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**

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.:

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

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**:
  - generate fotons $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - 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 $\boldsymbol{\alpha} \cdot |\mathbf{0}\rangle + \boldsymbol{\beta} \cdot |\mathbf{1}\rangle$ 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 $\times$: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = 0,$ $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = 1$

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

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

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

Quantum computing and Shor factorization algorithm

many software systems and embedded devices with RSA, no update is possible

Problem and its algebraic context:

- given an RSA number $n = p \cdot q$ for prime factors p and q of a similar size, the goal is to find p or q

n p

- in order to break factorization problem it suffices to learn a nontrivial root r of 1:
    - $r \neq -1$
    - $r^2 = 1 \bmod n$

there 4 roots of 1:

$1, -1, a, b$:

$a = 1 \bmod p$, $a = -1 \bmod q$

- indeed
    - $r^2 - 1 = \overset{p}{(r-1)}\overset{q}{(r+1)} = 0 \mod p \cdot q$
    - therefore p divides either $r-1$ or $r+1$
    - if p divides $r-1$ then q cannot divide $r-1$ as then $r-1$ would be at least n, but $r-1 < n$, in this situation we compute $\mathrm{GCD}(n, r-1)$, the result must be p
    - if p divides $r+1$ then q cannot divide $r+1$ and therefore q must divide $r-1$. In this case $\mathrm{GCD}(n, r-1)$ yields q

similar: primality testing

- if for a given $a < n$ we find s such that $a^s = 1$, then with probability ≥ 0.5 we get $a^{s/2}$ as a nontrivial root of 1. Indeed:
  - by Chinese Reminder Theorem a number $a < n$ is represented by

    $$a_p = a \bmod p \text{ and } a_q = a \bmod q$$

  - given a and b we may compute representation of $a \cdot b \bmod n$ by computing $a_p \cdot b_p \bmod p$ and $a_q \cdot b_q \bmod q$
  - there are two roots of 1 modulo $\mathrm{prime\,number}\; p\text{: } 1 \text{ and } p - 1$
  - if $a^s = 1 \bmod n$, while $a^{s/2} \neq 1 \bmod n$, then $a^{s/2} \bmod p$ is 1 or -1
  - there are the following cases:
    1. $a^{s/2} = 1 \bmod p$, $a^{s/2} = -1 \bmod q$
    2. $a^{s/2} = -1 \bmod p$, $a^{s/2} = 1 \bmod q$
    3. $a^{s/2} = -1 \bmod p$, $a^{s/2} = -1 \bmod q$ $= -1$

    the last case corresponds to $-1 \bmod n$, the first two ones to a nontrivial roots of -1
- so it suffices to find such an s - the order of a. By repeating the procedure for different a's we finally find a nontrivial root of $-1 \bmod n$

Quantum operations and gates

- **a quantum computer should perform some operations on qubits**, technical realization is a challenge, but in theory possible
- we consider l-qubit numbers as representing numbers mod 2^l (well, this is fuzzy as each bit is fuzzy as a qubit), in this way we a get quantum state for each $a < q = 2^l$
- **Hadamard transformation:** an easy way to create a quantum state such that takes any value a (denoted $|a\rangle$) with the same probability. The way to achieve this is:
  - create the state $|0....0\rangle$
  - apply Hadamard transformation gate to it. That is, each ccordinate is transformed by

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1,1 \\ 1,-1 \end{pmatrix}$$

so $|0\rangle$ is transformed to

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

$x_1 \cdot (1,0 \ldots 0) + x_2 \cdot (0,1,\ldots 0) + \ldots$

Quantum Fourier transform:

- regular FT: $(x_1, \ldots, x_N)$ transformed to $(y_1, \ldots., y_N)$ where

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \cdot e^{(2\pi i \cdot j \cdot k)/N}$$

- quantum:

$\sum x_i \cdot |i\rangle$ transformed to $\sum y_i \cdot |i\rangle$ where

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \cdot e^{(2\pi i \cdot j \cdot k)/N}$$

- in other words:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{(2\pi i \cdot j \cdot k)/N} \cdot |k\rangle$$

an „efficient implementation" is based on similar algebra as for DFT

Shor's algorithm (based on presentation of Eric Moorhouse)

1. fix q such that $2n^2 < q < 3n^2$, $q = 2^l$ (or a product of small primes)

   we use states with $2l$ qubits, notation $|a, b\rangle$ or $|a\rangle|b\rangle$

2. **initial state:** prepare state $|0,0\rangle$ and apply Hadamard transformation to the first register.

   the result is the state with each $|a, 0\rangle$ with the same probability

$$|\psi\rangle = \frac{1}{\sqrt{q}} \cdot \sum_{a=0}^{q-1} |a, 0\rangle$$

3. **random $\boldsymbol{x}$:** fix $x < n$ at random

4. **quantum exponentiation:** to the state $|\psi\rangle$ apply the transformation

$$|a, 0\rangle \rightarrow |a, x^a \bmod n\rangle$$

the result is

$$\frac{1}{\sqrt{q}} \cdot \sum_{a=0}^{q-1} |a, x^a \bmod n\rangle$$

(there is a theory how to make such a computation with quantum gates)

5. **measure the second register:** the result is some k. But then the measured state changes to

$$\frac{1}{\sqrt{M}} \cdot \sum_{a \in A} |a, k\rangle$$

where A is the set of all a such that $x^a = k \bmod n$

so $A = \{a_0, a_0 + r, a_0 + 2r....\}$ where r is the **order** of x and $M = |A|$ (so $M \approx q/r$)

$$\frac{1}{\sqrt{M}} \cdot \sum_{d=0}^{M-1} |a_0 + d \cdot r, k\rangle$$

$$x^{a_0+r} = x^{a_0} \cdot x^r = x^{a_0} \cdot 1 = x^{a_0} = k$$

6. **DFT on the first register:** this changes the state

$$\frac{1}{\sqrt{M}} \cdot \sum_{d=0}^{M-1} |a_0 + d \cdot r, k\rangle$$

to

$$\frac{1}{\sqrt{q \cdot M}} \cdot \sum_{c=0}^{q-1} \sum_{d=0}^{M-1} e^{2\pi i \cdot c(a_0 + d \cdot r)/q} \cdot |c, k\rangle$$

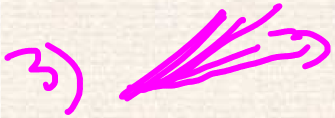
which is equal to

$$\sum_{c=0}^{q-1} \frac{e^{2\pi i \cdot c \cdot a_0/q}}{\sqrt{q \cdot M}} \sum_{d=0}^{M-1} e^{2\pi i \cdot c \cdot d \cdot r/q} \cdot |c, k\rangle$$

$$\sum_{c=0}^{q-1} \frac{e^{2\pi i \cdot c \cdot a_0/q}}{\sqrt{q \cdot M}} \sum_{d=0}^{M-1} \zeta^d \cdot |c, k\rangle$$

where

$$\zeta = e^{2\pi i \cdot c \cdot r/q}$$

3) 

2)

1)

$\zeta = 1$

$1+1+1+\ldots$

7. **measure the first register** (this is the key moment!!) of

$$\sum_{c=0}^{q-1} \frac{e^{2\pi i\cdot c\cdot a_0/q}}{\sqrt{q\cdot M}} \sum_{d=0}^{M-1} \zeta^d \cdot |c,k\rangle$$

- which c is read depends on the values of $\sum_{d=0}^{M-1} \zeta^d$ which in turn corresponds to the probability
- if $\underline{c\cdot r/q}$ is not very close to an integer, then the sum is $\boxed{\frac{1-\zeta^M}{1-\zeta}}$
- if $c\cdot r/q$ is an integer, then we sum up M ones
- so the former case is unlikely and the readings are concentrated around values c such that

$$c/q \approx d/r$$

$$d \approx \frac{c\cdot r}{q}$$

for an integer d

- the rest is a classical computation involving c, q and trying different d's. The search space is relatively narrow – advanced algebraic methods on traditional computers

$$\boxed{\frac{c}{q}} \approx \frac{d}{r}$$

DLP Systems

almost the same algorithm works for finding discrete logarithms , say modulo p

assume we are given x and have to compute m such that $x = g^m$

Steps

$x^0 \cdot g^{-0} = 1 \cdot 1 = \underline{1}$

1. define function $f(\alpha, \beta) = x^\alpha \cdot g^{-\beta}$, it is constant on pairs $(0,0)$, $(1,m)$, $(2,2m)$, $(3,3m)$, ...

2. construct

$x^1 \cdot g^{-m} = g^m \cdot g^{-m} = g^0 = \underline{1}$

$$\boxed{\frac{1}{p} \cdot \sum_{a,b \in Z_p} |a, b\rangle}$$

$$f(a, \delta + a \cdot m) = x^{a} \cdot g^{-\delta - am} =$$

$$= x^{a} \cdot x^{-a} \cdot g^{-\delta} = g^{-\delta}$$

3. apply a quantum circuit to get

$$\frac{1}{p} \cdot \sum_{a,b \in Z_p} |a, b, f(a,b)\rangle$$

4. measure the third register, if the result is $g^{-\delta}$, then the quantum state can be expressed as follows (for unknown δ):

$$\frac{1}{\sqrt{p}} \cdot \sum_{a \in Z_p} |a, \underline{\delta + a \cdot m}, g^{-\delta}\rangle$$

(we cannot derive δ directly from the 2nd component, as before..)

5. take QFT (and skip the 3rd component) to get

$$\frac{1}{p^{3/2}} \cdot \sum_{a,\mu,\nu \in Z_p} \omega_p^{\mu \cdot a + \nu \cdot (\delta + a \cdot m)} |\mu, \nu\rangle$$

$\mu+\nu\cdot m=$

that equals

$$\frac{1}{p^{3/2}} \cdot \sum_{\mu,\nu\in Z_p} \omega_p^{\nu\cdot\delta} \cdot \sum_{a\in Z_p} \omega_p^{a\cdot(\mu+\nu\cdot m)} |\mu,\nu\rangle$$

6. note that $\sum_{\alpha\in Z_p} \omega_p^{\alpha\cdot\beta}$ is equal to $\underline{p}$ if $\beta=0$, otherwise is equal to 0.

So in fact the state is

$$\frac{1}{p^{1/2}} \cdot \sum_{\nu\in Z_p} \omega_p^{\nu\cdot\delta} \cdot \sum_{a\in Z_p} |-\nu\cdot m,\nu\rangle$$

7. measure this state in the standard base to get some

$$|-\nu\cdot m,\nu\rangle$$

$\frac{-\nu\cdot m}{\nu} = -m$

now just divide the first component by the second one to get m

$$f_y(x) = \begin{cases} 1 & g^x = y \\ 0 & \text{otherwise} \end{cases}$$

Grover algorithm

a general algorithm for functions f such that $f(x) = 0$ except for a single z, where $f(z) = 1$

Goal: find z if you can compute f (via quantum gates)

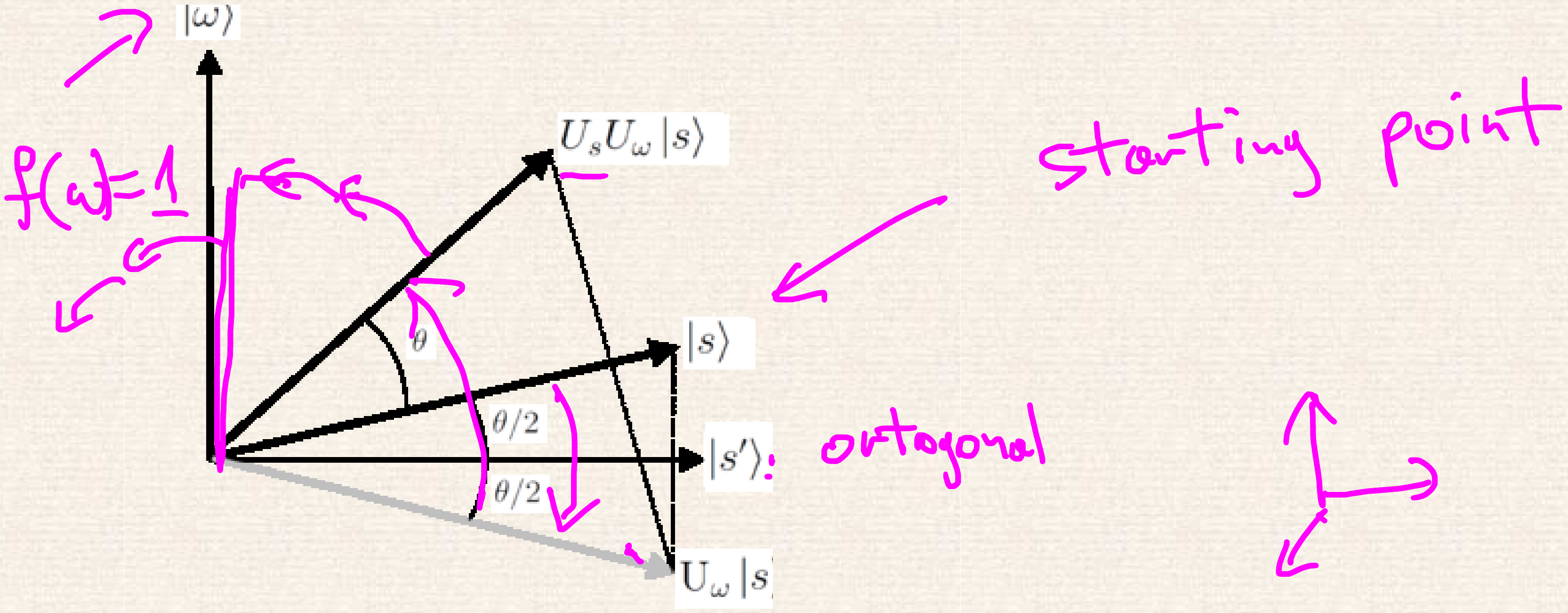
without quantum: if domain of f has N elements, then $N/2$ steps on average

Grover's algorithm: about $N^{1/2}$ quantum steps

(it has been shown that Grover's algorithm is optimal, no exponential speedup possible)

Grover algorithm - geometrical idea

(pict. from Wikipedia)



Consequences!

~~break~~ brute for Enc

$$\begin{tikzcd} 2^{256} \arrow[d, squiggly] \\ 2^{128} \end{tikzcd}$$

Knapsack systems

in focus again

Lattice

Other algebraic structures

e.g lattice based crypto – so called “postquantum cryptography”

CATACRYPT or catastrophy cryptography

- what happens if assumptions broken (e.g. DL solvable for some group)?
- ”use post-quantum crypto”

reality:

- post-quantum is at early stage, no industrial products, logistically impossible to replace
- no plans, scenarios, ...
- consequences of building a quantum computer or anything that breaks the current mechanisms:
    i. option 1: the situation is well hidden, the party controlling the means uses it without leaving traces but still claims the system is secure
    ii. option 2: disclosed, call for massive conversion to new products (may occur even if there is no quantum computer but it works for increasing sale numbers)
    iii. option 3: disclosed, neglected
- catastrophy is already there