Advanced cryptology

Quantum cryptography

prof. Ing. Róbert Lórencz, CSc., Ing. Tomáš Rosa, Ph.D.

České vysoké učení technické v Praze, Fakulta informačních technologií
Katedra počítačových systémů

Příprava studijních programů Informatika pro novou fakultu ČVUT je spolufinancována Evropským sociálním fondem a rozpočtem Hlavního města Prahy v rámci Operačního programu Praha — adaptabilita (OPPA) projektem CZ.2.17/3.1.00/31952 – „Příprava a zavedení nových studijních programů Informatika na ČVUT v Praze“.
Praha & EU: Investujeme do vaší budoucnosti

Tato přednáška byla rovněž podpořena z prostředků projektu č. 347/2013/B1a Fondu rozvoje vysokých škol Ministerstva školství, mládeže a tělovýchovy

Lecture overview

- Information properties
- Quantum bit - qubit
- Basic quantum cryptography characteristic
- Protocol BB84
- Quantum register
- Quantum computing phenomena
- Algorithms for quantum computers
- Quantum cryptology

Classic and quantum conception of information

- Classical information
  - Possible to copy at will. Especially it is possible to create completely identical copy of given message.
- Quantum information
  - Identical copy of unknown state cannot be made.
    - Based on Heisenberg uncertainty principle [1].
    - Reading of the message is influencing its contain.

[1] Heisenberg uncertainty principle is mathematical property of two canonically conjugates. The most known variables of this type are *location* and *momentum* of elementary particle in quantum physics.

$$\triangle x \triangle p \geq \frac{\hbar}{2},$$

where $\hbar$ is so called reduced Planck constant.
With increasing precision of definition of the first conjugate variable, the definition of the second is diminishing and so even without a regard on machine quality.
Claim from classic physic: we can foretold the system behavior, when we know initial state.
For quantum physics does not apply: we can never find out the initial state of the system with sufficient precision $\Leftarrow$ we cannot measure precisely both these conjugate variables at the same time.

Classical and quantum cryptography

- Classical cryptography
  - Has to even with possibility of unlimited copying of the classical information carrier.
    - ★ Usage of keys with extreme lengths – one-time pad principle.
    - ★ Relies on computational complexity.

- Quantum cryptography
  - Based on impossibility of making the identical copy of unknown quantum state.
    - ★ At first is transmitted the key, which is canceled with positive eavesdrop detection.

Cryptographic engineering – birth of new cryptosystem

- We must find out the right problem
  - Definition of its unmanageability
    - Principal logic impossibility - Vernam cipher
    - Computational complexity, and so on. - asymmetric methods
    - Physical (not technological!) limitations - quantum cryptography
  - Way of defining, fixing of weak (easily manageable) instances

- We must find the right reduction
  - By the type of the schema: cipher, signature, authentication, and so on.
  - How to change the problem of decryption to a problem of solving the given problem?
  - Furthermore, the problem must be define even especially solve/evade
    - With knowledge of some information (secret key) - ciphers, signatures, and so on.
    - With special way of computation (in a way of one-way function) - hash function

Quantum cryptography - main features

- Unconditional security
  - In theory the the system security can be proven without account of attackers means.
  - In theory you can achieve also absolute security.
  - It is assumed, that security of these systems won't be affected even in the age of quantum computers.
- Main focus is still on message transmission.
  - With preservation of quantum encrypted information are connected certain technological problems.
- Some types of schema are not sufficiently worked out.
  - Quantum schema of digital signature.

Unconditional security...

- Understand mainly with respect on computational power of rival.
  - Need of better precision and objective generalization.
- Also „unreal“ conditions are at last logical conditions and we must know them.

Logical conditions remains...

- Often „dressing“ of conditions
- We do not care about computational power, but we claim that:
  - Attacker has noisy signal income
  - Attacker has not enough of fast memory
  - Cannot influence area of radio broadcasting
  - ....
  - Does for an attacker apply the quantum mechanics?

Unconditional security - continuum

Based on qualitative difference

- We are focusing on meaning of purely logical conditions (limitations) in real world.
- We differ:
  1. technical conditions (DES encryption) i don't want to do it, i don't have money...
  2. technological conditions (RSA encryption) today i don't know how to handle, but someday maybe...
  3. physical conditions (quantum methods encryption) based on everything i will never be able to do it... (if I am not an alien...)

Quantum bit - qubit

- For a physical image of a qubit we consider arbitrary quantum mechanics defined object, which states are the elements of two dimension Hilbert space.
  - Photon (polarization, phase shift)
  - Electron (spin)
  - Atom (spin)
- Formally:
  - Corresponding to measured value (quantum system collapse), $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$, where:
    - $\omega_0, \omega_1 \in C$, $|0\rangle, |1\rangle$ are base vectors H_2
    - $|0\rangle, |1\rangle$ called eigenstates of qubit.
  - Measuring of qubit we get the corresponding value of exactly 1 eigenstate.
  - Superposition cannot be „seen“.
    - Coefficients ω_0, ω_1 defines the distribution of measure outcomes.
    - P[MEASURE= $|\alpha\rangle$] $= |\omega_\alpha|^2, \alpha \in \{0, 1\}$
    - By measuring the superposition expires and qubit passes into eigenstate.
- Measuring of one qubit we get at most 1 bit of classical information

Polarization coding

- Linear ($"+"$)
  - $|0\rangle_{(r)} = "|"$
  - $|1\rangle_{(r)} = "-"$
  - $|\psi\rangle = \omega_{(r),0}|0\rangle_{(r)} + \omega_{(r),1}|1\rangle_{(r)}$
- Diagonal ($"\times"$)
  - $|0\rangle_{(d)} = "\diagdown"$
  - $|1\rangle_{(d)} = "\diagup"$
  - $|\psi\rangle = \omega_{(d),0}|0\rangle_{(d)} + \omega_{(d),1}|1\rangle_{(d)}$

Usage in cryptography

- *Heisenberg uncertainty principle*: cannot exactly determine the state of given qubit in linear and diagonal base.
  - With correctly chosen diagonal base you can for example say:
    - $|0\rangle_{(r)} = \sqrt{\frac{1}{2}}\,(|0\rangle_{(d)}+|1\rangle_{(d)})$
    - $|1\rangle_{(r)} = \sqrt{\frac{1}{2}}\,(|0\rangle_{(d)}-|1\rangle_{(d)})$
  - Interpretation: With increasing definition of state accordingly to a linear basis, equally lower is the state defined accordingly to a diagonal basis and vice versa.

Protocol BB84 - Benett-Brassard 1984

Absolutely secure cryptosystem

- The perfect cryptosystems exist.
- For example **One-Time Pad (OTP)**
- But the problem is the secure distribution of keys.

Solution:

- Distribution of key (establishing the shared key) based on quantum principle ensuring the perfect secrecy.
- Protocol BB84 is used to establish the symmetric key with usage of quantum phenomenons..
  - Which is then user for a one-time pad system.
- Based on usage of Heisenberg uncertainty with connection of polarization coding.
- With minor changes is the BB84 used and developed till today.

Protocol BB84 - example of communication

1. Sender (Alice): Generates arbitrary binary sequence and executed its polarization coding with arbitrary chosen base.

1	1	1	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
X	+	X	X	X	X	X	+	X	X	+	+	+	+	X	X	+	+	X	+	+	X	X	+	+
/	-	/	/	/	\	\	-	\	/	|	|	|	|	/	\	|	|	\	-	|	\	\	|	|

2. Receiver (Bob): Decodes received photons with arbitrary chosen base.

/	-	/	/	/	\	\	-	\	/	|	|	|	|	/	\	|	|	\	-	|	\	\	|	|
+	+	X	+	X	X	+	X	+	X	+	+	X	X	+	X	X	+	X	+	X	+	+	+	X
0	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	1

3. Sender (Alice): Tells Bob (publicly, of course with authentication of message origin), which base base in given step she used. The same is done with Bob, Bits, on which they both agreed, will be used for symmetric key.

	✓	✓		✓	✓				✓	✓	✓				✓		✓	✓	✓				✓	
	1	**1**		**1**	**0**				**1**	**0**	**0**				**0**		**0**	**0**	**1**				**0**	

Protocol BB84 - detection of wiretapping 1

- It is also necessary to perform wiretapping detection
  - The basic idea: The attacker (Eve) her tapping to affect the passing through qubits.
  - Alice and Bob victimize part of agreed key and by public channel (must authenticate the origin of messages) to compare received value values
  - Wiretapping is reflected as a transmission error.
  - With victimization *n* bits is the probability of detecting systematic wiretapping $1 - (3/4)^n$.
    - ★ Choice *n* this probability can be in the limit closer to value 1.
  - In current systems is still carried out amplification of privacy (privacy amplification).
    - ★ The aim is to further minimize Eva's information about agreed key, which (hopefully) was obtained undetected wiretapping.

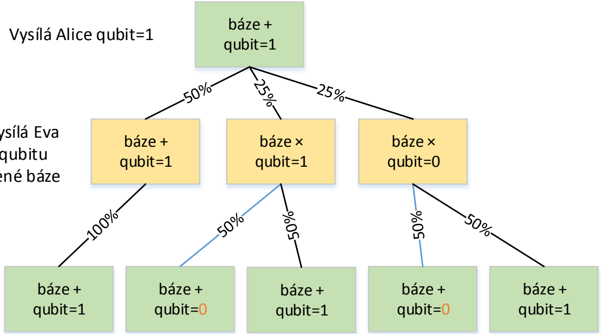
Protocol BB84 - detection of wiretapping 2

By observation or measuring a quantum system changes its status. Example: **qubit**, $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$, when **qubit** is observed, staus **qubitu** gets to collapse and so that either $\omega_0 = 0$ or $\omega_1 = 0$.

Vysílá Alice qubit=1

Přijímá a vysílá Eva hodnotu qubitu podle zvolené báze

Bob přijímá hodnotu qubitu v bázi shodnou s Alici



1 0 1 0 1

Pravděpodobnost, že Bob přijímá správnou hodnotu qubitu = 1 od Alici i když Eva odposlouchává

P = 0,5.1 + 0,25.0,5 + 0,25.0,5 = 0,75

Protocol BB84 - implementation aspects

Two kinds of communication:

- quantum
  - Necessary quality undisturbed communication channel between Alice and Bob.
    - ★ Optical cable without a common infrastructure elements.
    - ★ Necessary to know the model errors.
    - ★ Synchronization of transmission.
- Classical
  - We can use a common network infrastructure.
  - It is not necessary to ensure the confidentiality of messages transmitted.
  - It must be ensured authentication of origin of control messages between Alice and Bob.
    - ★ Use of the radio channel may not be sufficient.

Protocol BB84 - application aspects

- It is able to some extent substitute asymmetric systems in existing applications.
  - Intended particular with the aspect of theoretical threats coming from the field of quantum computers.
- Basically, two types of users:
  - Current users of asymmetric schemes
    - Get higher theoretical security.
    - somewhat lost in comfort.
    - Not all components can not replace (signature).
  - Současní uživatelé vojenských a zpravodajských systémů
    - Gain greater convenience while maintaining approximately the same level of security that they provide them with the current mechanisms based on long random keys

Experimental results - agreement on the key at a distance 23 km

Muller et al. 1995-96, Ribordy et al. 1998, 2000 (foto: Gisin et al. 2001)

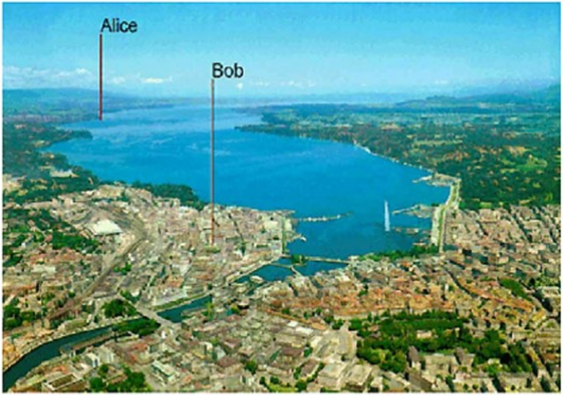


FIG. 13. Geneva and Lake Geneva. The Swisscom optical fiber cable used for quantum cryptography experiments runs under the lake between the town of Nyon, about 23 km north of Geneva, and the centre of the city.

Quantum register

- Suppose the length of n qubits.
  - States of the register are elements 2^n-dimensional Hilbert space.
  - Base vectors (eigenstates) - for example $n = 2$
    - $\mathbf{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$
    - $|\psi\rangle = \omega_{00}|00\rangle + \omega_{01}|01\rangle + \omega_{10}|10\rangle + \omega_{11}|11\rangle$
  - By measuring of the register, we get just one of the 2^n eigenstates.
    - Superposition can not directly "to see".
- Quantum register is the basis of a quantum computer.

The phenomena of quantum computing

- quantum parallelism
  - Thanks to the properties of the quantum register and linearity of its evolution can be used for n-qubit task parallel to solve all 2^n tasks simultaneously.
  - However, the measurement we get just one result → quantum parallelism can therefore not be so easy utilize directly.
- Interference
  - In parallel obtained results can interact.
  - Allows you to use the power of quantum parallelism.
- Interdependent states (entaglement)
  - The results measurement of two separate parts of the registry can be dependent (regardless of the distance between the two parts).
  - Closely related to the teleportation of quantum objects.

Algorithms for quantum computers 1

Shor's algorithm (Shor 1994)

- Solves a fundamental role in (probabilistic) polynomial time.
  - factorization
  - Discrete logarithm - in the general form
- Based on a sophisticated utilization of quantum Fourier transform and interconnection known results from number theory and general algebra.
- Fundamentally influenced of attention given to quantum computers.
- The main argument against the PKI (in its present form) in time of the existence of quantum computers.
- Practically tested on 7-qubit computer.
  - Factorization of number 15, December 19, 2001 (IBM Research).

Algorithms for quantum computers 2

- For practical impact requires *n* -qubit computer, where n is of the order 103 - 104.
  - Thus, there is no acute danger. All these forecasts are extremely heuristic nature and are in range of tens of years.

Grover's algorithm (Grover 1996)

- In unsorted list of length N items is able to find the given record with complexity $O(N^{1/2})$.
  - It was shown that this complexity is the smallest possible
- In cryptanalysis exploitable for brute force attacks.
  - The list consists of a set of keys and the selection criterion is given in the form of ŠT = EK(OT).
  - The symmetric key K with length of k bits can be found with complexity $O(2^{k/2})$.
    - ★ Roughly speaking, the algorithm bisects effective key length.

Quantum cryptology - how to respond to it

- From a theoretical point of view there is only one cryptology.
- In the future will likely coexist systems based on the quantum and classical approach to information processing
  - Can be expected especially hybrid systems.
  - Quantum cryptography does not require a quantum computer - can be expected to enforce before the extinction of some current schemes influence of quantum computers.
- If a system should have long moral life:
  - It should have a modular architecture allowing easy replacement kryptoschemes.
  - It is not appropriate to concentrate on one narrow kind of algorithm - the system must be based on the the general properties and be so open.
  - Reckon with the fact that every single algorithm can be suddenly weakened/broken. This is true regardless of the quantum computer.
  - It is necessary to evaluate the moral life of the protected data.
  - Necessary to monitor current developments in cryptology. The current form is certainly not definitive!