Security and Cryptography 2022

Mirosław Kutyłowski

VIII. QUANTUM CRYPTOGRAPHY

as there are problems to guarantee security of devices in the traditional way, maybe there is a way out using physics? three directions:

1) **quantum based random number generators**

2) **key transport**

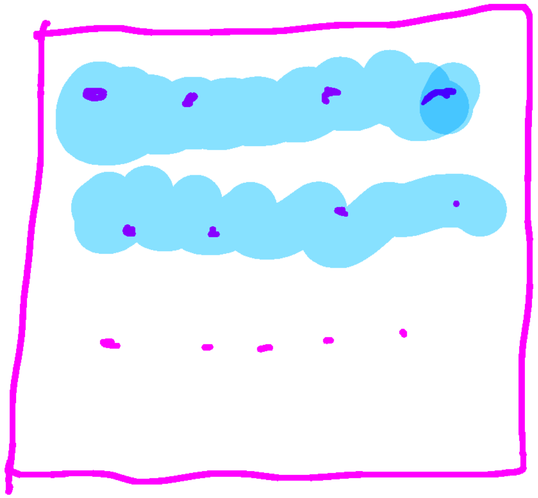
3) **quantum cryptanalysis**

TWINKLE $\approx$ TWIRLE

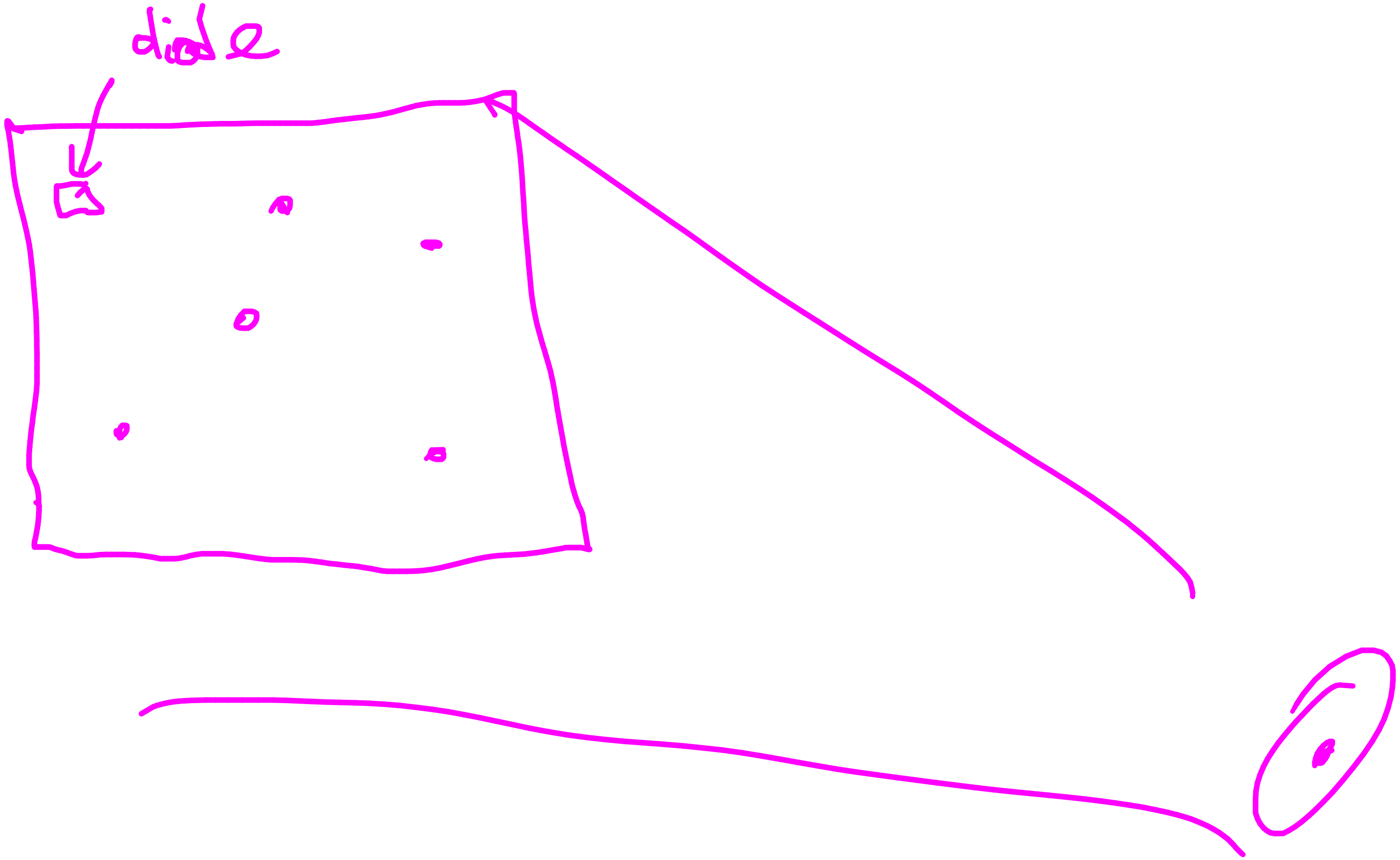
hypothetical computer   Weizmann Inst.

RSA

matrices, huge



look for a matrix that is not sparse



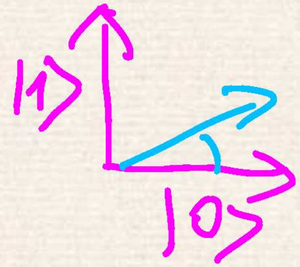
the impact:

RSA ~~→~~ from ~~to~~ 1K → 2K

Qubit concept

- instead of a bit with discrete states 0 and 1 we have a linear combination of basis vectors denoted by $|0\rangle$ and $|1\rangle$:

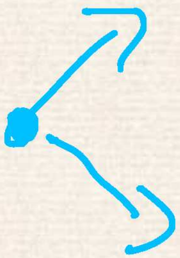
$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle$$



with α, β complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$

- a measurement of $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ yields $|0\rangle$ with pbb $|\alpha|^2$ and $|1\rangle$ with pbb $|\beta|^2$
- measurement may be performed only for an **orthogonal basis**.
- The basis can be different from $|0\rangle$ and $|1\rangle$. E.g.:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



$\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$

Measuring qubits

- **fundamental property:**

  measuring $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ for basis $|0\rangle$ and $|1\rangle$ yields both 0 and 1 with probability 0.5

- this seems to be a **perfect source of random bits**:

  1) generate fotons $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

  2) measure them in basis $|0\rangle$ and $|1\rangle$

- moreover: **reading changes the state to the state read:**
  - if the result is $|0\rangle$, then the physical state becomes $|0\rangle$ as well,
  - if the result is $|1\rangle$, then the physical state becomes $|1\rangle$ as well,
  - **there is no state $\alpha \cdot |\mathbf{0}\rangle + \beta \cdot |\mathbf{1}\rangle$ anymore.**

- **In fact, this is the core of Shor'a algorithm - a reading operation creates a change in a physical system that would be infeasible to compute on a classical computer**

- instead of a single bit we may have strings of qubits, say of length l where $l > n$

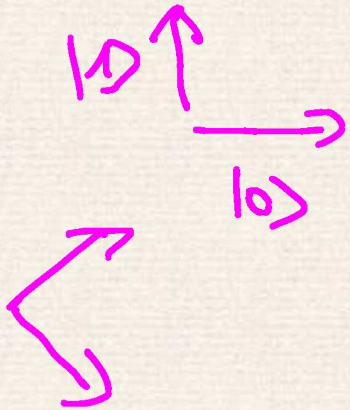
Random Number Generators

Problems:

- **high price**
- while physical source might be ok, reading circuit introduces high **bias**, very poor results (2017) in the standard randomness tests for devices available on the market
- bias can be removed via **additional logic**, but extra hardware may mean place for Trojans and the whole advantage is gone
- **quantum hacking** – attacks on the physical level?

Quantum key transport, BB84

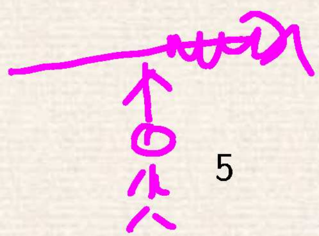
- Charles Bennett and Gilles Brassard, 1984, 1st quantum protocol, even implemented
- key agreement **immune to eavsdropping** (reading qubits is detectable)
- two **bases used**:
  - $|0\rangle$ and $|1\rangle$ (denoted $+$)
  - $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (denoted $\times$)



- **encoding of bits**:

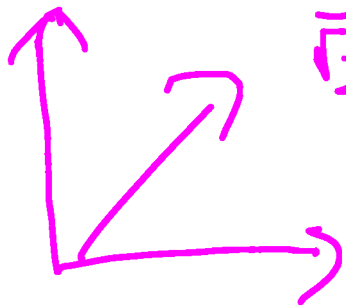
basis $+$: $|0\rangle = 0$ $|1\rangle = 1$

basis $\times$: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = 0,$ $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = 1$



+

<u>Read</u> 0 ↗ in X



$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

read 0 : ppb 0.5

1 ppb 0.5

Basis X :

read 0 : ppb 1

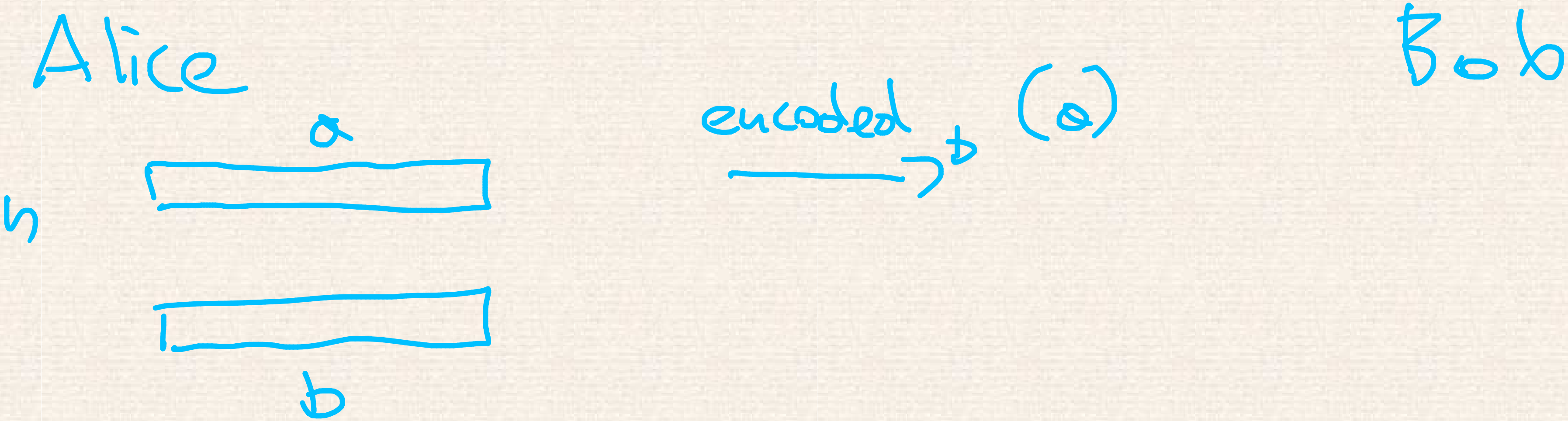
read 1 : ppb 0

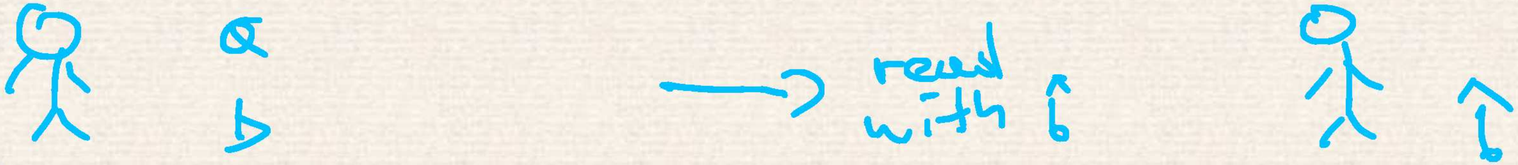
Steps:

1. Alice chooses at random bitstrings a and b of length n

2. for $i \leq n$ Alice encodes a_i according to basis indicated by b_i (0 indictes $+$, 1 indicates $\times$)

3. Alice sends n photons (codes for a)





4. Bob chooses at random string $\hat{b}$ of n bits,

5. For the ith photon, Bob measures the photons using the basis indicated by $\hat{b_i}$

6. Alice sends b to Bob over a traditional (public) channel, Bob sends $\hat{b}$ to Alice

7. Alice and Bob take the substring K of bits a_i such that $b_i = \hat{b_i}$

8. Alice chooses a subset of 50% of bits of K and discloses them to Bob

9. Bob checks how many of them disagree with his measurement. If above some threshold then it is likely that an adversary has measured the transmission as well and the protocol is aborted (environment may also create inconsistencies)

10. the unpublished substring of K may differ between Alice and Bob: an error correcting procedure applied (error correction attracts the bitstrings to the closest codewords, so if the strings of Alice and Bob differ slightly, then they result in the same codeword)

11. "privacy amplification": hashing to a much shorter string

1) $b_i = \hat{b}_i$

$\xrightarrow{a_i}$

Bob learns a_i

2) $b_i \neq \hat{b}_i$

$\xrightarrow{a_i}$

Bob learns random output

Trick to detect adversary

Adv.

$+ \longrightarrow$ 1) $+ \longrightarrow +$

1

0

2) $\times$

$\frac{1}{2}$

$\frac{1}{2}$

1

0

with pbb $\frac{1}{2}$ a_i sent $\neq$ a_i received by Bob

Similarly

Alice: Mallet Bob:

x $+$ x

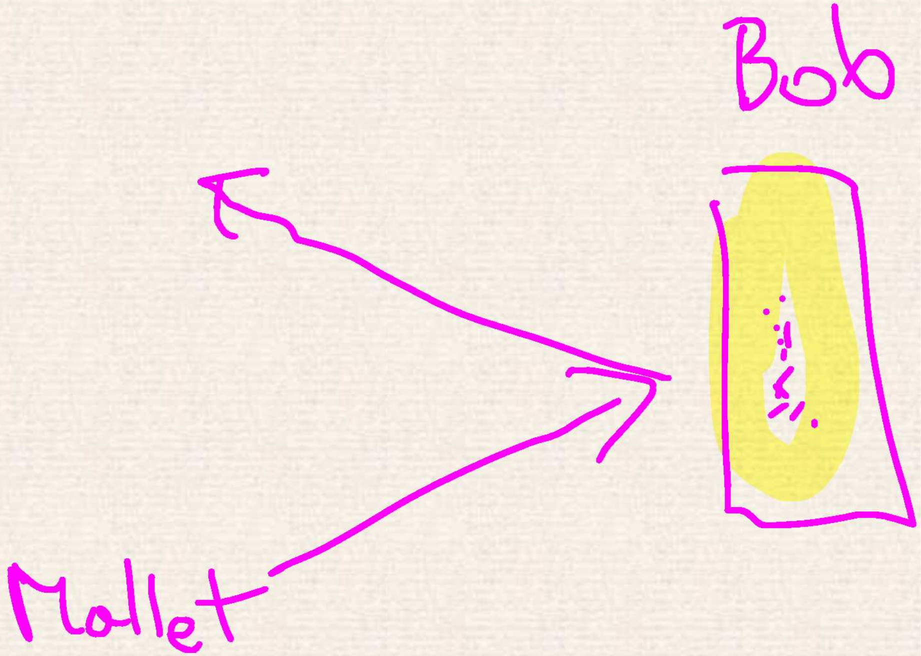
the same trouble!

effect of eavesdropping:

- assume that Alice chooses basis $\times$ to encode 0,
- eavesdropper Eve chooses a different basis for the measurement: namely $+$
- Eve gets $|0\rangle$ with pbb $.5$ and $|1\rangle$ with pbb $.5$, say $|0\rangle$ has been obtained
- at the same time the photon converted to $|0\rangle$ (important!)
- Bob measures the photon according to the basis $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- $|0\rangle = \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\Big)$, so both results of the measurements (i.e $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are equally probably for Bob, so the measurement of Bob indicates 1 with pbb $.5$
- corollary: eavesdropping creates inconsistency between Alice and Bob with pbb $.5$ once Eve chooses a different basis than Alice and Bob $\Rightarrow$ this is why 50% of agreed bits have to be checked

quantum hacking: in theory the algorithm is wonderful, but the problems come with physical realization

→ sending many photons to Bob at the time when his hardware already set for a measurement. Reflected photons show the basis used



changed READ

changed

Eckert algorithm:

- **entangled pair of photons**: measurement of one of them makes the mirror change of the other photon
- procedure:
  1. generate entangled qubits $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ by some source
  2. measure them by Alice and Bob on both ends of the channel

Properties:

- long distance transmissions possible, even to a moving airplane, satellite, etc
- over optical fibre or in free space (vacuum better)
- 1203 km between ground stations over satelite (China)
- both BB84 and Eckert can be used
- high price
- does not solve man-in-the-middle issue

Alice

Read $+$

Source

Bob

Read $+$

result

$|1\rangle$

$|0\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

result

if $|0\rangle$

if $|1\rangle$