Unconditional Authentication in Quantum Key Distribution via Hybrid Entangled Physical Unclonable Functions

Nicolas Laurent-Puig[1], Mina Doosti[2], Adriano Innocenzi[1], Eleni Diamanti[1]

[1]*Sorbonne Université, 75005, Paris, France*

[2]*School of Informatics, University of Edinburgh, EH8 9AB, Edinburgh, United Kingdom*

Quantum Key Distribution (QKD) provides the theoretical foundation for Information-Theoretic Security (ITS), ensuring that two parties can distribute a secret key immune to adversaries with unbounded computational power. A vulnerability is the authentication: the protocol strictly requires the classical channel to be authenticated to prevent Man-in-the-Middle attacks [1]. Standard solutions typically rely on pre-shared secret keys or Post-Quantum Cryptography (PQC), that reintroduces computational hardness assumptions that QKD is intended to eliminate. This has motivated research into alternative assumptions to support new solutions, in particular hardware-based assumptions like Physical Unclonable Functions (PUFs) [2]. PUFs exploit the stochastic, unclonable physical disorder introduced during device manufacturing to create a unique hardware fingerprint. Recent work has formally extended this concept to the quantum domain, defining the Quantum PUFs (qPUFs) [3]. Building upon this theoretical framework, we present the first experimental realization of an Entanglement-Based (EB) QKD protocol authenticated via a hardware-based security primitive: the Hybrid Entangled Physical Unclonable Function (HEPUF) [4].

Our implementation utilizes a high-fidelity polarization-encoded Bell-state source based on Type-II spontaneous parametric down-conversion (SPDC) in a Sagnac interferometer. Operating at telecom wavelengths, the source achieved a Bell-state fidelity of 99,12% [5]. The integrated protocol consists of a HEPUF authentication subroutine followed by an adapted EB-QKD. We successfully demonstrated secure key distribution over channel attenuations of 15, 20, and 27 dB, maintaining a Quantum Bit Error Rate (QBER) consistently below 0.6%. We further analysed two operational scenarios: a full-secrecy configuration where the HEPUF determines measurement bases adaptable to any protocol, and a high-efficiency configuration where the HEPUF provides the seed for Wegman-Carter authentication of the classical channel only implementable under certain assumptions of the following protocol. The latter demonstrated an order-of-magnitude increase in secret-key rates, proving the protocol's adaptability. These results validate that HEPUF-based authentication provides a robust solution to the authentication bottleneck in QKD.

Funding acknowledgement

We acknowledge financial support from the Horizon Europe research and innovation programme under the project QSNP (Grant No. 101114043) and the PEPR integrated project QCommTestbed (ANR-22-PETQ-0011), which is part of Plan France 2030.

References

[1] M. Mosca, Cybersecurity in an era with quantum computers: Will we be ready?, IEEE Security & Privacy 16, 38 (2018)).

[2] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Physical one-way functions, Science 297, 2026 (2002)

[3] P. Arapinis, M. Delavar, J. Doosti, and E. Kashefi, Quantum physical unclonable functions: Possibilities and impossibilities, Quantum 5, 475 (2021)

[4] S. Goswami, M. Doosti, and E. Kashefi, Hybrid authentication protocols for advanced quantum networks (2025), arXiv:2504.11552.

[5] L. dos Santos Martins, N. Laurent-Puig, P. Lefebvre, S. Neves, and E. Diamanti, Realizing a compact, highfidelity, telecom-wavelength source of multipartite entangled photons, Opt. Express 33, 53468 (2025).