Міністерство освіти і науки України
Сумський державний університет
Наукове товариство студентів, аспірантів,
докторантів і молодих вчених СумДУ

ПЕРШИЙ КРОК У НАУКУ

Матеріали
IX студентської конференції
(Суми, 25 лютого 2018 року)

Суми
Сумський державний університет
2018

QUANTUM CRYPTOGRAPHY

Shamonin K.E, student, SSU KB-71,

To advance most popular encryption algorithms such as public-key encryption and signature-based schemes, methods of quantum cryptography can be used. The main advantage of quantum cryptography is the fact it cannot be broken by any non-quantum computers and eavesdropping is impossible in quantum key distribution.

Fundamental quantum mechanics is used in quantum key distribution to guarantee the safety of data transmitted. It is based on entangled pairs of photons in E91 protocol or photon polarization states in BB84 protocol.

BB84 protocol is known after its inventors and year of publication. The security is based on using one of four polarized states of photons, usually a pair of vectors are used to transmit a bit of information. B92 protocol uses only two positions. To check if any eavesdroppers try to steal information sender and receiver compare their messages, because according to Heisenberg's indeterminacy principle it is impossible to read the message without distorting the text. The main disadvantages are complicated implementation and short distance of transmitting (up to 50km).

E91 protocol uses the scheme of entangled pair of photons. These photons can be created by anyone and given to sender and receiver, after a short verification they can be used to transfer information. The principle of operation is based on fact that if any of characteristics is changed on the first photon, this characteristic change on the second photon, so messages can be transmitted even to the other part of universe faster than speed of light, but scientists consider it is impossible to transfer information faster the speed of light. And, of course, it can be used to encrypt the message using pair of polarized states to encode a bit of information.

These methods have the range of disadvantages as complicated implementation, influence of subatomic particles, disability to save data for a long period of time, but with the development of techniques and experiments as Quantum Experiments at Space Scale the methods of quantum cryptography will come after RCA method, used now.

English language advisor: Plokhuta T.M.