Tutorial: Device-independent Quantum Information Processing

Roger Colbeck (University of York)

Outline

- Explain what device-independence means
- Motivate its use
- Discuss the main ideas focussing on QKD
- Discuss what it means for a protocol to be secure
- Drawbacks of device-independence
- Related notions
- Other tasks we might want to do device-independently

What is device-independence?

- No knowledge/assumptions about how certain components work
- In the past it has also been called self-testing
- Another word for it is trustworthy (in contrast to trusted)

Cryptographic scenarios in which we might want to use it

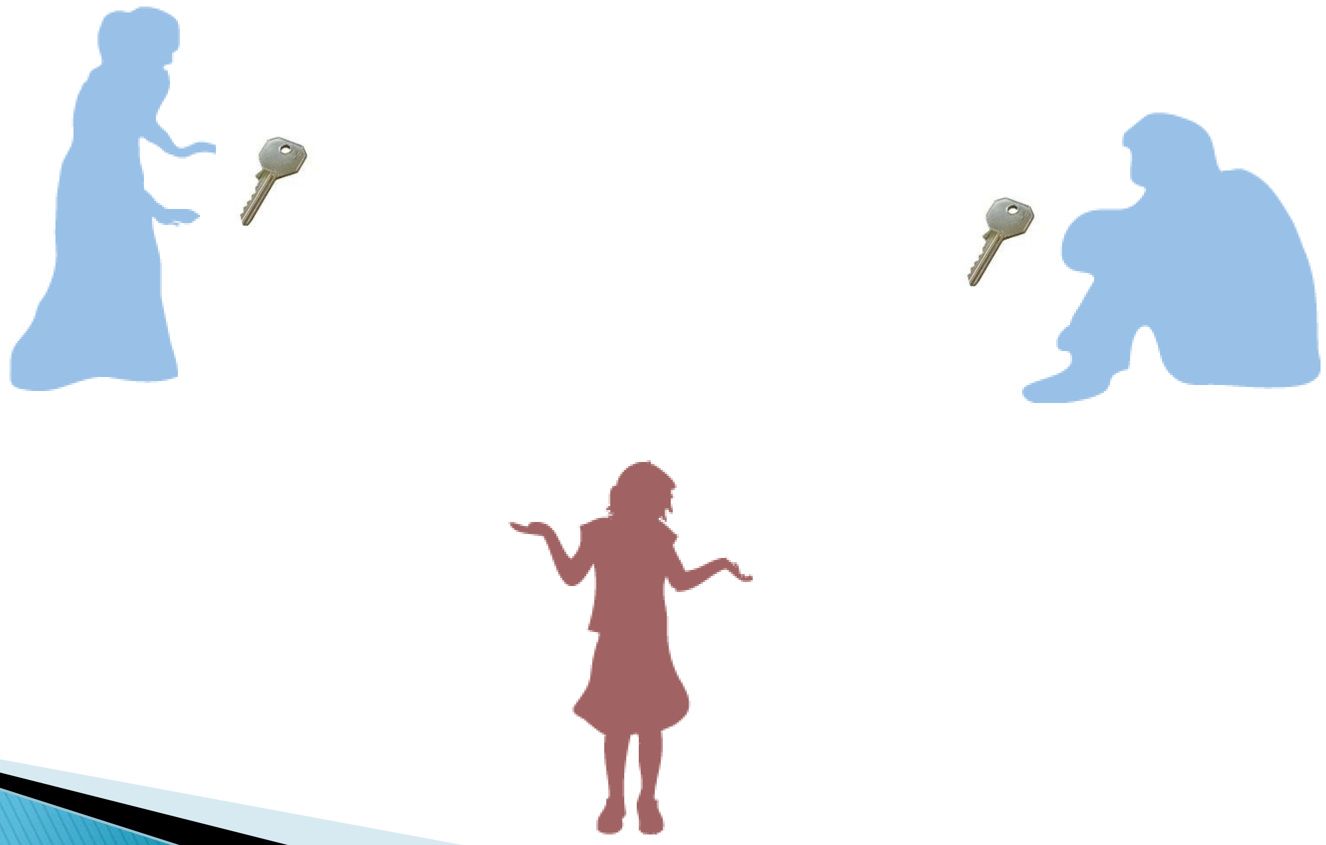
- Key distribution

- Randomness expansion/amplification

- Verified quantum dynamics/delegated computation

Focus on key distribution

Focus on key distribution



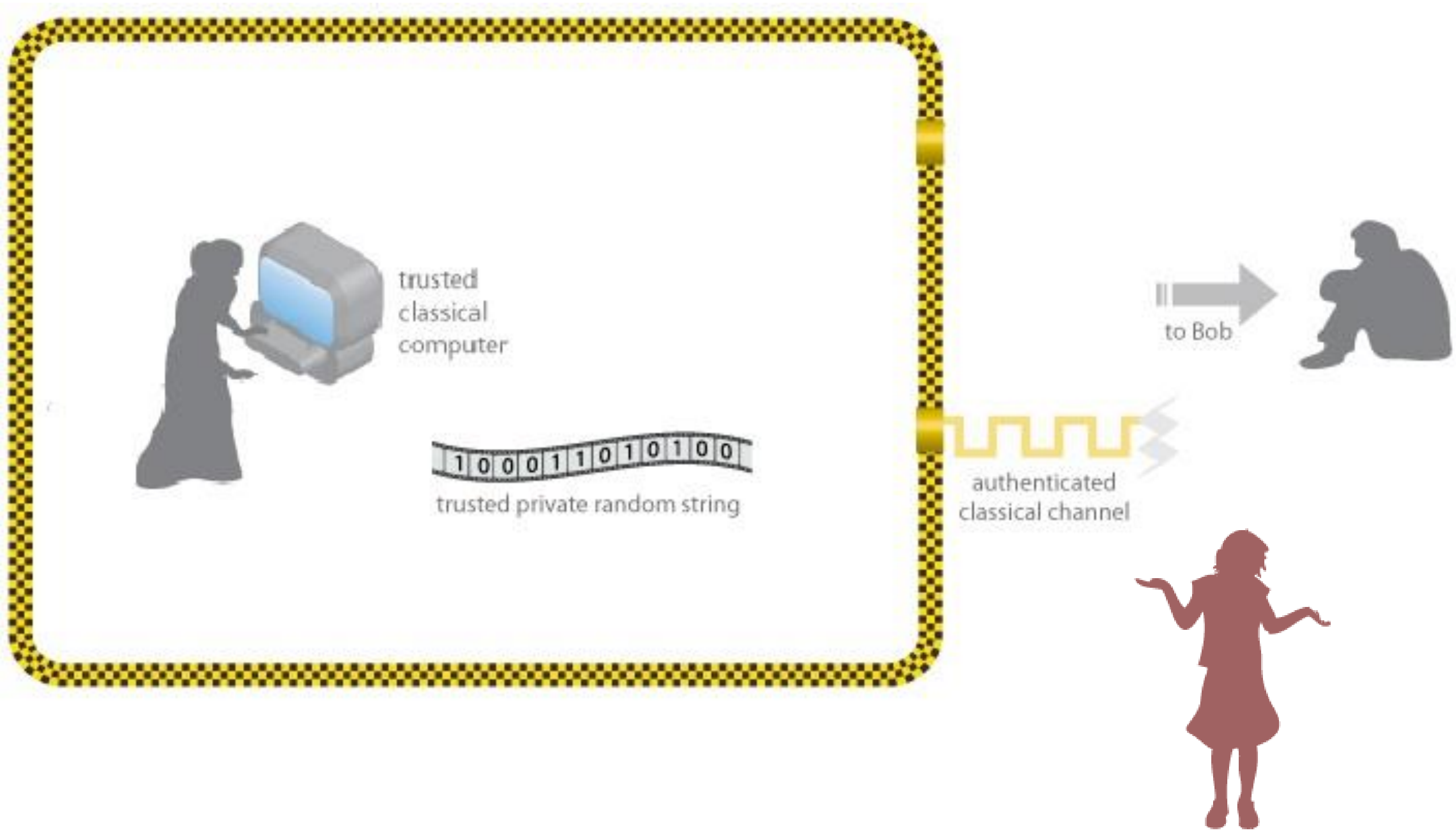
What do we want in a cryptosystem?

- Secure
- Reliable
- Easy to implement
  - Technologically feasible
  - Requires few devices
- Have a fast rate
- Long distance (size of Earth)

Security

- Protocol should come with a rigorous, precisely formulated security proof and statement of validity
  - E.g., if the protocol is used correctly, then no adversary can break it given unlimited time/resources (unless physics is wrong)
  - Or: Given current technology, it will take an adversary at least 150 years to break.

The setup (classical)

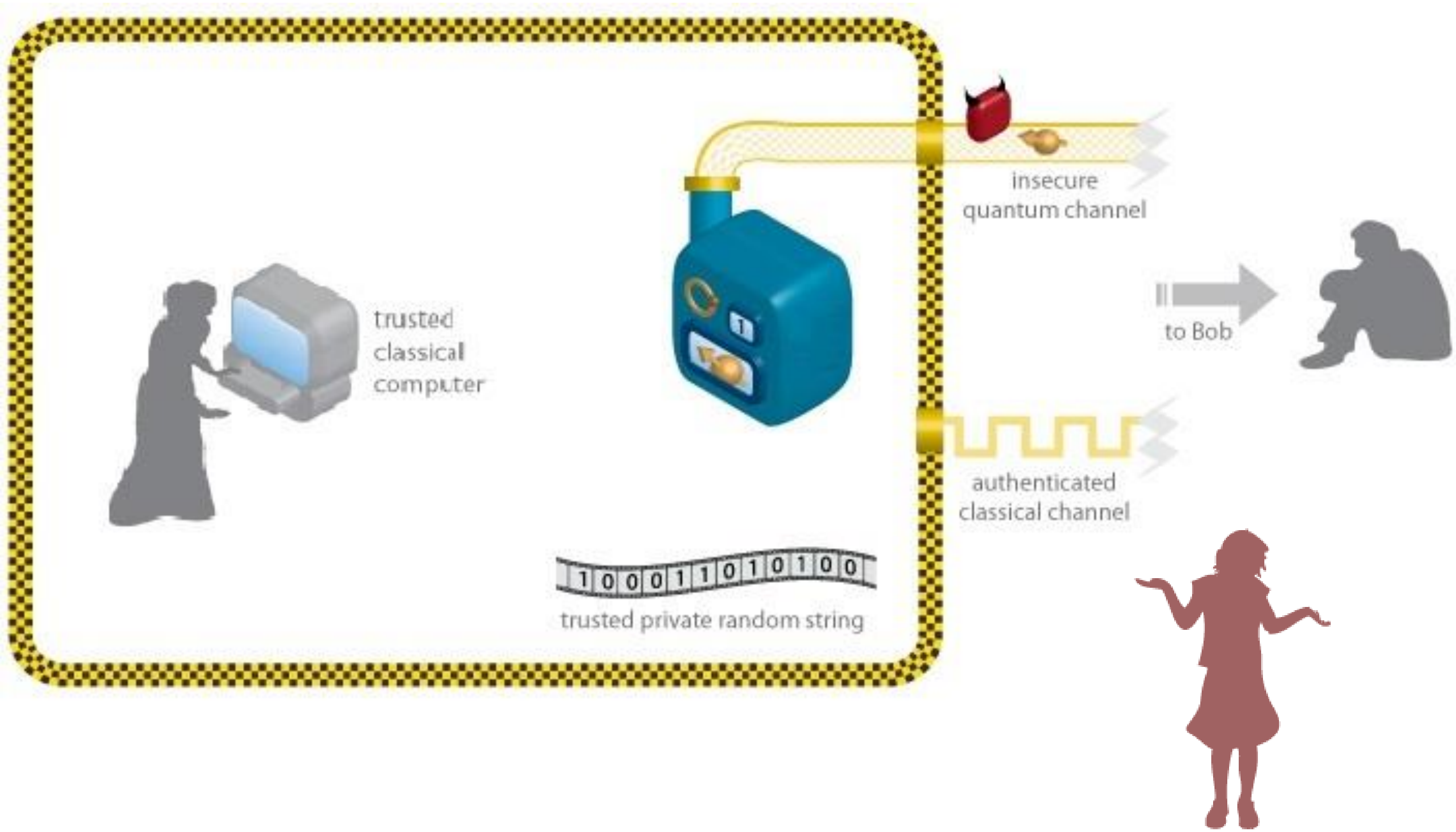


The setup (classical)

Drawbacks:

- Cannot have unconditional security (Eve limited only by physics within setup)
- Cannot even prove hardness of hacking in general
- For some protocols, quantum computers would allow a fast hack

The setup (quantum)



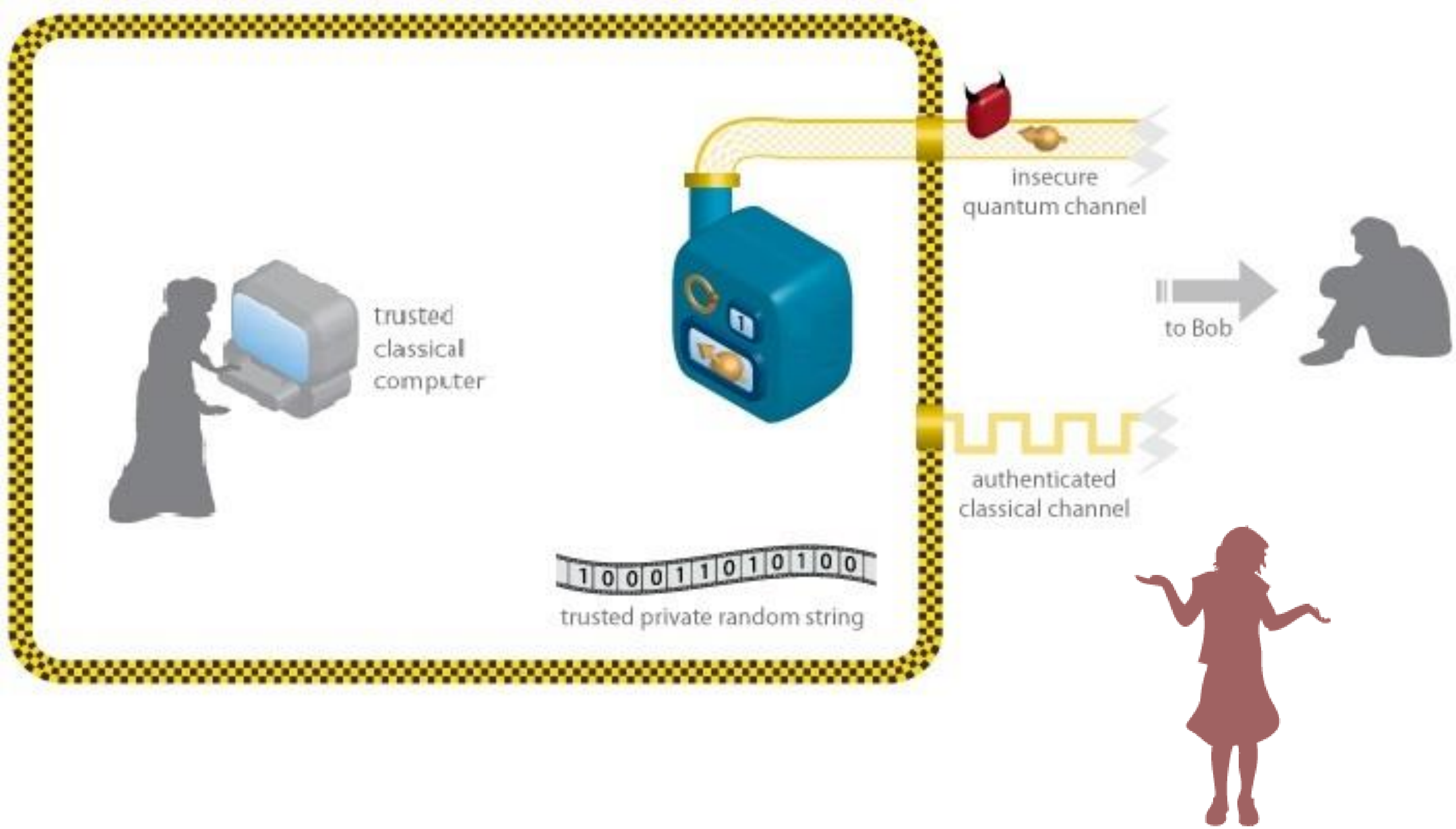
The setup (quantum)

Removes classical drawbacks; in particular, can have unconditional security.

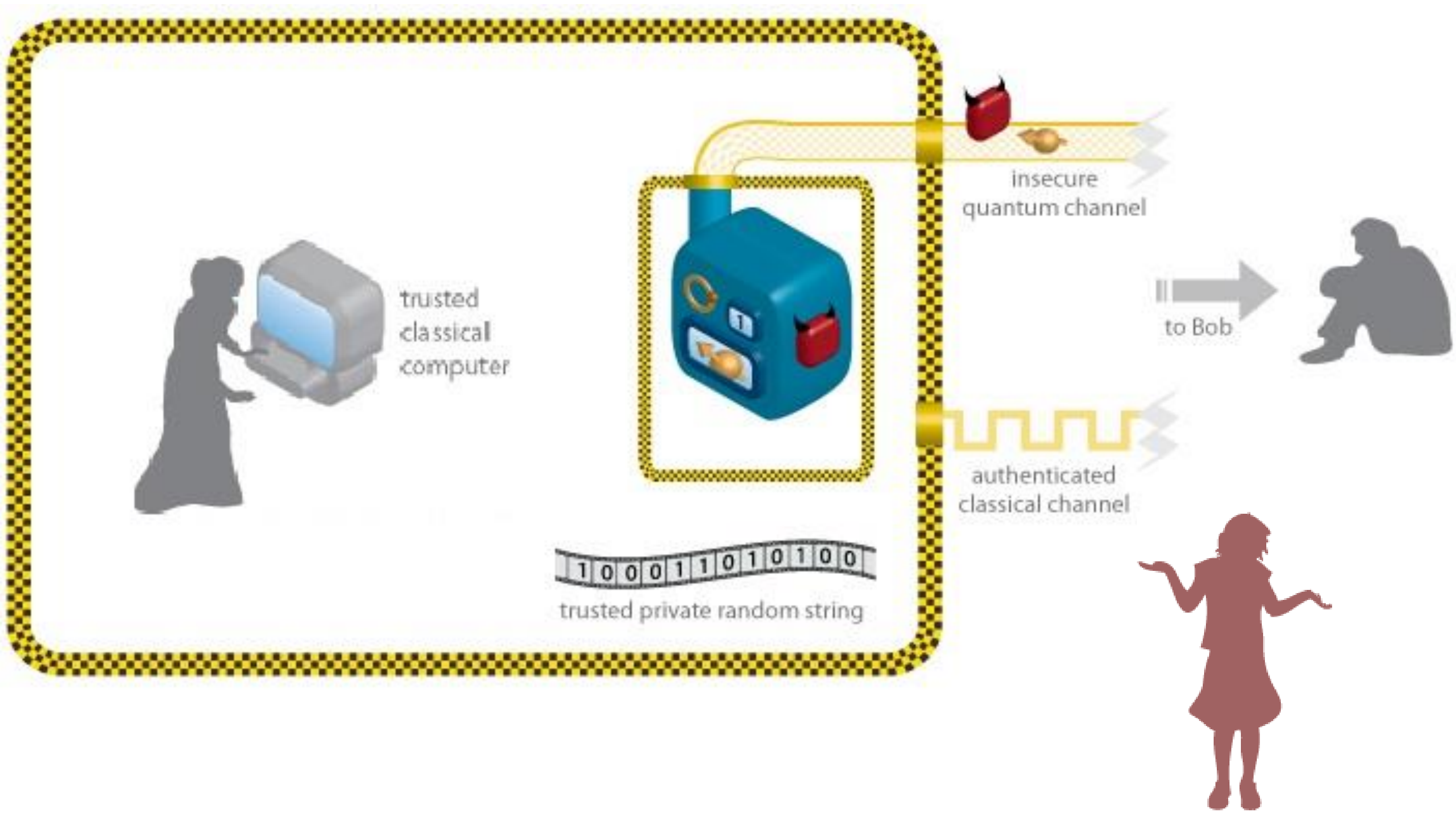
New drawbacks:

- Technologically harder to implement
- Security relies on the devices behaving as modelled in the security proof

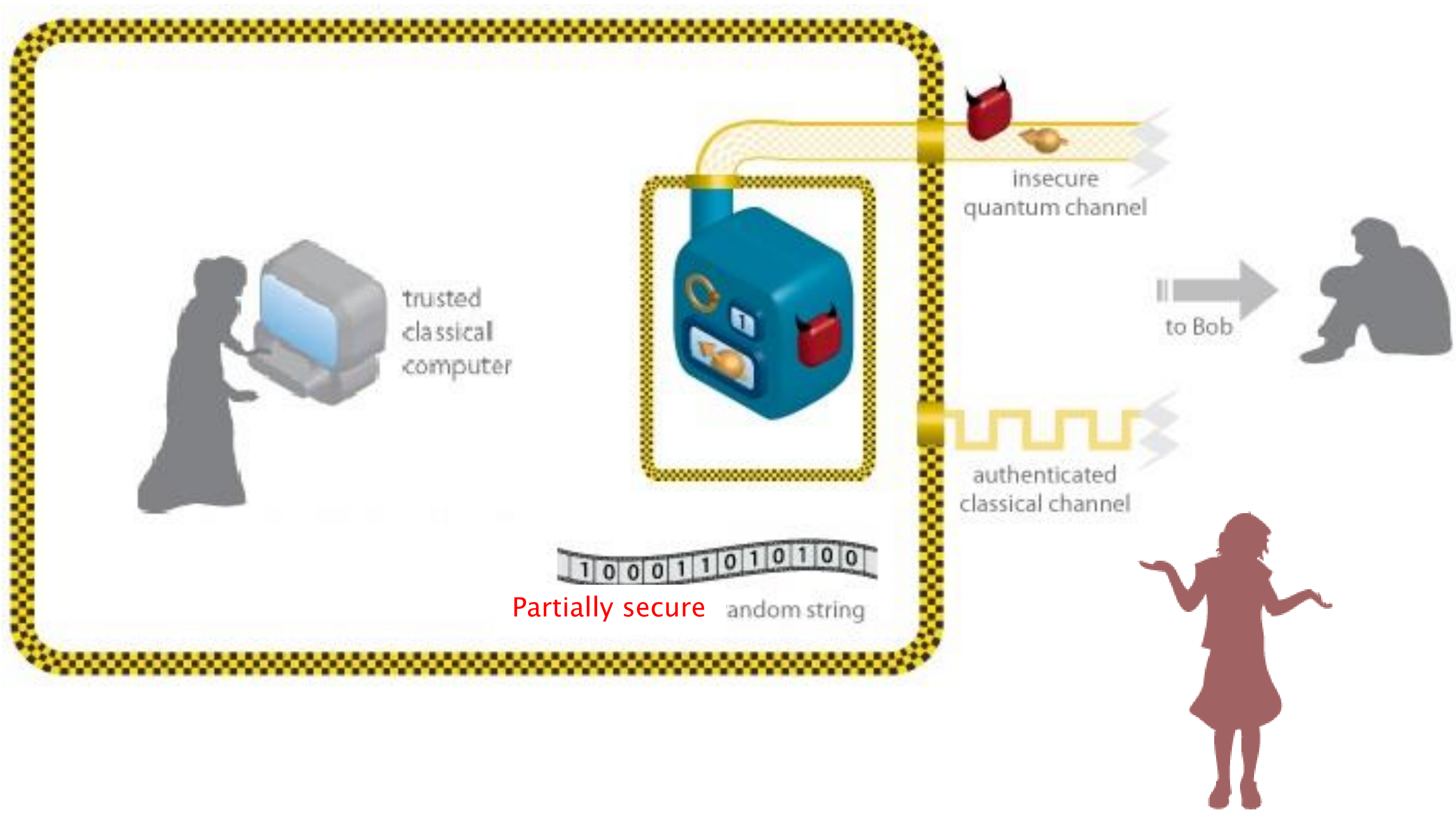
The setup (quantum)



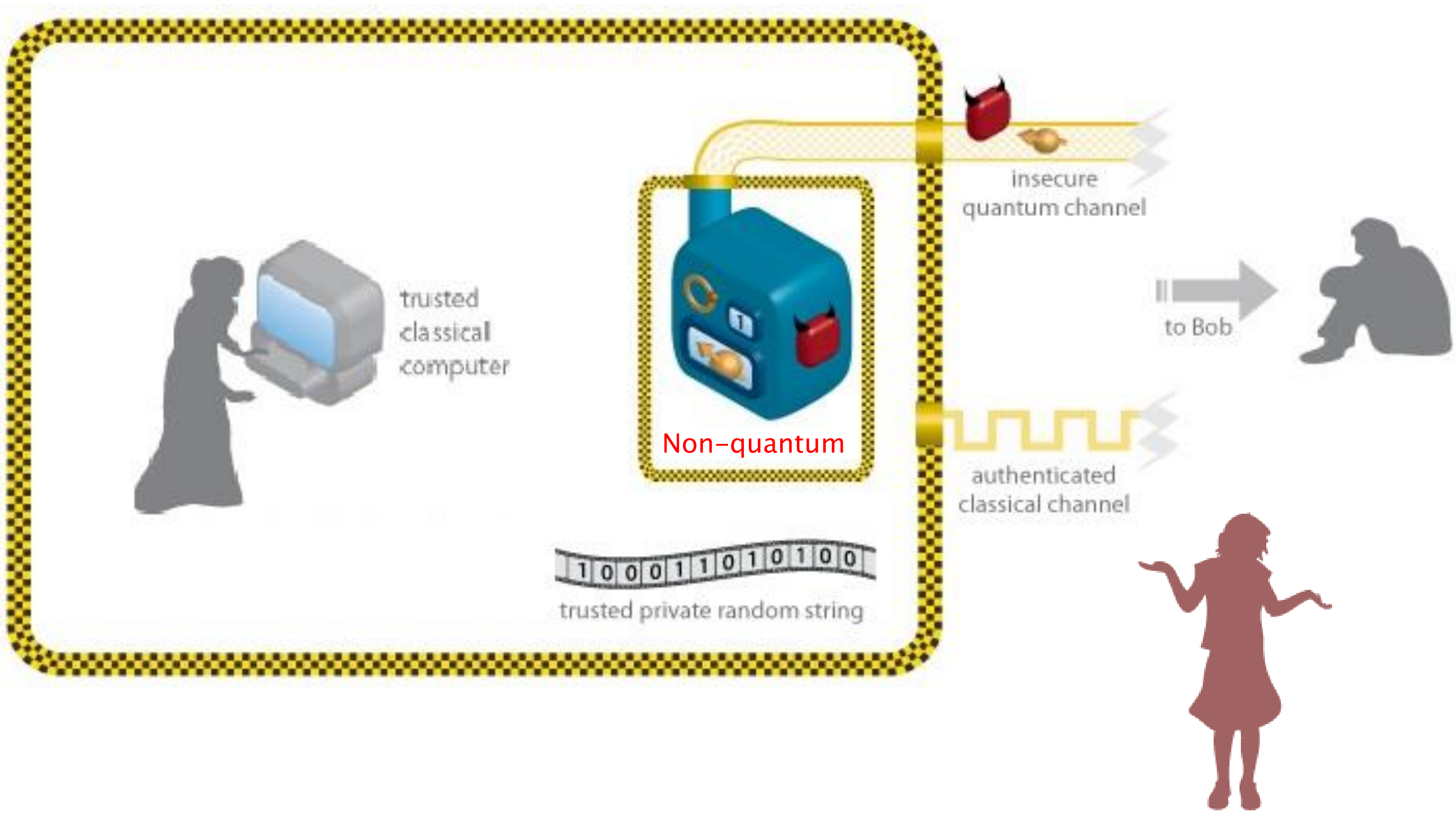
The setup (device-independent)



Various other scenarios



Various other scenarios



Device-independence

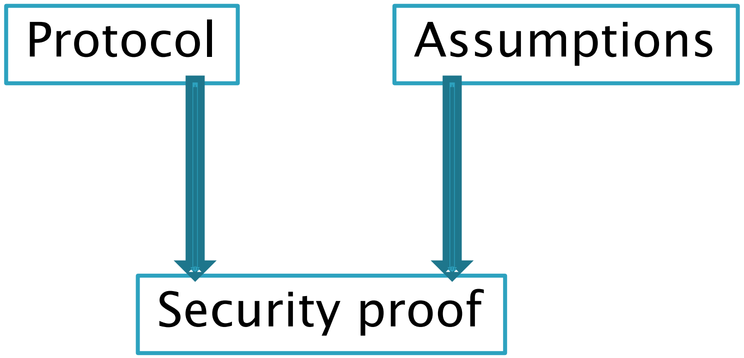
- No assumptions made about the workings of the devices used.
- However, we do need some assumptions, in particular, both strong lab walls and initial randomness [necessary for cryptography]

Motivation

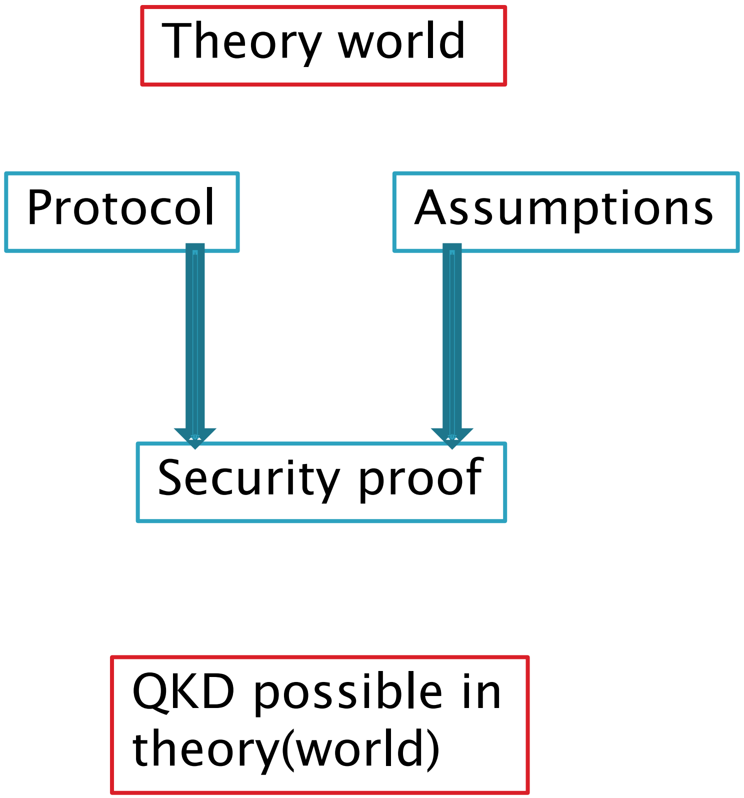
- We have secure QKD protocols, like BB84: why do we need device-independence?

- Why stop trusting the device?

Security proofs



Security proofs



Security proofs

Theory world

Protocol

Assumptions

Security proof

QKD possible in theory(world)

Real world

Is our theory world proof relevant in the real world?

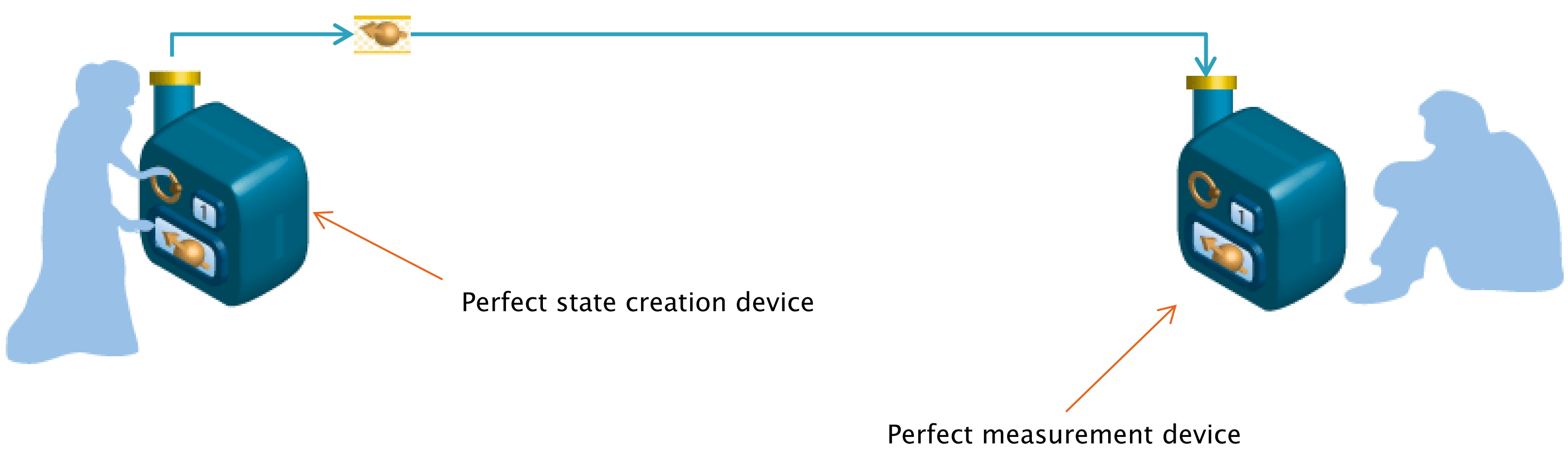
Security proofs

- Require precise set of assumptions

Security proofs

- Require precise set of assumptions
  - Easy to come up with precise assumptions

    E.g. Have perfect single photon emitters and detectors that can measure single photons in any basis



Security proofs

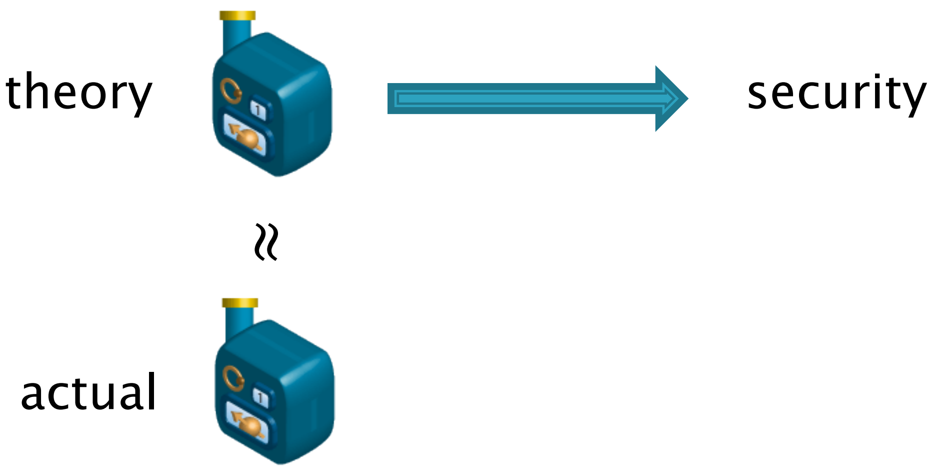
- Require precise set of assumptions
  - Easy to come up with precise assumptions

    E.g. Have perfect single photon emitters and detectors that can measure single photons in any basis

  - Difficult to make realistic: needs highly detailed specification of the physics of the device – very complicated.

Security proofs

- Mismatch between the modelling and reality can lead to exploitable security flaws.
- Hacking attacks have highlighted this*.



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

Security proofs

- Mismatch between the modelling and reality can lead to exploitable security flaws.
- Hacking attacks have highlighted this*.
- 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 devices.

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

Security proofs

Weaker assumptions → More security

Security proofs

Weaker assumptions $\longrightarrow$ More security

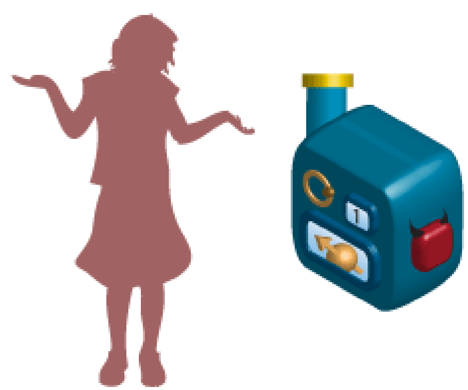
- Device-independence tries to remove all the assumptions on the devices

- Removes this mismatch problem between the real world and theory world

Security proofs

Weaker assumptions → More security

- No assumptions on devices means the security proof has to work even with maliciously constructed devices.



Security proofs

Weaker assumptions $\longrightarrow$ More security

- Protocol remains secure if devices fail or are tampered with

- Protocol checks the workings of the devices on-the-fly (hence, self-testing)

Device-independence

- Security proofs based on weaker assumptions give more real-world security
- DI protocols effectively check working of devices "on-the-fly": prevents accidental errors
- Alternative is hack-and-patch approach to achieve improved practical security

Device-independence: main ideas

Device-independence: main ideas

- Want to test the devices

$X_1, X_2, \ldots$

$A_1, A_2, \ldots$

$f(A_1, A_2, \ldots, X_1, X_2, \ldots) \in \{\text{pass, fail}\}$

Adversary knows f
Adversary may possess a system that is entangled with the device

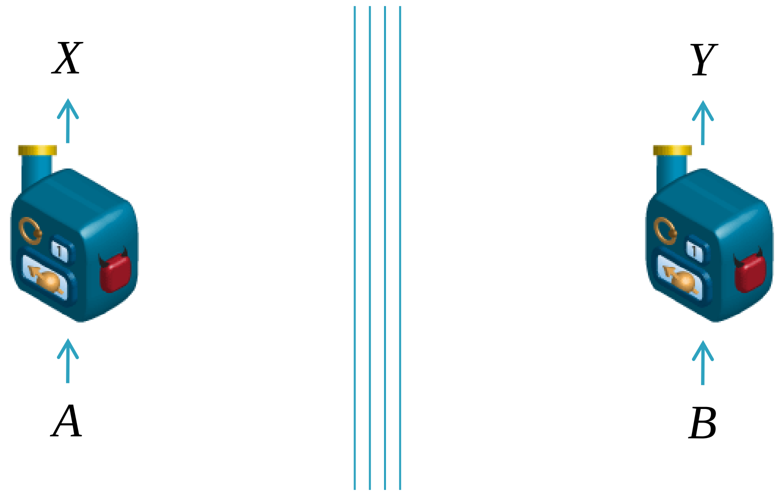
Device-independence: main ideas

Bell inequality violation → Non-classical behaviour

(loophole-free)

Device-independence: main ideas

- Bell-inequality violation



$P_{XY|AB}$ violates a Bell inequality
A and B random
Devices cannot communicate

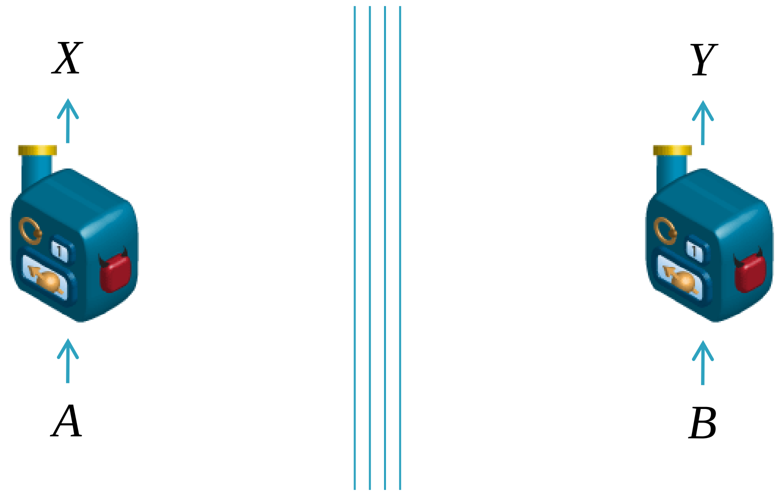
Bell's theorem

Eve cannot know X

Roughly the idea of Ekert 91

Device-independence: main ideas

- Bell-inequality violation



$P_{XY|AB}$ violates a Bell inequality
A and B random
Devices cannot communicate

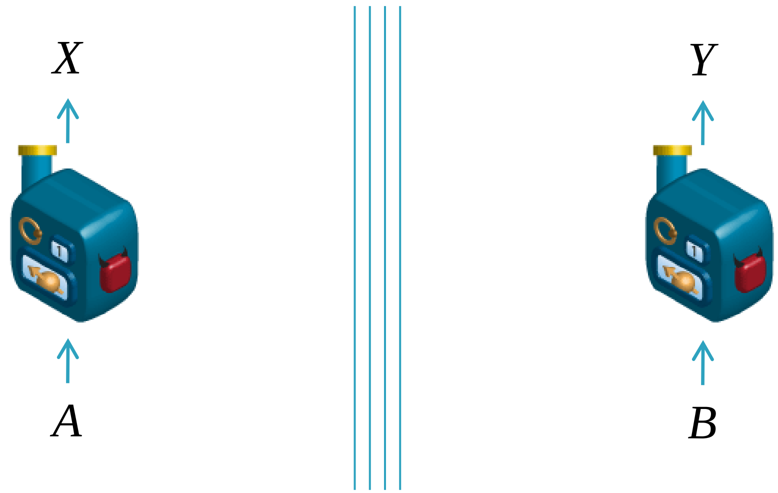
Bell's theorem

Eve cannot know X

- Doesn't mean that X is perfectly secret
- Nor that $X = Y$

Device-independence: main ideas

- Bell-inequality violation



$P_{XY|AB}$ violates a Bell inequality
A and B random
Devices cannot communicate

Bell's theorem

Eve cannot know X

- E.g. CHSH game winning probability

Device-independence: main ideas

- CHSH game

$X \in \{0,1\}$

$A \in \{0,2\}$

$Y \in \{0,1\}$

$B \in \{1,3\}$

Win if
$X = Y$ for $(\mathrm{A},\mathrm{B}) = (0,1), (2,1)$ or $(2,3)$
$X \neq Y$ for $(A,B) = (0,3)$.

- $P_{cl} \leq \frac{3}{4}$ $\qquad$ $P_{qm} \leq \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.85.$

(Bell value 2) $\qquad$ (Bell value $2\sqrt{2}$)

Device-independence: main ideas

$X \in \{0,1\}$

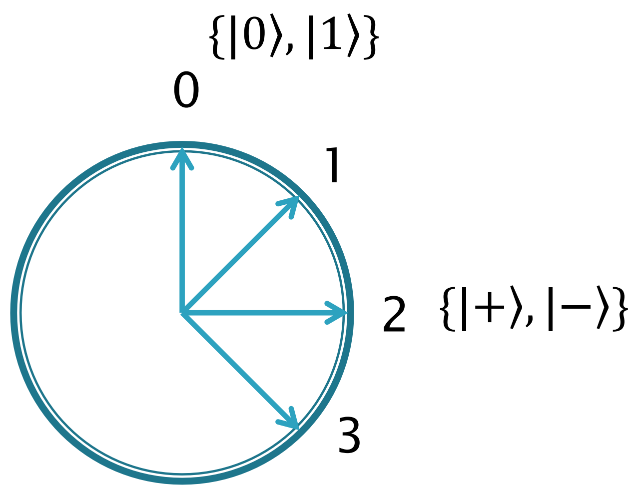
$A \in \{0,2\}$

$Y \in \{0,1\}$

$B \in \{1,3\}$

Win if
$X = Y$ for $(\mathrm{A},\mathrm{B}) = (0,1), (2,1)$ or $(2,3)$
$X \neq Y$ for $(A, B) = (0,3)$.

- $P_{qm} \leq \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.85$



$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Device-independence: main ideas

Maximum quantum violation $\Rightarrow$ Alice and Bob share max entangled (pure) state

$\Downarrow$

No entanglement with Eve

$$|\psi\rangle_{AB} \otimes |\phi\rangle_E$$

$\Rightarrow$ Eve has no information about Alice's and Bob's outcomes
Alice and Bob are correlated

$\Downarrow$

Alice and Bob can generate key secure against Eve

Device-independence: main ideas

Near maximum quantum violation

Alice and Bob share state close to max entangled

Almost unentangled with Eve

Eve has almost no information about outcomes
Alice and Bob correlated

Alice and Bob can generate key secure against Eve

Device-independence: main ideas

Near maximum quantum violation

$\Downarrow$

Eve has almost no information about outcomes
Alice and Bob correlated

$\Downarrow$

Alice and Bob can generate key secure against Eve

Proof ingredients

- Protocol acts like a filter: for a significant probability of not aborting, the devices must have a large Bell inequality violation almost every time.
- Large Bell inequality violations implies difficulty for Eve to guess.
- If Eve cannot guess the output well, then we can compress the string to one she cannot guess at all. [privacy amplification]

Connecting Bell violation with Eve's knowledge

$P_{XY\|AB}$	B	1		3	
	Y	0	1	0	1
A	X				
0	0	$\frac{1}{2}-\varepsilon$	ε	ε	$\frac{1}{2}-\varepsilon$
	1	ε	$\frac{1}{2}-\varepsilon$	$\frac{1}{2}-\varepsilon$	ε
2	0	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$	ε
	1	ε	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$

$$P_{\text{win}} = 1 - 2\varepsilon$$

How much can Eve know about X?

Connecting Bell violation with Eve's knowledge

$P_{XY\|AB}$	B	1		3	
	Y	0	1	0	1
A	X				
0	0	$\frac{1}{2}-\varepsilon$	ε	ε	$\frac{1}{2}-\varepsilon$
	1	ε	$\frac{1}{2}-\varepsilon$	$\frac{1}{2}-\varepsilon$	ε
2	0	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$	ε
	1	ε	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$

$$P_{\text{win}} = 1 - 2\varepsilon$$

How much can Eve know about X?

$$P_{XY|AB} = \sum_z p_z P_{XY|ABz}$$

Convex combination

Quantum-realizable distributions

Connecting Bell violation with Eve's knowledge

$P_{XY\|AB}$	B	1		3	
	Y	0	1	0	1
A	X				
0	0	$\frac{1}{2}-\varepsilon$	ε	ε	$\frac{1}{2}-\varepsilon$
	1	ε	$\frac{1}{2}-\varepsilon$	$\frac{1}{2}-\varepsilon$	ε
2	0	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$	ε
	1	ε	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$

$$P_{\text{win}} = 1 - 2\varepsilon$$

How much can Eve know about X?

$$P_{XY|AB} = \sum_z p_z P_{XY|ABz}$$

Convex combination

Any non-signalling distribution

Connecting Bell violation with Eve's knowledge

$P_{XY\|AB}$	B	1		3	
	Y	0	1	0	1
A	X				
0	0	$\frac{1}{2}-\varepsilon$	ε	ε	$\frac{1}{2}-\varepsilon$
	1	ε	$\frac{1}{2}-\varepsilon$	$\frac{1}{2}-\varepsilon$	ε
2	0	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$	ε
	1	ε	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$

$$P_{\text{win}} = 1 - 2\varepsilon$$

How much can Eve know about X?

$$P_{XY|AB} = \sum_z p_z P_{XY|ABz}$$

Convex combination

Any non-signalling distribution

$$P_{XY|AB} = (1-4\varepsilon)\left[\begin{array}{cc|cc} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \hline \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \end{array}\right] + \varepsilon\left(\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] + \left[\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right] + \left[\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right] + \left[\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right]\right)$$

Eve has no knowledge about X

Eve knows X perfectly

Connecting Bell violation with Eve's knowledge

$P_{XY\|AB}$	B	1		3	
	Y	0	1	0	1
A	X				
0	0	$\frac{1}{2}-\varepsilon$	ε	ε	$\frac{1}{2}-\varepsilon$
	1	ε	$\frac{1}{2}-\varepsilon$	$\frac{1}{2}-\varepsilon$	ε
2	0	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$	ε
	1	ε	$\frac{1}{2}-\varepsilon$	ε	$\frac{1}{2}-\varepsilon$

$$P_{\text{win}} = 1 - 2\varepsilon$$

How much can Eve know about X?

$$P_{XY|AB} = \sum_z p_z P_{XY|ABz}$$

Convex combination

Any non-signalling distribution

$$P_{XY|AB} = (1-4\varepsilon)\begin{array}{|cc|cc|}\hline \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \hline \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \hline \end{array} + \varepsilon\left(\begin{array}{|cc|cc|}\hline 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline \end{array} + \begin{array}{|cc|cc|}\hline 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline \end{array} + \begin{array}{|cc|cc|}\hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \hline \end{array} + \begin{array}{|cc|cc|}\hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline \end{array}\right)$$

Eve has no knowledge about X

Eve knows X perfectly

Non-signalling Eve can guess X with probability

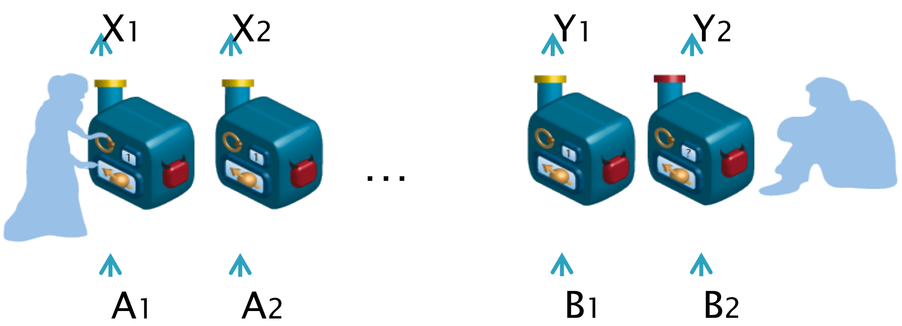
$$4\varepsilon + \frac{1}{2}(1-4\varepsilon) = \frac{1}{2} + 2\varepsilon$$

Device-independent QKD proofs

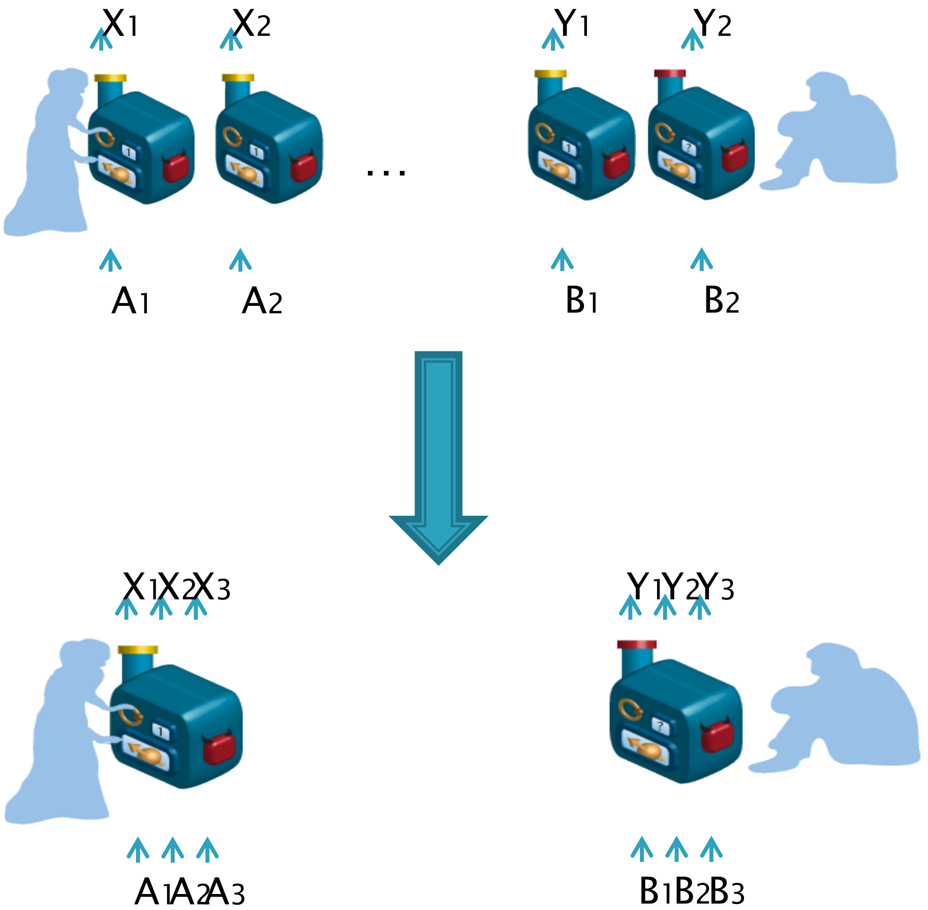
First idea:
Mayers-Yao FOCS 98

Proofs with restricted Eve:
AGM PRL **97**, 120405 (2006),
Scarani et al. PRA **74**, 042339 (2006)
...

Proofs with unrestricted
Eve but many devices:
BHK, PRL **95**, 010503 (2005)
Masanes et al., IEEE **60** 4973 (2014)
HR, arXiv:1009.1833
MPA, N. Comms. **2**, 238 (2011)

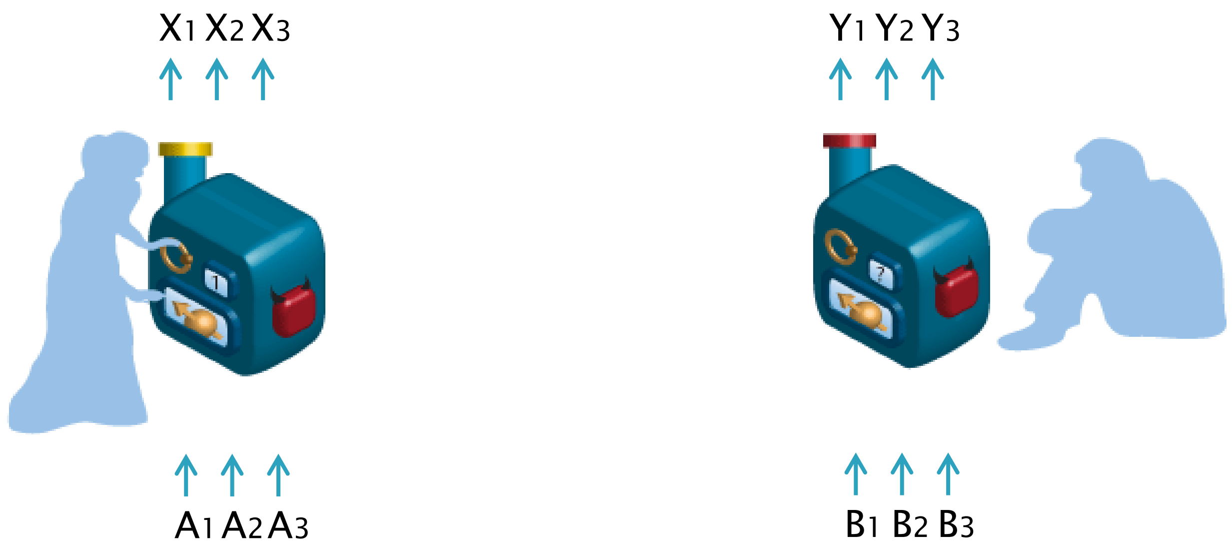


Device-independent QKD proofs

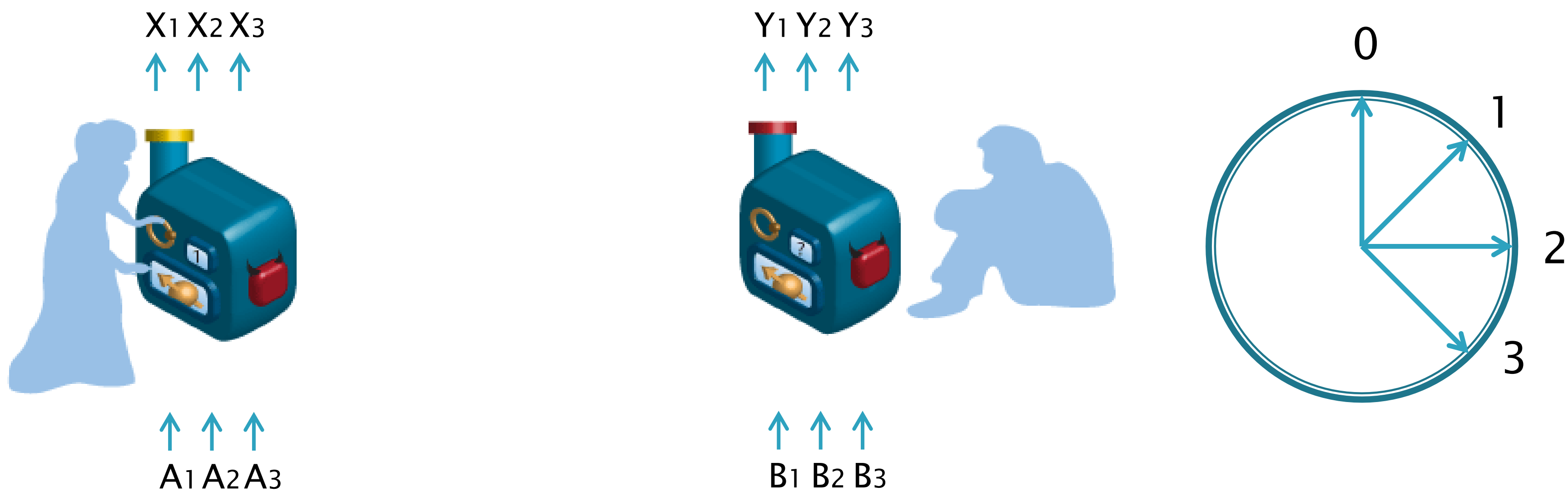


Proofs with unrestricted
Eve and few devices:
BCK, PRA **86**, 062326 (2012)
RUV, Nature **496**, 415 (2013)
VV, PRL **113**, 140501 (2014)

Device-independent QKD protocol: Main ideas (roughly follows VV)



Device-independent QKD protocol: Main ideas (roughly follows VV)



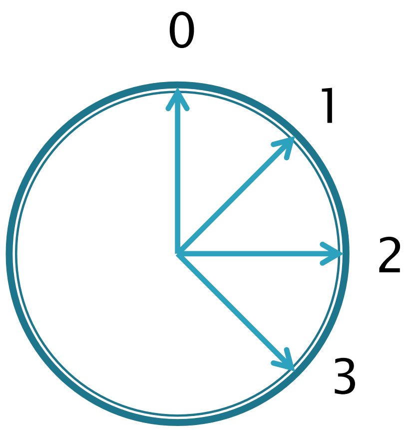
- $A_i \in \{0,1,2\}$, $B_i \in \{1,3\}$ (chosen uniformly at random).
- These inputs are made and outcomes recorded.
- Alice chooses small subset of rounds to be test rounds and tells Bob

Device-independent QKD protocol: Main ideas (roughly follows VV)

- $A_i \in \{0,1,2\}$, $B_i \in \{1,3\}$ (chosen uniformly at random).
- These inputs are made and outcomes recorded.
- Alice chooses small subset of rounds to be test rounds and tells Bob
- For the test rounds the inputs and outputs are publicly shared
- If the fraction of test rounds with $A_i \neq 1$ that win the CHSH game is below $\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)-\eta$, then abort
- If the fraction of test rounds with $A_i, B_i = 1$ that have different outcomes is above η, then abort
- Remaining rounds with $A_i, B_i = 1$ yield raw key

Protocol structure

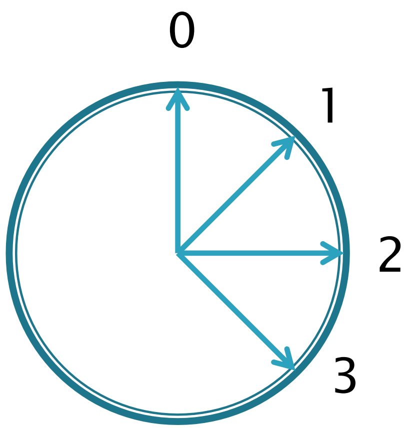
	A	X		B	Y
	1	1		1	1



$$|\psi\rangle_{AB} \approx \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Protocol structure

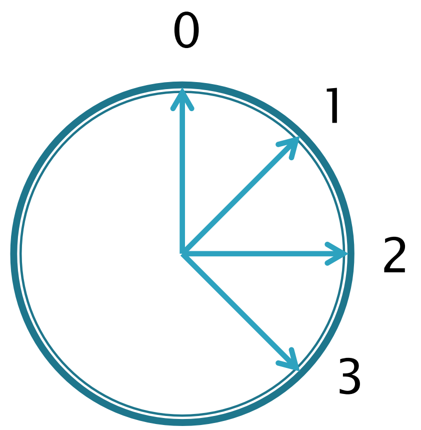
	A	X		B	Y
	1	1		1	1
	2	0		1	1



If $(\mathrm{A}, \mathrm{B}) = (0,1), (2,1)$ or $(2,3)$, want $X = Y$
If $(A, B) = (0,3)$ want $X \neq Y$

Protocol structure

	A	X		B	Y
	1	1		1	1
T	2	0		1	1
	1	1		3	1
T	1	0		1	0
T	0	0		1	0
	2	1		3	1
	1	0		1	1
	0	1		3	0
	0	1		3	1
	1	0		3	0
T	2	1		1	1

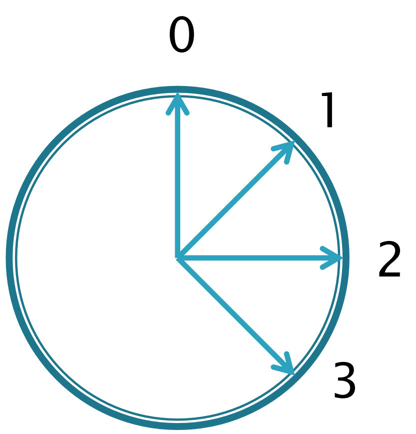


Use T rounds to check CHSH wins and error rate

K rounds form raw key

Protocol structure

	A	*X*		*B*	*Y*
K	1	1		1	1
T	2	0		1	1
	1	1		3	1
T	1	0		1	0
T	0	0		1	0
	2	1		3	1
K	1	0		1	1
	0	1		3	0
	0	1		3	1
K	1	0		1	0
T	2	1		1	1



Use T rounds to check CHSH wins and error rate

K rounds form raw key

Protocol structure

	A	X		B	Y
K	1	1		1	1
T	2	0		1	1
	1	1		3	1
T	1	0		1	0
T	0	0		1	0
	2	1		3	1
K	1	0		1	1
	0	1		3	0
	0	1		3	1
K	1	0		1	0
T	2	1		1	1

Raw key is processed to give final key

$S_A = 10010101\ldots$
$S_B = 11011101\ldots$

Error correction

$10010101\ldots$
$10010101\ldots$

Privacy amplification

$01101\ldots$
$01101\ldots$

Security definition

- What does it mean for a protocol to be secure?
- Define ideal
- Imagine Alice and Bob will randomly decide either to perform the real protocol or the ideal.
- The real protocol is secure if it is virtually impossible to distinguish the two.

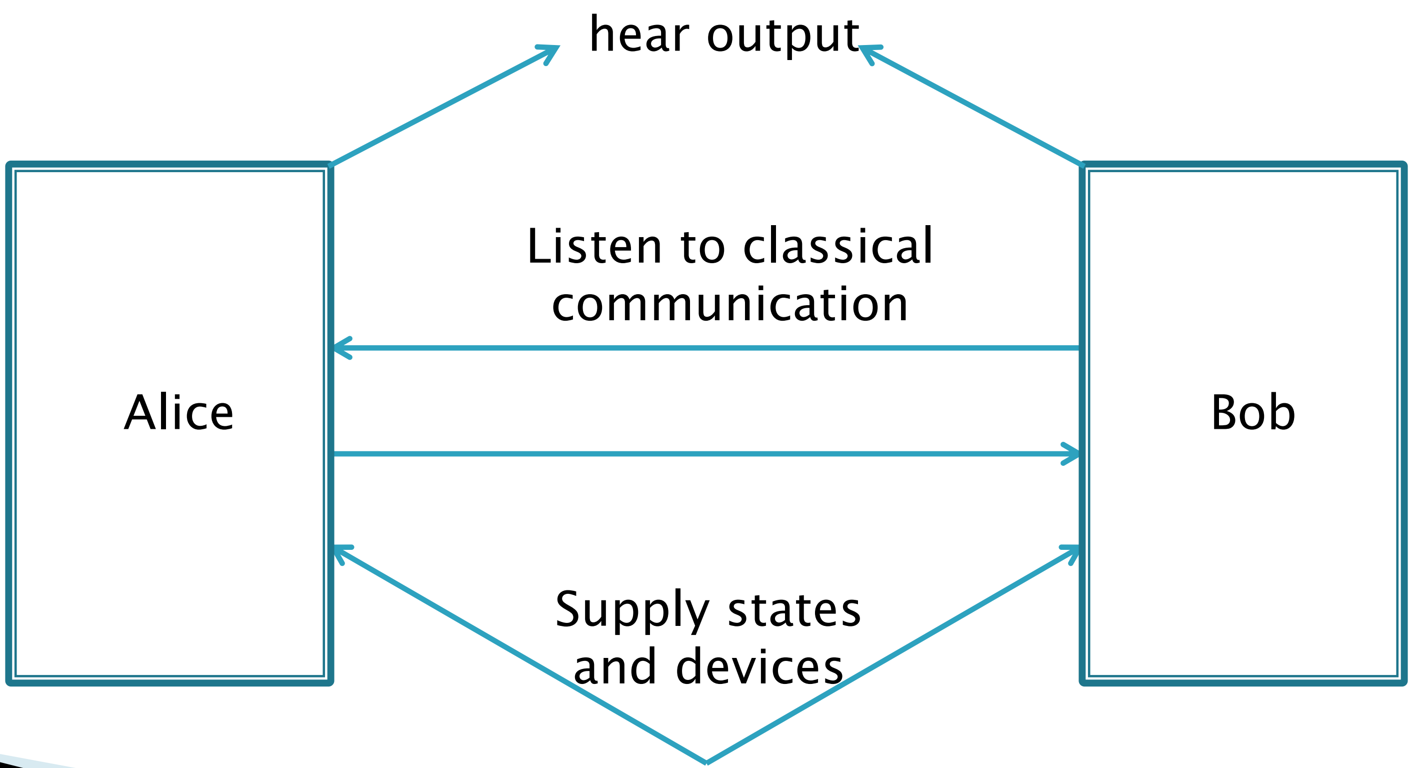
Composable security

- Larger protocol
  - 1.
  - 2.
  - …
  - n. Call key distribution sub-protocol
  - n+1.
  - …

Either use **Real** key distribution sub-protocol, or **Ideal**

How well can we tell the difference?

Security definition



The ideal

- We want the final state to have the form

$$\tilde{\rho}_{ABE} = \sum_x \frac{1}{|X|} |x\rangle\langle x|_A \otimes |x\rangle\langle x|_B \otimes \rho_E$$

The ideal

- We want the final state to have the form
$$\tilde{\rho}_{ABE} = \sum_x \frac{1}{|X|} |x\rangle\langle x|_A \otimes |x\rangle\langle x|_B \otimes \rho_E$$
- However, we **don't** simply define the ideal to output a state of this form.
- (It would be easy to distinguish this from the real protocol, e.g. by forcing real to abort)

The ideal

- Instead, take the ideal protocol to be the real protocol modified such that if it does not abort, right at the end Alice and Bob replace their output by a perfect key.

$$\sum_x \frac{1}{|X|} |x\rangle\langle x|_A \otimes |x\rangle\langle x|_B \otimes \rho_E$$

The ideal

- With the ideal defined in this way, it is impossible to distinguish the real and ideal based on abort.
- Only way to distinguish is if both:
  - The protocol does not abort; and
  - The output can be distinguished from perfect key.

$$D\left(\rho_{ABE}, \sum_x \frac{1}{|X|} |x\rangle\langle x|_A \otimes |x\rangle\langle x|_B \otimes \rho_E\right) > 0$$

real

The ideal

- Thus, the security statement is a bound on the *a priori* probability that the protocol does not abort and the output can be distinguished from perfect key over all possible devices.

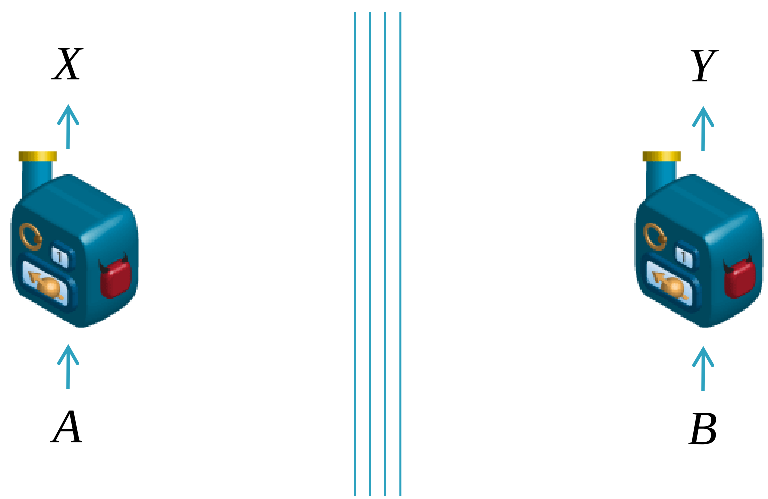
- NB: we don't make statements of the form "Given the protocol did not abort, the key is secure (except with very small probability)"

Technological challenges

- We have theoretical proofs: what about in practice?

Technological challenges

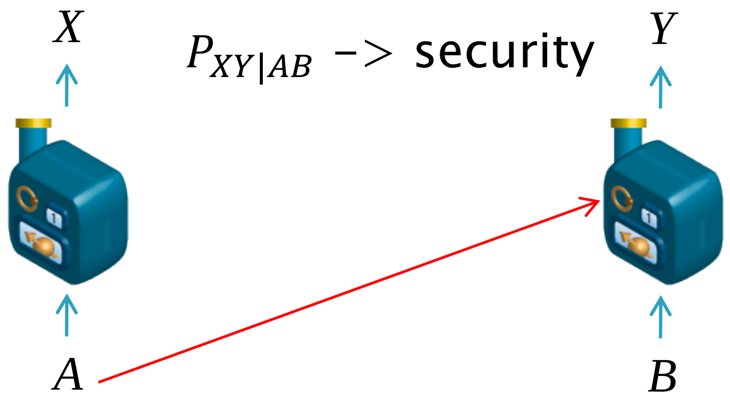
- What about in practice?
- Several technological challenges:
  - Need to close detection loophole



$P_{XY|AB}$ must violate a Bell inequality
In order to verify this, have to include failure to detect events

Technological challenges

- What about in practice?
- Several technological challenges:
  - Need to close detection loophole
  - (Note: no need to close locality loophole; although it doesn't hurt)



Technological challenges

- What about in practice?
- Several technological challenges:
  - Need to close detection loophole
  - (Note: no need to close locality loophole; although it doesn't hurt)
  - Current proofs tolerate a noise rate of up to ~8%.

Technological challenges

- Closing the detection loophole is the key challenge
- Easy in the lab, hard over long distances
- How to scale up small distance demonstrations.

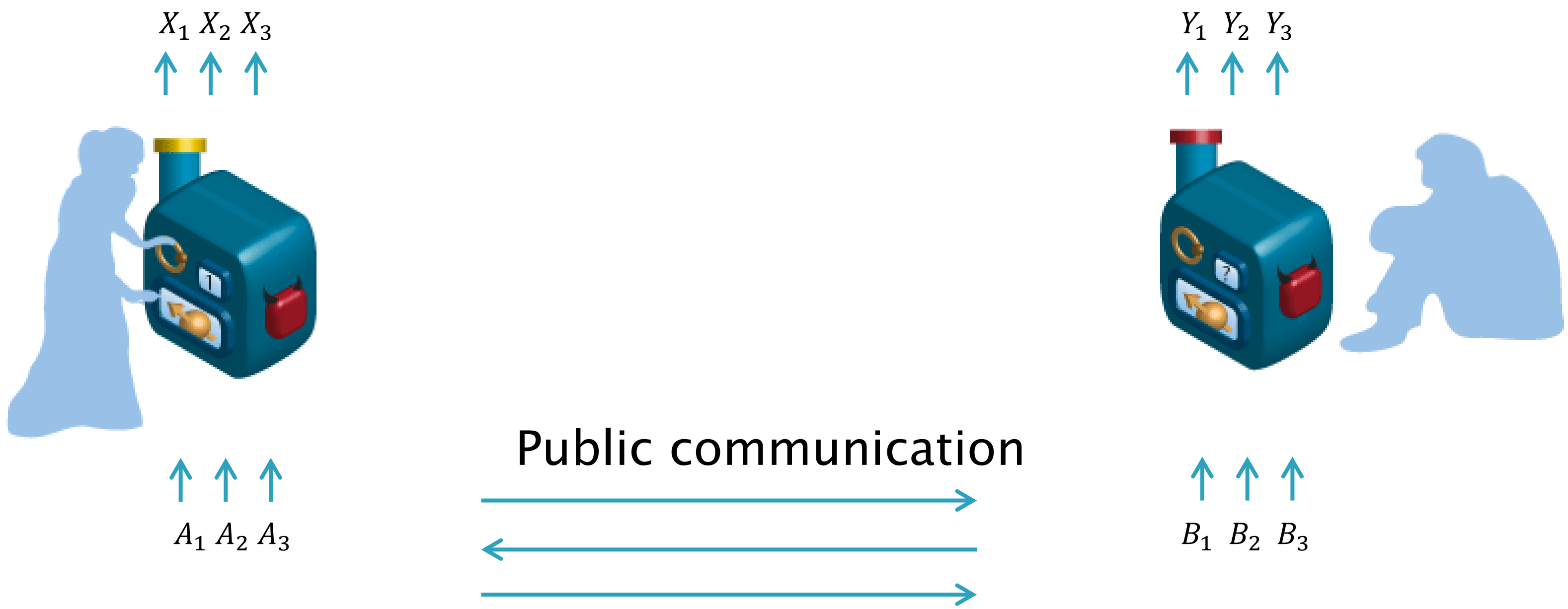
Theoretical challenges

- We have protocols and security proofs for unconditionally secure device-independent QKD but…
- The catch: without assumptions on the devices, for known secure protocols the devices cannot be reused for multiple instances of the same protocol

[BCK PRL **110**, 010503 (2013)]

Device-reuse problem

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

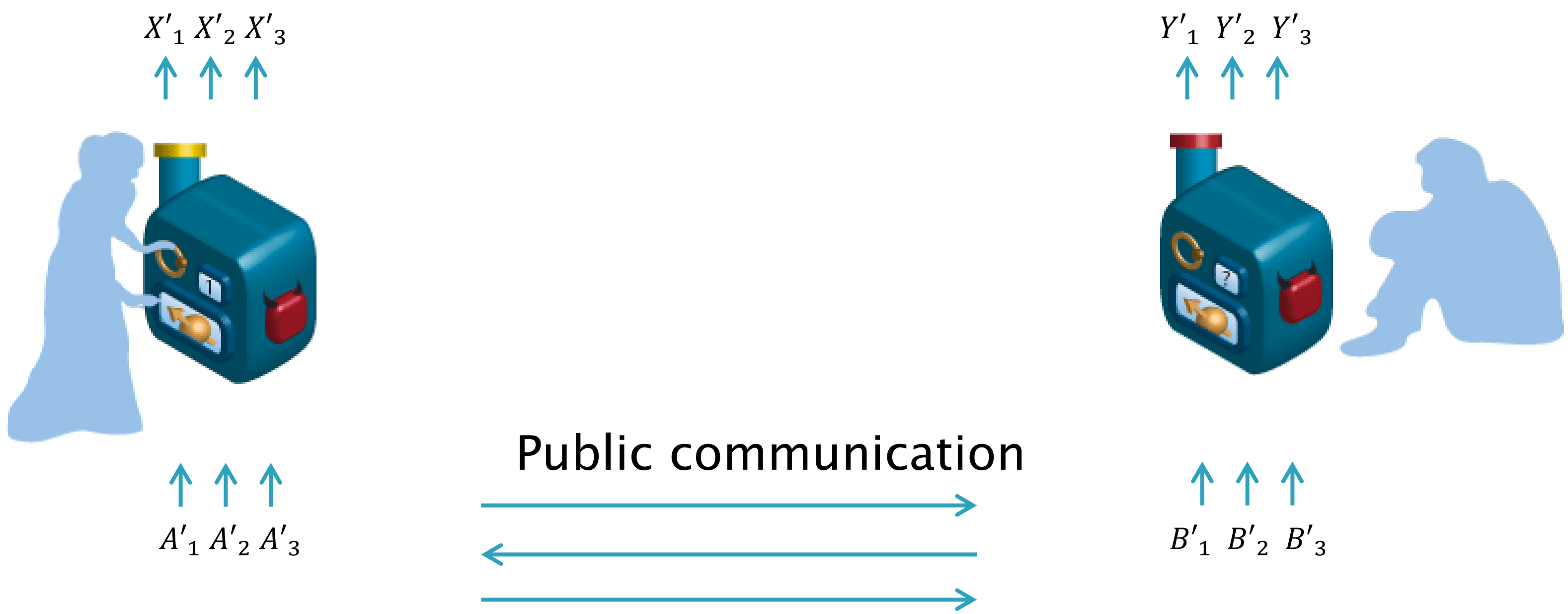


$S = f(X_1, X_2, \dots)$

$S = g(Y_1, Y_2, \dots)$

Device-reuse problem

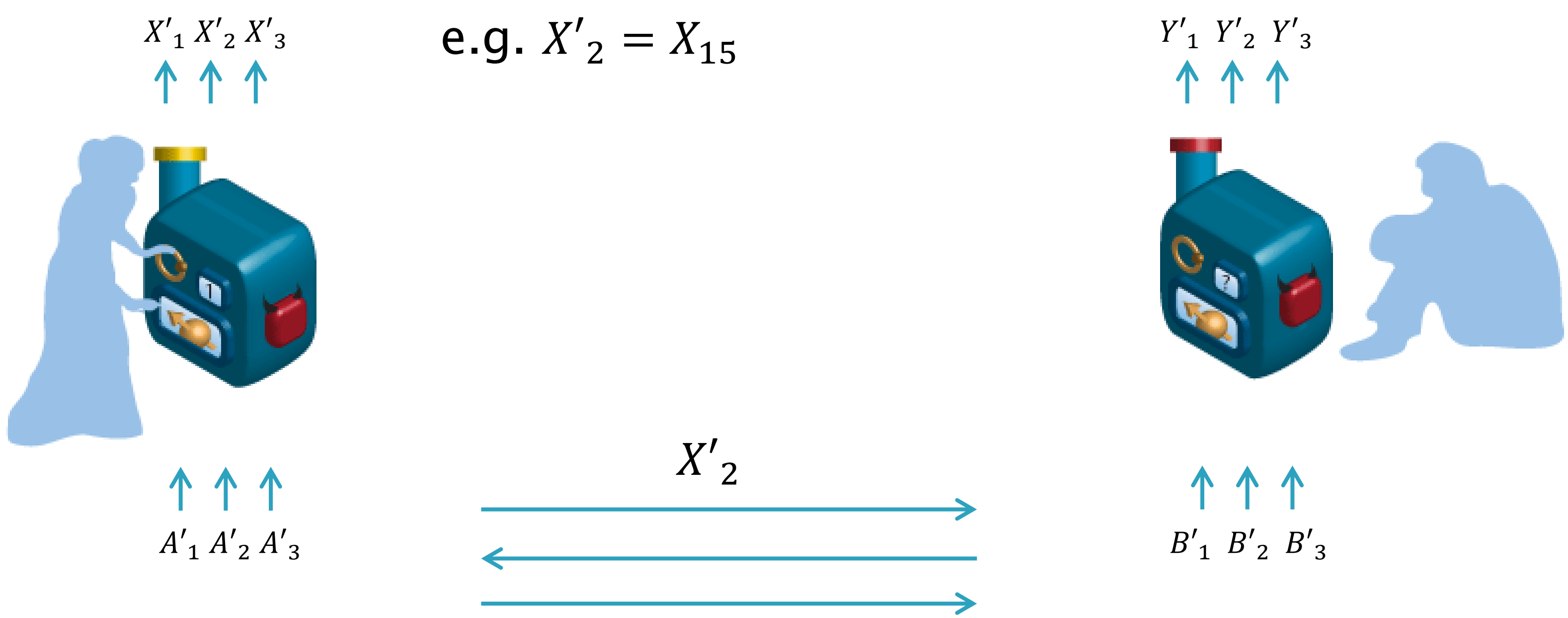
- Reuse it to generate second key



$S' = f'(X'_1, X'_2, \dots)$ $\qquad$ $S' = g'(Y'_1, Y'_2, \dots)$

Device-reuse problem

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



$S' = f'(X'_1, X'_2, \dots)$

$S' = g'(Y'_1, Y'_2, \dots)$

Device-reuse problem

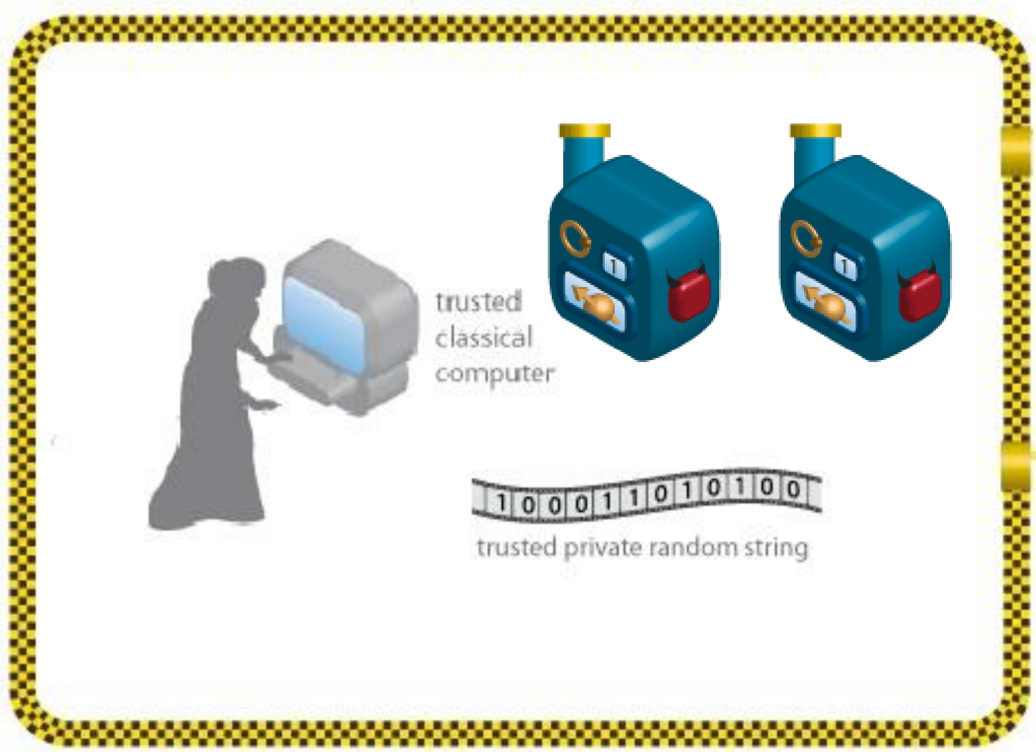
- If an untrusted device with memory is used to generate a secure key, it can leak data relevant to the first key and potentially compromise it
- This problem is present in all existing protocols

Theoretical challenges

- Possible solutions:
  - New protocols that avoid device-reuse problem
    - There are some proposals but they require additional measurement devices (2 per party)
    - Also need a new security notion
  - Weaker notion in the spirit of device-independence but making *some* assumptions on the devices
    - What are reasonable assumptions? Main idea of device independence is to avoid the need to classify the devices. Assumptions should be readily verifiable.
    - Measurement-device-independence and other semi-device independent solutions

[BP, PRL **108** 130502 (2013) and LCQ, PRL **108** 130503 (2013)]

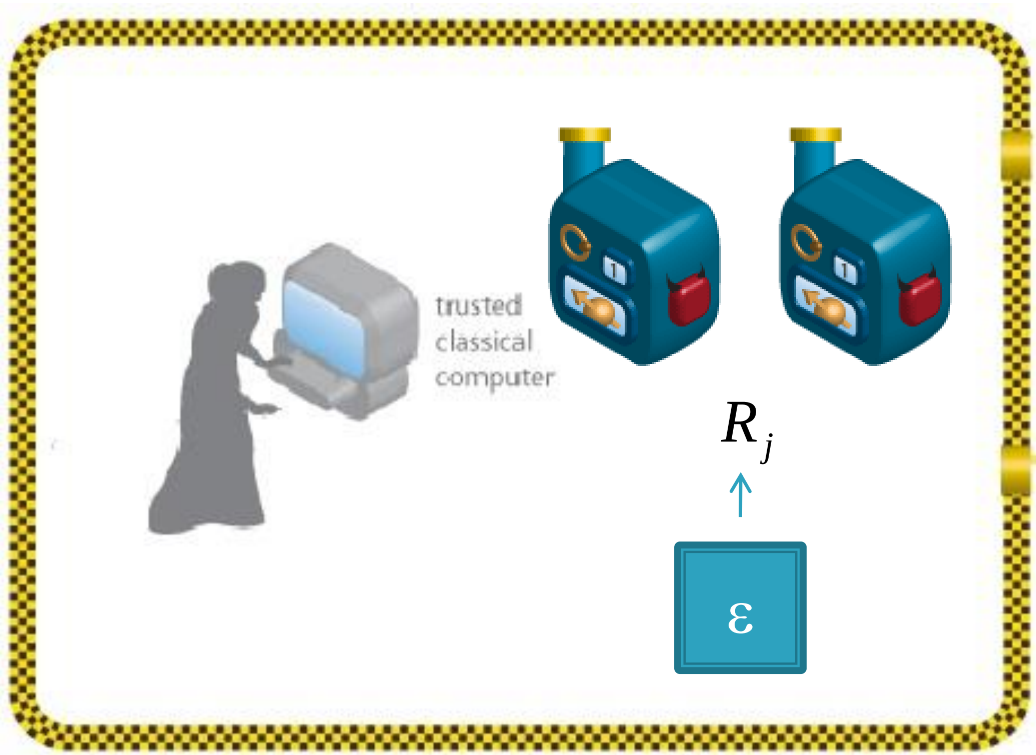
Randomness Expansion



C/CK, JPhysA **44**, 095305 2011
Pironio+, Nature **464**, 1021 2010
PM, PRA **87**, 012336, 2013
FGS, PRA **87**, 012335, 2013
VV, Phil Trans **370**, 3432, 2012
CY, last year's QIP
MS, last year's QIP and this

Want to generate longer private random string

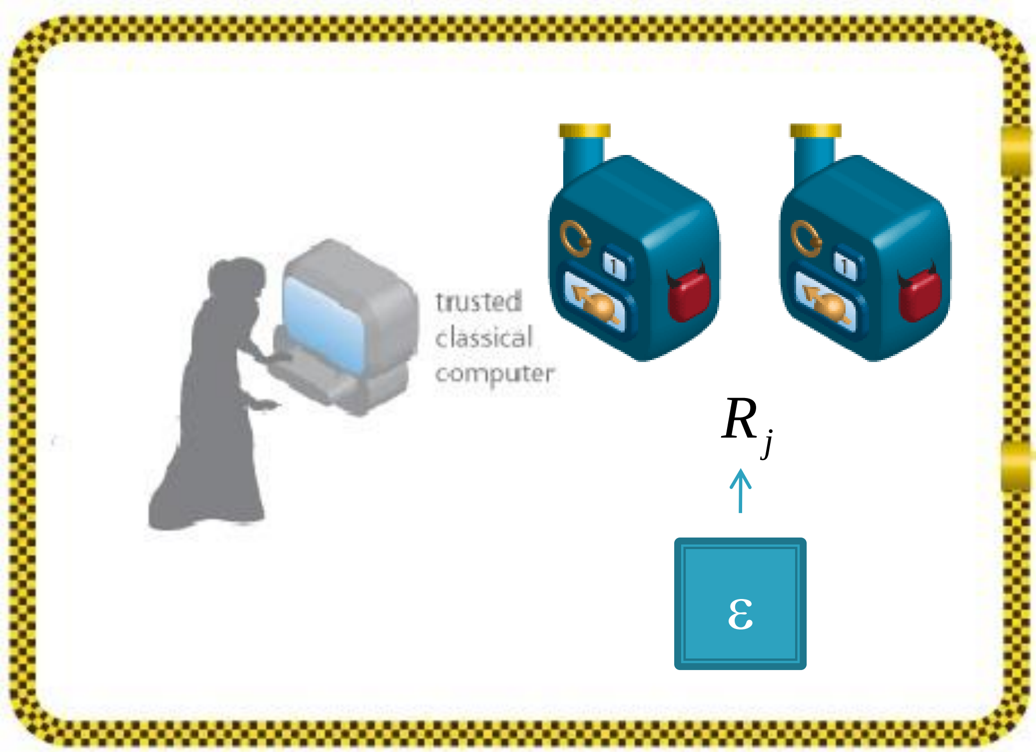
Randomness Amplification



Imperfect randomness:
- Looks random to Alice
- Partly correlated with other information (that may be held by Eve)

Want to generate perfectly random string

Randomness Amplification



Imperfect randomness:

- Looks random to Alice
- Partly correlated with other information (that may be held by Eve)

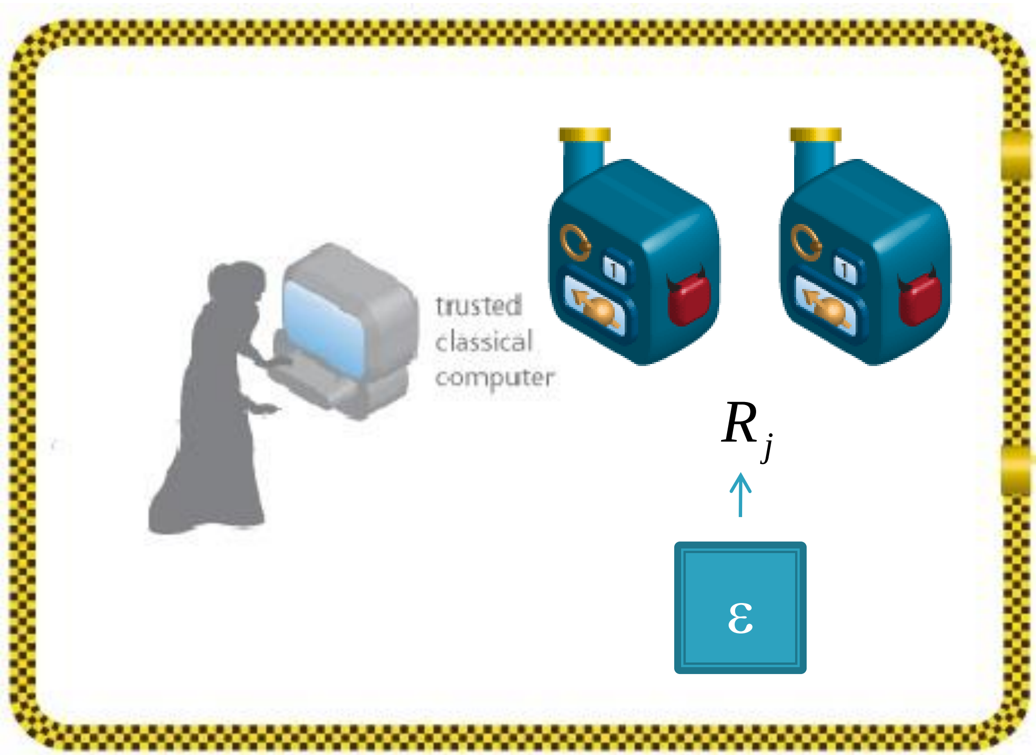
E.g., Santha-Vazirani source [FOCS 84]

Limitation to the bias of each bit conditioned on previous ones and adversary.

$$P_{R_j|W} \in [\frac{1}{2} - \epsilon, \frac{1}{2} + \epsilon]$$

Want to generate perfect random string

Randomness Amplification

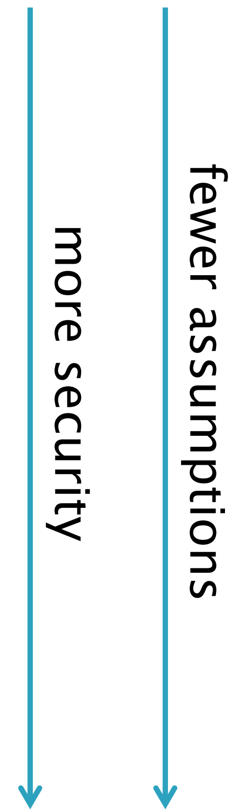


CR, N.Phys **8** 450 (2012)
Gallego+, N. Commun **4**, 2654 (2013)
Brandao+, last year's QIP
CY, last year's QIP
CSW, last year's QIP

Want to generate perfect random string

Summary

- Classical protocols aim to provide time-limited security
- Standard quantum protocols allow this to be upgraded to unconditional security
- Device-independent protocols allow security against device failure or tampering



Summary

- Device-independence aims to allow us to push cryptography into the trustworthy regime:
  - **weaker assumptions -> more security**
  - certify security on-the-fly (calibration errors automatically caught).
- Open challenges
  - Closing the detection loophole at distance for QKD
  - Avoiding the device-reuse problem
    - New protocols allowing for device reuse
    - Modified notion of device independence
    - Better noise tolerance (in theory)