Three-party quantum-secured veto protocol using hybrid emitter architecture in a metropolitan fiber network

Thomas W. Sandø[1,2], Ferreira Diogo[4], Federico Valbusa[4], Martin Achleitner[4], Thomas Lorünser[4], Michael Hentschel[4], Peter Schiansky[1], Raphael Joos[5], Michael Jetter[5], Simone L. Portalupi[5], Peter Michler[5], Mathieu Bozzio[1], Mariano Lemus[3], Alessandro Trenti[4], Philip Walther[1,2,6] and Hannes Hübel[4]

[1] *University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), 1090 Vienna, Austria*
[2] *Vienna Doctoral School in Physics (VDSP), University of Vienna, Faculty of Physics, 1090 Vienna, Austria*
[3] *Instituto de Telecomunicações, Quantum Physics of Information (QPI) Group, 1049-001 Lisbon, Portugal*
[4] *Austrian Institute of Technology (AIT), Center for Digital Safety & Security, 1210 Vienna, Austria*
[5] *Institut für Halbleiteroptik und Funktionelle Grenzflächen, Center for Integrated Quantum Science and Technology (IQST) and SCoPE, University of Stuttgart, Allmandring 3, 70569 Stuttgart, Germany*
[6] *Institute for Quantum Optics and Quantum Information (IQOQI) Vienna, Austrian Academy of Sciences, Vienna, Austria*

Multi-party quantum cryptography protocols enable a range of applications like secret sharing and secure e-voting [1], yet they are still rarely field-tested. We develop a three-party quantum secure veto protocol over a deployed fiber network using a hybrid source architecture: an actively encoded 1554 nm quantum dot (QD) source at node A, a passively encoded heralded spontaneous parametric down-conversion source at node B, and a passive detector node C.

The protocol reveals whether any party vetoes while hiding the vetoing identity, achieved through quantum oblivious transfer based on the assumption of one-way functions [2,3]. This assumption is a distinction of this protocol, since its security does not rely on public-key cryptography nor on adversarial quantum storage constraints.

We use an InAs QD grown on a thin-film InGaAs metamorphic buffer on a GaAs wafer, placed in a circular Bragg grating, emitting at a measured fiber-coupled brightness of 5% and $g^{(2)}(0)=0.015$. The QD is excited using longitudinal acoustic phonon-assisted excitation providing robustness to power and wavelength fluctuations as well as inherently scrambling photon-number coherence [4], ideal for real-world implementations. The quantum states are encoded in the polarization of the emitted photons using electro-optic modulation with active polarization stabilization. We leverage the low multiphoton emission probability of the QD to bridge the longest link of approximately 10 dB loss.

Benefitting from a hybrid emitter network, we will enable a three-party quantum-secured veto over metropolitan fiber, relying on one-way function assumptions. This points to a practical path for deploying privacy-preserving multi-party cryptography.

[1] M. Bozzio, C. Crépeau, P. Wallden, P. Walther, Rev. Mod. Phys. **97**, 045006 (2025).
[2] M. Lemus, P. Schiansky, M. Goulão, M. Bozzio, D. Elkouss, N. Paunković, P. Mateus, P. Walther, PRX Quantum **6**, 040308 (2025).
[3] M. F. Ramos, M. Hentschel, F. Valbusa, C. Luchian, M. Achleitner, A. Trenti, M. C. Slater, M. Lemus, T. Lorünser, H. Hübel., arXiv:2501.05327 (2025).
[4] M. Bozzio, M. Vyvlecka, M. Cosacchi, C. Nawrath, T. Seidelmann, J. C. Loredo, S. L. Portalupi, V. M. Axt, P. Michler & P. Walther, npj Quantum Information **8**, 104 (2022).