Pis'ma v ZhETF, vol. 81, iss. 7, pp. 437 – 441

Using of small-scale quantum computers in cryptography with many-qubit entangled states

K. V. Bayandin, G. B. Lesovik

L. D. Landau Institute for Theoretical Physics RAS, 117940, Moscow, Russia

Submitted 13 December 2004
Resubmitted 9 March 2005

We propose a new cryptographic protocol. It is suggested to encode information in ordinary binary form into many-qubit entangled states with the help of a quantum computer. A state of qubits (realized, e.g., with photons) is transmitted through a quantum channel to the addressee, who applies a quantum computer tuned to realize the inverse unitary transformation decoding the message. Different ways of eavesdropping are considered and the estimation of the time, needed for determining the secret unitary transformation, is given. It is shown, that using even small quantum computers can serve as a basis for very efficient cryptographic protocols. For a suggested cryptographic protocol the time scale on which communication can be considered secure is exponential in the number of qubits in the entangled states and in the number of gates used to construct the quantum network.

PACS: 03.67.–a

1. Introduction. In 1982 Feynman suggested that simulation of a quantum system using another one could be more effective than using of classical computers which demand exponential time depend on the size of the system [1]. Later on discussions focused on the possibility of using quantum-mechanical systems for solution of classical problems. For example Deutsch's algorithm [2] of verification of balanced function was the first quantum algorithm that works more efficiently than the classical analog.

The most famous in this class Shor's quantum factorizing algorithm [3] is capable to destroy widespread cryptographic system RSA [4]. That fact made a strong expression and speeded up the development of quantum cryptography [5] and quantum information processing in general.

It is important to note that quantum mechanics destroying classical ways of coding still gives the possibility of constructing new ones. At present there exist many ways of coding which essentially use the quantum mechanics.

As an example the quantum algorithm of key distribution using orthogonal states should be mentioned [6]. It was first experimentally realized by Bennet and Brassard [7], they were able to carry out the transmission only at a distance of forty centimeters. Later a communication line of several kilometers was realized [8].

Another example was first experimentally demonstrated in 1992 [9]. The method uses pairs of entangled photons, part of which with the help of Bell inequalities of the special form [10] can be used to reveal attempts of eavesdropping.

In the present article another method of coding is proposed. It uses quantum computers for creating entangled states of several qubits. Safety of that method is based on the complexity of tomography for that states.

Later it will be convenient to treat a single qubit as a spin-1/2. To transmit information Alice (sender) first transfers it into a set of units and zeros and divides the numerals into groups of K bits. Then for every group she creates a set of K spins in pure states, the spin corresponding to a numeral gets the projection along the fixed Z-axis if the numeral is zero and the projection opposite to the axis otherwise. After that Alice employs a preset unitary transformation $\widehat{U}$ for every group of K spins, thus obtaining a set of entangled quantum-mechanical states, in future called as messages,

$$|\Psi_k\rangle = \widehat{U}|k\rangle, \qquad (1)$$

where $|k\rangle$ is an unentangled state of spins with certain projections along the Z-axis, the projections are defined by the sequence of units and zeros for the binary record of the number k.

Having received K entangled spins, Bob (receiver) employs the inverse unitary transformation $\widehat{U}^{-1}$, thus obtaining the original separable state of spins with defined projections, which can be measured, and thereby the secret message can be decoded.

It is natural that only Alice and Bob know the unitary transformation $\widehat{U}$, provided that Eve (eavesdropper) trying to measure the entangled quantum states will obtain probabilistic results defined by the quantum mechanics.

Further we will consider the ways of learning how to decode the transmitted information, and mainly how much time it takes. We will consider two different ways: quantum tomography of every entangled state and simple guess of quantum gate network. The obtained results allow to estimate for how long Alice and Bob may safely use the unitary transformation without changing it.

2. Quantum tomography of an entangled state. In the simplest case Eve can determine the secret unitary transformation if she knows what information exactly is sent by Alice. We leave the question about ways how she can do that, we just will consider that, having intercepted the message, Eve exactly knows what information is encoded by Alice. So for simplicity in this section we deal with many identical entangled states.

The strategy for Eve is to employ quantum tomography for a lot of identical intercepted entangled states. In the paper [11] it was shown that the density matrix of state of certain spins can be derived without using quantum computers. The idea of the method is based on the measurement of probability $p(\mathbf{n}_1, m_1; ...; \mathbf{n}_K, m_K)$ for every spin $\widehat{s}_i$ projected into the state m_i along the direction $\mathbf{n}_i$. The density matrix is determined by Monte-Carlo integration

$$\widehat{\rho}_{\rm calc} = \sum_{\{m_i\}=-\frac{1}{2}}^{\frac{1}{2}} \int ... \int \frac{d\mathbf{n}_1 ... d\mathbf{n}_K}{(4\pi)^K} p(\mathbf{n}_1, m_1; ...; \mathbf{n}_K, m_K) \widehat{K}_{S_1}(\mathbf{n}_1, m_1) ... \widehat{K}_{S_K}(\mathbf{n}_K, m_K), \quad (2)$$

where the kernel $\widehat{K}_{S_i}(\mathbf{n}_i, m_i)$ acts in the space of i-th spin.

Let us introduce distance in space of density matrices

$$|\widehat{\rho}_1, \widehat{\rho}_2| = \sqrt{\sum_{i,j} |\widehat{\rho}_1 - \widehat{\rho}_2|^2_{ij}}, \qquad |\widehat{\rho}| = \sqrt{\sum_{i,j} |\widehat{\rho}|^2_{ij}}. \quad (3)$$

It is known that in Monte-Carlo method relative precision of integration converges as inverse square of the number of used points [12]. In our case we have

$$\alpha = \frac{|\widehat{\rho}_{\rm calc} - \widehat{\rho}_{\rm true}|}{|\widehat{\rho}_{\rm true}|} \approx \frac{1}{\sqrt{N}}, \quad (4)$$

where N is the number of different sets of directions used for measurement of spins.

Now we note that for every set of fixed directions for every spin it is necessary to measure all probabilities for every combination of indices $\{m_i\}$. This takes about $\mathrm{const} \cdot 2^K$ intercepted messages.

Thus we obtain that in order to derive every the density matrix with precision α it is necessary to intercept

$$N_{\rm intercepted} \approx \mathrm{const} \cdot \alpha^{-2} \cdot 2^K \quad (5)$$

messages.

To compose the desired unitary transformation, Eve have to derive the density matrices $\{\rho_k\}$ for all 2^K entangled states. Every density matrix $\{\rho_k\}$ has a single eigen value 1 and an eigen vector $|\Psi_k\rangle$

$$\widehat{\rho}_k = |\Psi_k\rangle\langle\Psi_k|. \quad (6)$$

Eve should find eigen vectors of 2^K density matrices for all entangled states and put them together, thus she will get the matrix $2^K \times 2^K$ for the unitary transformation $\widehat{U}$ in the basis composed of vectors $|k\rangle$. Since the problem of finding eigen vector for a matrix takes about 2^{2K} elementary operations, then the whole problem takes about

$$N_{\rm operations} = 2^{3K} \quad (7)$$

operations, provided that we have a classical computer which can operate with

$$N_{\rm data} = 2^{2K} \quad (8)$$

complex numbers.

On top of it all Eve for practical applications must construct a quantum network by the unitary transformation. As we will see in the next section the number of necessary basic gates is

$$N_{\rm gates} \approx 2^{2K}. \quad (9)$$

Therefore, as Alice and Bob increase the number of bits contained in a single message, the number of necessary intercepted messages, the time of deriving of the unitary transformation and the complexity of the constructed quantum network grow exponentially.

3. Guess of the unitary transformation. Complicated unitary transformations can be constructed using simple ones which mix states of one or two qubits. Examples of actively studied gates for quantum networks are based on superconducting circuits [13], resonant cavities [14], linear ion traps [15] and nuclear magnetic resonance [16].

The operation of a quantum computer can be presented as a network of sequential simple unitary transformations. The whole unitary transformation has the form

$$\widehat{U} = \widehat{U}_M \widehat{U}_{M-1} ... \widehat{U}_2 \widehat{U}_1. \quad (10)$$

Ekert and Jozsa showed [17] that any unitary transformation of qubits can be represented as a network of every possible single-qubit gates and one type of double-qubit gate. As an example of double-qubit gate may serve the "controlled NOT", which acts like $|a, b\rangle \to |a, a \oplus b\rangle$.

Due to the fact that every gate has its counterpart which carries out the inverse transformation, we can simply construct the inverse transformation

$$\widehat{U}^{-1} = \widehat{U}_1^{-1}\widehat{U}_2^{-1}...\widehat{U}_{M-1}^{-1}\widehat{U}_M^{-1}. \quad (11)$$

Although the way of constructing of the quantum network by the matrix of the unitary transformation was presented in [17], in general case the algorithm requires polynomial number of gates over the dimension of the matrix $\widehat{U}^{-1}$, so in our case it takes exponential number of gates in the number of qubits. Nevertheless Alice and Bob do not need to construct a quantum network to get a certain unitary transformation, instead they can just arrange about a particular one.

Consider that Alice and Bob possess identical quantum computers which can carry out any of L different simple unitary transformations, provided that there exists an inverse transformation for every one in the set. If Alice and Bob use simple transformations M times, then the number of possible quantum networks is

$$N_{\text{quant}}(L, M) = L^M. \quad (12)$$

Eve has no chance to guess the correct unitary transformation trying every quantum network, taking into account that M and L should be greater than square number of qubits K^2, because Alice and Bob a least need to mix every qubit with each over.

As one can see, the dependance (12) is again exponential. This formula yet does not take into account the fact that for every trial network Eve must do several measurements of quantum states to realize whether the network is guessed right or not. Let

$$p = |\langle k|\widehat{U}_{\text{guess}}^{-1}\widehat{U}|k\rangle|^2 \quad (13)$$

be the probability of erroneous acceptance of a trial unitary transformation $\widehat{U}_{guess}$ instead of the right one $\widehat{U}$. Then the probability not to distinguish this two transformations after n measurements is

$$P = p^n = e^{n \ln p}. \quad (14)$$

Since for overwhelming majority of quantum networks the probability p is far less than one, a few measurements is enough to realize that the network is erroneous.

As a result we conclude that to increase the security of the cryptographic method Alice and Bob should increase not only the number of qubits but also the number of used quantum gates.

4. The case of a priori known time correlarions. Earlier we supposed that Eve knew what information is particularly coded into the entangled states. Now we will assume that she knows only time correlations between messages of K classical bits. The correlations can be described by the value

$$\xi_{kl}(y) = \langle p_k(x)p_l(x + y)\rangle_x, \quad (15)$$

where $p_k(x)$ equals to unity if x-th message is $|k\rangle$, and zero otherwise.

We suppose that Eve posses a *priory* information like the frequencies of appearance and the correlations between K-bit messages which were sent by Alice. And she tries to construct a quantum network which gives the same frequencies and correlations.

The estimated value of intercepted messages necessary for deduction of the unitary transformation is divided into two parts: the number of trial unitary transformations and the number of necessary measurements for each of them to understand whether the correlations are proper or not. The first part of the problem is due to the entanglement and the second is the same to the case of classical cipher of replacement.

The number of trial unitary transformations is defined by the formula (12). For the calculation of the correlations it is necessary to measure a number of quantum states polynomial in the value 2^K

$$N_{cl} \approx P_n\left(2^K\right), \quad (16)$$

where the power n of polynomial $P_n(x)$ corresponds to taking into account of long time correlations. This can be understood in the following way: for calculation of correlations it is essential to evaluate the probabilities of appearance for the successions of n messages, so it is desirable to meet all possible successions.

The final number of messages to be intercepted is

$$N_{\text{net}} \approx N_{\text{quant}} * N_{cl}. \quad (17)$$

5. Discussion. In the suggested way of encoding of information the number of intercepted messages necessary for Eve is exponential in the number of used qubits and quantum gates. This is clearly seen from equations (5), (12) and (17).

According to the obtained estimations it is necessary for Eve to derive the structure of every 2^K entangled states, that is to intercept

$$N \approx C \times 2^{2K} \quad (18)$$

messages. This corresponds to transmission of

$$N_{\text{bit}} \sim K \times 2^{2K} \quad (19)$$

bits of classical information.

On contrary according to (12) it is necessary for Alice and Bob to preset M numbers less than L to define the order of simple unitary transformations. As we pointed earlier M amd K are of order K^2, therefore the number of bits required for this is

$$N_{\rm key} \sim K^2 \cdot \log_2 K^2. \qquad (20)$$

This expression (20) gives the length of the secret key which must be shared by Alice and Bob. They can use a protocol of quantum key distribution to get it. The expression (19) shows how many classical bits can be safely transmitted using that secret key.

Let us estimate for how long Alice and Bob may use the unitary transformation without changing it. For this let us consider the enciphering of telephone calls, which require transmission of about fifty thousand bits per second. If the quantum computer operates with $K = 8$ qubits, then according to our estimations Eve should intercept $N \approx 65 \cdot 10^3$ messages, so Alice can send about $N \cdot K = 5 \cdot 10^5$ classical bits or can talk to Bob for ten seconds. If the computer operates with $K = 16$ qubits, then the time of guessing of the unitary transformation equals to a couple of weeks. And in the case of $K = 24$ qubits the time of secure conversation for Alice and Bob rises to four thousand years.

Though the suggested protocol requires a preset secret key, it still has an advantage over classical block cipher algorithms, which is also believed to be secure for transmission of exponential number of bits in the length of the key. The example of RSA system and Shor's algorithm shows that quantum mechanics can greatly simplify the breaking of codes based on complexity of classical algorithms. On contrary the safety of the suggested protocol is assured by fundamental laws of nature.

The main advantage of the suggested protocol is that Alice and Bob, having arranged about the secret transformation once, can use it for a long time. The transmission is carried out in one direction, as opposed to the protocols of secret key distribution, which require repeated transmissions from Alice to Bob and in the opposite direction.

It should be mentioned that according to the section 4 the problem of determination of the secret unitary transformation is added to the classical cryptographic problems. The main source of additional security is the fact that the cloning of a state is forbidden for any quantum-mechanical system [18]. Due to this theorem the measurement in a wrong basis may give less information, as opposed to the classical case where once intercepted message readily can be used for calculation of correlations. In the quantum case a part of intercepted entangled states must be used with inevitable distraction for determination of the secret unitary transformation.

Another thing is that according to the noncloning theorem [18] Eve destroys the quantum state measuring it in a wrong basis, and therefore she is unable to send the same state to Bob. In accordance with basic principles of quantum cryptography [6] Bob can easily notice the attempts of eavesdropping, therefore he can ask Alice to stop the transmission. Also similar to the case of relativistic quantum cryptography [19] Bob can detect the attempt of eavesdropping by the time delay for coming messages.

Although the considered protocol looks promising, there are some problems in its realization. First, it appears that the construction of quantum computers handling with tens of qubits is still the matter of future. Second, due to small decoherence times for the systems with massive entangled particles, photons stay the best objects for transmission of quantum states, but the conversion of a state of qubits into a state of photons is a challenging problem for experimentalists. Nevertheless, some efforts have been made to study coupling between photons and qubits [20], and to convert pairs of spin-entangled electrons to pairs of polarization-entangled photons[21]. At last, during the transmission of photons there is inevitable influence of medium on their states, and therefore using of some quantum error-correction techniques will be needed [22].

To conclude, we presented estimations showing that for the suggested cryptographic protocol the time of secure using of secret unitary transformation is exponential in the number of qubits within the entangled states and in the number of gates used to construct the quantum network.

Although we can not at the moment present a rigorous proof of the proper statements for a general Eve's attack, the suggested protocol in our opinion can serve as an interesting alternative to the existing schemes in quantum cryptography. The main advantage of the cryptographic protocol is that using even relatively small quantum computers with couple of dozens qubits allows to have a practical scheme, more efficient than existing ones in several respects (e.g. weaker loading of communication channel).

We acknowledge discussions with S. Molotkov, G. Blatter, R. Renner, M. Feigelman, M. Skvortzov, and financial support through the Russian Science-Support Foundation, the Russian Ministry of Science, and the Russian Program for Support of Scientific Schools.

---

1. R. Feynman, Int. J. Theor. Thys. **21**, 467 (1982).

2. D. Deutsch, Proc. R. Soc. London **A400**, 97 (1985).
3. S.I.A.M. Journal on Computing **26**, 1484 (1997).
4. R. Rivest, A. Shamir, and L. Adleman, *On Digital Signatures and Public Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).
5. Dirk Bouwmeester, Artur Ekert, and Anton Zeilinger, *The Physics of Quantum Information*, Springer-Verlag (2000).
6. C. H. Bennet and G. Brassard, *Proc. IEEE Int. Conference on Computer Systems and Signal Processing*, IEEE, New York, 1984.
7. C. H. Bennet et al., J. Cryptol. **5**, 3 (1992).
8. A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).
9. A. K. Ekert et al., Phys. Rev. Lett. **69**, 1293 (1992).
10. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Hol, Phys. Rev. Lett. **23**, 880 (1969).
11. G. M. D'Ariano, L. Maccone, and M. Paini, quant-ph/0210105.
12. W. H. Press, S. A. Teukolsky, W. T. Veterlingt, and B. P. Flannery, *The Art of Scientific Computing*, Chapters 7.6 and 7.8, Cambrige University Press, 1988–1992.
13. M. H. Devoret, A. Wallraff, and J. M. Martinis, cond-mat/0411174.
14. *Cavity Quantum Electrodynamics, Advances in atomic, molecular and optical physics*, Supplement 2, Ed. P. Berman, Academic Press, 1994; S. Haroche, in *Fundamental systems in quantum optics, les Houche summer school session LIII*, Eds. J. Dalibard, J. M. Raimond and J. Zinn-Justin, North Holland, Amsterdam, 1992.
15. J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995); J. F. Poyatos, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 1322 (1998).
16. N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).
17. A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733.
18. W. K. Wooters and W. H. Zurek, Nature (London), **299**, 802 (1982).
19. S. N. Molotkov and S. S. Nazin, quant-ph/0106046.
20. R. J. Schoelkopf et al., Nature (London) **431**, 162 (2004).
21. V. Cerletti, O. Gywat, and D. Loss, cond-mat/0411235.
22. E. Knill and R. Laflamme, Phys. Rev. **A54**, 900 (1997).