1 - Introduction

30 września 2010
12:33

Kryptografia i Komunikacja Kwantowa

1.1 History ...

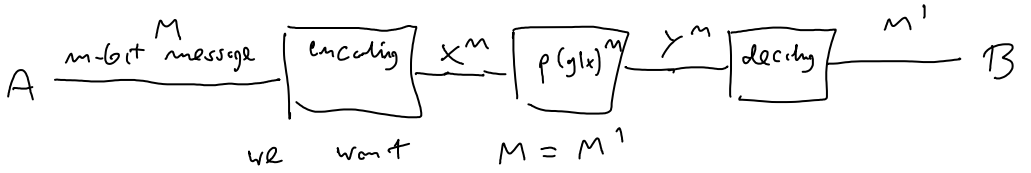
- CEASAR, substitution ciphers
- ENIGMA (1912)

- breaking Enigma (1931-1945)
  (Rejewski, Turing)
- 1949 (Shannon)
  (data compression
  channel capacity
  security of one-time pad)
- 1977 (RSA) (security based on mathematical unproven beliefs)
- 1984 (BB84) (security based on laws of physics)
- 1990 - ... (security proofs for quantum cryptography implementations)

1.2 Communication

A wants to send some message to B using physical channel
non trivial since in general there is noise

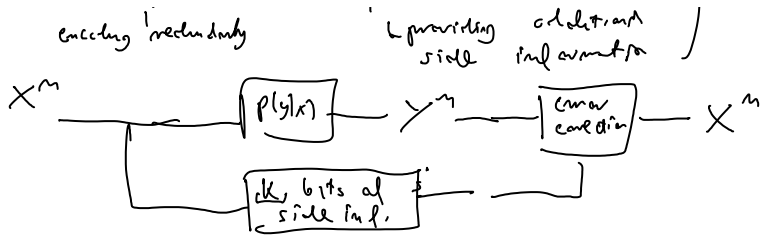
How to send message reliably? (probability of error $< \varepsilon$)
Encode redundant data.
Message is m-bit long, encode in n-bit long codeword



we want $M = M'$

- Channel capacity: $C = \lim_{n\to\infty} \frac{m}{n}$ for which ε arbitrary small ($M \neq M'$)
  Shannon coding theorem (1949)

(Error correction: before or after)



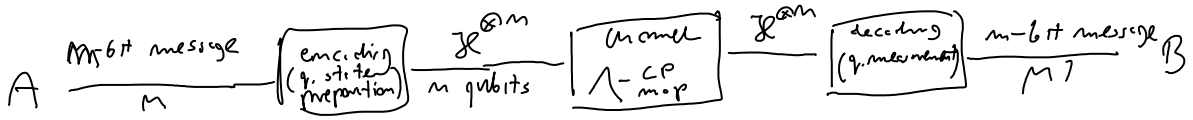
- example:
  - CD disk (1,6 μm) (192 bits encoded in 588 physical bits)
    800 MB — correctr 220 errors/s
  - DVD disk (better error correction)
    (0.74 μm) 4,7 GB

$$4{,}7\ \text{GB} \neq \left(\frac{1{,}6}{0{,}74}\right)^2 \cdot 0{,}18$$

{ the rest from better error correction

1.3 Q. Communication

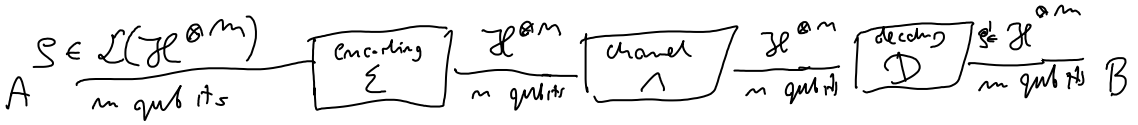
1.3.1 Classical information over Q channel



classical capacity of a quantum channel $\lim_{n\to\infty} \frac{m}{n}$

HSW theorem (1997)
(Holevo-Schumacher-Westmoreland

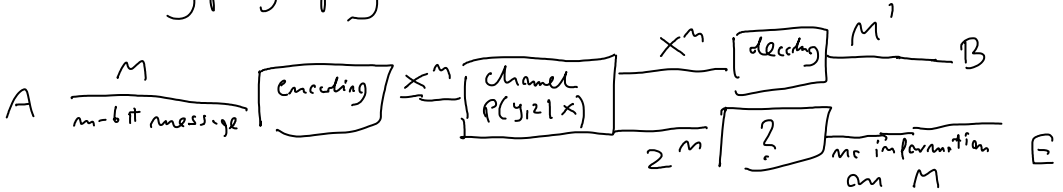
1.3.2 Quantum information over a quantum channel



$$F(S, S') \approx 1 \qquad C = \lim_{n\to\infty} \frac{m}{n}$$

LSD theorem
Lloyd, Shor, Devetak (1997)

1.4 Cryptography



possible only when channel A→B „better" than A→E

- because A & B share some common private key (one time pad)
- because B announced public key and only he can effectively decode ... (RSA)

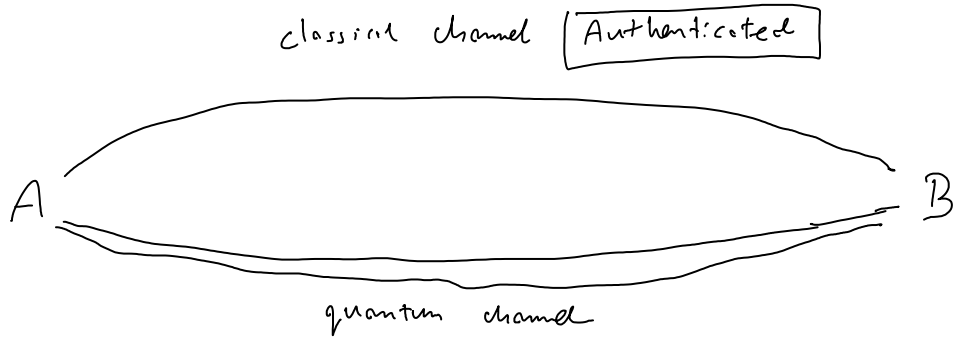
— because A and B preshared quantum key distribution (BB84)

secret capacity $C_s = \lim_{n\to\infty} \frac{m}{n}$ Csiszar Körner theorem (1978)

1.5 Quantum key distribution

Idea: the more E learns about A & B communication the larger disturbance she introduces. Detecting disturbance in A→B channel we may bound the knowledge of E and be sure whether channel A→B is better than A→E ?
(no-cloning theorem, indistinguishability of nonorthogonal q-states)

BB84 (Bennett, Brassard 1984)



a) A sends to B, with $p = \frac{1}{4}$ one of four states of a qubit (pol. of a photon)

$|\leftrightarrow\rangle^{(0)}$, $|\updownarrow\rangle^{(1)}$

$|\swarrow\rangle$, $|\searrow\rangle$

$|\swarrow\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + |\updownarrow\rangle)$

$|\searrow\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle - |\updownarrow\rangle)$

n times

b) B measures randomly in basis 1: $\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$
or 2: $\{|\swarrow\rangle, |\searrow\rangle\}$

A	0	1	0	0	0	1	1	0	0
	↔	↕	↔	↙	↙	↘	↕	↔	↙
	✚	✕	✕	✕	✚	✕	✕	✚	✕
B	0	?	?	0	?	1	?	0	0

c) B announces on the public channel his choices of basis. A and B keep only bits measured in correct basis.
If no disturbance (noise eavesdropper) was present bits should be perfectly correlated

d) A and B measure level of disturbance QBER (fraction of bits which are different) they reveal randomly chosen m bits

e) Quantum mechanics allows to derive a bound on max information of E which she could obtained introducing given QBER [optimal attacks]

If $QBER < QBER_{th}$ then channel A → B ["is better"] than channel A → E

Otherwise protocol aborts

f) A & B perform [error correction]

g) A & B perform [privacy amplification], reduces E information to 0 at the cost of shortens their key.

Points f), g) are classical but need quantum input derived in point e) - security proofs.

Remark: part of the final key is kept to provide [Authentication] for the next protocol

We need a short private key to start for authentication

So in fact we have: Quantum key growing protocol

(it is important that key needed for authentication is short enough — small fraction used for further authentication)