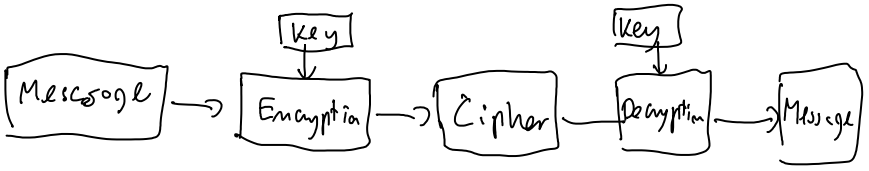
Wyklad4

8 marca 2011
15:56

Classical cryptography

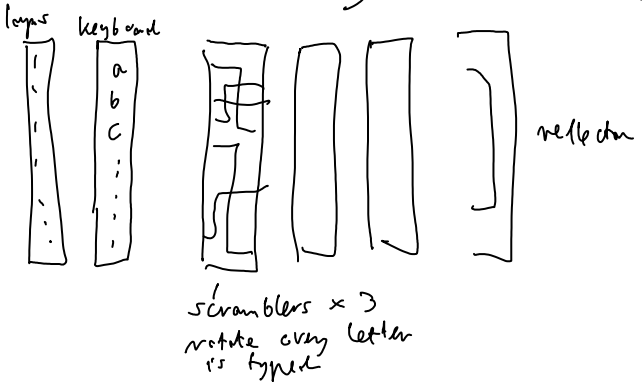
General scheme:



- CEASAR → DFBTBS
  only 26 keys easy to break
- general substitution cipher
  26! keys, but... frequency analysis
- ENIGMA
  1912 – opatentowana
  1926 – wprowadzona do użytku
  1931 – francuzi cyklodują plany Enigmy
  budują repliki (ale to dopiero pierwszy krok)

Knowing encryption scheme ≠ breaking the encryption scheme

Being able to decrypt the cipher without a key ≡ breaking the encryption scheme



Initial setting of scrambling wheels – the key

26 × 26 × 26 a little to small

Initial setting of scrambling wheels – the key

$26 \times 26 \times 26$ a little to small

$\times 6$ permutations of scramblers

before scramblers additional plugboard swiping 6 pair of letters.

In total 10^{16} keys

(if only plugboard was used one could break using freq. analysis)

key = F (permutation) A G W (initial setting of scrambling wheels) B G ... (six pairs of letters to be swapped)

ENIGMA was used for radio communication

Germans had a different key for every day

To increase security, each message had its own key which was encoded using the day key.

Because of noise message key was repeated twice.

- Marian Rejewski 1934 broke the ENIGMA knowing that scramblers orientation is transmitted twice.

  A G W 2 C D

  We know that A and 2 encrypt the same symbol

  He analyzed cycles $A \to 2 \to \dots \to A$

  The form of the cycles depend (length) only on scrambler settings and not on plugboard (only $\sim 100\,000$ keys)

  He classified them and was able to learn scramblers orientation → then frequency analysis for plugboard

- unfortunately in 1939 germans modified the ENIGMA adding 2 more scramblers. His techniques were translated to the British (Turing, Bletchley Park)

- Is there a 100% secure cipher

  yes: one-time pad.

  key length = message length

  If A and B have random bit sequence of the length of the message. A just adds mod 2 key to the message and B does the same for decoding.

  Cipher is completely random.

  Problem – key needs to be very long.

  If ... distributed ... key ... is crucial

Problem – key needs to be very long.
How to distribute the key? Very impractical

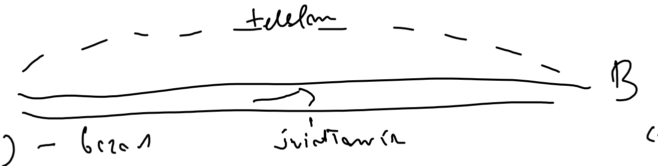
- RSA (1977) classical way to circumvent the problem based on the assumption that factoring is a hard problem

Quantum key distribution (Q. cryptography)

Ideas: – You cannot learn anything about a quantum state without disturbing it

– nonorthogonal states cannot be distinguished

- BB84



1. $|\leftrightarrow\rangle, |\updownarrow\rangle$ – baza 1 (0, 1)
   $|\nearrow\rangle, |\searrow\rangle$ – baza 2

2. po komunikacji zostawiają tylko te bity które zmierzone były w tej samej bazie

	0	~~0~~	1	~~1~~	1	1	~~0~~	~~0~~
A	↔	↙	↕	↔	↘	↕	↔	↙
B	+	+	+	×	×	+	×	+
	0	~~0/1~~	1	~~0/1~~	1	1	~~0/1~~	~~0/1~~

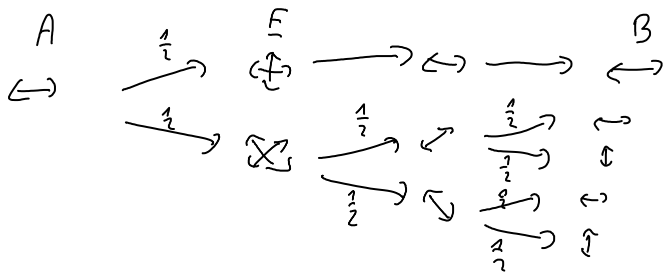
3. następnie ujawniają część aby sprawdzić czy poziom błędów jest dostatecznie mały

4. wtedy mają pewność że nikt nie mógł wyciągnąć zbyt dużo informacji

W szczególności jeśli nie ma błędów mamy pewność że nikt nie mógł podsłuchać. Dlaczego?

- Intercept & Resend attack

  – przypadkowo w jednej z baz QBER = 25%



Jeśli widzimy, że nie ma błędów QBER=0 mamy pewność że nikt nie podsłuchał. Ale ....

W praktyce jednak zawsze są błędy wynikające z szumu. Czy jak widzimy poziom błędów < 25% to jesteśmy bezpieczni. Nie. Bo przecież mogą istnieć subtelne ataki. Jaki poziom błędów jest tolerowalny? Może jest inny limit a taki? Trzeba dokładniej zbadać!

Im większy poziom błędów tym więcej informacji mógł zdobyć podsłuchiwacz. • Assume for simplicity individual attacks !

A 00110100

B 001[0]0100

E 0[1]11[0]10[1]

After basis reconciliation there is a probability distribution describing correlation between bit value of A, B, E : $p(a,b,e)$

$p(a,b) = \sum_e p(a,b,e)$ $\qquad$ $p(a,e) = \sum_b p(a,b,e)$

$a=0 \Rightarrow b=0 \quad p=1-QBER$, $\quad b=1 \quad p=QBER$ $\qquad$ $a=0 \Rightarrow e=0 \quad p=1-\varepsilon$, $\quad e=1 \quad p=\varepsilon$

$a=1 \Rightarrow b=1 \quad p=1-QBER$, $\quad b=0 \quad p=QBER$ $\qquad$ $a=1 \Rightarrow e=1 \quad p=1-\varepsilon$, $\quad e=0 \quad p=\varepsilon$

QBER – poziom błędów u B , ε – poziom błędów u E

Intuition if correlations between A and B are stronger (they share more information) then correlations between A and E :

$\sim \quad QBER < \varepsilon$

it is possible to extract some secure key by classical procedures of error-correction + privacy amplification. Im mniejszy QBER tym chętniej mówimy kwantowej wersji że E nie wiele wie czyli ma duży ε.

Dla danego QBER musimy znaleźć optymalny atak (dający minimalne ε) i jeśli ...

atak (dający mniejsze e) i jeśli wciąż
QBER < ε to możemy wysłać klucz

Error-Correction

- Interactive error correction protocol (1992, Bennett et al)

Iteration:

- A and B apply random permutation
- A and B divide their N bits in subblocks of length n

$$N = k \cdot n$$

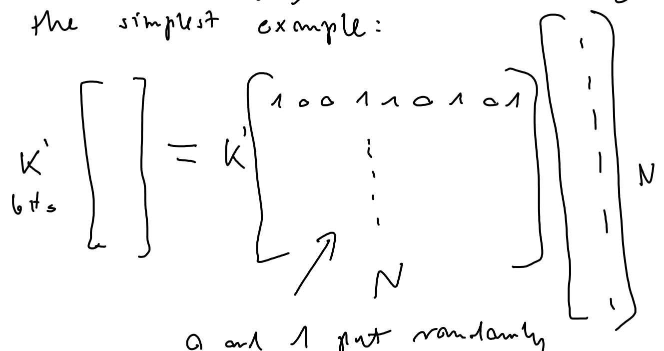
(the length of the block should be such that it is not very probable that there are more than 1 error)

- They check parities of bits in each subblock; if it does not agree → bisection
- If all parity errors were corrected they repeat the iteration with larger block size ..

Privacy amplification – Idea

A and B share N perfectly correlated bits while E knows effectively N−K bits
[after error-correction $K = N(I(A{:}B) - I(A{:}E))$]

A and B apply a random hashing function, the simplest example:



0 and 1 put randomly

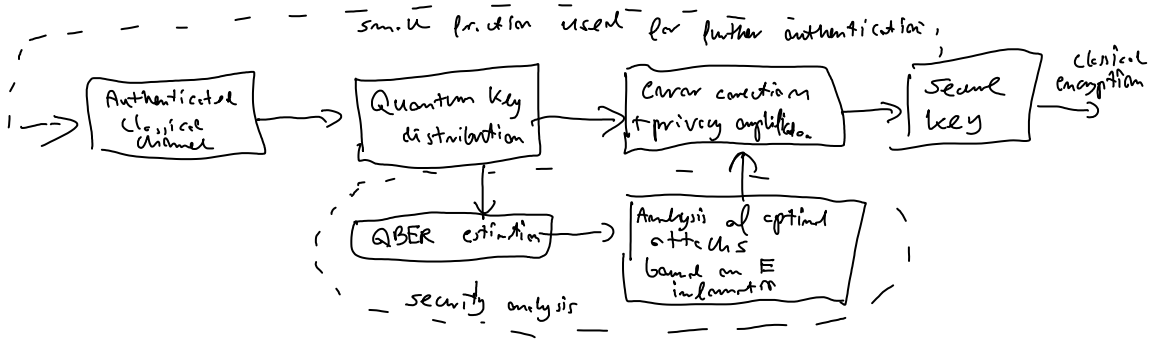
It will spread any error of E to all bits of the final key provided $K' \leq K$

Jest jeszcze jeden brakujący element:
Autentykacja A i B muszą wiedzieć że do siebie mówią.

m - message. Using key K we generate MAC
(message authentication code)
with some block cipher encryption and transmit:
(m, MAC) MAC = $f_K(m)$
Someone possessing K can verify that indeed MAC
is obtained from m
Wcinc żeby funkcja f_K generowała
możliwie różne MAC dla różnych m

Na szczęście istnieją procedury gdzie
można wybrać K ~ log m
Więc jeśli klucz do autentyfikacji można
wziąć mały kawałek klucza z
wcześniej Kwantowej dystrybucji kluczy

Poglądowy obrazek:

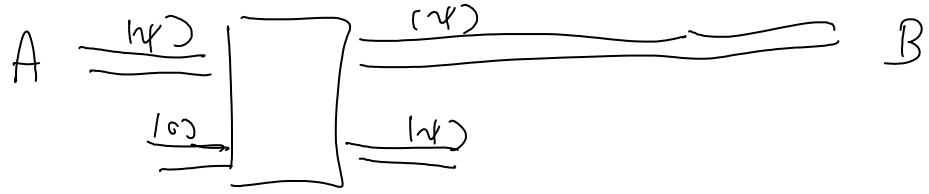


Quantum Key Growing Protocol

Klasowanie

Wydaje się że najprostszym sposobem atak
[illegible] stanu kwantowego

Test sklonowania stanu kwantowego



E

Polega na odtworzeniu bez i zmiany stanu kopii w drugiej bazie

Tw. Nie istnieje operacja zgodna z mech kwantowa klonująca wszystkie dwa nieortogonalne stany kwantowe

Dowód

Niech $|\psi_1\rangle, |\psi_2\rangle$ – dwa różne nieortogonalne stany kw

$0 < \langle\psi_1|\psi_2\rangle < 1$

Dygresja:
Jak matematycznie opisujemy stan dwóch układów

$$|\varphi_1\rangle \otimes |\varphi_2\rangle = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \otimes \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \\ b_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{bmatrix} =$$

↑ il. tensorowy

$|\varphi_1\rangle = a_1|0\rangle + b_1|1\rangle$
$|\varphi_2\rangle = a_2|0\rangle + b_2|1\rangle$

$= a_1 a_2 |0\rangle\otimes|0\rangle + a_1 b_2 |0\rangle\otimes|1\rangle + b_1 a_2 |1\rangle\otimes|0\rangle + b_1 b_2 |1\rangle\otimes|1\rangle$

Jeśli mamy $|\varphi_1\rangle\otimes|\varphi_2\rangle$ i $|\varphi_1'\rangle\otimes|\varphi_2'\rangle$
to ich il. skalarny

$$\langle\varphi_1|\otimes\langle\varphi_2| \cdot |\varphi_1'\rangle\otimes|\varphi_2'\rangle = \langle\varphi_1|\varphi_1'\rangle \cdot \langle\varphi_2|\varphi_2'\rangle$$

Załóżmy, że klonowanie jest możliwe: istnieje op
Unitarne t. że:

$$|\psi_1\rangle \otimes |0\rangle \xrightarrow{U} |\psi_1\rangle \otimes |\psi_1\rangle$$

$$|\psi_2\rangle \otimes |0\rangle \longrightarrow |\psi_2\rangle \otimes |\psi_2\rangle$$

Wiemy że U zachowuje il. skalarne:

Widzimy że U zachowuje il. skalarne:

$$\langle \psi_1|\psi_2\rangle \cdot \langle 0|0\rangle = \langle \psi_1|\psi_2\rangle \cdot \langle \psi_1|\psi_2\rangle$$

$$\langle \psi_1|\psi_2\rangle = \langle \psi_1|\psi_2\rangle^2$$

to możliwe tylko gdy $\langle \psi_1|\psi_2\rangle = 0$ lub 1 spełnione ✓

Mamy tu bliski związek z rozróżnialnością stanów: gdyby klonowanie było możliwe moglibyśmy wypróbkować wiele kopii i rozróżnić bez problemu.
To że mamy fundamentalne ograniczenie na rozróżnialność implikuje zakaz klonowania.