Security

8. Intruduction to elliptic curve cryptography and quantum cryptography

prof. Ing. Róbert Lórencz, CSc.

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 contents

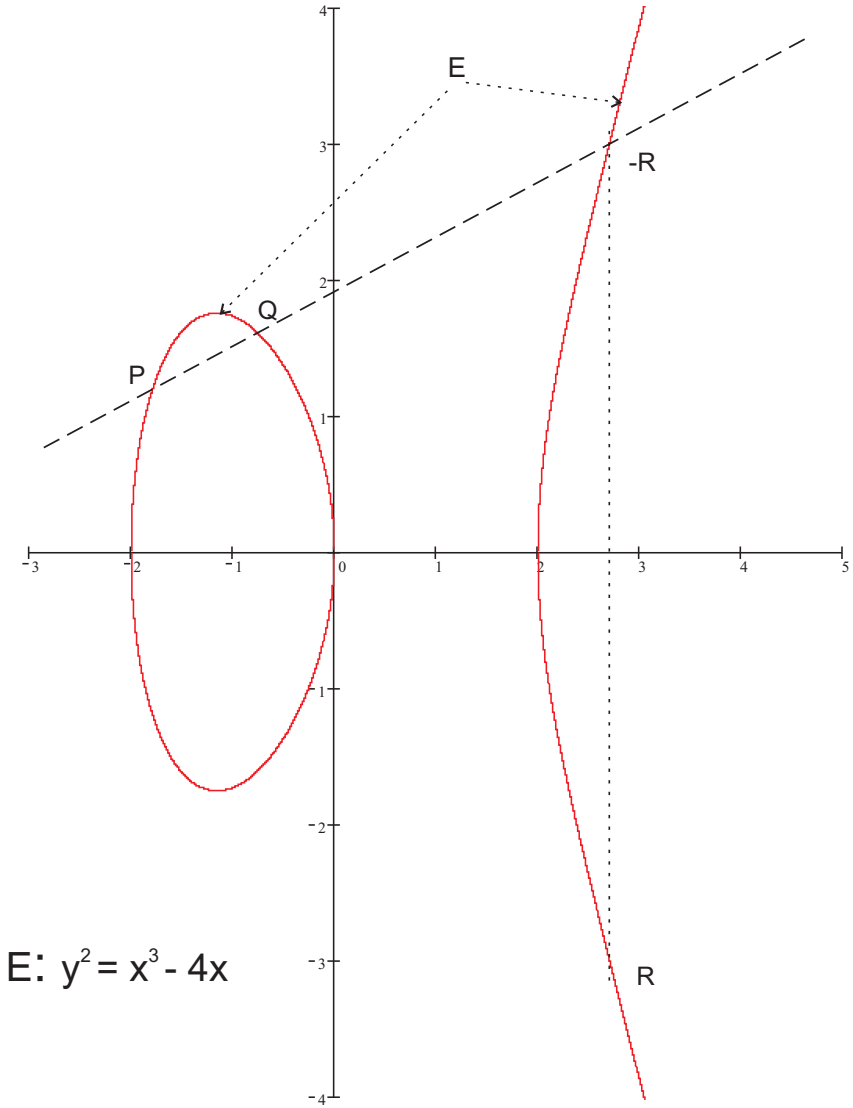
- History
- Mathematical background
- Elliptic curve over $GF(p)$
- ECC and the discrete logarithm problem
- Encryption using ECC
- Properties of information
- Quantum bit - qubit
- Basic characteristics of quantum cryptography
- Protocol BB84

History

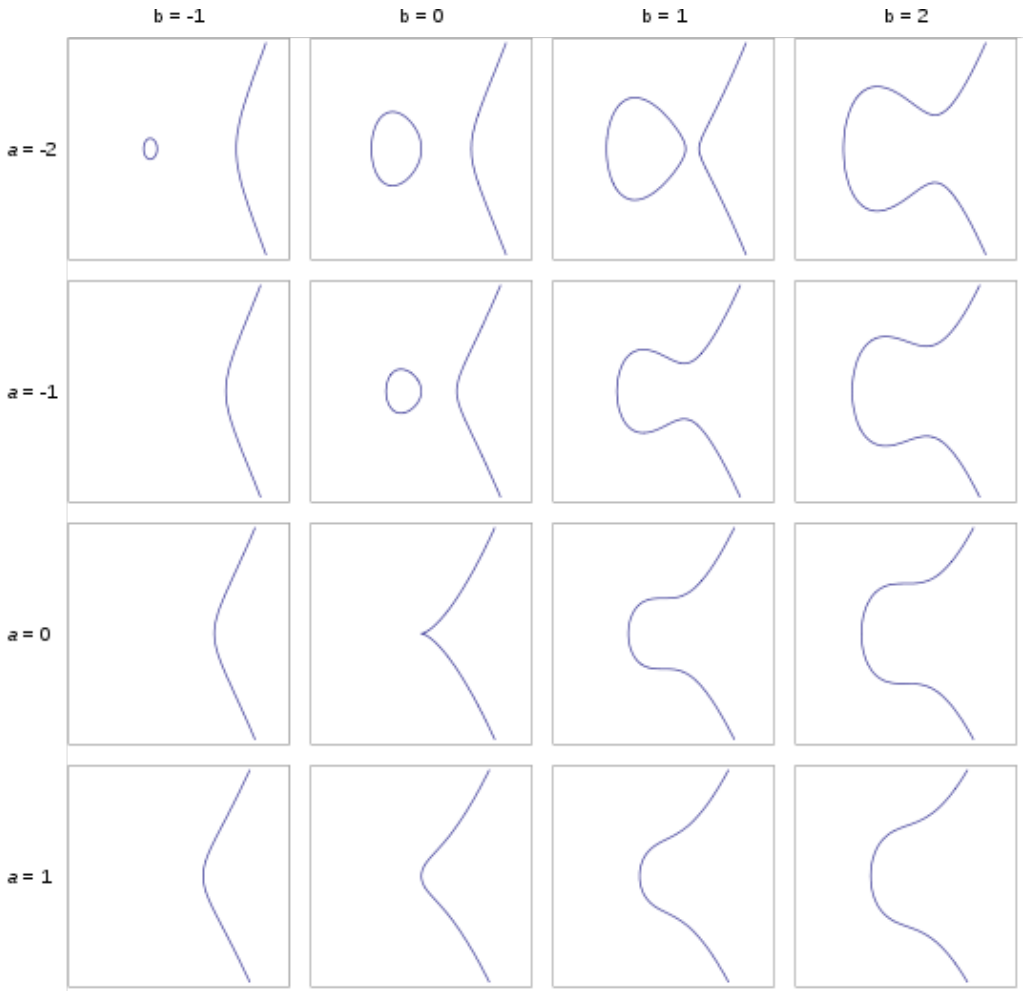
- The elliptic curve cryptography (ECC) is a modern and promising trend of current cryptology.
- ECC provides another way of realising an electronic signature.
- In some aspects ECC exhibits better results than other current cryptosystems.
- Today, ECC is a part of many worldwide standards and has become an alternative to RSA.
- One advantage of ECC is its speeds and low hardware requirements.
- Elliptic curves are a special case of cubic curves.
- The name elliptic comes from the fact that planar cubic functions used to be used to calculate the circumference of ellipses.
- The properties of elliptic curves were studied by the german mathematician K. T. W. Weierstrass (1815 — 1897).
- V. Miller and N. Koblitz discovered, independently of each other, that elliptic curves can be used in public key cryptography (1985).

Mathematical background (1)

- Elliptic curve E is a set of points in a plane, which satisfy the equation
$$y^2 = x^3 + ax + b. \qquad (1)$$
- By adding two different points P and Q from E, we once again receive a point from E, and thus satisfying equation (1).
- A geometric interpretation of the sum: We draw a line through points P = [x_P, y_P] and Q = [x_Q, y_Q], and this line will intersect the curve E in point –R.
- The result of the sum is point R, which is reflectionally symmetric to –R with respect to the horizontal axis x. These points are called *opposite.*



Mathematical background (2)



$$y^2 = x^3 + ax + b$$

Mathematical background (3)

- The slope of the line connecting P $\neq$ Q is

$$s = \frac{y_Q - y_P}{x_Q - x_P}. \tag{2}$$

- Coordinates of point R = $[x_R, y_R]$ satisfy

$$x_R = s^2 - x_P - x_Q \quad \text{and} \quad y_R = s(x_P - x_R) - y_P. \tag{3}$$

- When P = Q $\Rightarrow$ their connecting line is a tangent to E and its slope is

$$s = \frac{3{x_P}^2 + a}{2y_P}. \tag{4}$$

- By adding two opposite points (P = – Q) we should get a "0 point".
- Such a line won't intersect E, resp. will intersect it in ∞. $\Rightarrow$ we define the operations on this "point in ∞"as $\Rightarrow$ P + (–P) = O. *Point in ∞ is the name of the "0 point"of curve E.*
- *We define: P + O = P, O + O = O a O = –O.*
- *This way we have defined additions for $\forall$ pairs of points on E, including 0.*

Elliptic curve over $GF(p)$ (1)

The use of elliptic curves in cryptology

When applying elliptic curves to cryptology, we work with discrete values (integers, binary strings, m-tupes of bits) $\Rightarrow$

- We consider fields GF(2^m) and GF(p), where p is prime.
- Both fields are used in practive – each of them has its advantages.
- To simplify the explanation we will only consider GF(p) from now on.
- The elliptic curve over GF(p) is defined as a point O in ∞ together with a set of points P = [x, y], where x and y are elements of GF(p) which satisfy the equation $y^2 = x^3 + ax + b$ in GF(p), i.e.

$$y^2 \equiv x^3 + ax + b \pmod{p} . \tag{5}$$

Elliptic curve over $GF(p)$ (2)

- The coefficients a and b are also elements of GF(p) and must satisfy the condition
$$|4a^3 + 27b^2|_p \neq 0. \tag{6}$$
- A set defined in this manner forms a group, coefficients a and b can be selected arbitrarily (public parameters of the cryptosystem).
- In this group we define the opposite point to 0 as O = –O, and for the other non-zero points P = [x_P, y_P] $\in$ E we define –P = [x_P, $|-y_P|_p$], furthermore we define P + –P = O and P + O = P for all P $\in$ E.
- Point O is called the zero point, because of its behavior in additions in group E. The sum of non-zero points P + P is defined as R = P + P = [x_R, y_R], where the slope s is
$$s = \left|\frac{3{x_P}^2 + a}{2y_P}\right|_p \tag{7}$$

Elliptic curve over $GF(p)$ (3)

- and the coordinates of R are

$$x_R = \left| s^2 - x_P - x_Q \right|_p \quad \text{and} \quad y_R = \left| s(x_P - x_R) - y_P \right|_p . \tag{8}$$

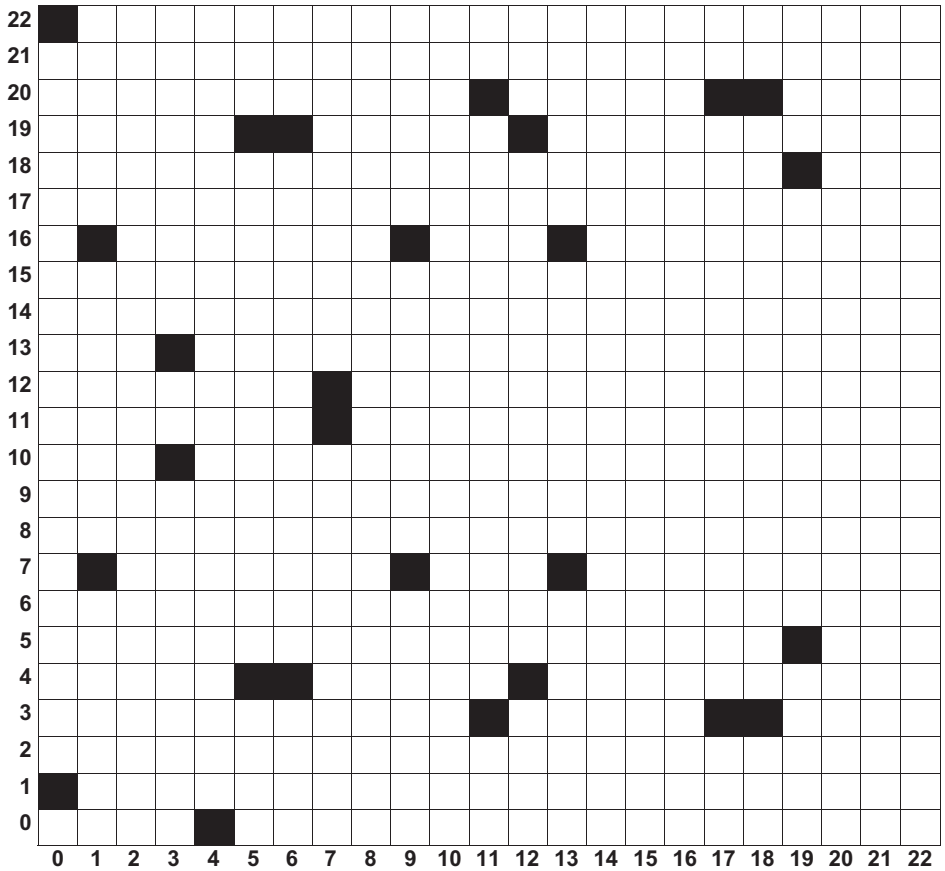
- The sum of two different non-zero and non-opposite points P = $[x_P, y_P]$ and Q = $[x_Q, y_Q]$ of curve E is defined as P + Q = R = $[x_R, y_R]$, where the slope s is

$$s = \left| \frac{y_Q - y_P}{x_Q - x_P} \right|_p \tag{9}$$

- and the coordinates of R are

$$x_R = \left| s^2 - x_P - x_Q \right|_p \quad \text{and} \quad y_R = \left| s(x_P - x_R) - y_P \right|_p . \tag{10}$$

Elliptic curve over $GF(p)$ (4)



(0,1)	(6,4)	(12,19)	(0,22)
(6,19)	(13,7)	(1,7)	(7,11)
(13,16)	(1,16)	(7,12)	(17,3)
(3,10)	(9,7)	(17,20)	(3,13)
(9,16)	(18,3)	(4,0)	(11,3)
(18,20)	(5,4)	(11,20)	(19,5)
(5,19)	(12,4)	(19,18)	O

28 points of the elliptic curve $y^2 = x^3 + x + 1$ over $GF(23)$

Elliptic curve over $GF(p)$ (5)

Example:

$E : y^2 \equiv x^3 + 2x + 2 \pmod{17}, \quad P = [5, 1], \quad 2P = ?$

$$2P = P + P = [5, 1] + [5, 1]$$

$$s = \left|\frac{3x_P^2+2}{2y}\right|_{17} = \left|(2 \cdot 1)^{-1} \cdot (3 \cdot 5^2 + 2)\right|_{17} = \left|9 \cdot 9\right|_{17} = \left|81\right|_{17} = 13$$

$$x_{2P} = \left|s^2 - x_P - x_P)\right|_{17} = \left|13^2 - 5 - 5\right|_{17} = \left|159\right|_{17} = 6$$

$$y_{2P} = \left|s(x_P - x_{2P}) - y_P\right|_{17} = \left|13(5 - 6) - 1\right|_{17} = \left| - 14\right|_{17} = 3$$

$$2P = [6, 3]$$

Zkouška:

$$3^2 \equiv 6^3 + 2 \cdot 6 + 2 \pmod{17}$$

$$9 \equiv 12 + 12 + 2 \pmod{17}$$

$$9 = 9$$

ECC and the discrete logarithm problem (1)

- To understand encryption and signatures using ECC, we need to recall the discrete logarithm problem.
- For a given point P on curve E we calculate points 2P, 3P, 4P, 5P, 6P etc., which gets us different points xP on E.
- Because there is a finite number of points on the curve (we call it #P), after given m steps the sequence will necessarily start repeating.
- in the repetition point mP is then mP = nP, where nP is one of the points already encountered. It follows that mP – nP = O $\Rightarrow$
- there is some $r = m - n, r < m$ such that rP = O. From that follows that the sequence P, 2P, 3P, 4P, 5P,... will always reach point 0 and then the cycle starts again from point P, because $(r + 1)$P = rP +P = O + P = P.
- The smallest such r, for which rP = O, is called the *order of point P*.

ECC and the discrete logarithm problem (2)

- It can be shown that the order of point P divides the order of the curve, if *the order of the curve* is defined as #E, the number of points on the curve.
- Different points of E have different orders. In cryptographic practive we choose such points whose order is equal to the largest prime in #E's factorization or its multiple, which is called co-factor.
- When a point has order r, it is guaranteed that the sequence P, 2P, 3P,... starts repeating no sooner than after r steps.
- In case r is a large number, such as 2^{256}, the sequence becomes really long.
- And this long sequence is particularly useful for encryption and electronic signature, in a direct relation to the discrete logarithm problem.
- If we choose number k as our private key and calculate $Q = kP$, then points P and Q can be published as part of the public key.

ECC and the discrete logarithm problem (3)

- The discrete logarithm problem is the problem of extracting from P and Q the secret number k such that Q = kP.
- It is obvious that for small orders of P this problem is trivial. For large r this task can't be solved effectively, that is, in polynomial time. This is the reason why we can publish P and Q.
- The most efficient method known for solving the discrete logarithm problem defined in this fashion is the so-called Pollard's ρ method, which has a complexity in the order of $(\pi r/2)^{1/2}$ steps.
- If $r = 2^{256}$, we get $\approx 2^{128}$ steps, which is about the same complexity as trying to solve a symmetric block cipher with a 128bit key.
- This is computationally infeasible, and for that reason the cipher is computationally secure.

Encryption using ECC

- We will demonstrate the encryption on an analogy of Diffie-Hellman's key exchange scheme.
- Users i and j want to exchange a secret information over a public channel.
- Each user has received from a trustworthy source the public key of the other user. In the case of ECC we also expect that they share the same curve E and its point P.
- Let d_i resp. Q_i be the private resp. public key of user i, and simialarly d_j and Q_j be keys of user j. Then both users can establish a shared key — point Z on curve E, without commmunicating with each other.
- User i calculates Z as $d_i Q_j$ and user j as $d_j Q_i$. These points are equal, because $Z = d_i Q_j = d_i(d_j P) = (d_i d_j)P$ and at the same time $Z = d_j Q_i = d_j(d_i P) = (d_j d_i)P$.
- In other words, each user adds the public key (point) of the other user n times, where n is the private key. Because both users started in the same point P, they will reach the same point Z.

Classical and quantum information

- Classical information
  - Can be copied. It is possible to create an identical copy of a given message.
- Quantum information
  - It is not possible to create an identical copy of an unknown quantum state.
    - ⋆ Caused by the Heisenberg's uncertainty principle [1].
    - ⋆ Reading a message modifies its content.

[1] Heisenberg's uncertainty principle is the mathematical property of two canonically conjugated variables. The best known such variables are the *position* and the *momentum* of an elementary particle in quantum physics.

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

where $\hbar$ is the reduced Planck constant.
The more precisely we measure one of the conjugated variables, the less precisely can we measure the other, regardless of the quality of our tools.
Classical physics: We can predict the behavior of a system, if we know its initial state.
Quantum physics: The initial state can't ever be precisely measured $\Leftarrow$ we can't precisely measure both conjugated variables.

Classical and quantum cryptography

- Classical cryptography
  - Needs to consider the ability to create unlimited copies of information-carrying media.
    - ⋆ Using extremely long keys – the one-time pad principle.
    - ⋆ Depending on the computational security.

- Quantum cryptography
  - Is predicated by the impossibility of creating identical copies of an unknown quantum state.
    - ⋆ We transfer the key first, and if we detect an eavesdropper, we don't use that key.

Cryptography engineering – birth of a new cryptosystem

- We need to find the right problem
  - Express why it can't be broken
    - ★ Principial logical impossibility - Vernam's cipher
    - ★ Computational complexity etc. - asymmetric methods
    - ★ Physical (not technological!) limitations - quantum cryptography
  - How to define the data, how to prevent creating weak (easily solvable) instances

- We need to find the right reduction
  - Depending on the scheme: encryption, signature, authentication etc.
  - How to express task solution in terms of solving the selected problem?
  - Furthermore, we need to be able to solve special cases of the problem
    - ★ If we know some information (secret key) – ciphers, signatures etc.
    - ★ If we use some special computational process (calculating in the right direction) – hash functions

Quantum cryptography - main factors

- Unconditional security
  - We can theoretically prove that a system is secure regardless of the opponent's abilities.
  - We can theoretically achieve absolute security.
  - We assume that these systems won't be affected even when quantum computers become widely available.
- The current research focuses on transporting the messages.
  - Storing quantum-encrypted information is currently technologically challenged.
- Some schemes are not adequately researched yet.
  - Quantum digital signature schemes.

Unconditional security...

- Was understood mostly in terms of the computational power of an adversary.
  - Needs to be made more precise – an objective generalization.
- Even "un-realistic"conditions are logical conditions and we need to know them.

Logical conditions remain...

- Frequent "re-dressing"of conditions
- We don’t talk about the computational power, but claim that:
  - the adversary receives a noisy signal
  - the adversary doesn’t have enough fast memory
  - the adversary can’t influence wide-area radio signals
  - ....
  - the adversary isn’t constrained by quantum mechanics?

Unconditional security - contd.

It's a qualitative difference!

- We are considering logical conditions (limitations) in the real world.
- We need to differentiate between:
  1. technical conditions (breaking DES) I don't want to do it today, can't be bothered, not enough money...
  2. technological conditions (breaking RSA) I don't know how to compute it today, but one day perhaps...
  3. physical conditions (breaking quantum cryptography) likely I won't ever be able to do it... (unless I am an extra-terrestrial...)

Quantum bit - qubit

- The physical realization of qubit can be any object described in terms of quantum mechanics whose states are elements of a two-dimensional Hilbert space:
  - Photon (polarization, phase shift)
  - Electron (spin)
  - Atom (spin)
- formally:
  - related to the measured value (a 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 the basis vectors H_2
    - $|0\rangle, |1\rangle$ are called the eigenstates of the qubit.
  - By measuring a qubit we get a value related to exactly one eigenstate.
  - Superposition can't be "seen".
    - Coefficients ω_0, ω_1 define the distribution of the results of measurements.
    - P[MEASUREMENT= $|\alpha\rangle$] $= |\omega_\alpha|^2, \alpha \in \{0, 1\}$
    - By performing the measurement we destroy the superposition and a qubit achieves one eigenstate.
- By measuring one qubit we can get at most 1 bit of classical information.

Polarization encoding

- 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's uncertainty principle*: We can't accurately measure the state of a qubit according to both linear and diagonal basis.
  - We can choose a diagonal basis such that:
    - $|0\rangle_{(r)} = \sqrt{\frac{1}{2}}\,(|0\rangle_{(d)} + |1\rangle_{(d)})$
    - $|1\rangle_{(r)} = \sqrt{\frac{1}{2}}\,(|0\rangle_{(d)} - |1\rangle_{(d)})$
  - Interpretation: The more definitive is the state respective to the linear basis, the less definitive it is respective to the diagonal basis, and vice versa.

BB84 procokol - Benett-Brassard 1984

Absolutely secure cryptosystems

- We know of perfect cryptosystems.
- For example **One-Time Pad (OTP)**
- The problem of secure key distribution remains.

Solution:

- The key distribution can be implemented using a quantum process which guarantees a perfect security.
- Protocol BB84 uses quantum mechanics to establish a shared symmetric key
  - Which is then used in a classical one-time pad system.
- Based on the Heisenberg's uncertainty principle as applied to the polarization encoding.
- BB84 is, with minor modification, still used and studied today.

BB84 procokol - example of communication

1. Sender (Alice): Generates a random binary sequence and performs its polarization encoding in a randomly 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
X	+	X	X	X	X	X	+	X	X	+	+	+	+	X	X	+	+	X	+	+	X	X	+	+
/	-	/	/	/	\	\	-	\	/	|	|	|	|	/	\	|	|	\	-	|	\	\	|	|

2. Recipient (Bob): Decodes received photons according to a randomly 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, but with authentication) which base she chose for which qubit. Bob does the same. The bits where both chose the same base, will be used to create the symmetric key.

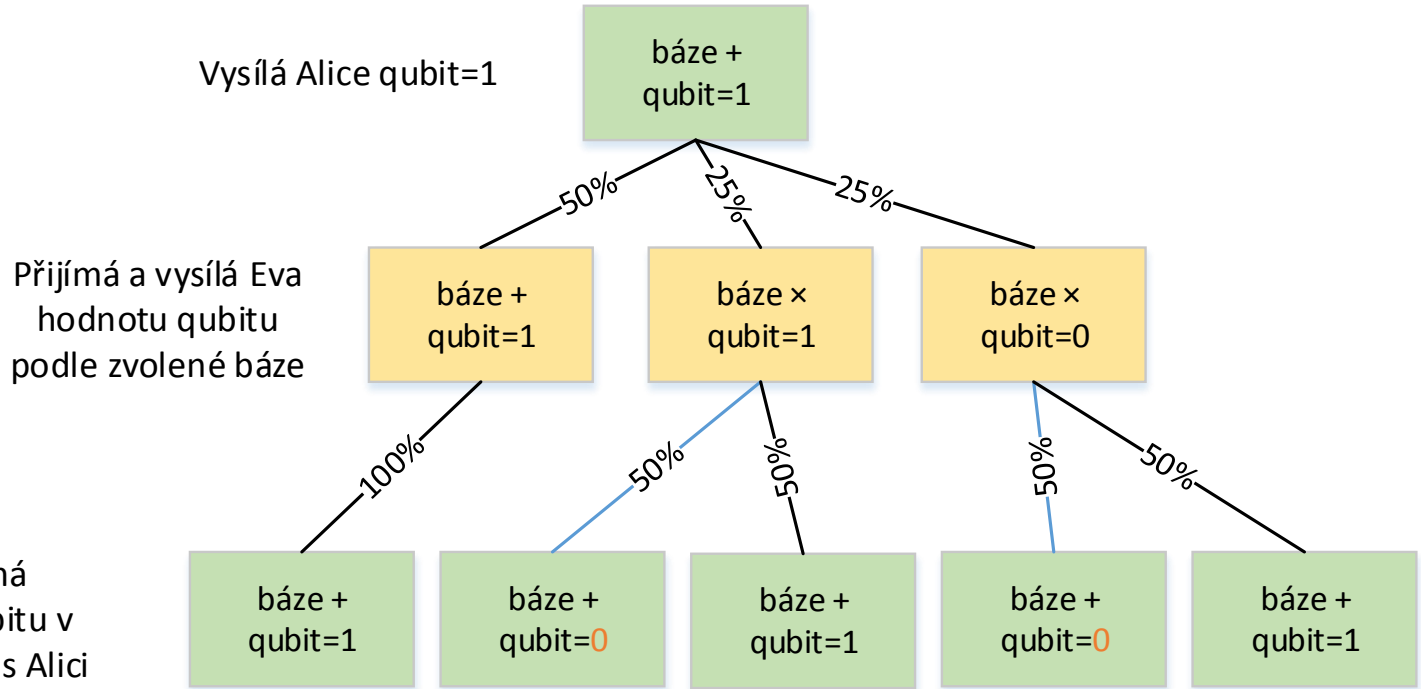
	✓	✓		✓	✓				✓	✓	✓				✓		✓	✓	✓				✓	
	1	**1**		**1**	**0**				**1**	**0**	**0**				**0**		**0**	**0**	**1**				**0**	

BB84 protocol - detecting an eavesdropper 1

- Now they need to perform detection of an eavesdropper.
  - Basic idea: The attacker (Eve) will modify the state of qubits by observing them.
  - Alice and Bob sacrifice a part of their established key and through a classical channel (with authentication!) compare the values they received.
  - Eve will appear as an error during transmission.
  - If they sacrifice n bits, they can detect continually active Eve with probability $1 - (3/4)^n$.
    - ⋆ By choosing the n they can achieve the probability as close to 1 as they desire.
  - Current cryptosystems additionally perform privacy amplification.
    - ⋆ The goal is to minimize what information about the shared key Eve could possibly get from an undetected eavesdropping.

BB84 protocol - detecting an eavesdropper 2

When observed or measured, a quantum system changes its state. Example: **qubit**, $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$, when **qubit** is measures, the **qubit's** state collapses into either $\omega_0 = 0$ or $\omega_1 = 0$.



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

BB84 - protocol - Implementation aspects

Two kinds of communication:

- Quantum
  - Requires a high-quality low-noise communication channel between Alice and Bob.
    - ⋆ Optical cable without common infrastructure elements.
    - ⋆ The error model must be known.
    - ⋆ Transmission must be synchronized.
- Classical
  - Can use common network infrastructure.
  - Does not need to ensure privacy of the transported messages.
  - Must ensure authentication of the source of the control messages between Alive and Bob.
    - ⋆ Radio transmission may not be sufficient.

BB84 protocol - Application aspects

- Can replace asymmetric systems in current application, to a certain degree.
  - It was created especially as an answer to the theoretical threats which will come with quantum computers.
- Two types of users:
  - Current users of asymmetric schemes
    - ★ Get a higher theoretical security.
    - ★ Lose some of the convenience.
    - ★ Not all components can be replaced (yet) - digital signatures.
  - Current users of military and intelligence systems
    - ★ Get higher convenience with the same level of security they get from current mechamisms based on long random keys.

Experimental results - key established over the distance of 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.