CLASSICAL AND QUANTUM CRYPTOGRAPHY AND NUMBER THEORY

A. S. TRUSHECHKIN[1,2] and I. V. VOLOVICH[1]

[1]*Steklov Mathematical Institute, Russian Academy of Sciences, Gubkin st. 8 Moscow 119991, Russia*

[2]*Moscow Engineering Physics Institute, Kashirskoe sh. 31 Moscow 115409, Russia*

In cryptography number theory and complexity theory play one of the central roles. For example, the security of the widespread cryptographic protocol RSA is based on the assumption of the lack of effective (polynomial) algorithms solving the problem of the factorization of large integers. But it was shown that this problem can be solved in polynomial time on quantum computer. Quantum key distribution is considered as an alternative to public key cryptography. It allows legal parties to establish a common secret key without any computational assumptions.

In this work a general mathematical framework for quantum key distribution based on the concepts of quantum channel and Turing machine is suggested. The security for its special case is proved. The assumption is that the adversary can perform only individual (in essence, classical) attacks. For this case an advantage of quantum key distribution over classical one is shown.

A system G of quantum key distribution is a family of the following objects:

$$G = \left(\mathcal{K}, \mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_E, \Theta, \{q^{(n)}\}_{n\in\mathbb{N}}, \{M_B^{(n)}\}_{n\in\mathbb{N}}, \{\mathcal{M}_E^{(n)}\}_{n\in\mathbb{N}}\right).$$

Here $\mathcal{K}$ is a finite set (set of keys); $\mathcal{H}_A, \mathcal{H}_B$, and $\mathcal{H}_E$ are Hilbert spaces; $\Theta : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_E)$ is a channel (dual to CP map); the functions $q^{(n)} : \mathcal{K} \to \mathcal{S}(\mathcal{H}_A^{\otimes n})$ specify channels $Q^{(n)}$; $M_B^{(n)}$ is an observable (POVM) of the legal receiver; and $\mathcal{M}_E^{(n)}$ is a set of the observables available for the adversary.

Theorem. Suppose that there exists a finite set $\mathcal{A}$ and a channel Ξ specified by a function $\xi : \mathcal{A} \to \mathcal{S}(\mathcal{H}_A)$ that obey the property

$$C(\Theta_B \circ \xi) > C_1(\Theta_E \circ \xi),$$

where $\Theta_B = \mathrm{Tr}_{\mathcal{H}_E}\Theta$, $\Theta_E = \mathrm{Tr}_{\mathcal{H}_B}\Theta$, $C(\Theta_B \circ \xi)$ is the legal receiver's quantum channel capacity, and $C_1(\Theta_E \circ \xi)$ is the adversary's quantum channel capacity if the adversary can perform only individual measurements. Then, for any $\alpha, \beta \in (0,1)$ and any sufficiently large $n \in \mathbb{N}$, there exists a channel (random coder) F_A from $\mathcal{K}$ to $\mathcal{A}^n$ and a legal receiver's observable M_B such that for every adversary's measurement, the random values K_A, K_B and K_E, where $(K_B, K_E) = (M_B^{(n)} \otimes M_E^{(n)}) \circ \Theta^n \circ \Xi^n \circ F_A$, obey the following properties:
(i) $\Pr[K_A = K_B] \geq \alpha$;
(ii) $I(K_A; K_E) \leq 1 - \beta$. Here $I(\cdot;\cdot)$ is Shannon mutual information.

The first inequality means that the legal parties have the common key with the probability very close to one. The second one means that the adversary has only negligible information about this key.