Experimental semi-quantum key distribution with classical users

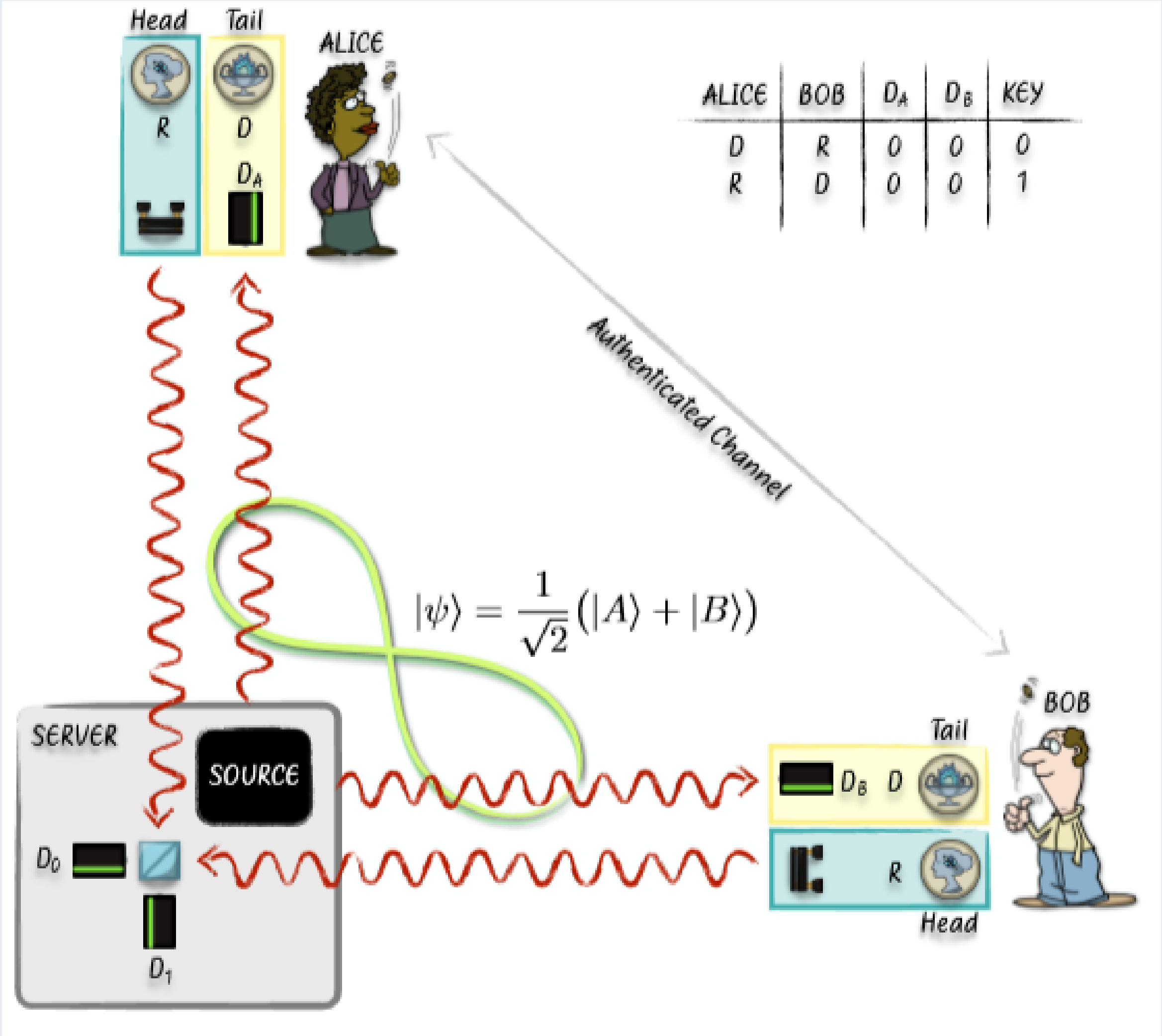
F. Massa[1], P. Yadav[2,3], A. Moqanaki[1], W. O. Krawec[4], P. Mateus[2], N. Paunković[2], A. Souto[5], and P. Walther[1]

1: Vienna Center for Quantum Science and Technology University of Vienna, Vienna, Austria; 2: Instituto de Telecomunicações, Lisboa and Dept. Matemática, Inst. Superior Técnico, Lisboa, Portugal; 3: Altran Portugal, Lisboa, Portugal; 4: Department of Computer Science and Engineering University of Connecticut, Storrs, CT USA; 5: LASIGE, Departamento de Informática, Faculdade de Ciências, Universidade de Lisboa, Portugal

Introduction

- Quantum Key Distribution (QKD) allows parties to establish secret keys, secure against computationally unbounded adversaries.
- This is impossible to achieve using classical communication only.
- "How quantum" must a protocol be to achieve this task?
- Semi-quantum cryptography [1] seeks to answer this question.
- In this work, we design a new QKD protocol where users are very limited: they may only detect the presence of photons or reflect photons
- Any more advanced quantum operation, such as performing an arbitrary measurement, is offloaded to an untrusted quantum server.

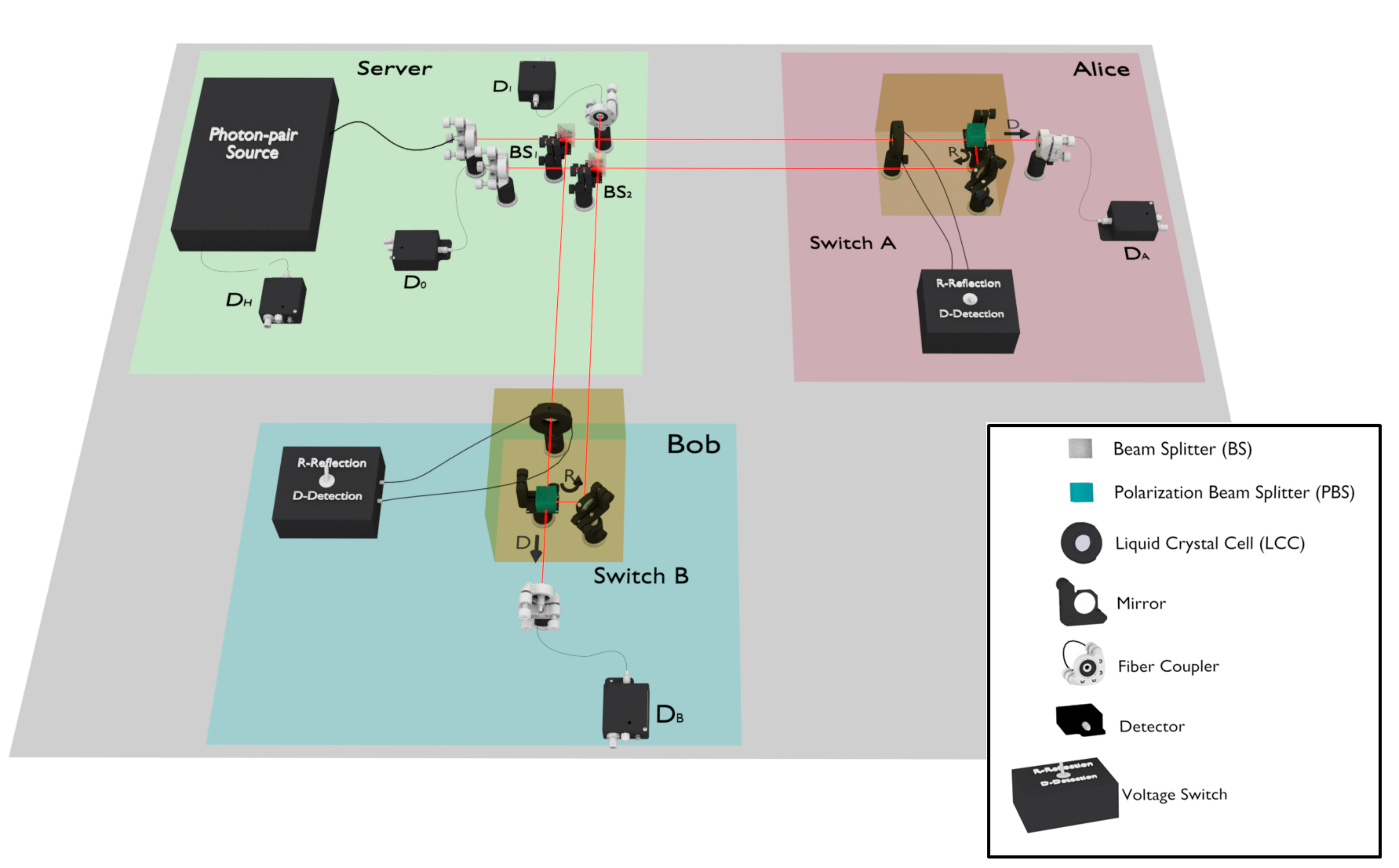
Our Protocol



ALICE	BOB	D_A	D_B	KEY
D	R	0	0	0
R	D	0	0	1

- Alice (A) and Bob (B) wish to establish a secret key. They can choose to Detect (D) photons or Reflect (R).
- A quantum server prepares a photon in a balanced superposition to A and B. On return, the server (if honest) should route the photon to a beamsplitter and perform a measurement, reporting the outcome D_0, D_1, or "vacuum."

Experimental Implementation



- The experimental setup for the demonstration of our protocol implements a folded Mach-Zehnder interferometer. The server sends a heralded photon to the users through a beamsplitter creating a superposition between A and B.
- Each user controls an optical switch composed of a liquid crystal cell (LCC) and a polarization beam splitter (PBS). This switch allows the users to steer the incoming photon either towards a fiber-coupled avalanche photo-diode (APB) for detection (D) or back towards the server (R).
- The phase between the two arms of the interferometer is such that whenever both users Reflect, detector D_0 clicks.
- The interferometer is passively stabilized and the phase is constant for about 100 s, after which the phase is actively reset to the initial value using a piezo transducer. See the full version [2] for more details.

Security Analysis

- We perform an information theoretic security analysis of the protocol assuming collective attacks in the finite key setting.
- We assume the server is adversarial and prepares a multi-photon state, entangled with its ancilla. We allow the server to perform any quantum operation on the return of the signal after A and B. We compute a bound on the *key rate* of our protocol $r = N_{sec}/N$.
- Note that this security analysis is complicated due to the increased capabilities of the server as compared to the limited, classical, nature of the users and also due to the two-way nature of the channel. For details on this proof see the full version [2].

Secret Key Rate

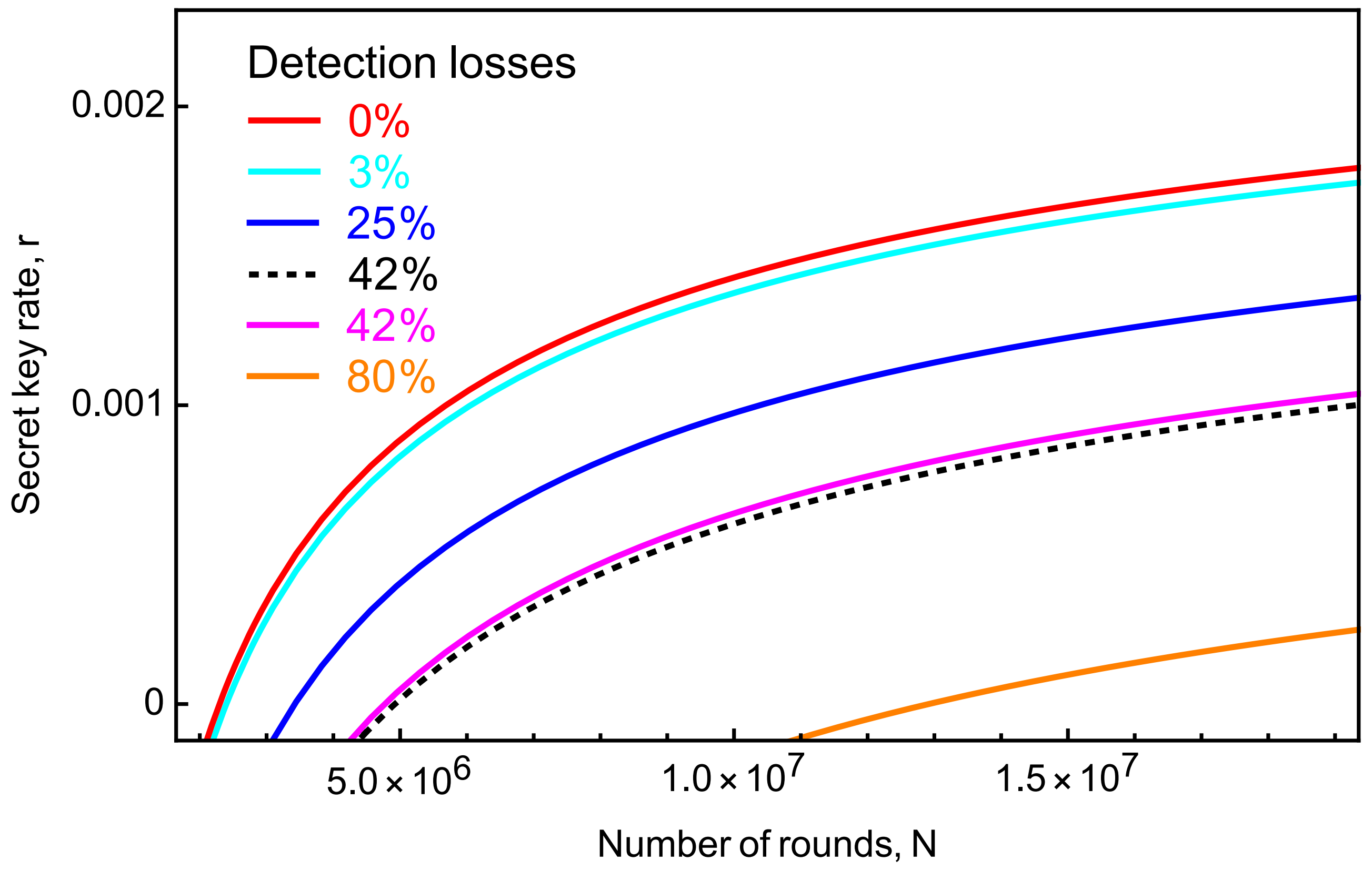


Figure 1:(From [2]) Secret key rate vs. number of iterations N for different detection loss. Black, dashed line is our experimental implementation with a detection loss of 42% while other, solid lines are simulations.

Closing Remarks

- In this work, we proposed, and experimentally implemented a novel QKD protocol allowing two restricted, nearly classical, users to establish a shared secret key with the help of an untrusted quantum server
- We also performed an information theoretic security analysis of this protocol.
- Full details can be found in [2]

References

[1] M. Boyer, D. Kenigsberg, and T. Mor.
Quantum key distribution with classical Bob.
Phys. Rev. Lett., 99:140501, Oct 2007.

[2] F. Massa, P. Yadav, A. Moqanaki, W. O Krawec, P. Mateus, N. Paunković A. Souto, and P. Walther.
Experimental quantum cryptography with classical users.
arXiv:1908.01780, 2019.