Unconditionally secure device-independent quantum key distribution with only two devices

Roger Colbeck (ETH Zurich)

Based on joint work with Jon Barrett and Adrian Kent

Physical Review A **86**, 062326 (2012)

Outline

- Motivation for device-independence
- Brief History
- Recent developments
- Main result
- Remaining problems and open questions

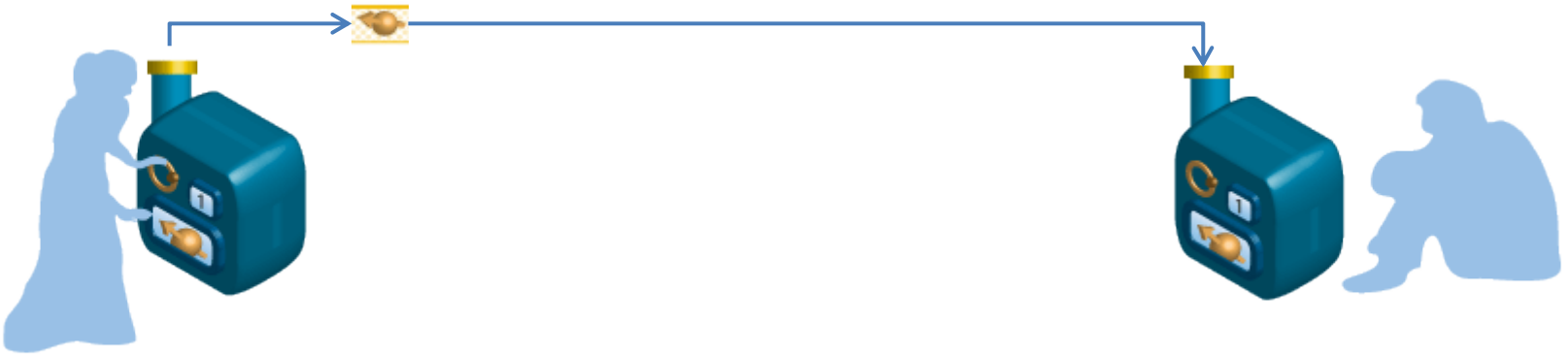
Two sides of cryptography

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…

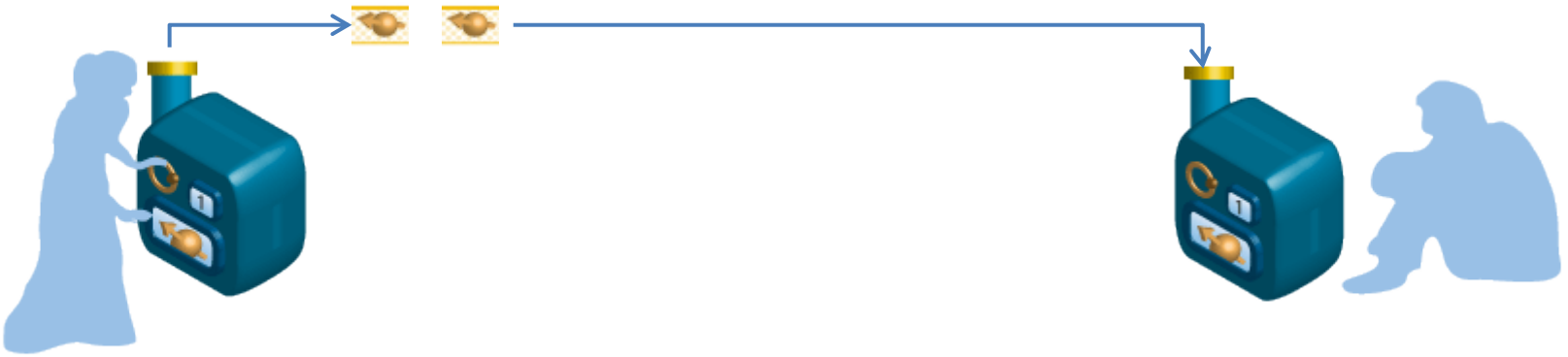
Practical

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

You must be joking ☺
What we can do is this…

Motivation

- Things can go wrong



- E.g. Alice's device may start sending multiple states
- If the protocol doesn't check this, then it is quickly rendered insecure
- Attacks exploiting the difference between real devices and how they are modelled are relevant in practice

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

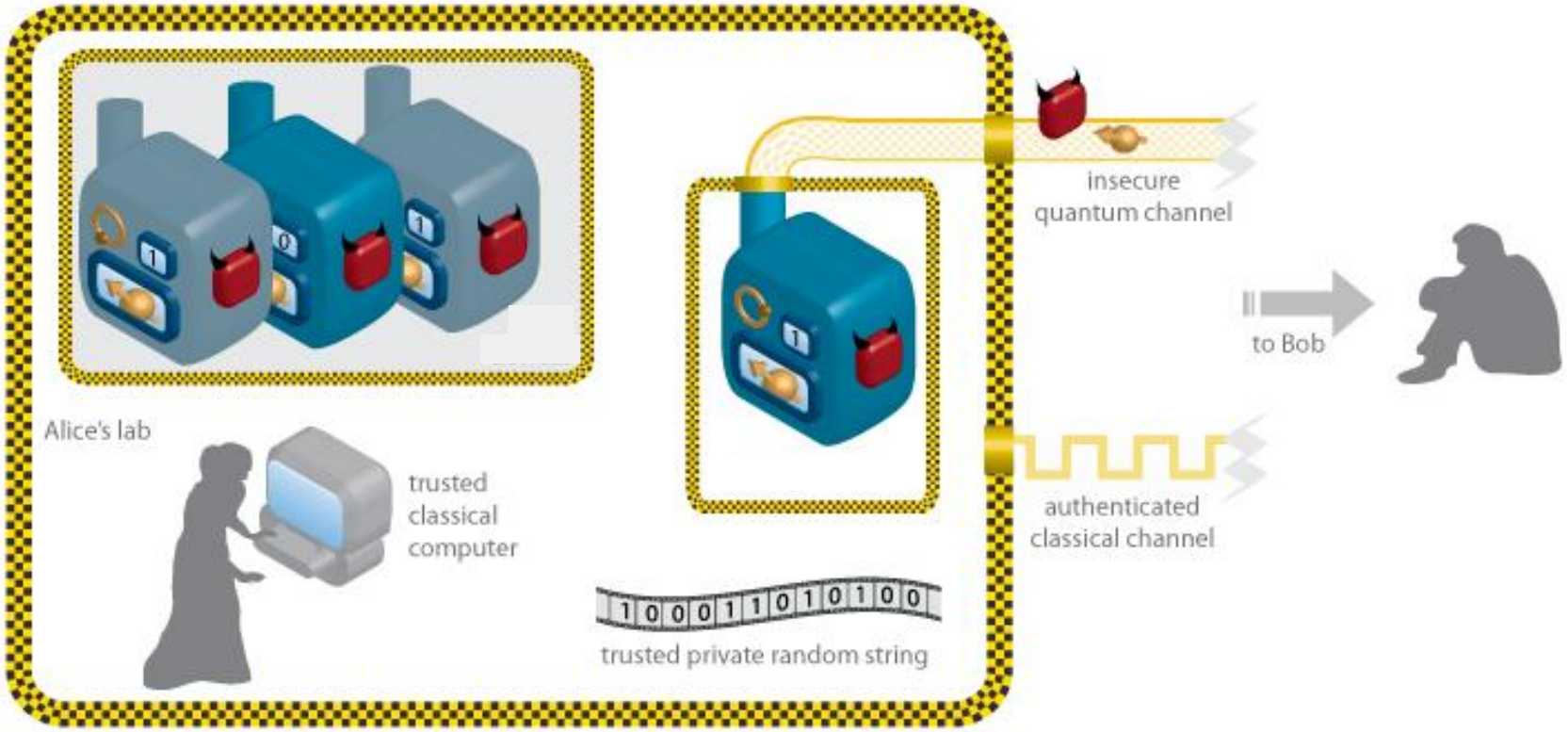
Motivation

- 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 quantum devices.
- Idea first introduced in [Mayers-Yao FOCS 98] and significantly developed in [AGM PRL **97**, 120405 (2006), Scarani et al. PRA **74**, 042339 (2006), …]

Device-independence

- No trust at all in any quantum devices used for the protocol.
- With device-independence, it wouldn’t matter if an adversary tampered with or substituted my devices: we would still have security.
- Clean, well-defined assumption
- Tests the devices during the protocol (if critical faults have developed, the protocol aborts)

Device-independence assumptions



Limitations of prior works

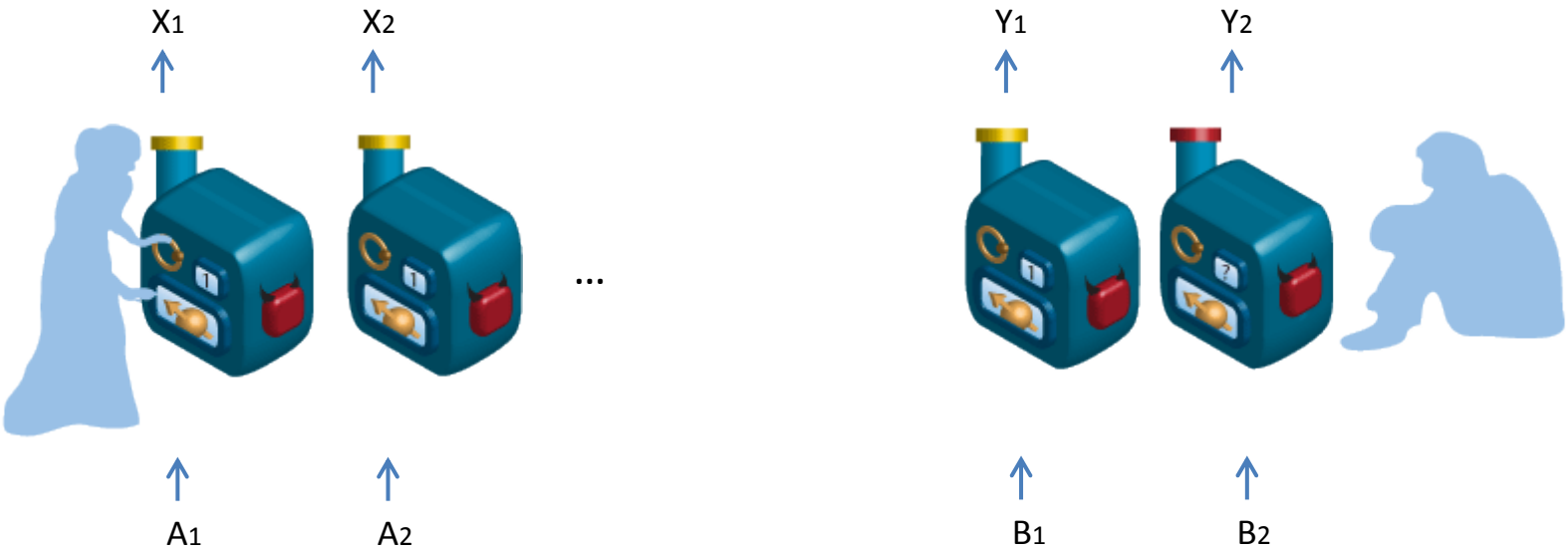
- Various protocols have been proven unconditionally secure with no trust on the devices, for example:
  - BHK, PRL **95**, 010503 (2005)
  - Masanes et al., quant-ph/0606049
  - HR, arXiv:1009.1833
  - MPA, N. Comms. **2**, 238 (2011)
- All have the weakness that the security proofs apply only with many separated devices

Recent developments

- 3 recent works show that this limitation can be removed (all at QIP13). Each uses a different technique to achieve security with only two devices.

Recent developments

- 3 recent works show that this limitation can be removed (all at QIP13). Each uses a different technique to achieve security with only two devices.



Old proofs

Recent developments

- 3 recent works show that this limitation can be removed (all at QIP13). Each uses a different technique to achieve security with only two devices.

New proofs

Our technique

- In the spirit of minimizing assumptions, our protocol is secure against a non-signalling (not necessarily quantum) adversary.
- Design the protocol in such a way that the optimal eavesdropping attack is i.i.d.
- Exploit a set of “super-strong” quantum correlations
- Correlations are monogamous in non-signalling sense.

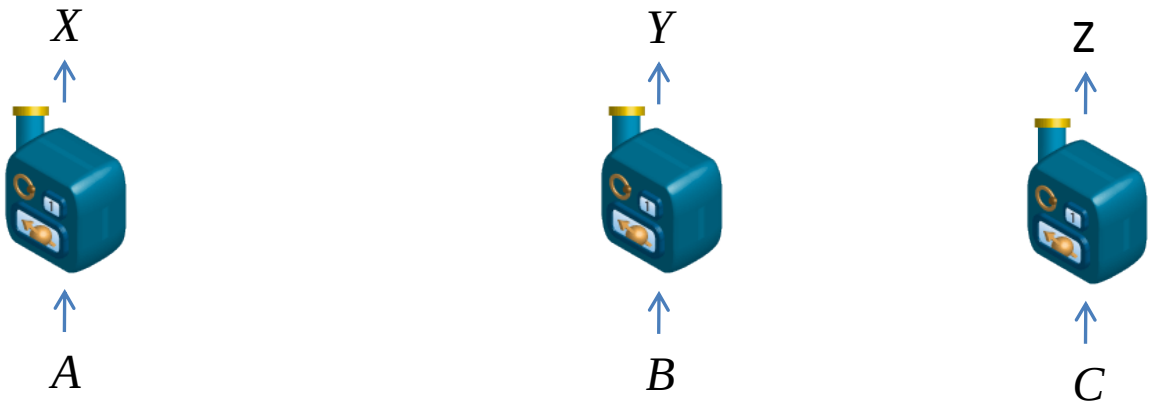
Our technique

- Non-signalling monogamy:

$P_{XY|AB}$ is the distribution from particular measurements on a maximally entangled state

Our technique

- Non-signalling monogamy:



$P_{XY|AB}$ is the distribution from particular measurements on a maximally entangled state

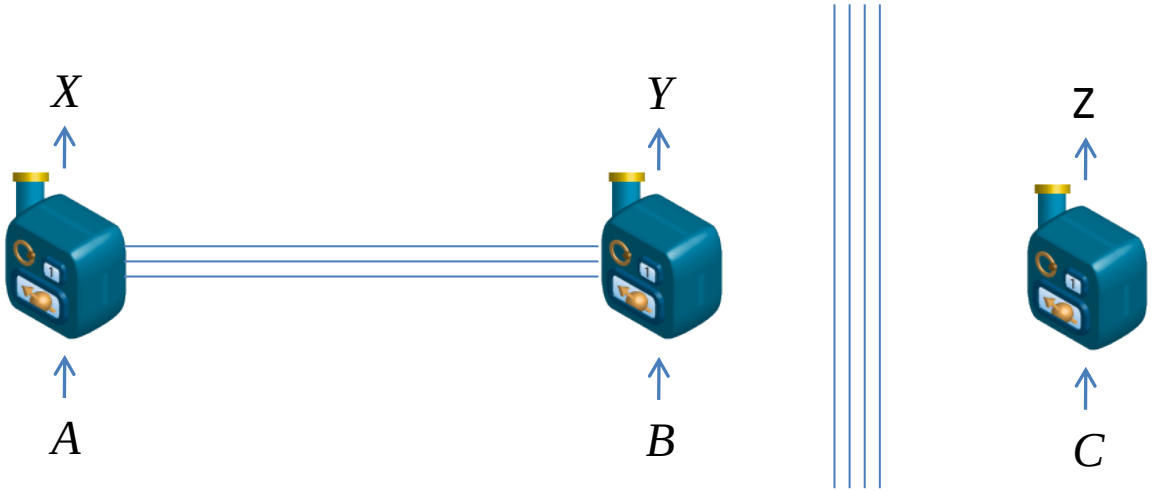
$P_{XYZ|ABC}$ non-signalling

Uniform distribution on X

$$P_{XZ|ABC} = P_{\bar{X}} \times P_{Z|ABC}$$

Our technique

- Non-signalling monogamy:



$P_{XY|AB}$ is the distribution from particular measurements on a maximally entangled state

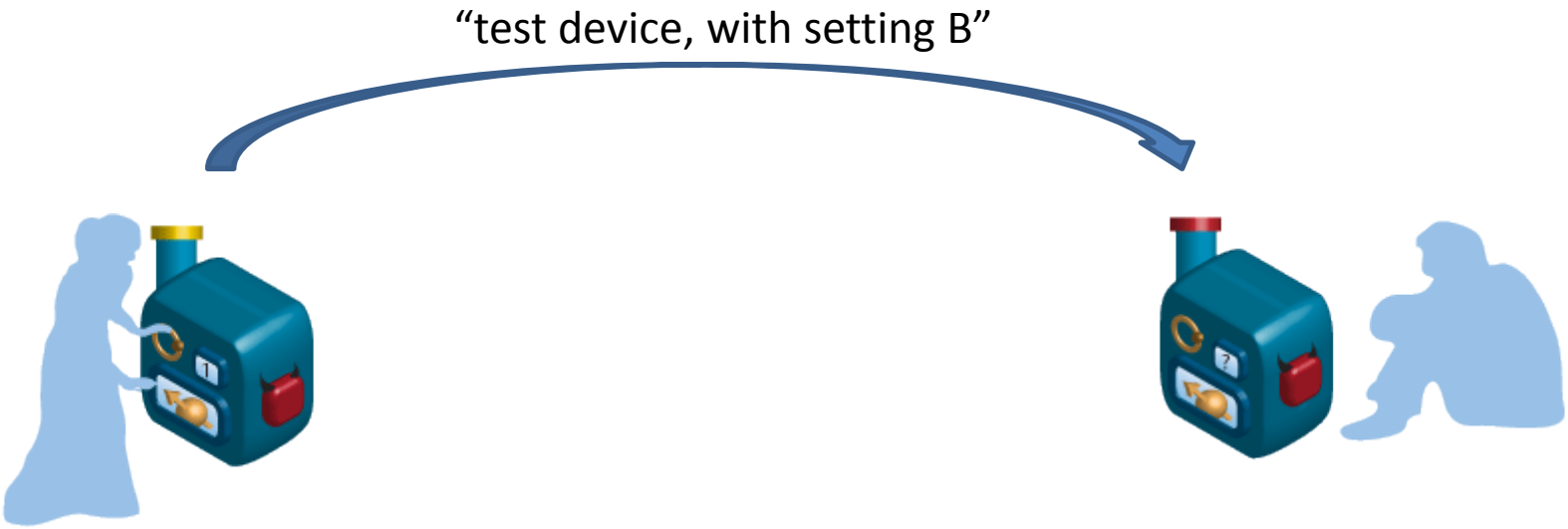
$P_{XYZ|ABC}$ non-signalling

Uniform distribution on X

$$P_{XZ|ABC} = P_{\bar{X}} \times P_{Z|ABC}$$

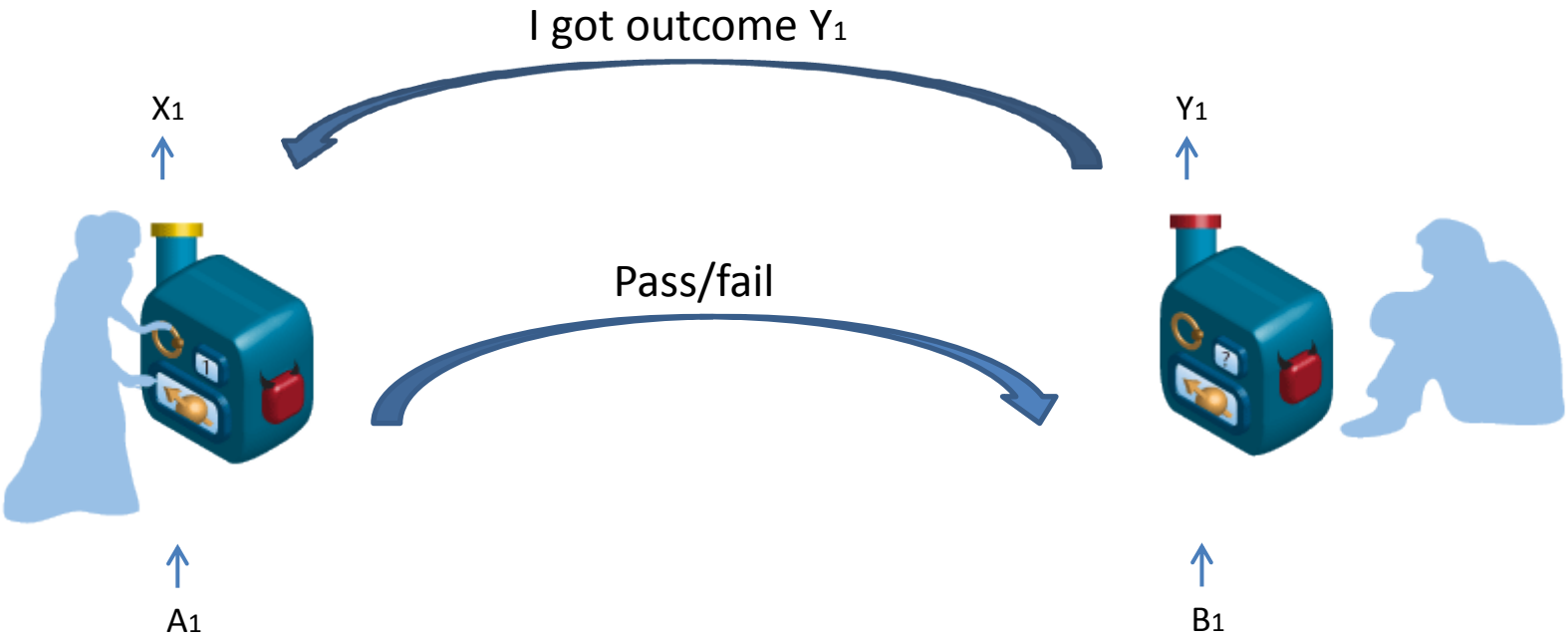
Our technique

- On each round, Alice randomly decides whether to test the devices (high probability) or to generate key (low probability).



Our technique

- On each round, Alice randomly decides whether to test the devices (high probability) or to generate key (low probability).



Our technique

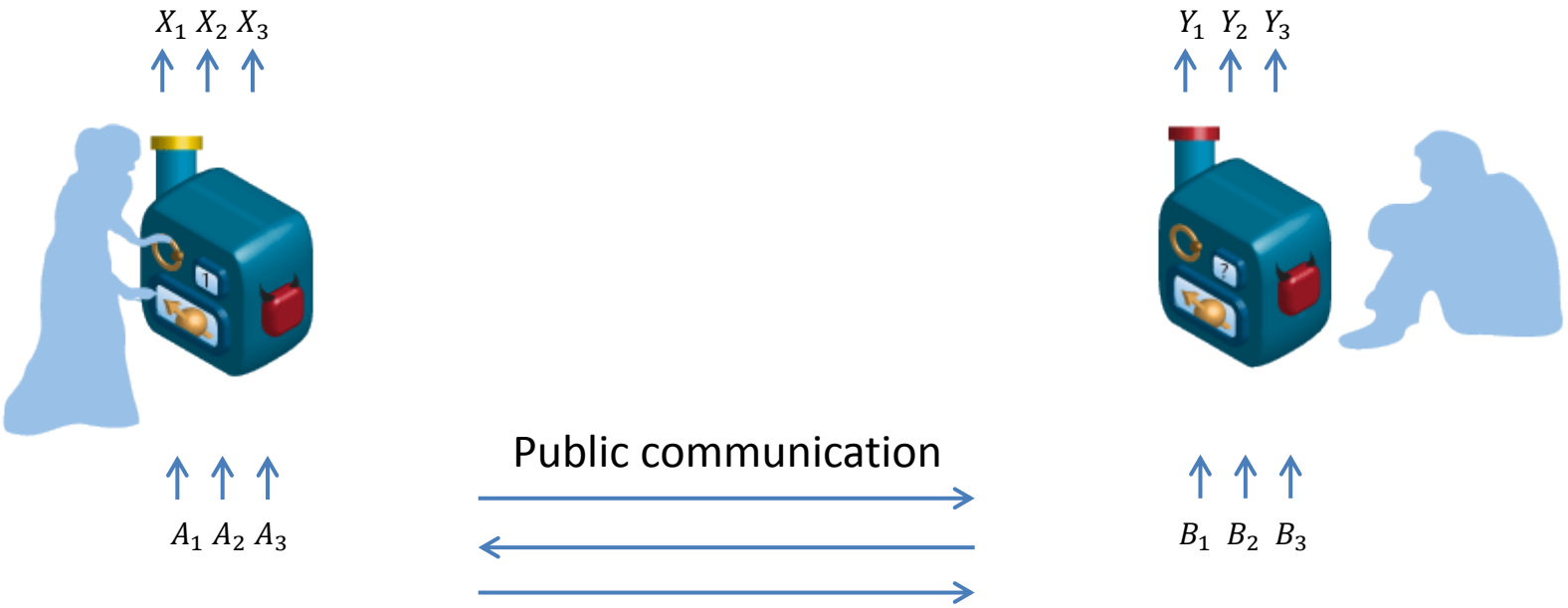
- If the test passes, the whole protocol repeats.
- We can strengthen Eve by giving the devices back to her before repeating the protocol
- Eventually, Alice will randomly choose to generate key, in which case, Alice and Bob both make measurements and take their outcomes to be key bits
- (Note that our protocol does not need privacy amplification).

Drawbacks of our protocol

- Inefficient and has low tolerance to noise (in contrast to previous talk)
- Although it allows device reuse within the same protocol, devices cannot be reused in future protocols
  - If the same (untrusted) devices are reused in future protocols, this can compromise previously generated keys [BCK PRL **110**, 010503 (2013)]

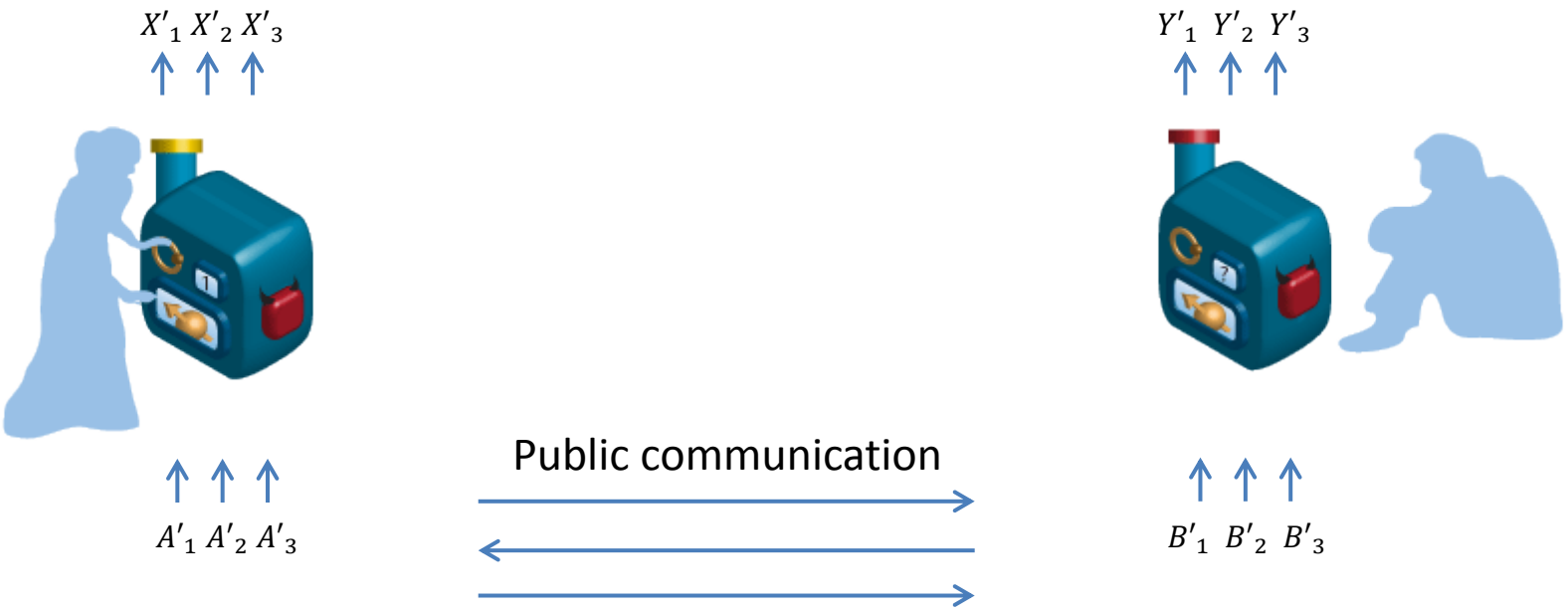
Device-reuse problem

- Consider a malicious device with memory and using it to generate a secure key



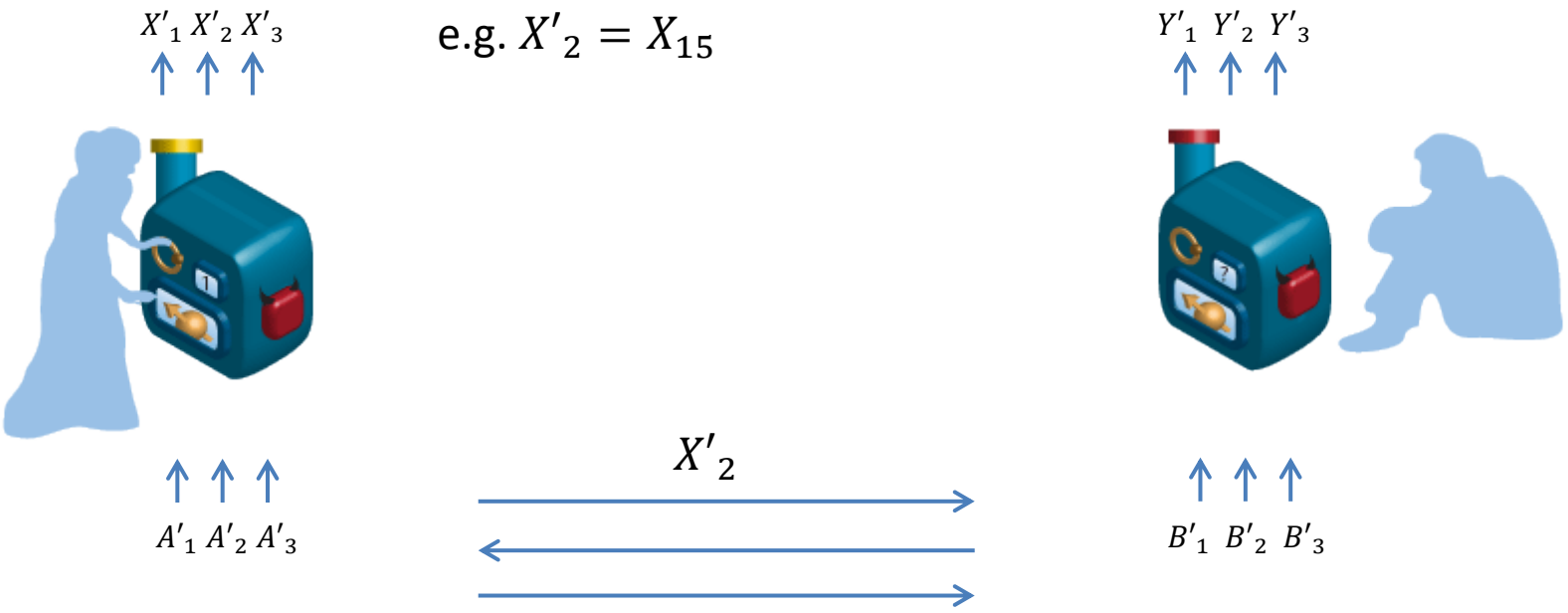
Device-reuse problem

- Reuse it to generate second key



Device-reuse problem

- Device with memory can re-output previous bits via a pre-agreed strategy



Device-reuse problem

- If a malicious device with memory is used to generate a secure key, it can leak data relevant to the first key and potentially compromise it

- This problem is present in all existing protocols

Open questions

- Prove security of a protocol that solves the problem of reusing untrusted devices in multiple protocols
- Need for new security notion
  - Universal device-reuse (reuse of untrusted devices in an arbitrary future application) is not possible
  - However, we think restricted device reuse is possible (reuse the devices only in certain ways)
- Are there efficient and noise tolerant protocols secure against non-signalling adversaries?