Receiver-device-independent QKD

Marie Ioannou[1], Maria Ana Pereira[1], Davide Rusca[1], Fadri Grünenfelder[1], Alberto Boaron[1], Matthieu Perrenoud[1], Alastair A. Abbott[1,2], Pavel Sekatski[1], Jean-Daniel Bancal[1,3], Nicolas Maring[1], Hugo Zbinden[1] & Nicolas Brunner[1]

[1]Department of Applied Physics University of Geneva, 1211 Geneva, Switzerland

[2] Univ. Grenoble Alpes, Inria, 38000 Grenoble, France

[3] Université Paris-Saclay, CEA, CNRS, Institut de physique théorique, 91191, Gif-sur-Yvette, France

Overview

Key point:

- Protocol with **one partially trusted party** and a complete untrusted receiver (in comparison to [1]).
- **No assumptions on the receiver**, proof against attacks on detectors (in comparison to [2]).
- **Simple prepare-and-measure implementation**, no need for entanglement (in comparison to [3]).

Main results:

- **Proof of principle experiment** demonstrating the feasibility of our proposal.
- Protocols that can tolerate an **arbitrarily low transmission efficiency**.

Prepare-and-measure scenario

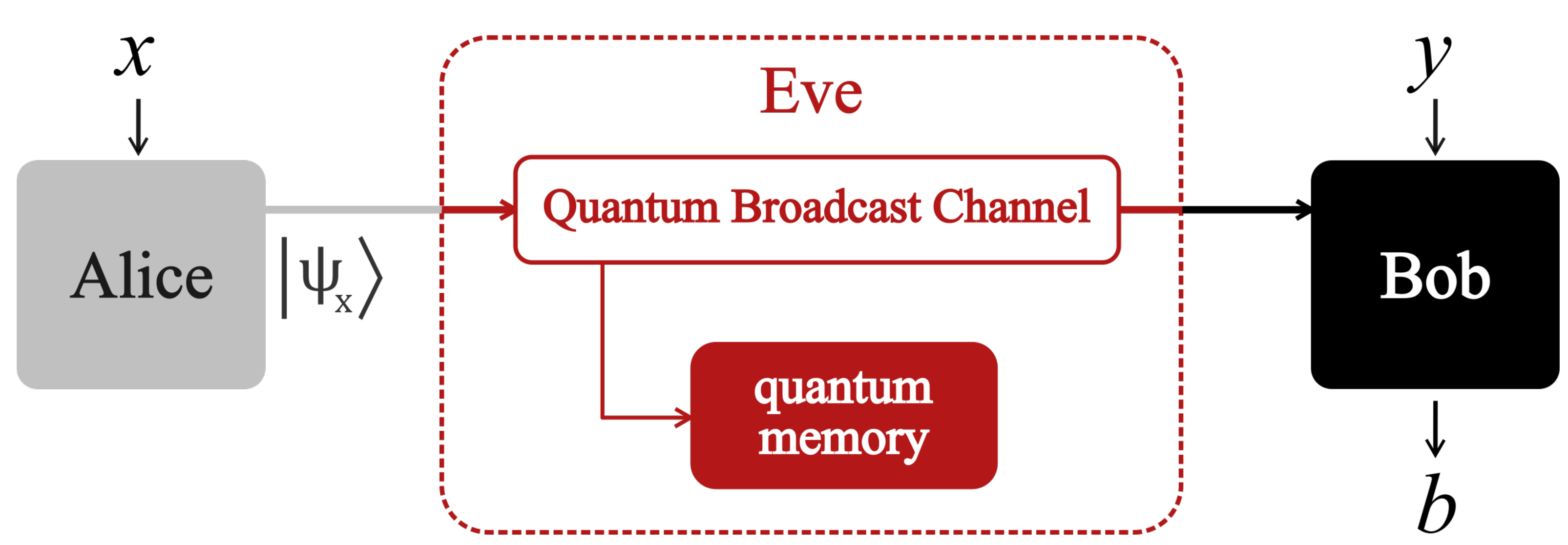

Fig. 1: Scenario: Based on the observed data $p(b|x,y)$, and the assumption that Alice's preparations $|\psi_x\rangle$ have bounded overlap, Alice and Bob can establish a secret key

Assumptions common to all QKD protocols:

1. x, y are chosen independently from Eve
2. No information about x and y leaks to Eve, except via the quantum and classical communication specified in the protocol at the given round
3. Validity of quantum physics.

Additional assumption:

1. The inner-products $\gamma_{x,x'} = \langle\psi_x|\psi_{x'}\rangle$ with $x, x' = 0, ..., n-1$ are bounded.

Protocol

1. Alice chooses :
   - $\mathbf{r} = (r_0, r_1)$ with $0 \leq r_0 < r_1 \leq n-1$,
   - a key bit k with $k = 0, 1$.
2. Alice sets $x = r_k$ and sends a coherent state $|\psi_x\rangle = |\alpha\cos(\theta/2)\rangle_H \left|\alpha\sin(\theta/2)e^{i\phi_x}\right\rangle_V$
3. Bob chooses a basis with $y = 0, 1..., n-1$
4. Bob's measures $B_{0|y} = |\psi_y^{\perp}\rangle\langle\psi_y^{\perp}|$, $B_{1|y} = |\psi_y\rangle\langle\psi_y|$

   Expected statistics: $p(b=0|x,y) = 1 - e^{-|\alpha|^2 \sin(\theta)^2 \sin\left(\frac{2\pi(x-y)}{n}\right)^2}$
5. If $b = 0$ and $y = r_0$ or $y = r_1$ raw key is generated; else the round is discarded

Security analysis

Lower bound on asymptotic key rate per round [4]:

$$R = (H_{\min}(A|E, \text{succ}) - H_2[\text{QBER}])\, p(\text{succ}) \tag{1}$$

- QBER, $p(\text{succ})$ estimated from the data $p(b|x,y)$
- Estimation of $H_{\min}(A|E, \text{succ})$ can be relaxed to a hierarchy of semi-definite programs (SDPs) using solely $p(b|x,y)$ and $\gamma_{x,x'}$ [5].

Experimental realization

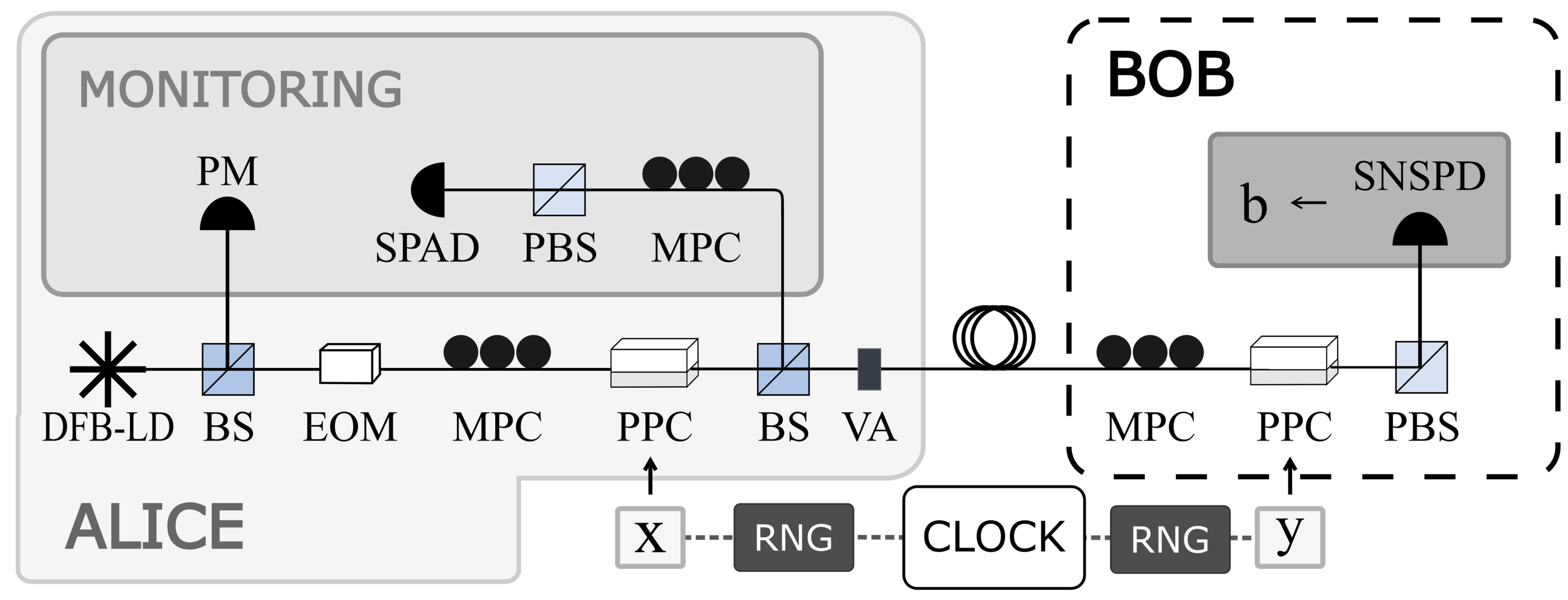

Fig. 2: Experimental setup

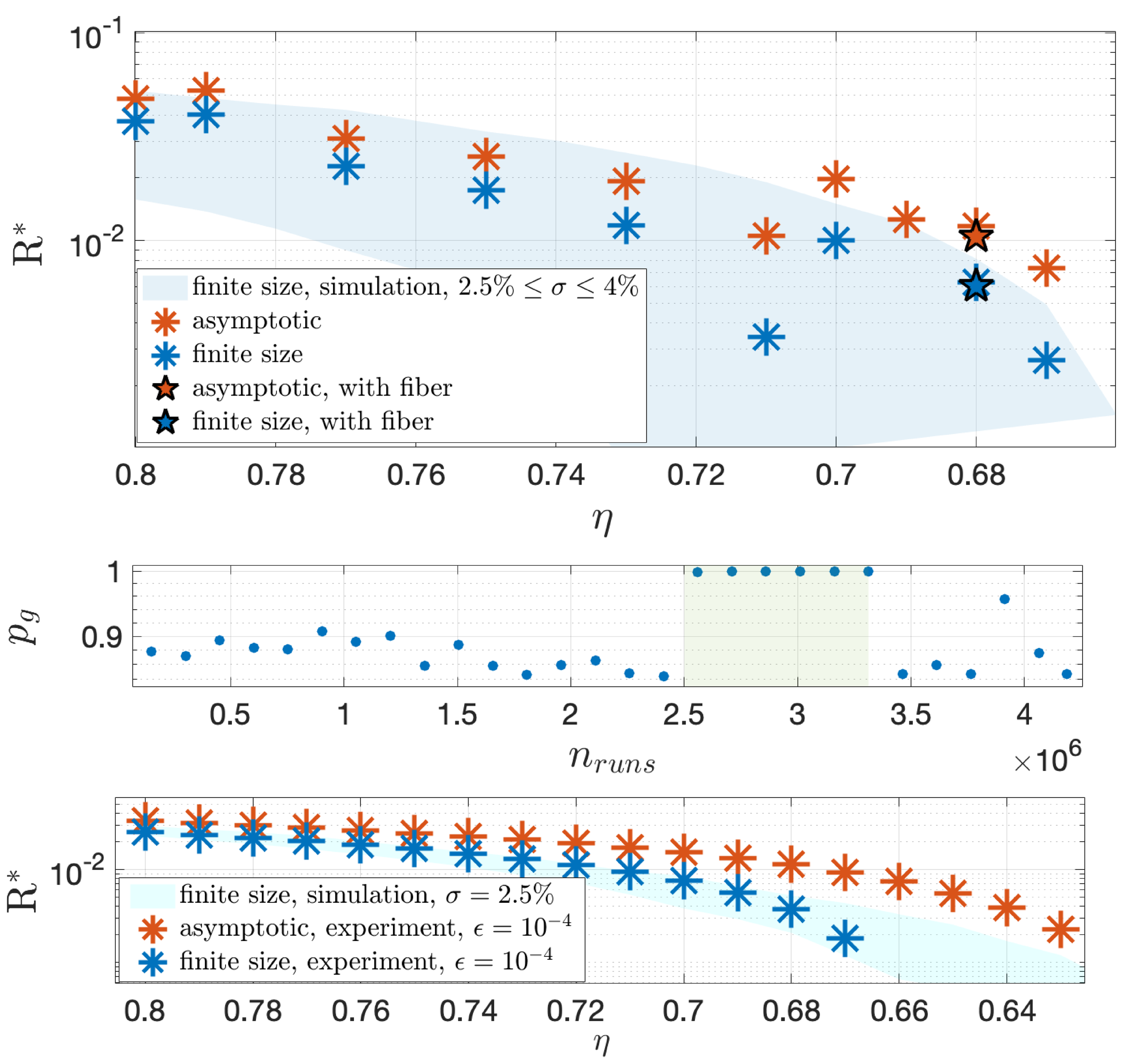

Fig. 3: Experimental results. (Top) Key rate R as a function of the transmission η for the protocol with $n = 2$ states. (Middle) Illustration of the self-testing feature of the protocol. (Bottom) Key rate R vs transmission η for the protocol with $n = 3$ states, showing enhanced robustness to losses.

References

- [1] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
- [2] M. Tomamichel, C. Lim, N. Gisin, et al., Nat Commun **3**, 634 (2012).
- [3] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).
- [4] I. Devetak and A. Winter, Proc. Roy. Soc. **A461**, 207 (2005).
- [5] Y. Wang, I.W. Primaatmaja, E. Lavie et al., npj Quantum Inf. **5**, 17 (2019).

LaTeX TikZposter