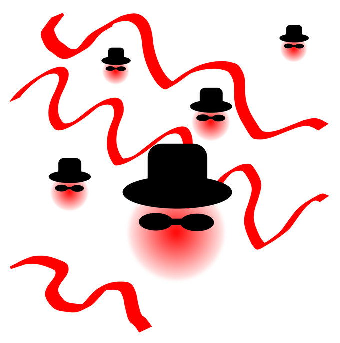
Multi-photon and side-channel attacks in mistrustful quantum cryptography



Mathieu Bozzio[1], Adrian Cavaillès[2], Eleni Diamanti[2], Adrian Kent[3,4] and **Damián Pitalúa-García**[3] (dp373@cam.ac.uk)
[1]Faculty of Physics, University of Vienna, VCQ, Boltzmanngasse 5, 1090 Vienna, Austria
[2]Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, F-75005 Paris, France
[3]Centre for Quantum Information and Foundations, DAMTP, University of Cambridge, United Kingdom
[4]Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

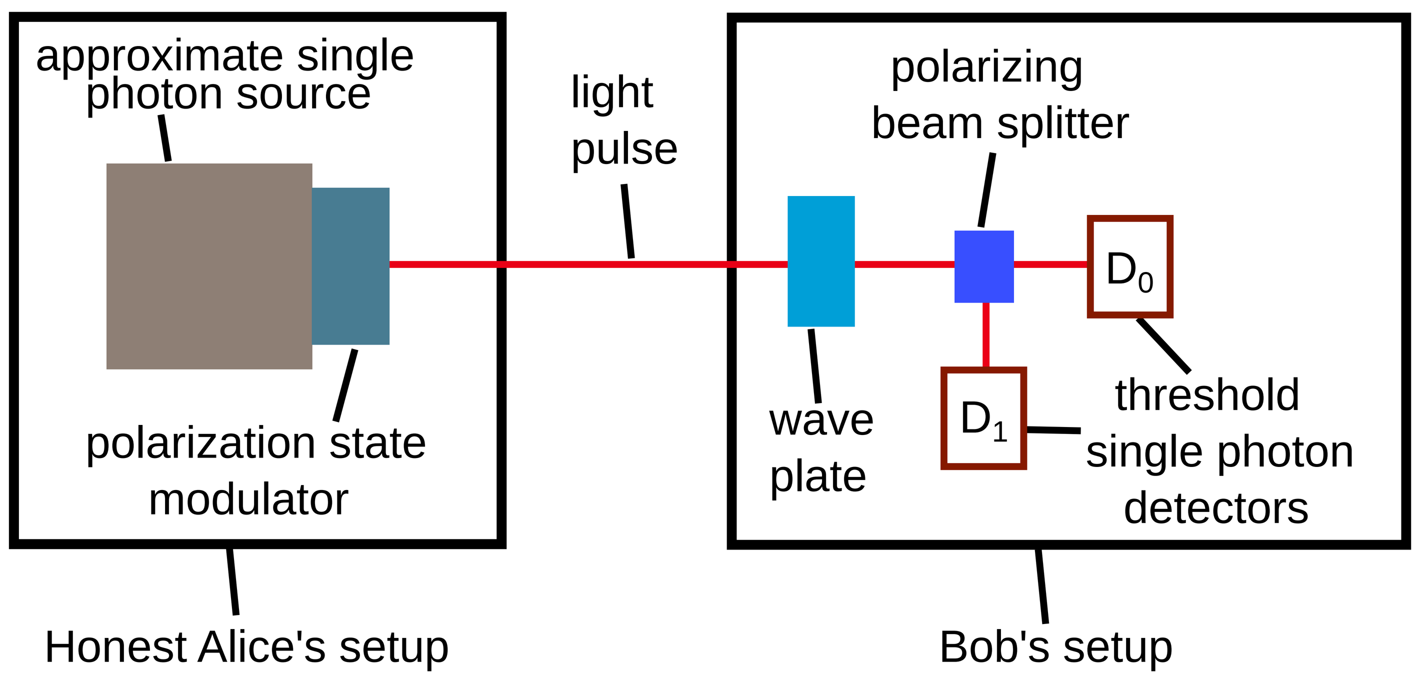
1 Abstract

- **Mistrustful quantum cryptography (MQC) is a large field and one of the major applications envisaged for a global quantum internet.**
- **It includes important tasks like bit commitment, coin flipping, oblivious transfer and secure computations.**
- **We indentify [1] new *multi-photon* attacks on practical implementations of MQC with photonic setups, and show that some previous implementations were vulnerable.**
- **We illustrate the power of these attacks with an experiment.**
- **We also discuss side-channel attacks.**

2 Private measurement of an unknown qubit state

- Many interesting protocols in MQC use some version of the following task.

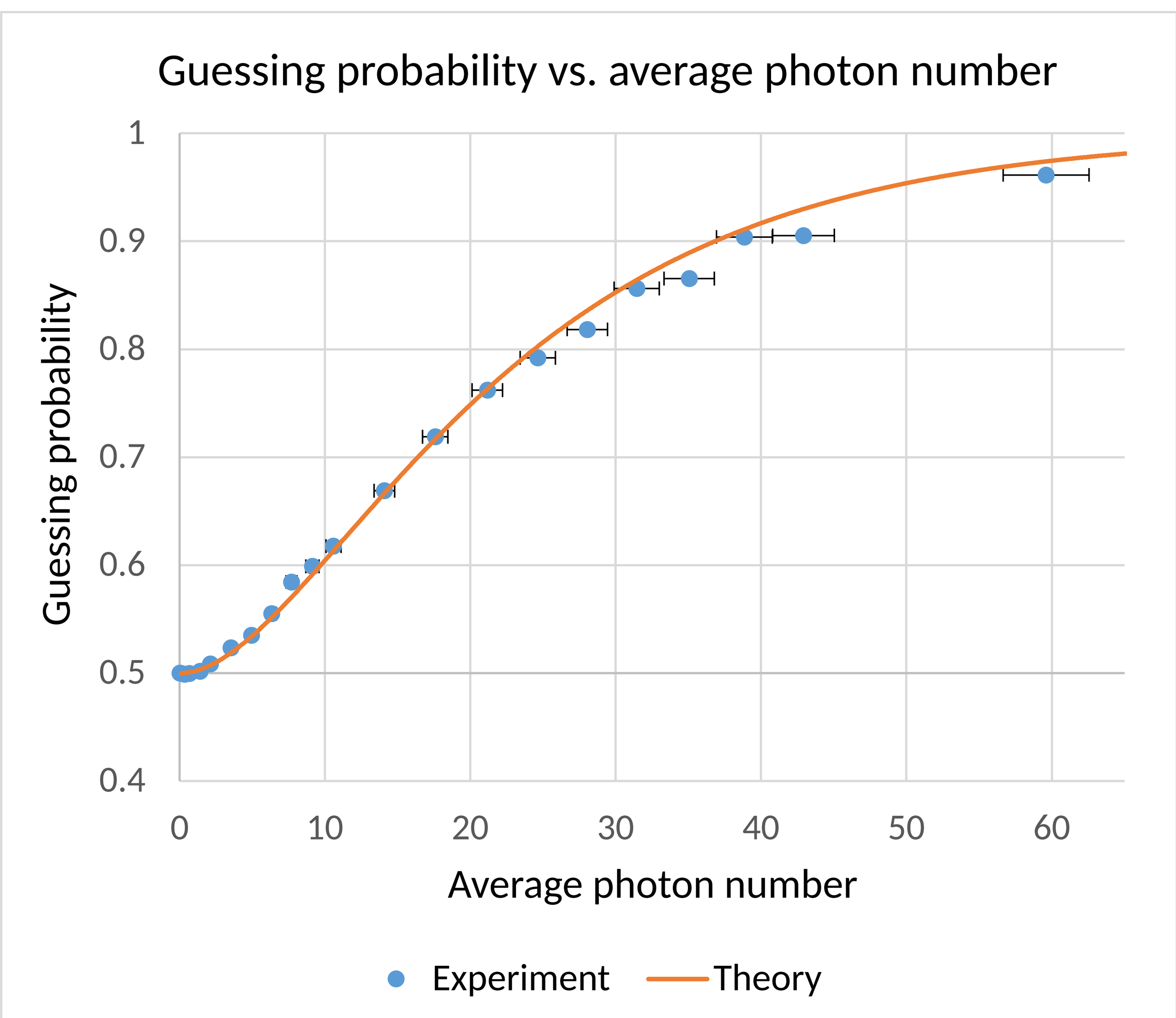
1. Alice sends Bob a random BB84 state (other states can be considered too).
2. Bob generates a random bit b privately and measures the received state in one of the two BB84 basis (computational if b = 0, or Hadamrd if b = 1).
3. Bob sends a bit message m to Alice reporting whether a measurement outcome was produced (m = 1) or not (m = 0).



- *Security against Alice*: the probability that Alice guesses b should be arbitrarily close to 1/2. (Here we assume Bob is honest.)
- Security against Alice can be achieved in ideal settings, where step 3 is not needed. However, in practice, losses, imperfect detectors and other experimental imperfections require step 3, compromising security.
- Morover, in practice, multiple detectors click with non-zero probability.
- *Reporting strategy*: Bob must carefully choose which measurements are reported in step 3. Here we focus on the setup illustrated above.
- *Multi-photon attacks*: dishonest Alice sends a pulse with arbtrary number of photons encoding an arbitrary quantum state, and tries to guess b from m.

3 Reporting only single clicks

- *Reporting strategy I*: Bob sets m = 1 if only one detector clicks.
- *Multi-photon attack I*: Alice sends Bob a photon pulse with a large number of photons in the same BB84 state (discussed in [2]). Ideally, if Bob measures in Alice's basis then only one detecctor clicks, otherwise both detectors click. Thus, Alice learns b from the message m. We illustrate Alice's guessing probability for an experimental simulation of the attack.



4 Reporting if at least one detector clicks

- *Reporting strategy II*: Bob sets m = 1 if at least one detector clicks (used in squashing models in QKD and in Ref. [2]).
- If detector efficiencies are equal then this protects Bob perfectly from arbitrary multi-photon attacks (Lemma 1 in Ref. [1]).
- Guaranteeing exactly equal efficiencies is impossible, but attenuators help.
- *Multi-photon attack II*: any strategy by Alice that allows her to exploit the difference in Bob's detection efficiencies when Bob sets m = 1 with unit (high) probability if both detectors click.

5 Symmetrization of losses

- *Reporting strategy III*: Bob discards detection events from the most efficient detector (basis), aiming to equalize his reporting probabilities [3].
- This can offer very good protection to Bob if Alice does not send pulses with more than one photon (Lemma 2 in [1]). But, dishonest Alice may send multi-photon pulses. Thus, Bob is not guaranteed protection.

6 Probabilistic reporting strategies

- *Probabilistic reporting strategies*: Bob sets m = 1 with a probability that depends on which detectors click. The previous strategies are special cases.
- *Trivial reporting strategy*: Bob sets m = 1 with the same probability (e.g., unity) for all detection events. It is the only known reporting strategy offering perfect protection against arbitrary multi-photon attacks. But it requires extremely good setups with very low losses and high detection efficiencies to be useful in practice (e.g., to guarantee correctness of the protocols).

7 Main result

- Theorem 1 in Ref. [1]: if the detection efficiencies are different, then the only probabilistic reporting strategy guaranteeing perfect protection against arbitrary multi-photon attacks is the trivial reporting strategy.
- This implies that symmetrization of losses (introduced in Ref. [3]) does not guarantee the claimed protection.

8 Multi-photon attacks on previous implementations

- We showed that [2-6] are vulnerable to multi-photon attacks (Table I in [1]).

9 Discussion

- In multi-photon attacks, dishonest Alice sends multi-photon pulses and obtains information about Bob's measurement basis.
- The trivial reporting strategy is the only known perfect protection, but it requires state of the art experimental setups to be useful in practice.
- Some countermeasures are: using attenuators to make detection efficiencies very close, using different setups to probabilistically infer if a pulse is multi-photon, aborting with double clicks, using variations of the task considered (e.g., a reversed version). But all these open other problems [1].
- We also extensively analized a setup with four detectors (Appendix D4 in [1]), including extensions of multi-photon attacks I and II.
- In side-channel attacks, Alice controls further degrees of freedom. There is not currently any perfect protection against arbitrary side-channel attacks.
- Measurement-device and fully-device independent protocols have other security and implementation problems, e.g., loopholes (see Discussion in [1]).
- A countermeasure providing unconditional security, in principle, against arbitrary side-channel attacks comprises Bob filtering Alice's signal via teleportation. However, a practical problem is that there is a nonzero probability of producing more than one pair of entangled photons. We believe this requires further investigation.

[1] M. Bozzio, A. Cavaillès, E. Diamanti, A. Kent and D. Pitalúa-García "Multi-photon and side-channel attacks in mistrustful quantum cryptography", to appear in *PRX Quantum*, preprint arXiv:2103.06970.
[2] Y. Liu et al., "Experimental unconditionally secure bit commitment", *Phys. Rev. Lett.* **112**, 010504 (2014).
[3] N. Ng et al., "Experimental implementation of bit commitment in the noisy-storage model", *Nat. Commun.* **3**, 1326 (2012).
[4] T. Lunghi et al., "Experimental bit commitment based on quantum communication and special relativity", *Phys. Rev. Lett.* **111**, 180504 (2013).
[5] A. Pappa et al., "Experimental plug and play quantum coin flipping", *Nat. Commun.* **5**, 3717 (2014).
[6] C. Erven et al., "An experimental implementation of oblivious transfer in the noisy storage model", *Nat. Commun.* **5**, 3418 (2014).