Security of key distribution while transmissing via an optical fiber with depolarization and absorption

Sotnikova A.A., Miroshnichenko G.P.

The main concepts

Quantum cryptography is a method of communication protection; it is based on quantum physic's principles. While classical cryptography use only math's methods.

- Alice – secret information transmitter
- Bob – recipient
- Eve – eavesdropper
- Open text – our secret information
- Secret key – it is used for information encryption, Alice and Bob generate it.

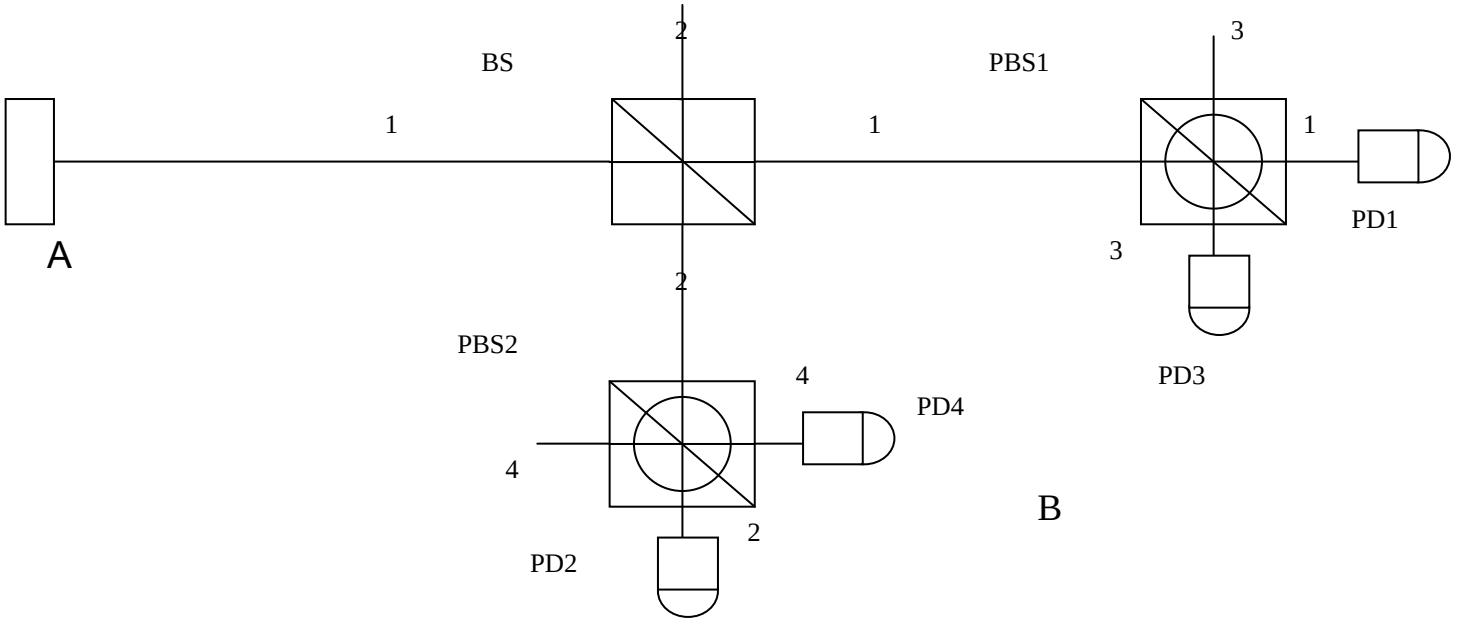
Fundamental law of quantum physic

- The impossibility of perfectly copying (or cloning). Eve can’t measure one parameter without deformation another. She always makes changes in the message.
- Heisenberg uncertainty principle.

The problem

- Real channel is not ideal and introduce some transmission errors.
- Error rate is a question.

Installation diagram



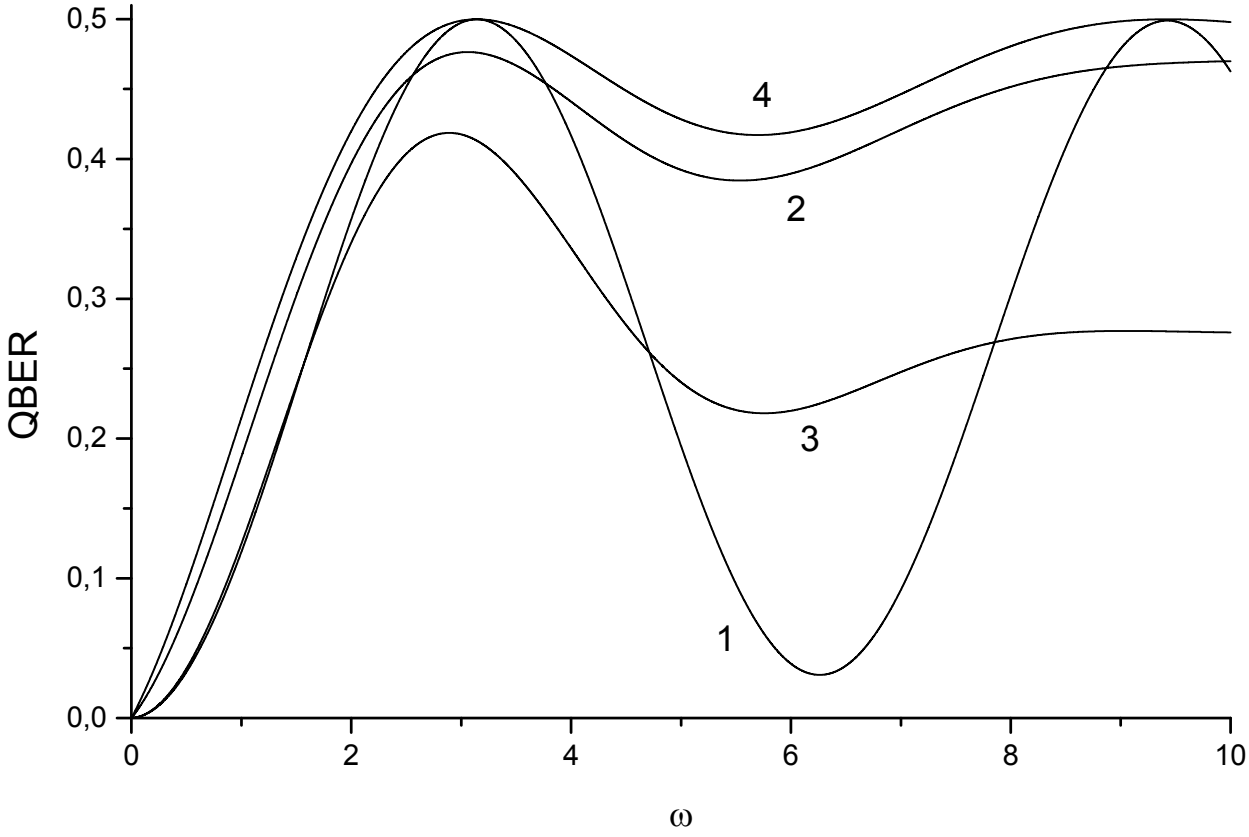
A-Alice's transmitter, it generates photons with random polarization($|H\rangle$, $|V\rangle$, $|\Psi_4\rangle$, $|\Psi_2\rangle$) and transmits it to Bob.

B- Bob's analyzer, at first photon gets on the beam splitter, then depending on type of polarization goes either on polarizing beam splitter 1, or on PBS 2, after one of 4 photo detector responses.

QBER

Error (incorrect bits) is also appear as a result of depolarization in the channel which is not ideal. In literature degree of security key distributed is defined by parameter- rate of errors appearance quantum bits – QBER.

$$\mathrm{QBER} = \frac{1}{2}\left(1 - \frac{1}{2}\left(1 + \cos(\omega)\cdot\exp\left(-\frac{1}{2}\left(\frac{\sigma}{\xi}\omega\right)^2\right)\right)\exp\left(-\frac{\gamma}{\xi}\omega\right)\right)$$


QBER
0,0
0,1
0,2
0,3
0,4
0,5
0
2
4
6
8
10
ω
1
2
3
4

Results

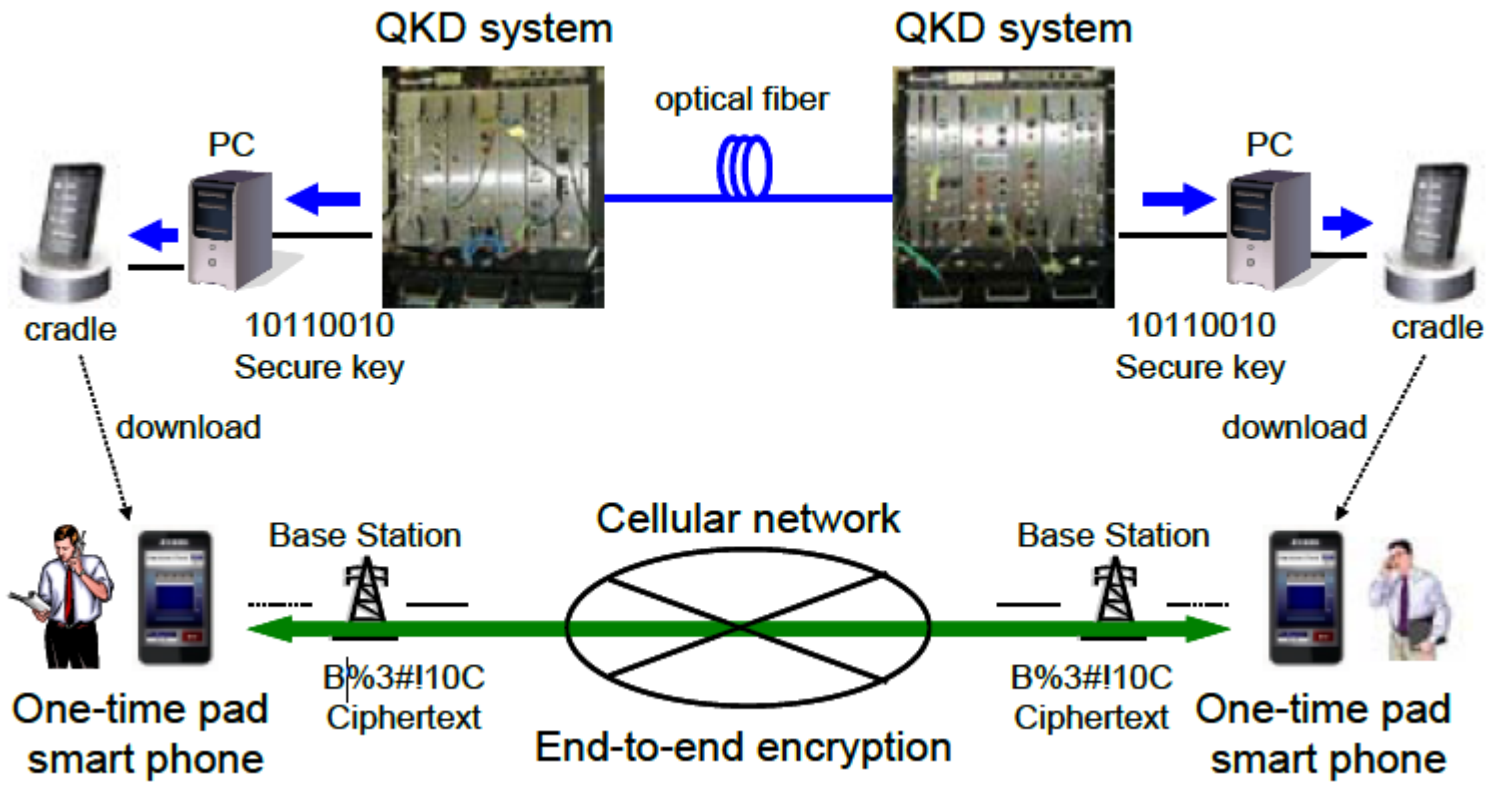
- In the research transmission error introduced by channel imperfection is investigated. Two characteristics of real channel: depolarization and absorption are considered.
- The main result of this work is that the right choice of the quantum channel's OF fabrication method will allow lowering QBER to the critical level equal to 0.11, below which distributed key can be used for cryptographic purposes.

Practical implementation

in 2007th in Switzerland were produced Swiss Quantum Network

Map of the SwissQuantum network. Two nodes are in the Geneva city centre and the third one is on the site of CERN in France (the border is in red). The white lines are drawn for illustration: they do not represent the fibers

In 2011th demonstration of Tokyo Quantum network. They conducted a test teleconference on the distance 45 km via OF. In the future is supposed using such technologies for mobile communication.



Schematic diagram of the QKD system with one-time pad smartphones

Thank you for your attention!

Questions?