Device independence

Peter Brown
Télécom Paris / Inria
peter.brown@telecom-paris.fr

QKD is an emerging commercial technology

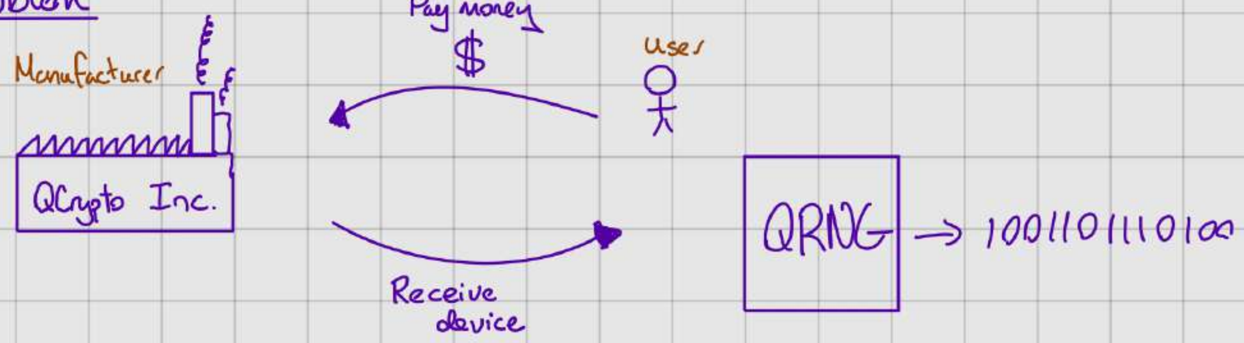
embarrasing and expensive if broken!

- Manufacturers should be able to guarantee security to users

- Users should be able to verify the security

What if the supplier is malicious?
- NSA reportedly paid for RSA backdoor
- CIA secretly owned popular crypto company Crypto AG for 50 years!

The user's problem



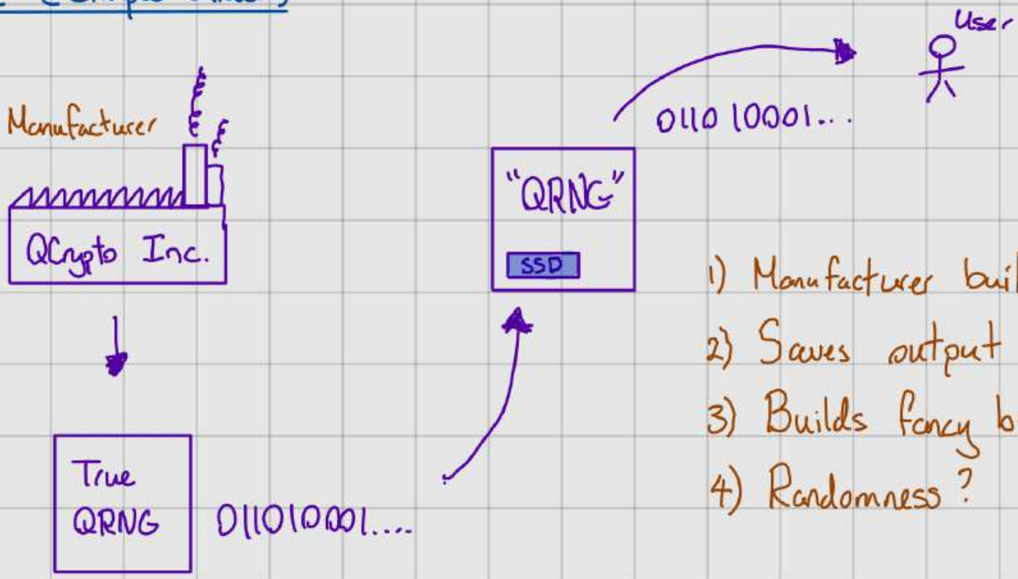
Can a user verify the device produces random bits?

- Statistical tests
  - → approx 50% 0 and 50% 1
  - → No long streaks 0000....00111111....111.
  - → Test for dependencies between bits
  - (See Diehard test suite!)

- Look inside box
  - → Requires expert knowledge
  - → Probably violates warranty

- Trust manufacturer

Example (Simple attack)



1) Manufacturer builds true QRNG
2) Saves output to some harddrive
3) Builds fancy box containing harddrive
4) Randomness?

- "QRNG" outputs string from a true QRNG
- Effectively indistinguishable from a real device

Problem: Manufacturer knows the output!

Security issue if want to use RNG for cryptography.

A manufacturer's problem

An honest manufacturer builds a BB84 QKD system

See lecture of M. Lucamarini

We have a security proof for BB84 against an eavesdropper Eve :)

A mathematical theorem : $\boxed{\text{Protocol} + \text{Assumptions} \Rightarrow \text{Security}}$

Changing either likely invalidates security.

The problem:

Real World ≠ Theory World

Small deviations from assumptions of protocol can break security proof.

Example

By honest error the source produces two particles

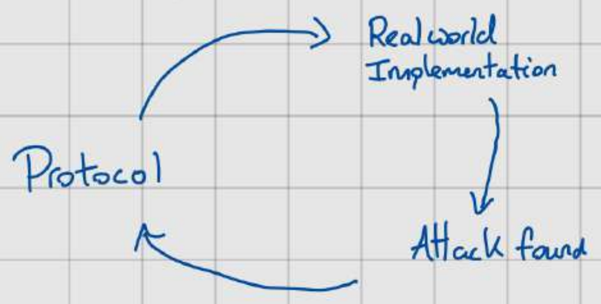
$$|0\rangle^{\otimes 2},\ |1\rangle^{\otimes 2},\ |+\rangle^{\otimes 2},\ |-\rangle^{\otimes 2}$$

This is a big problem. Eve can intercept 1 of the particles and measure. She gains information about the state Alice prepared without disturbing the state Bob receives. I.e. without being detected!

Alice and Bob think they are secure...

Broken Assumption ⟹ Possible Attack

Can we patch quantum crypto?



Similar to software patches

- Once attack is discovered we can try to adapt the protocol to secure against it.
  - May be hard:
    - new security proof?
    - new hardware? $$
    - only known attacks can be patched...

As we will see soon, device-independent cryptography allows us to circumvent most attacks and hence this issue!

Assumptions, assumptions, assumptions...

We *need* assumptions:

1) Trusted classical computer
2) No unwanted leakage

} Somewhat necessary $\forall$ cryptography

3) Source of private randomness / Key ← Authenticate channel / Seed protocol
4) Quantum theory is correct / complete — Rules of Quantum apply
5) Security model for adversary — What can Eve do?
6) Quantum devices are characterised

↑ Alice prepares $|\psi\rangle$
Bob measures M

The DI mantra

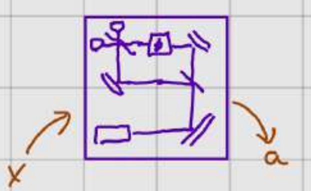
$$\boxed{\text{Minimal Assumptions!}} \Rightarrow \text{minimal attacks}$$

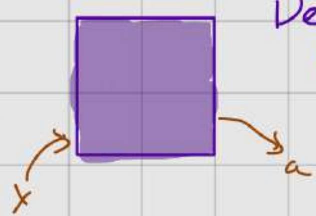
in particular we mostly aim to weaken 5 and 6

↑ Others can also be weakened!

Devices can be built by Eve
- Strengthen adversary
- No assumptions on quantum devices

↗ Protection against malicious manufacturer.



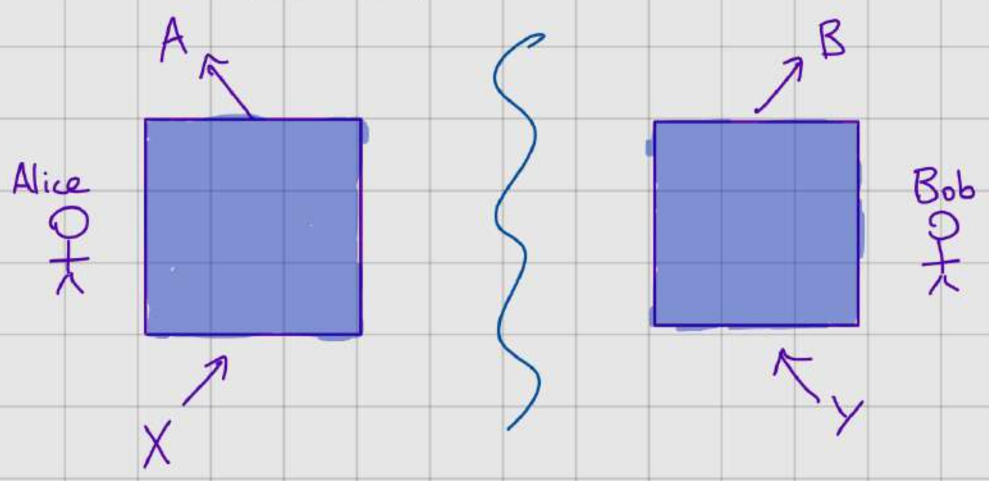


Devices become black boxes from security proof / user perspective. (No trust)

Goal:
- Protocol based on minimal assumptions
- Protocol aborts when insecure

↑ Protects both user & manufacturer even against unknown attacks.

The tool: Bell-experiments



We have an experiment where Alice and Bob give random inputs X, Y to their devices and receive outputs A, B.

We assume binary in examples
$A, B, X, Y \in \{0,1\}$

Assumptions:

- Inputs X, Y and outputs A, B are from finite sets
- Inputs X, Y chosen uniformly and independently of everything

  Trusted randomness assumption "Free choice"
- Alice and Bob's devices cannot communicate during each round of the experiment.

  No unwanted leakage assumption

  A round consists of inputs chosen and outputs received.

Question: What $p(a,b|x,y)$ can we observe in the experiment?

Depends on what information the devices share!

Remark (No-signalling)

The assumptions of the experiment already imply that Alice's local statistics should not depend on Bob's input and vice-versa. Mathematically we express this as

$$\sum_a p(ab|xy) = p_B(b|y) \qquad \forall\, b, x, y$$

$p_B(b|xy)$

$$\sum_b p(ab|xy) = p_A(a|x) \qquad \forall\, a, x, y$$

$p_A(a|xy)$

p_A - Alice's local distribution
p_B - Bobs local distribution

Scenario 1 - Independent devices

Suppose Alice and Bob's devices act completely independently.
Then,

$$p(a,b|x,y) = p_A(a|x)\, p_B(b|y)$$

Big restriction on possible $p(ab|xy)$ that can be observed.

Example

Let $X=Y=0$, we can write $p(ab|00)$ as a vector

$$\begin{pmatrix} p(00|00) \\ p(01|00) \\ p(10|00) \\ p(11|00) \end{pmatrix} = \begin{pmatrix} p_A(0|0)\, p_B(0|0) \\ p_A(0|0)\, p_B(1|0) \\ p_A(1|0)\, p_B(0|0) \\ p_A(1|0)\, p_B(1|0) \end{pmatrix}$$

where $p_A(a|x) = \sum_b p(ab|xy)$ is the marginal distribution

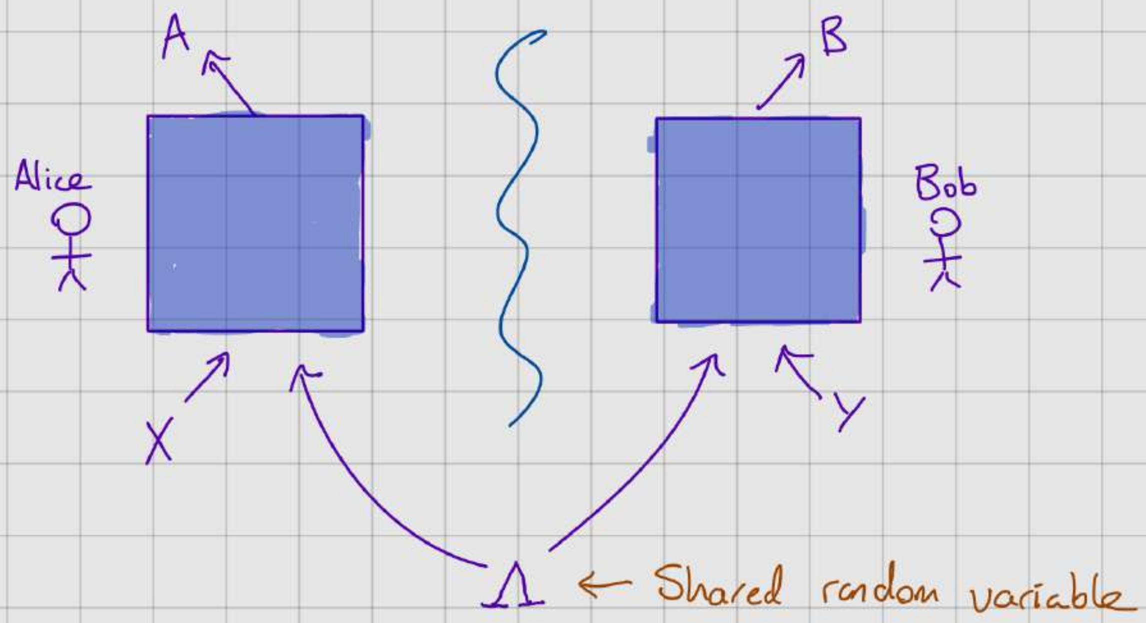
It is <u>impossible</u> to find p_A and p_B such that

$$\begin{pmatrix} p(00|00) \\ p(01|00) \\ p(10|00) \\ p(11|00) \end{pmatrix} = \begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{pmatrix}$$

perfectly correlated coins.

Impossible distribution with independent devices.

Scenario 2 - Local / Classical devices



In order to generate stronger correlations Alice and Bob's device's can use some preshared randomness. Such a distribution takes the form

$$p(ab|xy) = \sum_{\lambda} p_{\Lambda}(\lambda)\, p_A(a|x\lambda)\, p_B(b|y\lambda)$$

We call such $p(ab|xy)$ 'classical' or 'local'.

Alice's outcome depends on input x and the value λ of the shared random variable

Similarly Bob's outcome depends only on his input y and shared λ

The shared randomness Λ allows them to correlate their outcomes.

Example

Take Λ to be a uniform bit. If $\lambda = 0$ then $\underbrace{\text{Alice and Bob always output } 0}_{\text{Independent strategy}}$.

$p_A(0|x) = 1$
$p_B(0|y) = 1$

If $\lambda = 1$ then Alice and Bob always output 1.

And we see

$p(ab|X=0, Y=0, \Lambda=0)$ $p(a,b|X=0, Y=0, \Lambda=1)$

$$\begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{pmatrix} = \underset{p_{\Lambda}(0)}{\frac{1}{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \underset{p_{\Lambda}(1)}{\frac{1}{2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Many more distributions are possible with shared randomness!

Remarks

1) [Fine 82] Any local distribution can be expressed as a convex combination of deterministic distributions.

$$p(ab|xy) = \sum_{\lambda} p(\lambda) \underbrace{p(a|x,\lambda)}_{\in\{0,1\}} \underbrace{p(b|y\lambda)}_{\in\{0,1\}}$$

This immediately implies that local distributions contain no certifiable randomness. Anyone who has access to the classical information Λ could in principle know with certainty the outcomes of the devices upon learning the inputs.

Eve could have access to Λ also.

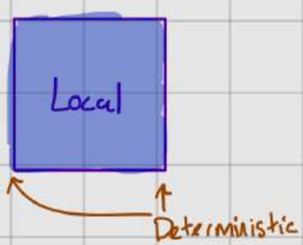
However the converse is also true. If the distribution is not local (nonlocal) then there cannot exist some information Λ which renders the outcomes deterministic I.e., nonlocal distributions are necessarily random!

Even from perspective of adversary Eve.

But do nonlocal distributions exist?

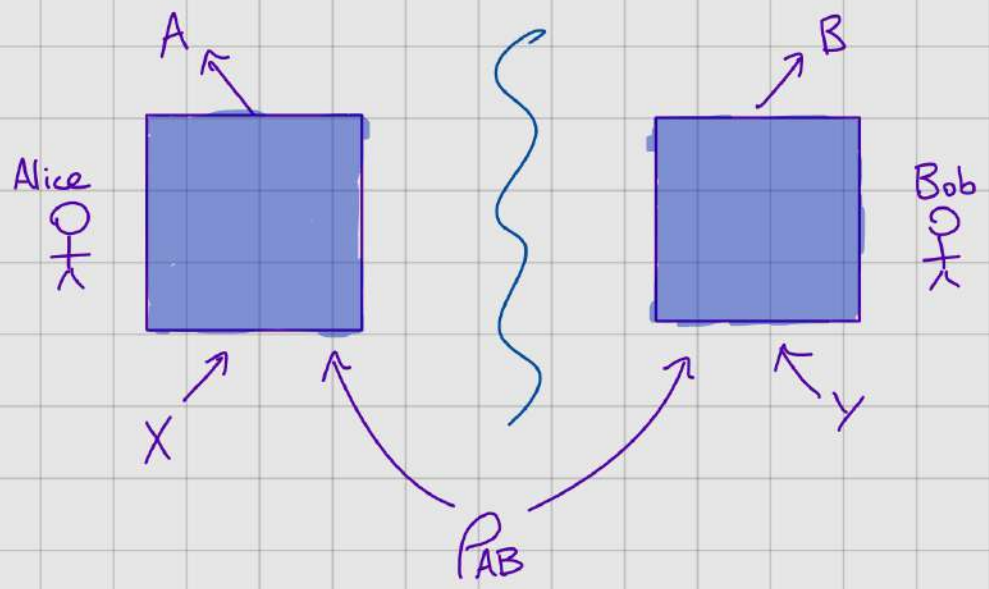
2) Geometrically we can write distribution $p(ab|xy)$ as a vector

$$\begin{pmatrix} p(00|00) \\ p(01|00) \\ \vdots \end{pmatrix} \in \mathbb{R}^{|A||B||X||Y|}$$



- Set of local distributions forms a convex polytope.
- Extremal points are deterministic distributions

Scenario 3 - Quantum devices



Rather than sharing classical information Λ, the devices could also share some quantum information (a bipartite state ρ_{AB})

Then when receiving input $X=x$, Alice's device measures some POVM $\{M_{a|x}\}_a$ and outputs the measured outcome a.

Simarly when Bob's device receives input $Y=y$ it measures POVM $\{N_{b|y}\}_b$.

Assumption 4

By rules of quantum theory the distribution can be written as

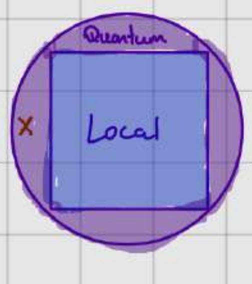
$$p(ab|xy) = \mathrm{Tr}\left[\rho_{AB}\left(M_{a|x} \otimes N_{b|y}\right)\right]$$

We call such distributions 'quantum'.

Bell's Theorem (1964)

There exist quantum distributions that are nonlocal.

Geometrically we have



- Local distributions are a strict subset of quantum distributions.

Imagine we run our Bell-experiment and observe the distribution marked with $\times$ above.

Under the assumptions of a Bell-experiment

$\Longrightarrow$ The devices cannot be local $\Rightarrow$ The devices must be sharing an entangled state

Exercise: Show that a separable state produces local correlations.

<u>Device-independent test of entanglement</u>

After analysing the statistics we know there must have been entanglement without knowing anything about how the devices produced their statistics!

- Nonlocal correlations also imply the outputs A,B must contain fresh, private randomness.

Example CHSH game

Take $A,B,X,Y \in \{0,1\}$, $p(x,y) = \frac{1}{4} \quad \forall x,y$

We think of X,Y as questions and A,B as answers. The goal of the game is to respond with a 'winning' answer pair (a,b) given a question pair (x,y). An answer pair (a,b) is 'winning' for a question pair (x,y) if

addition mod 2

$$a \oplus b = xy$$

I.e.

xy \ ab	00	01	10	11
00	✓	✗	✗	✓
01	✓	✗	✗	✓
10	✓	✗	✗	✓
11	✗	✓	✓	✗

✓ – (a,b) wins for given (x,y)

✗ – (a,b) loses for given (x,y)

Given questions (x,y) are chosen uniformly, what's the probability that Alice and Bob win the game?

how they answer, given questions

Depends on the probability distribution $p(a,b|x,y)$

$$= \frac{1}{4}\big(p(00|00) + p(11|00) + p(00|01) + p(11|01) + p(00|10) + p(11|10) + p(01|11) + p(10|11)\big)$$

$$\boxed{\mathrm{Win}(p) := \frac{1}{4}\sum_{a\oplus b = xy} p(ab|xy)}$$

Prob win CHSH game when playing with distribution p.

By Bell's theorem we know there are more quantum distributions then classical distributions. So maybe quantum players can win more often?

Best classical winning probability

$$\max_{p\in \mathrm{Local}} \mathrm{Win}(p) = 3/4$$

Best classical strategy is always output 0.

If we play the game and win more than 3/4 $\Rightarrow$ our devices are quantum and producing randomness!

Best quantum winning probability

$$\max_{p\in \mathrm{Quantum}} \mathrm{Win}(p) = \cos^2(\pi/8) \approx 0.853$$

Quantum can win significantly more then classical!

The best quantum strategy.

Can verify that winning prob of $\cos^2(\pi/8)$ can be achieved by the system

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

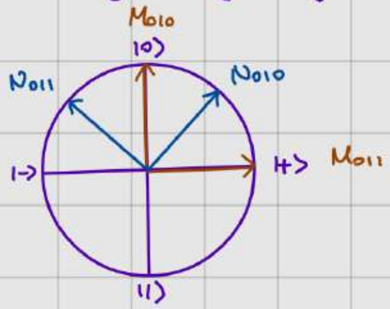
$$M_{0|0} = |0\rangle\langle 0|$$

$$M_{0|1} = |+\rangle\langle +|$$

$$N_{0|0} = \begin{pmatrix} \cos^2(\pi/8) & \cos(\pi/8)\sin(\pi/8) \\ \cos(\pi/8)\sin(\pi/8) & \sin^2(\pi/8) \end{pmatrix}$$

$$N_{0|1} = \begin{pmatrix} \cos^2(\pi/8) & -\cos(\pi/8)\sin(\pi/8) \\ -\cos(\pi/8)\sin(\pi/8) & \sin^2(\pi/8) \end{pmatrix}$$

Or in terms of observables $M_x = M_{01x} - M_{11x}$ $N_y = N_{01y} - N_{11y}$



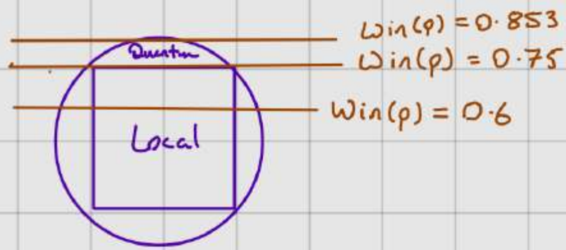
$M_0 = Z$ $\qquad N_0 = \frac{Z+X}{\sqrt{2}}$

$M_1 = X$ $\qquad N_1 = \frac{Z-X}{\sqrt{2}}$

where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Remarks

1) Geometrically the CHSH game winning probability corresponds to a linear functional on the prob space



$\text{Win}(p) \leq 3/4$ is an inequality satisfied by all local distributions. Such inequalities are commonly known as Bell-inequalities.

2) We already know some quantum distributions imply entanglement and randomness. Some special quantum distributions are also self-testing. I.e., they imply the whole quantum system (state and measurements).

Up to some symmetries.

For example, the winning probability $\text{Win}(p) = \cos^2(\pi/8)$ self-tests the above system. Effectively, if we know that our devices win with probability $\cos^2(\pi/8)$ then they must be using the above system to do so!

Security intuition

Self-testing gives some intuition as to why DI cryptography is secure.

1) Play CHSH game with 2 untrusted devices and observe $\text{Win}(\rho) = \cos^2(\pi/8)$

Not practical, just for intuition. However $\text{Win}(\rho) > 3/4 \Rightarrow$ randomness has been generated.

2) By self-testing we know they were measuring

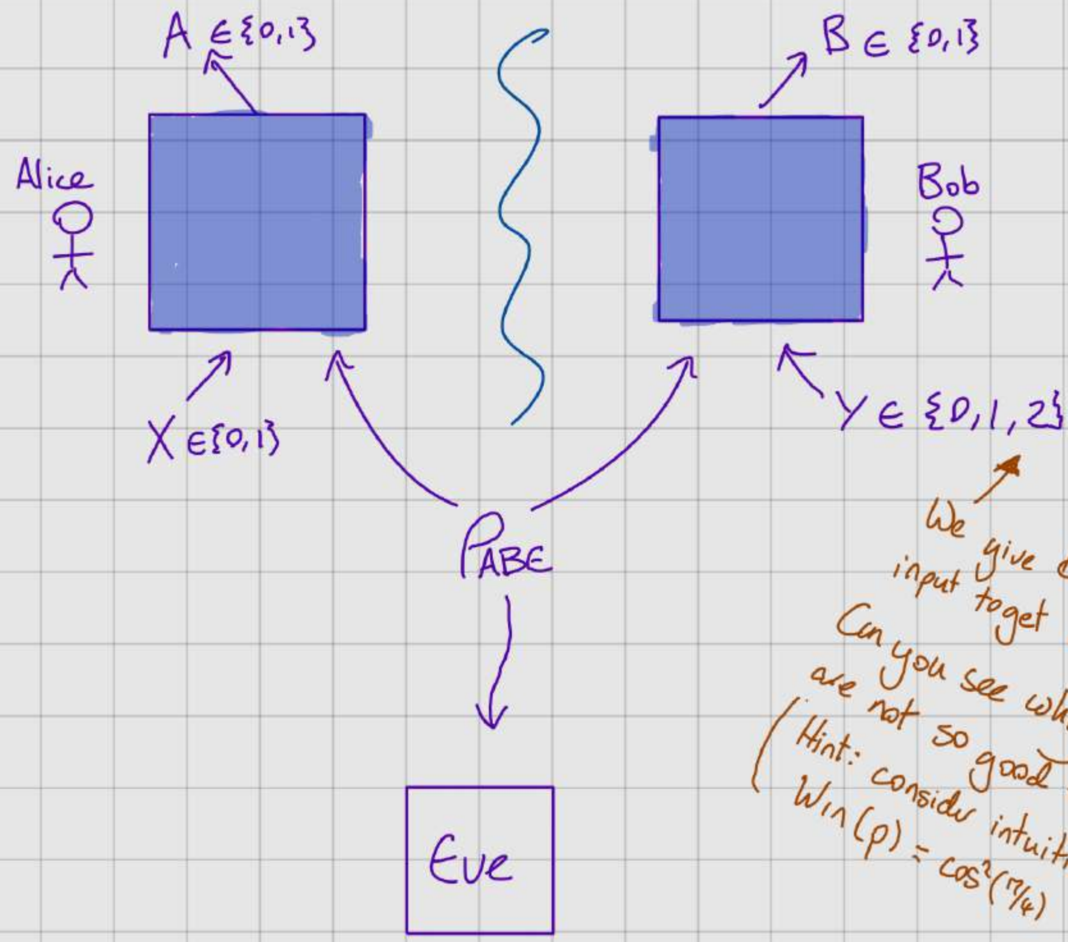
$$|\psi\rangle_{AB} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$\leftarrow$ Maximally entangled state $\Rightarrow$ Eve has no entanglement!

3) We also know Alice's measurement on input $X=0$ is $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

$\Rightarrow$ Alices measurement on input $X=0$ produces 1 uniformly random and secure bit of randomness!

A DIQKD Protocol



We give Bob a 3rd input to get better key. Can you see why inputs $\{0,1\}$ are not so good for QKD? (Hint: consider intuition when $\text{Win}(\rho) = \cos^2(\pi/4)$)

* In DI the source and measurements are not trusted. Hence, they are assumed to be controlled (chosen) by Eve. She may also share entanglement with the source ρ_{AB} to gain more information about the outputs.

<u>A protocol</u> ← This is a toy protocol. Real protocols are often a little different to help with security proof.

1) (Device interaction)
For $n \in \mathbb{N}$ rounds do:

With probability $\gamma \in [0,1]$ we <u>test</u> the devices

- (Test) Choose $X, Y \in \{0,1\}$ randomly and record outcomes.

Otherwise with probability $1-\gamma$ we <u>generate key</u>

- (Key gen) Choose $X=0$, $Y=2$ and record outcomes.

2) (Parameter estimation)
Estimate fraction of rounds where CHSH game won. If too small then abort!

↑ E.g. below 3/4

3) (Post processing)
Alice and Bob then perform error correction & privacy amplification on their raw keys from the key gen rounds to generate secure key.

Intuition: At parameter estimation we find $Win(p) > 3/4$

$\Downarrow$

When Alice inputs $X=0$ her output contains randomness

$\Downarrow$

If Bob sucessfully performs error correction then he has a raw key equal to Alice's both of which contain randomness

$\Downarrow$

After privacy amplification they then have secret keys!

QBER

If $\mathbb{P}[A \neq B | X=0, Y=2]$ is too large then error correction will force protocol to abort

Security with minimal assumptions! No need to trust source or measurements. Hence user protected against malicious manufacturer. And manufacturer protected against unknown attacks.

What's the catch?

$\boxed{\text{DI is hard to implement}}$

→ Needs high quality entanglement / low losses.

Example (Detection loophole)

What should we do if Alice's device does not produce an outcome?

1) Ignore the round
2) Record outcome as a 0.

We violated an implicit assumption that the devices produce an output.

Option (1) seems innocent but we open up attacks. This issue is known as the detection loophole.

An attack: Suppose whenever the device receives input $X=1$ it refuses to produce an outcome. And Alice & Bob's devices always output 0. If we ignore no-outcome rounds we never encounter a round where $X=Y=1$ and hence $A=B=0$ always wins.

The fraction of rounds won will be 1

Greater than maximum quantum winning probability!

local strategy wins with prob 1 if we ignore rounds.

Thus we are forced to do option (2). However no-click rounds are junk statistics which we are forced to keep and which quickly push $\mathrm{Win}(p) \leq 3/4$:(

Detection efficiency $\lesssim 2/3 \implies \mathrm{Win}(p) \leq 3/4$:(

Current DIQKD protocols require Detection efficiency $\gtrsim 80\%$

- No other noise sources
- No finite size effects

likely needs to be much higher

Nevertheless we had 3 proof of principle experiments

1) Zhang et al. Nature 607 2022 } Trapped atoms
2) Nadlinger et al. Nature 607 2022 }
3) Liu et al. PRL 129 2022 } Photonic (Potential security problems with protocol used in (3))

1) 700m / 0.0008 bits/s Win(p) = 0.822
2) 2m / 3.4 bits/s Win(p) = 0.835
3) 220m / 2.6 bits/s Win(p) = 0.756

Current Challenges

Robust to losses / finite size

1) How to make efficient / practical DI protocols?

Need efficient ways to analyse.

- Explore protocols with more inputs/outputs
- Better finite size proofs ← see talk by T. van Himbeeck
- Heralding → Better experiments for Bell-inequality violations
- New protocols (post processing / advantage distillation / ...)

See R. Wolf talk

2) Composability of DI protocols
- Currently no composable security definition for DI

Memory attacks: As no characterisation of devices they may remember key from previous protocols and leak them in later ones...

3) What protocols can be made DI?

See talk of M. Pittaluga

4) What about semi DI? MDI / Source DI / Energy bounds

add additional assumptions to make implementation easier.