

Memory Attacks on Device-Independent Quantum Cryptography

Roger Colbeck

Joint work with Jon Barrett and Adrian Kent

arXiv:1201.4407



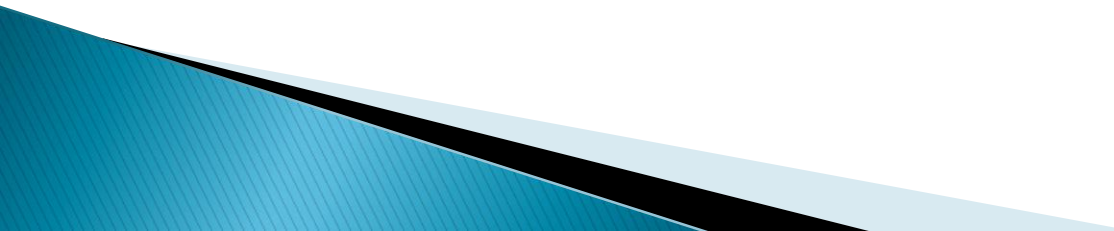
Two sides of cryptography

Theoretical

Start with 'clean', well-defined assumptions and try to prove security based on these.

Practical

Try to build devices that satisfy the theoretical assumptions as closely as possible.



Two sides of cryptography

Theoretical

Start with 'clean', well-defined assumptions and try to prove security based on these.

e.g. have a device that emits single photons in a state of my choice and can perform arbitrary measurements with arbitrarily high fidelity.

Practical

Try to build devices that satisfy the theoretical assumptions as closely as possible.

Two sides of cryptography

Theoretical

Start with 'clean', well-defined assumptions and try to prove security based on these.

e.g. have a device that emits single photons in a state of my choice and can perform arbitrary measurements with arbitrarily high fidelity.

Practical

Try to build devices that satisfy the theoretical assumptions as closely as possible.

You must be joking 😊
What we can do is this...

Two sides of cryptography

Theoretical

Start with 'clean', well-defined assumptions and try to prove security based on these.

Hmm...ok, I have to change my assumptions and work on my proof...

Practical

Try to build devices that satisfy the theoretical assumptions as closely as possible.

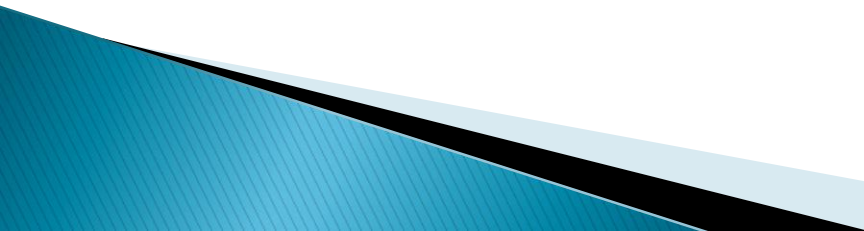
You must be joking 😊
What we can do is this...

Motivation

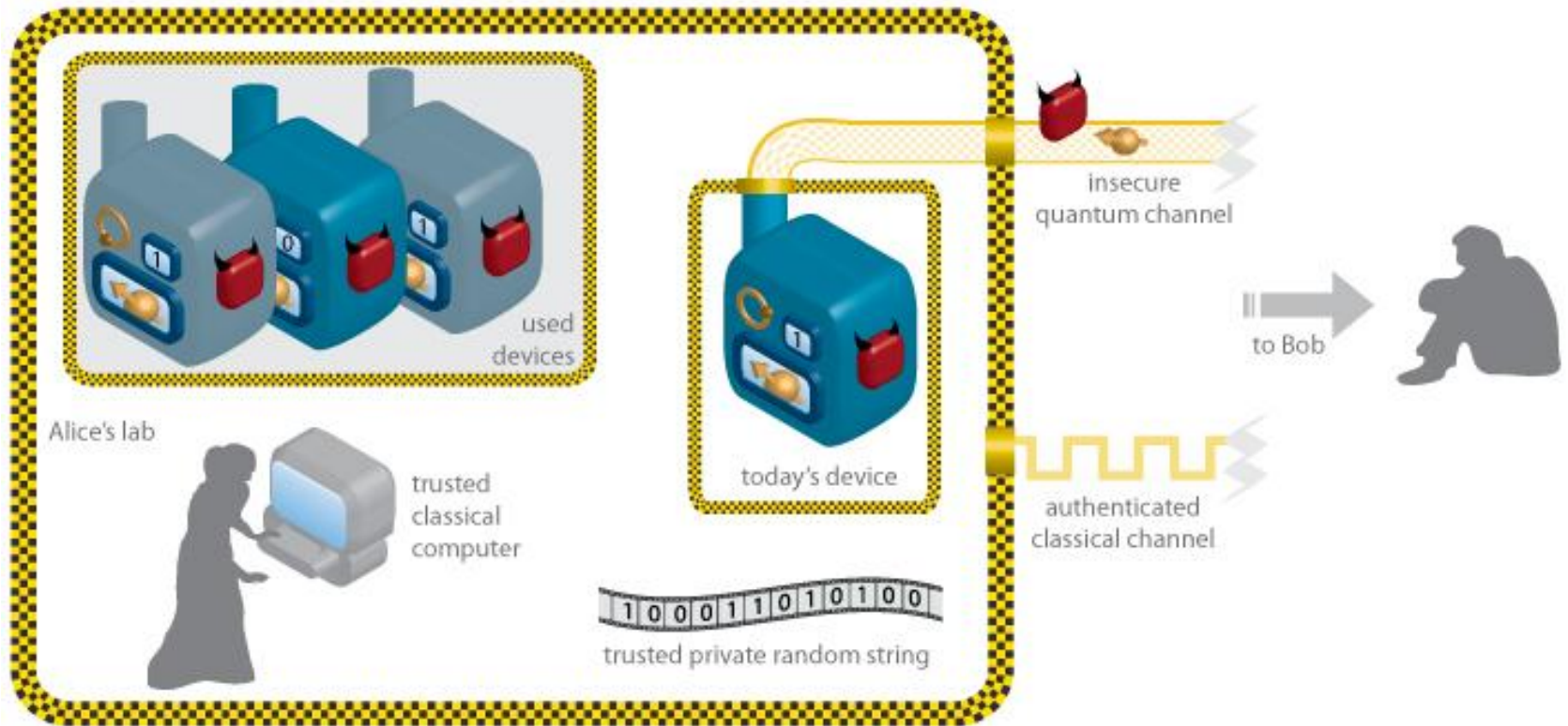
- ▶ Recent hacking attacks* have highlighted that certain implementations do not satisfy the assumptions of the proof.
- ▶ Basing a proof on weaker assumptions makes it easier for a particular implementation to come closer to satisfying the assumptions.
- ▶ Motivates **device-independence**, in which one tries to prove security without making any assumptions about the workings of certain devices.

*e.g. Gerhardt et al. N. Comms 2 (2011)

Device-independence

- ▶ No trust at all in any quantum devices used for the protocol.
 - ▶ NB: More recently, some other weaker concepts related to device-independence have been introduced (e.g. “semi device-independence”). The results of this talk don’t necessarily apply to these weaker forms.
 - ▶ With device-independence, it wouldn’t matter if an adversary tampered with or substituted my devices: we would still have security.
- 

Device-independence assumptions



Existing device-independent QKD schemes

- ▶ There exist unconditionally secure device-independent QKD schemes*.
- ▶ Most of these protocols require as many devices as candidate entangled pairs for the proof to go through, while more recent works show how to avoid this. BCK 1209.0435, RUV 1209.0448
- ▶ For practical device-independent QKD, we would like to be able to use a small number of devices, and to reuse those devices.
- ▶ I will show that naïve reuse can lead to supposedly secret data being compromised.

*BHK PRL 95 (2005), Masanes et al. quant-ph/0606049, HR arXiv:1009.1833, MPA N.Comms 2 (2010)

Composability of device-independent QKD

- ▶ We don't only want to generate secure key, we also want to be able to use it for things, e.g. one-time pad encryption.
- ▶ Proving security according to a composable security definition allows this.
- ▶ However, in a device-independent scheme, there is an additional composability issue.
- ▶ Devices equipped with a memory can remember all their inputs and outputs and can try to leak them if they are reused.
- ▶ This can compromise the security of a previously-generated key.

Illustration of the attack

Assume a QKD protocol of the following form:



- 1. State distribution.** The quantum states needed in the protocol are either supplied by Eve or created by Bob with half sent to Alice.

Illustration of the attack

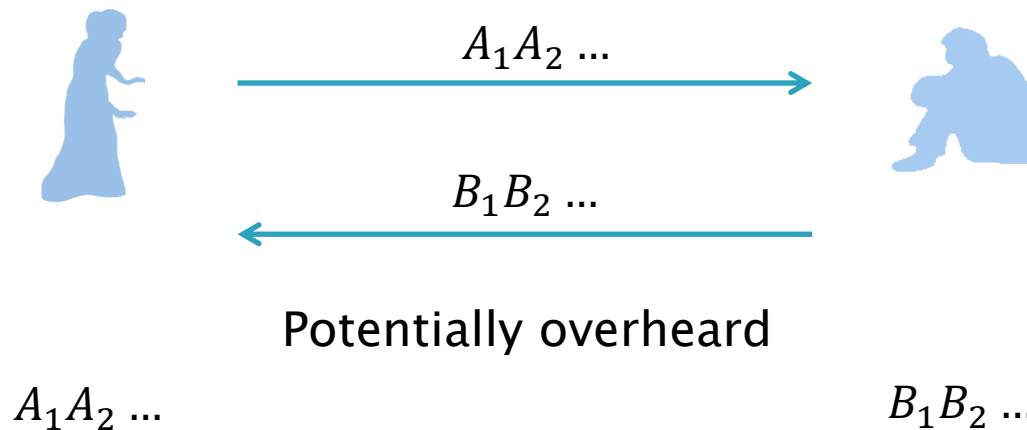
Assume a QKD protocol of the following form:



2. Alice and Bob repeatedly make random inputs to their device and record their outcomes (in total they make M inputs). NB: They have only one device each.

Illustration of the attack

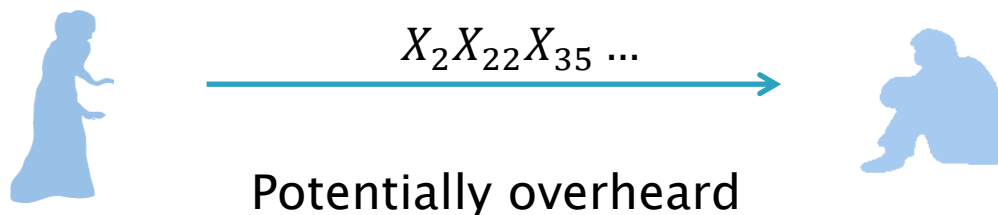
Assume a QKD protocol of the following form:



3. Alice or Bob publicly announce their measurement choices, and check that they had a sufficient number of suitable input combinations for the protocol. If not, they abort.

Illustration of the attack

Assume a QKD protocol of the following form:

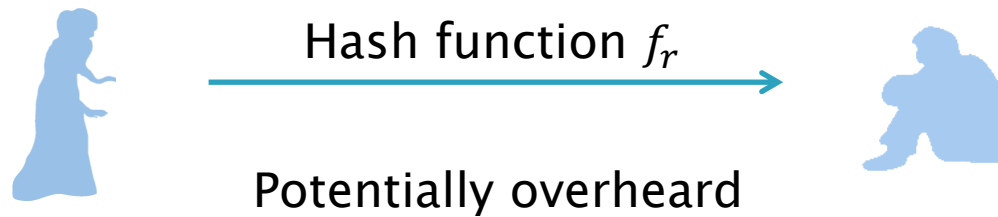


$X_1 X_2 X_3 X_4 \dots$

- 4. Parameter Estimation.** Alice randomly and independently decides whether to announce each output bit to Bob, doing so with probability μ (where $M\mu \gg 1$). Bob uses the communicated bits and his corresponding outputs to compute some test function (e.g. the CHSH value), and aborts if it lies outside a specified range.

Illustration of the attack

Assume a QKD protocol of the following form:



$$f_r(X_1X_3X_4\dots)$$

5. Alice and Bob perform **error correction** and **privacy amplification** by public discussion.

Illustration of the attack

- ▶ Suppose that we have a protocol of this form that is secure for one use.
- ▶ If the same devices are used to generate an additional key with the same protocol, then information about the first key can leak:
 - The parameter estimation step provides a channel from the devices to Eve, so raw data used from the first key can be leaked while generating the second.
 - The state distribution step provides a channel from Eve to the devices. This could be used to tell the devices the error-correction and privacy amplification functions used for the first key.
 - Abort/not abort provides a channel to Eve.

Illustration of the attack

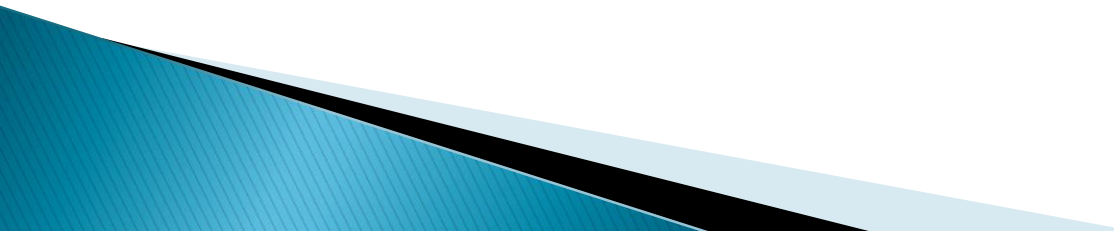
- ▶ Suppose Alice and Bob have used the devices once and generated a key.
 - ▶ They then reuse the devices for a second key.
 - ▶ I will show how Eve can gain bits of the first key while the second one is generated.
 - ▶ The attack is pretty simple, and can be performed essentially without detection.
- 

Illustration of the attack

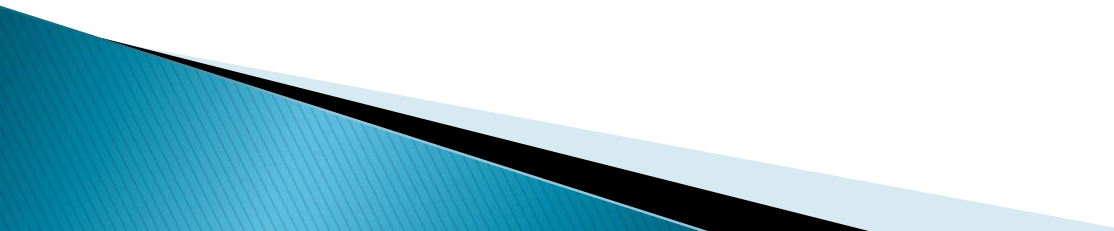
- ▶ The first key is generated following the protocol, i.e., Eve supplies the correct states and performs the correct measurements.
 - ▶ The devices are programmed to remember any data they have received, i.e. they know all their own inputs and outputs, but (if Alice and Bob perform the protocol correctly), nothing else.
 - ▶ When the second key is generated, Eve does the following
- 

Illustration of the attack

During state distribution, Eve also tells the devices the error correction and privacy amplification functions used for the first key.

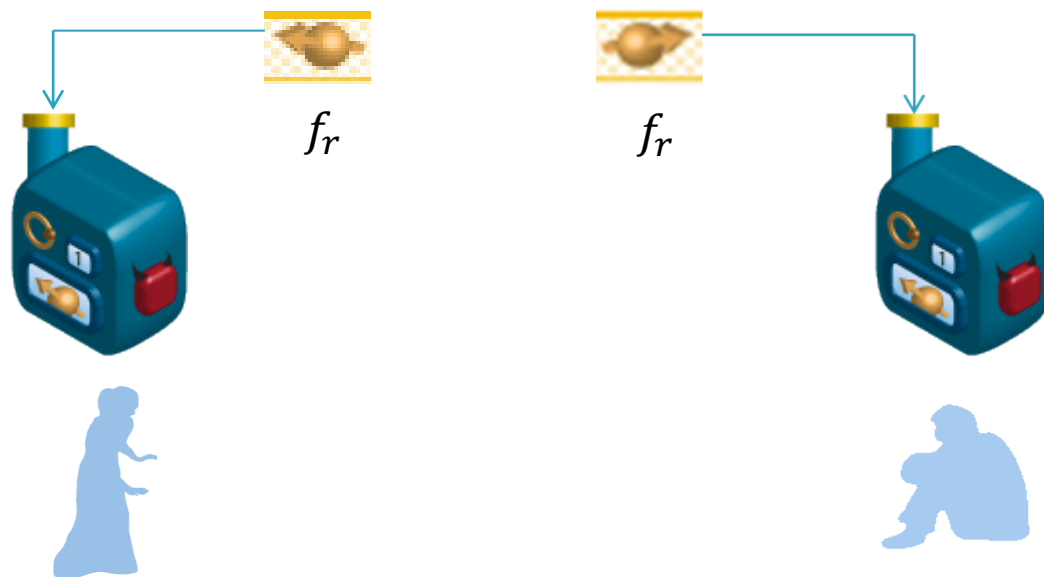
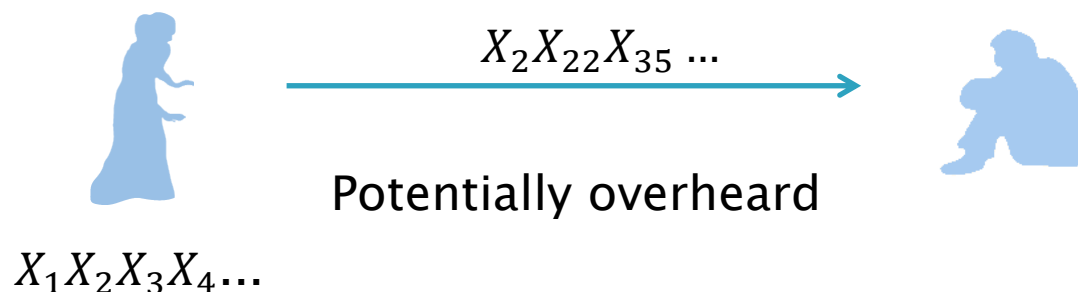


Illustration of the attack

- ▶ Alice's device can now internally compute the first key (it knows the raw string).
- ▶ During the generation of the second key, Alice's device substitutes genuine outputs with bits of the first key, e.g. X_2 could be the first bit.
- ▶ If these are transmitted in the parameter estimation phase of the protocol, they are directly leaked to Eve.




4. Alice randomly and independently decides whether to announce each output bit to Bob, doing so with probability μ (where $M\mu \gg 1$).

Other attacks

- ▶ For the attack I just presented, it is relatively easy to find a patch
- ▶ However, the specific attack is not so important, but rather the theoretical point that current protocols have this weakness.
- ▶ Other attacks are also presented in [arXiv:1201.4407](https://arxiv.org/abs/1201.4407)
- ▶ We also have some new ideas for how to construct a secure protocol that get around these in restricted scenarios. (some are already in the paper; another will appear in the next version)

Conclusions

- ▶ We have illustrated attacks that apply to device-independent quantum cryptography with no trust of devices when devices are reused.
 - ▶ There are existing security proofs of device-independent QKD protocols that show that the key is composable (in the sense that it can be used in any application).
 - ▶ However, the proofs do not cover the case where the devices used to generate it are reused. Some require many devices.
 - ▶ For all existing schemes, when extended to two devices, these attacks apply.
- 

Outlook

- ▶ In spite of these attacks, the device-independent model remains useful, and a promising way to reduce the assumptions required for quantum cryptography.
 - ▶ However, it needs new types of protocol and modified notions of composability
- 