

Dephasing assisted quantum key distribution

Daniel R. Sabogal^{1 *}, Daniel F. Urrego², Juan Rafael Álvarez³,
Juan P. Torres^{2,4}, Alejandra Valencia¹

¹ Laboratorio de Óptica cuántica, Univ. de Los Andes, 4976 Bogotá, Colombia.

² ICFO – Institut de Ciències Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain.

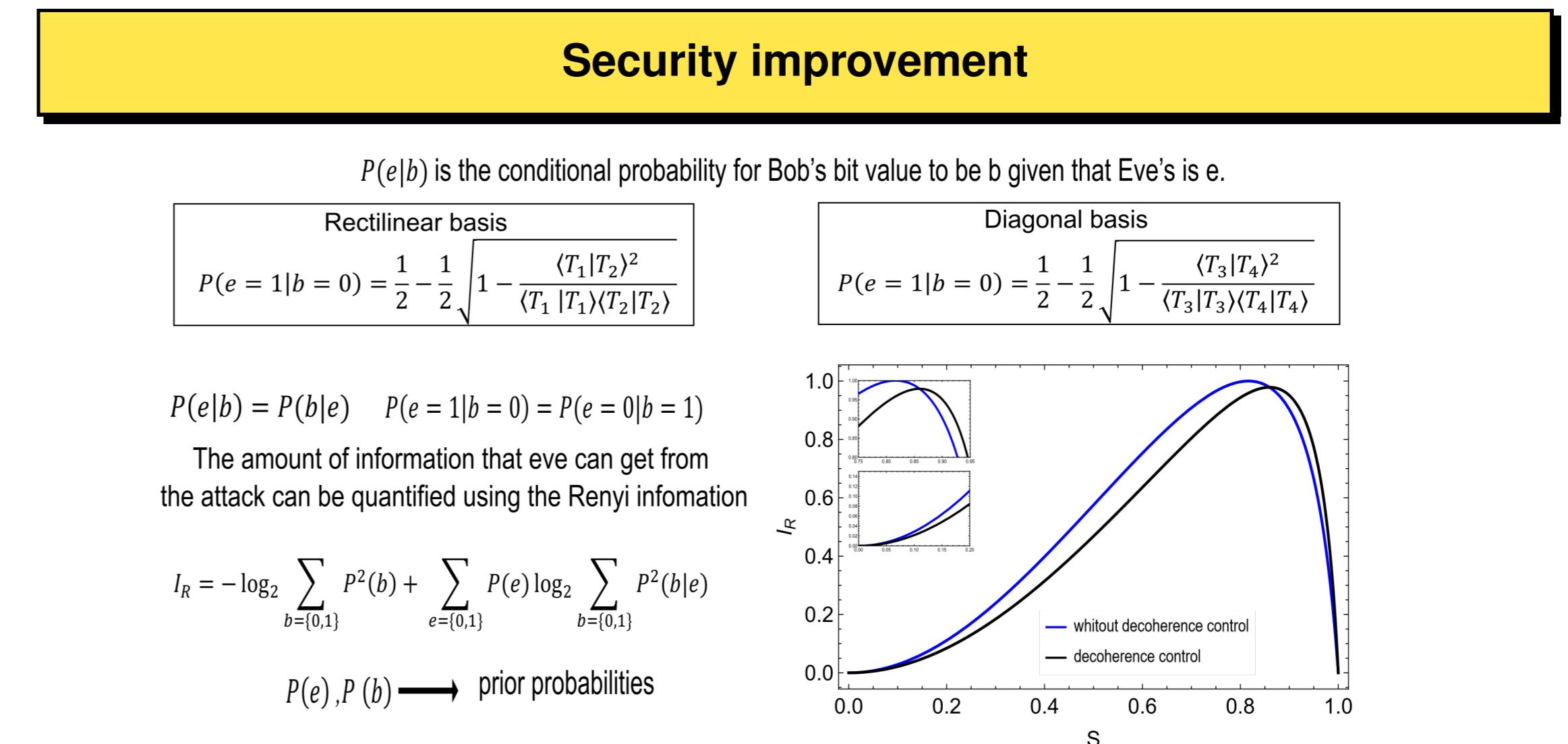
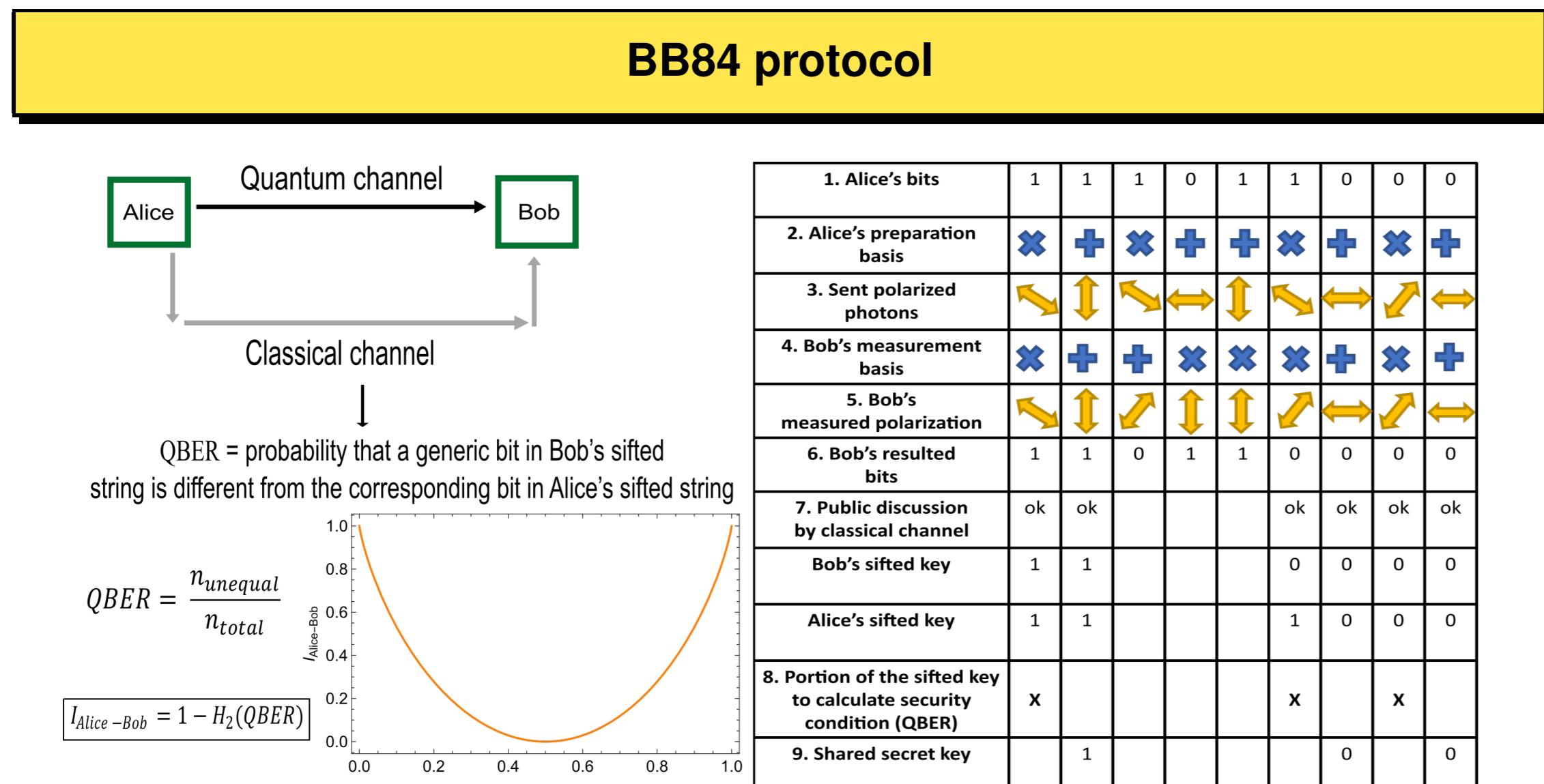
³ Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom

⁴ Department of Signal Theory and Communications, Universitat Politècnica de Catalunya, Barcelona, Spain.

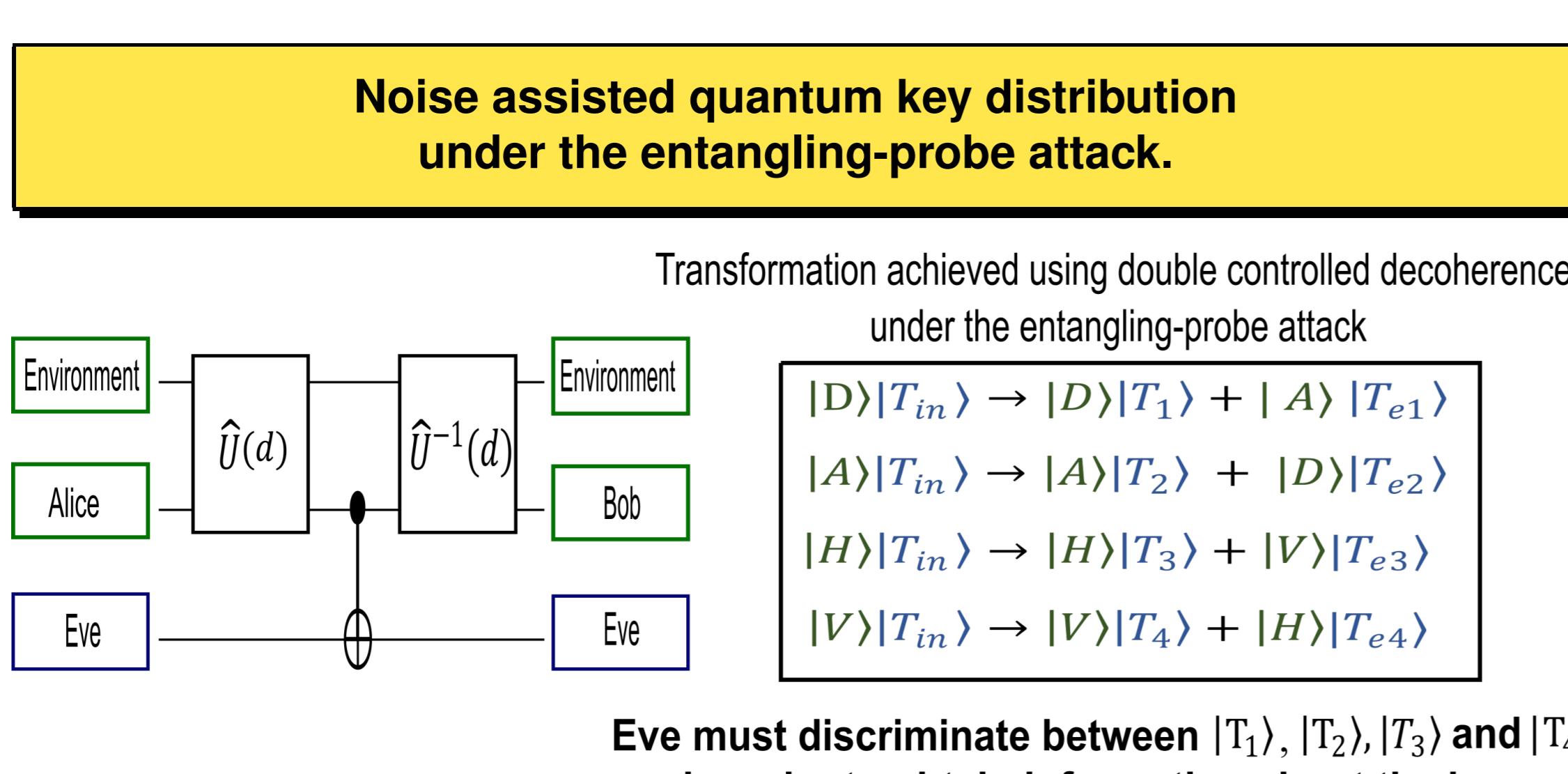
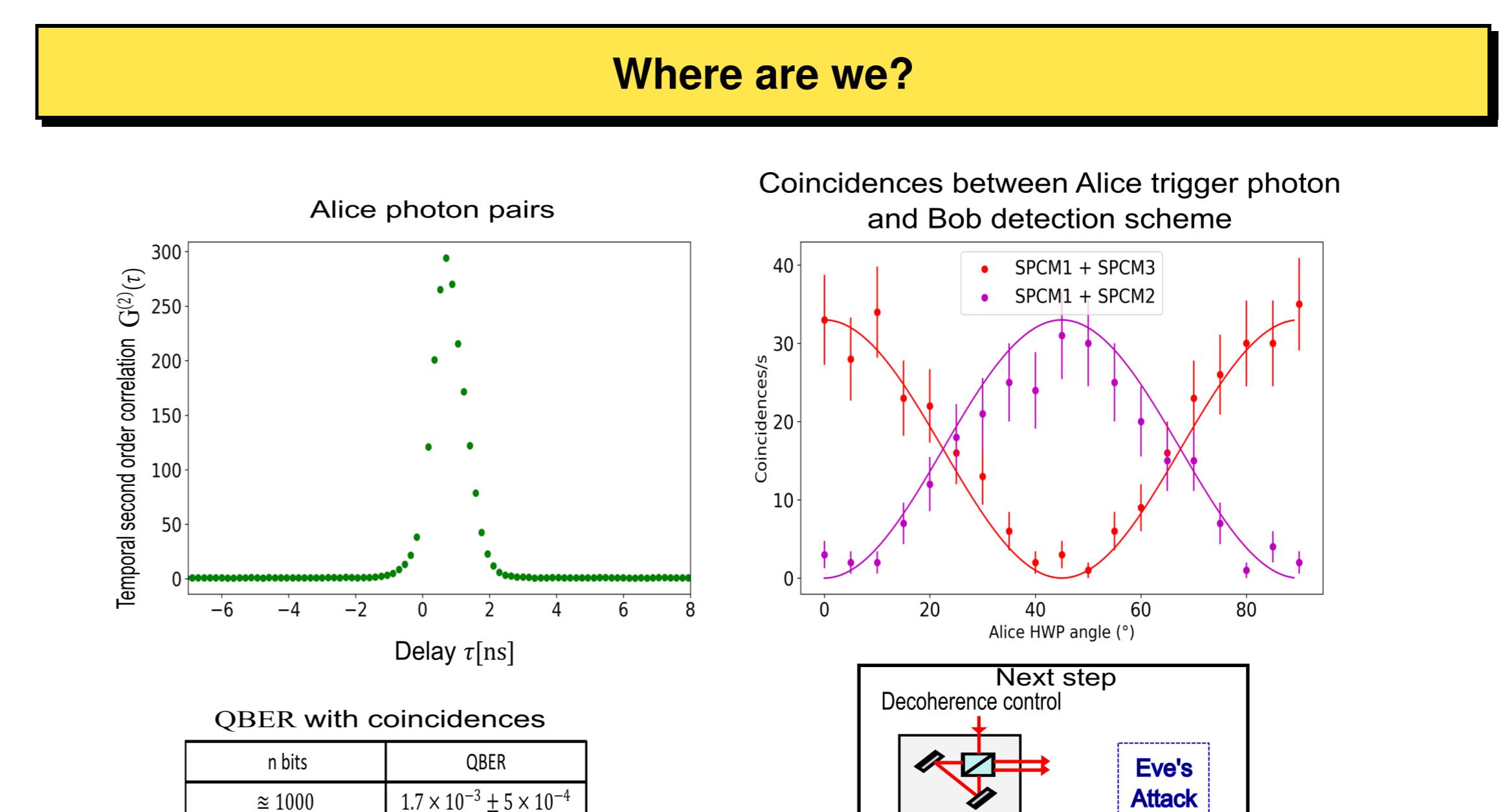
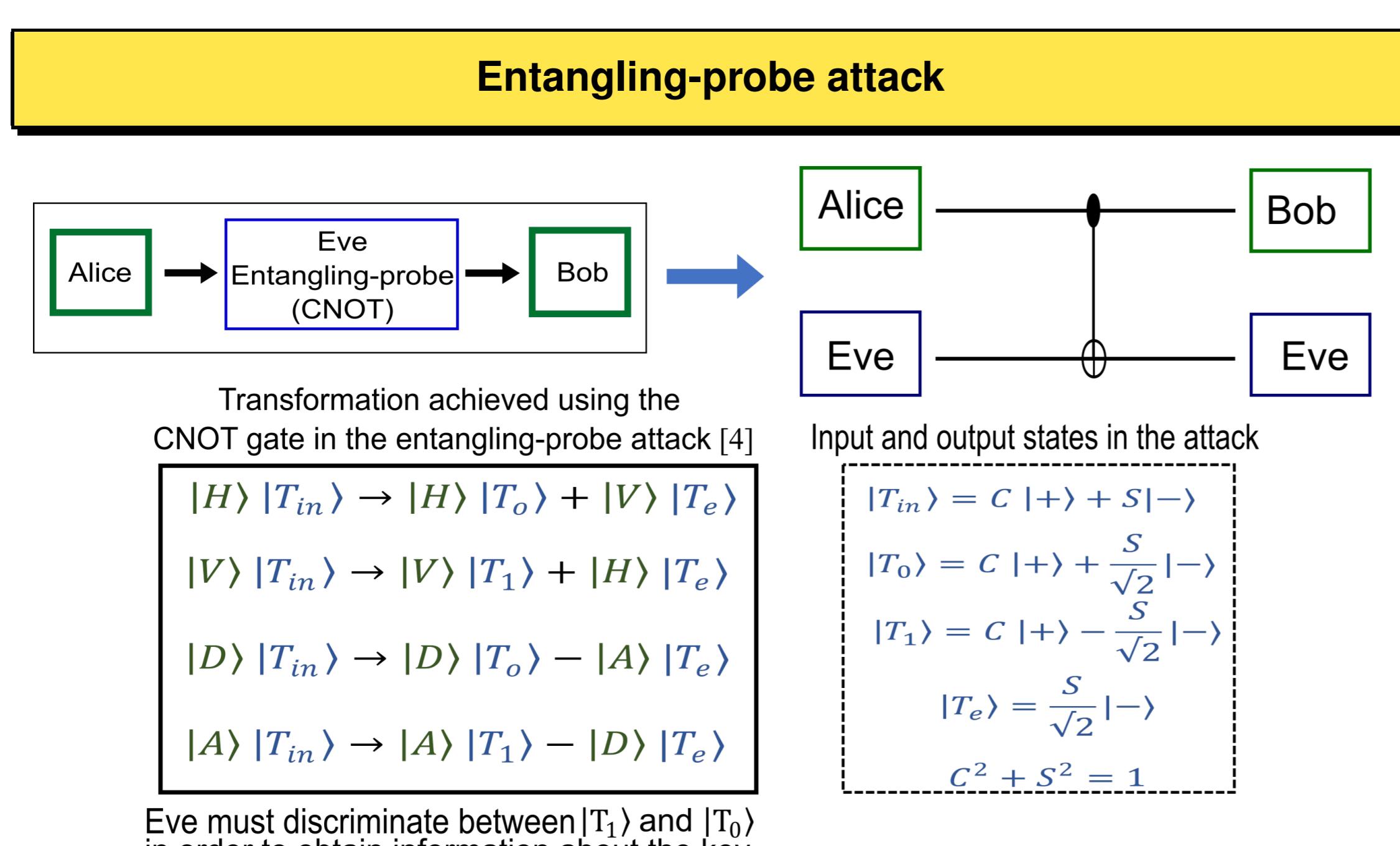
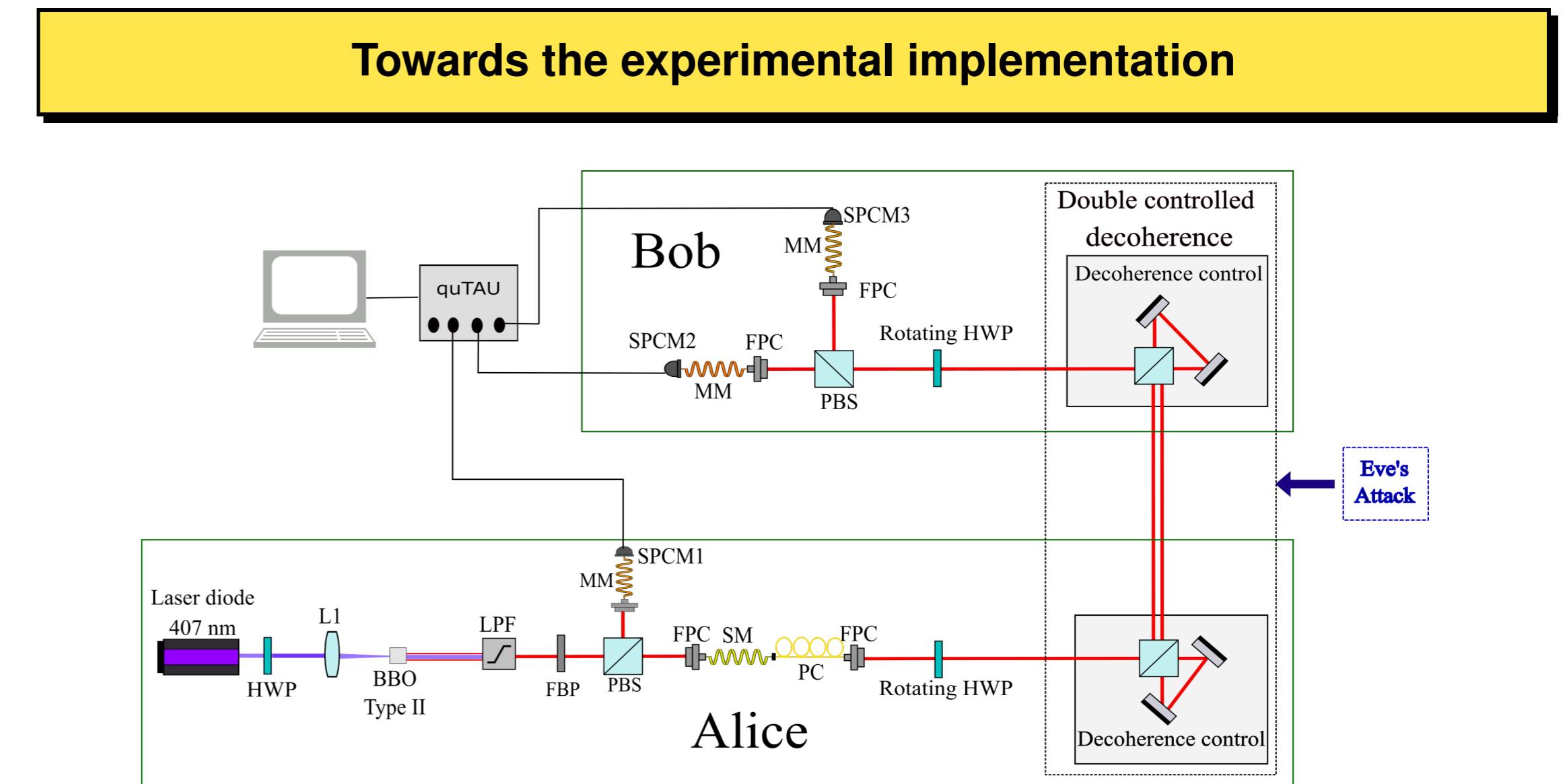
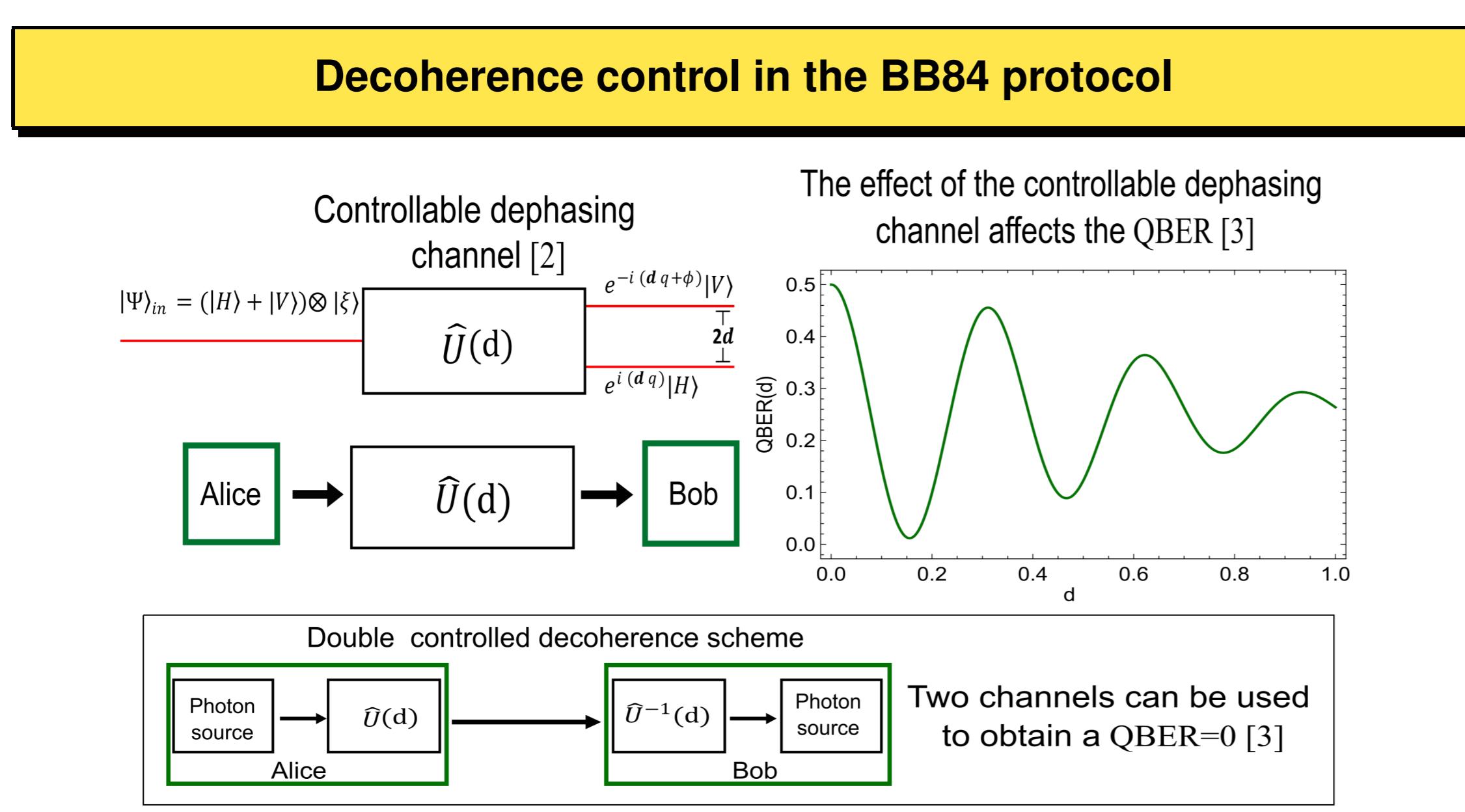
^{1*}dr.sabogal@uniandes.edu.co

Abstract

The BB84 protocol was the first quantum cryptography method to distribute a secret key using polarized photons. Decoherence is inevitable in any practical implementation of quantum key distribution schemes. In this project, we are studying theoretically the effect of controlling decoherence in the security of the BB84 protocol under the entangling-probe attack and developing an experimental implementation to study this phenomenon.



Double controlled decoherence in the BB84 protocol reduces the amount of information that an eavesdropper can obtain in the entangling-probe attack



Theoretically, we found that the use of the double decoherence control scheme in the BB84 protocol reduces the amount of information an eavesdropper can obtain in the entangling-probe attack. Experimentally, we are developing a setup to study how decoherence control affects the security of the BB84 protocol under the entangling-probe attack.

Conclusions

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, p. 8, 1984.

[2] D. F. Urrego, J.R. Álvarez, O. Calderón- Losada, J. Svozilík, M. Nuñez, and A. Valencia, "Implementation and characterization of a controllable dephasing channel based on coupling polarization and spatial degrees of freedom of light," Opt. Express, vol. 26, no. 9, pp. 11 940–11 949, Apr 2018

[3] A. F. Herrera Fernández, "Noise assisted quantum key distribution," 2019.

[4] T. Kim, I. Stork genannt Wersborg, F. N. C. Wong, and J. H. Shapiro, "Complete physical simulation of the entangling-probe attack on the bennett-brassard 1984 protocol," Phys. Rev. A, vol. 75, p. 042327, Apr 2007.