Noisy pre-processing facilitating a photonic realisation of device-independent quantum key distribution

Melvyn Ho[1,3], Pavel Sekatski[1], Ernest Y-Z. Tan[2], Renato Renner[2], Jean-Daniel Bancal[1,3], Nicolas Sangouard[1,4]

Fonds national suisse
Schweizerischer Nationalfonds
Fondo nazionale svizzero
Swiss National Science Foundation

[1]Department of Physics, University of Basel, Klingelbergstrasse 82, 4056 Basel, Switzerland
[2]Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland
[3]Department of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland
[4]Institut de physique théorique, 91191, Gif-sur-Yvette, France

DIQKD

Key distribution with black boxes [1,2]

Stringent requirements:

- High transmission probability
- Large amount of data

Our aim: Relax this!

Introduce a simple modification to the DI protocol : noisification

- Previously used in DDQKD [3]
- New DIQKD security proof

Protocol

1. Distribution + measurement

   $|\psi\rangle_{AB}, A_1, A_2, B_0, B_1, B_2$

2. Sifting + parameter estimation (CHSH)

   $S = \langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle$

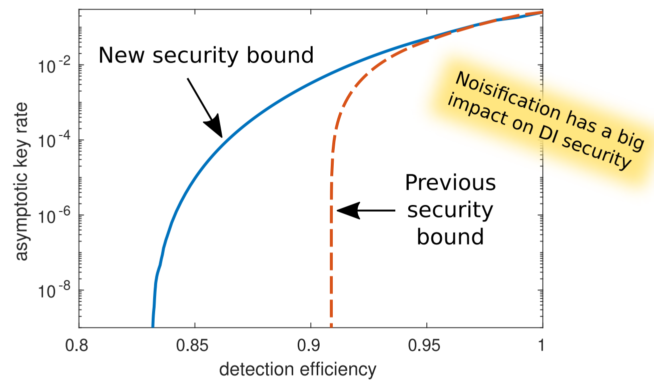
3. Noisy pre-processing

   Reference bit flipped with probability p: $A_1 \to \hat{A}_1$

4. Error correction

5. Privacy amplification

Main result



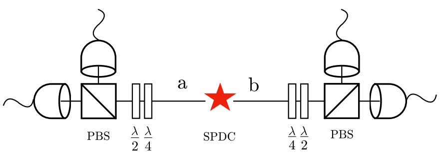
Eve's uncertainty:

$$H(\hat{A}_1|E) \geq 1 - h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right) + h\left(\frac{1+\sqrt{1-p(1-p)(8-S^2)}}{2}\right)$$

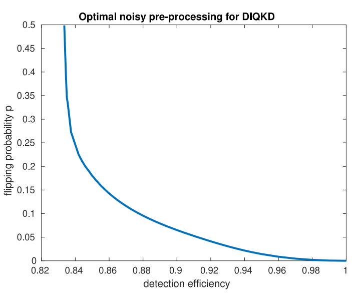
correction due to noisification

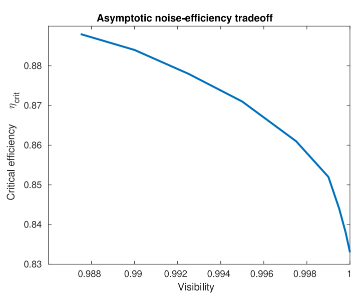
Implementation

Photonic:
- \+ fast
- \+ low noise
- \- losses



State: $|\psi\rangle = (1-T_g^2)^{N/2}(1-T_{\bar{g}}^2)^{N/2}\Pi_{k=1}^N e^{T_g a_k^\dagger b_{k,\perp}^\dagger - T_{\bar{g}} a_{k,\perp}^\dagger b_k^\dagger}|\underline{0}\rangle$





Proof sketch

- Entropy accumulation theorem (EAT) [4]

  Consider $\psi_{ABE}^{\otimes n}$

  Asymptotic key rate: $r \geq H(\hat{A}_1|E) - H(\hat{A}_1|B_0)$

- Symmetrization

  $H(\hat{A}_1|E) = 1 - H(\rho_E) + \frac{1}{2}\sum_a H(\rho_{E|a})$

- Qubit reduction

  Jordan's lemma $A_x = \sum_\lambda A_x^\lambda \otimes |\lambda\rangle\langle\lambda| \quad B_y = \sum_\lambda B_y^\mu \otimes |\mu\rangle\langle\mu|$

  Block-diagonal state $|\psi^{\lambda,\mu}\rangle_{A'B'E} = \sum_{i=1}^4 \sqrt{L_i}|\Phi_i\rangle_{A'B'}|i\rangle_E$

  Alice's measurement parametrized by ϕ

  A concave bound for each block implies a bound on average

- $H(\hat{A}_1|E)_{\psi^{\lambda,\mu}}$ is an increasing function of ϕ

  The state that minimizes Eve's ignorance is independent of p

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007)
[2] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar and V. Scarani, New Journal of Physics 11, 045021 (2009)
[3] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. 95, 080501 (2005)
[4] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner and T. Vidick, Nat. Commun. 9, 459 (2018)
[5] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson and S. Wehner, Quantum Sci. Technol. 4, 035011 (2019)
[6] E. Woodhead, A. Acín, S. Pironio, arXiv:2007.16146