security analyses against this type of attack.
- The results found here add another countermeasure that can be deployed by Alice for time-bin QKD: the choice of the normalized round-trip time and the dimensionality of the time-bins.
- The prediction accuracy of Z-basis states increases when X-basis states are included.

References & Acknowledgments

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science 560, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quan-tum cryptography, Rev. Mod. Phys. 74, 145 (2002).
[3] A. Vakhitov, V. Makarov, and D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdroppingin quantum cryptography, Journal of Modern Optics 48,2023 (2001).
[4] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Invisibletrojan-horse attack, Scientific reports 7, 8403 (2017).

This research was funded by the BMFTR-project O-PEN (FKZ: 16KIS2015). The author B.C. gratefully acknowledges the financial support from Fundação para a Ciência e Tecnologia (FCT, Portugal), through doctoral grant 2024.06303.BDANA and project UIDB/04540/2020 contract LA/P/0095/2020.