Письма в ЭЧАЯ. 2009. Т. 6, № 7(156). С. 150–153



# PRINCIPLES OF THE NEW QUANTUM CRYPTOGRAPHY PROTOCOLS BUILDING

*V. Kurochkin* [a], *Yu. Kurochkin* [b]

[a] Institute of Semiconductor Physics of SB RAS, Novosibirsk, Russia

[b] Department of General and Applied Physics, Moscow Institute of Physics and Technology (State University), Moscow

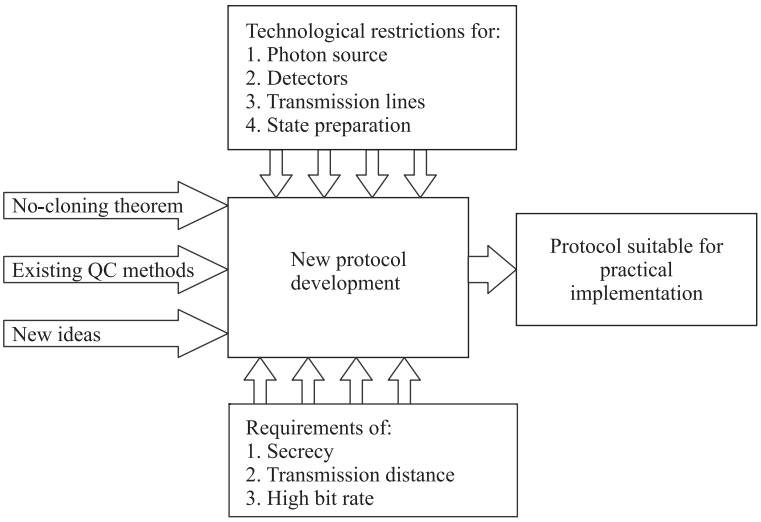
The main aim of the quantum cryptography protocols is the maximal secrecy under the conditions of the real experiment. This work presents the result of the new protocol building with the use of the secrecy maximization. While using some well-known approaches this method has allowed one to achieve the completely new results in quantum cryptography. The process of the protocol elaboration develops from the standard BB84 protocol upgrading to the building of completely new protocol with arbitrary large bases number. The secrecy proofs of the elaborated protocol appear to be natural continuation of the protocol building process. This approach reveals possibility to reach extremely high parameters of the protocol. It suits both the restrictions of contemporary technologies and requirements for high bit rate while being absolutely secret.

Основная цель протоколов квантовой криптографии — это максимальная секретность в условиях реального эксперимента. В этой работе представлены результаты построения нового протокола посредством максимизации секретности. Благодаря некоторым широко известным подходам этот метод позволил достичь абсолютно новых результатов в квантовой криптографии. Процесс разработки протокола развивается от совершенствования стандартного протокола BB84 к построению абсолютно нового протокола с произвольно большим числом базисов. Доказательства секретности разработанного протокола являются логическим продолжением процесса построения протокола. Этот подход открывает возможности достижения очень высоких параметров протокола. Он удовлетворяет как ограничениям современных технологий, так и требованиям высокой скорости генерации ключа, оставаясь абсолютно секретным.

PACS: 03.67.Dd, 01.30.Cc, 03.67.-a

## 1. PROTOCOL BUILDING

The aim of quantum cryptography is the establishing proofed secure communication between two parties (emitter and receiver or Alice and Bob) [1,2]. Quantum cryptography (QC) is the first approach in the history which allows one to solve this task. The first QC protocol is BB84 [1] which is still the most popular and convenient for experimental applications. Its secrecy has been proved mathematically [3]. What else is needed in quantum cryptography? The point is that with the use of current technologies the BB84 protocol has restriction in the transmission speed and distance. So, the aim of practical quantum cryptography is to achieve not only secrecy but also high bit rate and longer distance. Moreover, the quantum cryptography protocol should pass the scope of the present technologies (see the figure below).




Main principles of the quantum cryptography protocol building. In the initial position there are no-cloning theorem, existing quantum cryptography methods and new ideas. The new protocol is suppressed by the technological restrictions for the photon sources, detectors, transmission line properties and the state preparation possibilities. It should fulfill the requirements of the absolute secrecy, high enough transmission distance and bit rate suitable for the contemporary tasks

Quantum cryptography secrecy is based on the no-cloning theorem [2]. It points that it is impossible to make an exact copy of the quantum state. After no-cloning theorem the approximate cloning has appeared. It points that it is possible to make an imperfect cloning with some distribution [4]. In what case will the approximate cloning be most difficult? Considering the restrictions of the maximum cloning fidelity it is easy to see that the difficulty of the cloning increases with the number of possible states. The best security will be achieved in the case of the infinite state number. In other words, state should be able to be prepared in an arbitrary position of the Hilbert space.

In the case of arbitrary state preparation it is difficult to realize any data transmission. The first and the simplest approach is to increase the number of states in the BB84 protocol [5,6]. In this case, the secrecy of the transmission increases and the requirements for the single-photon sources become less severe. This method appears to be good when the standard BB84 is near the edge of its security bounds and the security needs to be increased a little. In any case for the increase of the bases number we pay by the transmission speed. Like in BB84 the key size decreases twice after the bases reconciliation, in this method the bases reconciliation leaves $1/M$ part of the key where $M$ is the bases number. So, this solution does not suit the requirement of the high bit rate.

In the best case the state transmitting by a QC protocol should be able to take arbitrary place from the infinity of possible states of the Hilbert space. Hence, our protocol should have as much states as possible in order to use all advantages of the no-cloning theorem, but it is needed to avoid drop of transmission speed down to zero because of the bases reconciliation process. In order to overcome the problem of the bit rate drop, we can refuse the basis

reconciliation process. Alice and Bob should synchronize their bases somehow. Usually for the public channel authentication Alice and Bob use some secret information distributed by some other way because if eavesdropper controls both quantum and public channel the transmission becomes completely insecure. These $N$ secret bits (for example, 64 or 128 bits) can be used for the bases definition. This $N$ secret bit will be called an «auxiliary key» and the key which is generated by this protocol will be called a «transmitting key». Position of the basis should be a complicated function depending on the secret information and number of pulse. Due to this secret information positions of all bases are secret. This function will define one of the $2^N$ possible bases sets known only to Alice and Bob. With the use of this function the auxiliary key bases of the qubit preparation and measurement will always coincide. In this case, there is no bases reconciliation process what causes the increase in the speed at least twice [7].

## 2. SECURITY PROOFS

To guarantee the entire secrecy of the protocol it is needed to keep both the auxiliary and the transmitting key secret. When the auxiliary key is unknown to the eavesdropper it is impossible to attack the transmitting key due to the Shores theorem. In classical case the transmitting key length cannot be longer than the auxiliary key length. But in quantum case this restriction can be challenged. The protocol will be secure until the auxiliary key is secret. This key should stay secret even when any part of the transmitting key has been revealed to public channel, for example, for error correction process. In other words, the auxiliary key secrecy should be independent of the transmitting key secrecy. The proof should be related to some true quantum limitation. Here the most suitable quantum limit will be the true quantum limit of measurement [8, 9]. It says that for the measurement of the quantum state with precision $1/K$ you need not less than $K$ photons. This is the true quantum limit and it is dedicated to the Heisenberg uncertainty principle. If the auxiliary key consists of $N$ bits it can define one of the $2^N$ bases sequences. For revealing what auxiliary key has been used an eavesdropper should measure at least $K = 2^N$ photons. For the protocol secrecy it should be chosen clear criteria. An eavesdropper cannot measure more photons than the number of photons which entered the quantum channel during the whole transmission. So, if $2^N$ photons have entered quantum channel it opens theoretical possibility to reveal all $N$ bits of the auxiliary key, but if only $2^{N/2}$ photons have entered the quantum channel eavesdropper can reveal only $N/2$ bits of the auxiliary key. If $N$ is large enough the rest $N/2$ unrevealed bits are enough to make the transmitting key secret.

For example, auxiliary key can be $N = 64$ bits, transmission line can be $l = 100$ km, attenuation — 0.2 db/km, laser power — 1 photon/pulse and quantum efficiency of detectors is 10%. Alice emits $K$ photons and Bob successfully receives $B = K \cdot 10^{-100 \cdot 0.2} \cdot 0.1$ qubits. Consider the condition $K \ll 2^N$, $B \cdot 10^{-3} \ll 2^{64} \approx 10^{19}$, $B \ll 10^{16}$. If Bob successfully measures $B = 10^8$ qubits, then $K = 10^{11}$ has entered quantum channel and eavesdropper has to guess which one of the $10^{19-11} = 10^8$ possible bases sequences has been used. Contrary to the classical case, eavesdropper has only one attempt to measure qubit received during the photon number splitting attack, for example, what makes these estimations strong enough to guarantee secrecy.

## CONCLUSIONS

Concluding the developed protocol it can be said that it is suitable for an experimental realization on the modern experimental setups. An approach of refusing fixed bases allowed one to increase the transmission distance without breaking security. Key bit rate rises at least twice because Alice and Bob's bases always coincide. Moreover, this protocol is tolerant to the photon number splitting attack so it is possible to increase the number of photons in the pulse what causes additional increase in the transmission speed. Ideas of this protocol can give rise to the additional direction of theory and experiment development. It also opens a lot of opportunities for elaborating more eavesdropper strategies. This protocol shows very good efficiency so it can be extremely useful for experimental realizations. This work was supported by the RFBR, grant 07-07-00263.

REFERENCES

1. *Bennett C. H., Brassard G.* // Proc. of IEEE Intern. Conf. on Computers, Systems and Signal Processing, Bangalore, India, 1984. V. 3. P. 175–179.
2. *Gisin N. et al.* // Rev. Mod. Phys. 2002. V. 74. P. 145.
3. *Shor P. W., Preskill J.* // Phys. Rev. Lett. 2000. V. 85. P. 441; quant-ph/0003004.
4. *Scarani V., Iblisdir S., Gisin N.* // Rev. Mod. Phys. 2005. V. 77. P. 1225.
5. *Kurochkin Y., Kurochkin V. L.* // Digest IV Intern. Symp. on Modern Problem of Laser Physics, Novosibirsk, Russia, 2004. P. 265–266.
6. *Acin A., Gisin N., Scarani V.* // Phys. Rev. A. 2004. V. 69. P. 012309; quant-ph/0302037.
7. *Kurochkin Y.* // Proc. of SPIE «Quantum Informatics-2004». 2005. V. 5833. P. 213.
8. *Giovannetti V., Lloyd S., Maccone L.* // Science. 2004. V. 306. P. 1330.
9. *Giovannetti V., Lloyd S., Maccone L.* // Phys. Rev. Lett. 2006. V. 96. P. 010401.