Security Arrangements in the Computer-Aided Election System

Application of Quantum Cryptography in the Electronic Voting System

Igor V. Limar, and Yevhen V. Vasiliu
Department of Information Security and Data Transfer
A.S. Popov ONAT
Odessa, Ukraine
e-mail: iv.limar@onu.edu.ua

***Abstract* — A cryptographic security scheme is proposed within the frame of a subsystem of the integrated computer-aided system that is intended for holding elections and counting the election returns. The solution is based on two quantum technologies of cryptographic security: quantum bit commitment and secret sharing**

Keywords — quantum bit commitment; quantum secret scharing; quantum cryptography; election

I. INTRODUCTION

Application of the «secret sharing» concept in the electronic voting systems with a view of ensuring a reliable vote count has been suggested in literature long ago and is well known [1]. Secret sharing procedures and the so-called «bit commitment» [2] used jointly in the electronic voting system were described as well. However, until present time no similar schemes based on quantum technologies were proposed for electronic voting systems. The solution proposed in this paper is founded just on the quantum bit commitment and the quantum secret sharing. Application of quantum technologies, specifically in the election automation systems, gives an advantage, as compared with the similar classic (non-quantum) cryptographic schemes, at least due to two reasons. First, classic cryptographic protocols, except for Vernam cipher that has certain deficiencies, are characteristic of the computational security only. At the same time, the quantum schemes, according to their essence, stand closer to Vernam cipher (which possesses the inherent unconditional security) by their reliability while being not susceptible, as distinct from Vernam cipher, to the risks associated with the human factor, and do not depend on the information volumes to be encoded to the same extent as said cipher. Second, the quantum cryptographic systems allow of detecting an adversary's attempt to penetrate the communication channel with a view of unauthorized capturing of information. As distinct from the quantum protocols, the classic cryptographic protocols do not provide such opportunity by itself.

II. USING QUANTUM BIT COMMITMENT AND QUANTUM SECRET SHARING IN THE ELECTRONIC VOTING SYSTEM

We propose the following scheme as shown in Fig. 1. Whenever a voter casts ballot for each individual candidate, the automatic device (that is monitored by journalists, observers of various parties and the central elective body), which hereinafter is called «Alice», forms at random a group of photons and sends it to the voting machine (hereinafter called «Bob»). These photons are in one of BB84-states as it is described in [3]. In so doing, «Alice» should be stationed in the immediate proximity (not exceeding 1 m) of the voting machine «Bob». All photons of said group reach Bob simultaneously. If a voter votes «nays», the voting machine (Bob) performs (immediately and simultaneously for all photons of that group) a quantum measurement in the basis $\{|0\rangle, |1\rangle\}$, and if a voter votes «yeas», the measurement is performed in the basis $\{|+\rangle, |-\rangle\}$. Hereinafter $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The procedure is reiterated for each enlisted candidate separately – Alice sends as many photon groups as the number of times the voter selects either «yeas» or «nays» with respect of each appropriate candidate. Afterwards, Bob immediately sends the results of measurement at the velocity of light to its two agents B_1 and B_2 that are symmetrically located on the right and left of Bob and, in their turn, are moved away from each other at a certain distance *d*. Both agents are sent the same data; actually, this is data duplication. The data is transferred in encrypted form. In so doing, the preliminary distribution of encryption keys is accomplished by means of BB84 protocol. All the above is intended for each voter who votes. On expiration of the legally allocated voting time the Bob's authorised agents B_1 and B_2 simultaneously and at the same moment of time transfer the voting data to two authorized agents of the election commission A_1 and A_2, accordingly. Besides, at the data transfer moment A_1 and A_2 agents should be in the immediate proximity (not exceeding 1 m) and at the same distance from agents B_1 and B_2, accordingly. In order to avoid data leaks and/or distortion of information, each relevant pair of agents A and B can be automatic devices installed in the enclosed and isolated against penetration (until the end of vote computation) space. Agents A_1 and A_2 verify whether the data obtained from agents B_1 и B_2, accordingly, coincides. Should the data be similar with both agents, it means that a sham attempt was not accomplished. Besides, A agents verify whether the obligation was taken within the time period $t_0 - d/2c$. Here, t_0 means the time when A agents received the data. Finally, both A agents verify whether polarization of the photons that Alice has sent to Bob (indeed, these polarization directions were fixed by Alice) conform with the results received from B_1 and B_2 agents. It is this data that informs Alice's agents and the election commission members about the choice of the voter (and about the obligation undertaken by him/her) – "0" (nays) or "1"

(yeas). Certainly, there also exists a control of the error rate (which is inevitable because the communication channel is imperfect) not exceeding such threshold value which has been established for checking channel interception by an illegal intruder. Application of the quantum bit commitment scheme makes allegations (if any claims are attempted) of whichever group of voters unworkable with respect of alleged violations in the course of voting as the bit commitment performs, actually, a function of the electronic digital signature.

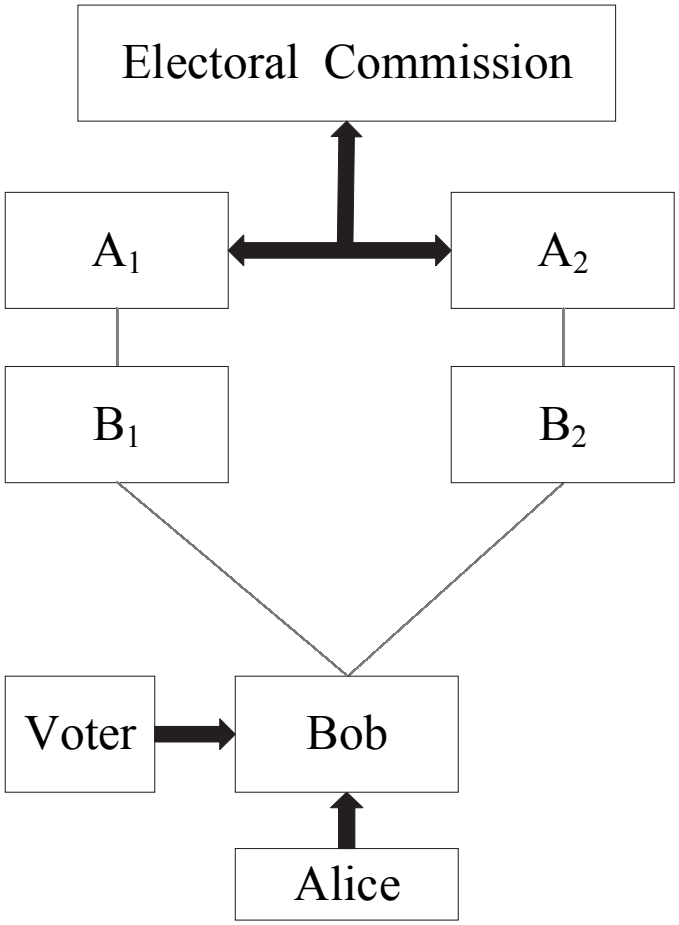

Fig. 1. The general scheme providing for information security of the electronic voting.

Upon receipt of data, each of two A agents executes secret sharing in compliance with the scheme described in [4] in accordance with the number of the election commission members, and transfers each part of the secret to each commission member, respectively. In order to complete the vote count procedure, all commission members should demonstrate their parts of the secret to each other. Otherwise, the vote count is impossible. Such scheme makes it impossible to traffic with the votes. Now we shall describe the secret sharing scheme for our case based on [4] – Fig. 2. Several members *n* of the election commission should get one share of secret each. To this end, the sequence of Greenberger–Horne–Zeilinger states (GHZ) is being prepared:

$$|\psi\rangle_{GHZ} = \frac{1}{\sqrt{2}}\left(|000...0\rangle + |111...1\rangle\right) \qquad (1)$$

Here, the states $|0\rangle = |z+\rangle$ and $|1\rangle = |z-\rangle$ are the eigenstates in case the photon polarization is measured in the rectilinear basis (in our situation it is designated as *z*). To simplify the description, we assume that the commission numbers two members only (later we shall extend the secret sharing possibility including an arbitrary number of the commission members). One of the participants which we call D (dealer) and which represents, in our case, an automatic device conjugated with devices A_1 и A_2 keeps by one photon out of GHZ triplet and sends each one of the remaining photons to one of two other participants of the secret sharing (we designate these commission members as M_1 and M_2). Thereupon all participants of the secret sharing procedure (in our simplified case of three participants these are: dealer D and two members of the election commission M_1 and M_2) should make a random choice of the polarization measurement basis for one of three photons that is kept by each participant respectively – each participant chooses his basis irrespective of and secretly from the other participants. When taking measurements in the diagonal basis (in our case it is designated as *x*) and in the circular basis (designated as *y*), the eigenstates can be expressed as:

$$|0\rangle_x = |+x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

$$|1\rangle_x = |-x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \qquad (2)$$

$$|0\rangle_y = |+y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right),$$

$$|1\rangle_y = |-y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right) \qquad (3)$$

In its turn, the eigenstates in the rectilinear basis are expressed through the eigenstates in the diagonal and circular bases:

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x + |1\rangle_x\right),$$

$$|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x - |1\rangle_x\right) \qquad (4)$$

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_y + |1\rangle_y\right),$$

$$|1\rangle = -\frac{i}{\sqrt{2}}\left(|0\rangle_y - |1\rangle_y\right) \qquad (5)$$

In the course of making quantum measurements in the diagonal and circular bases, values 0 and 1 may be obtained depending on which polarization takes place. Only a half of the performed measurements can be later used for the procedure associated with restoring the secret. This is predetermined by the circumstance that the bases selected by various participants

should coincide. However, if the bases are chosen at random, it can take place in 50% of the cases only.

Now, let us extend the number of the election commission members that share the secret from 2 to an arbitrary number. The GHZ set of triplets that are used for secret sharing is expressed as a sequence $[b_1(j), b_2(j),...b_i(j),...b_n(j)]$. Here, j is used for designating each GHZ triplet, and the subscript designates the numbers of the triplet parts that are kept by each corresponding member of the election commission – M_1, M_2, M_3, etc. At that point we consider that if the *i-th* participant makes use of the diagonal basis, the b value equals zero $b_i(j)=0$, and if the circular basis has been chosen, the b value equals unity $b_i(j)=1$, accordingly. It follows from (4) and (5) that the component $|00...0\rangle$ is expressed as:

$$|00...0\rangle = \prod_{i=1}^{n}\left(\sqrt{\frac{1}{2}}\left(|0\rangle_{b_i} + |1\rangle_{b_i}\right)\right) \quad (6)$$

The $|11...1\rangle$ component is written as:

$$|11..1\rangle = \prod_{i=1}^{n}\left(\frac{-i}{\sqrt{2}}\left(|0\rangle_{b_i} - |1\rangle_{b_i}\right)\right) \quad (7)$$

Due to reasons described in [4], it is impossible to share the secret if the circular basis has been chosen for measurement by an odd number of the participants. When the circular basis has been chosen by an even number of the participants, each GHZ-state is expressed as:

$$|\psi\rangle_{GHZ} = \frac{1}{2^{(n+1)/2}}\left(\prod_{i=1}^{n}\left(\sqrt{\frac{1}{2}}\left(|0\rangle_{b_i} + |1\rangle_{b_i}\right)\right) \pm \right.$$

$$\left. \pm \prod_{i=1}^{n}\left(\sqrt{\frac{1}{2}}\left(|0\rangle_{b_i} - |1\rangle_{b_i}\right)\right)\right) \quad (8)$$

If the circular basis has been chosen by the even number of the participants who share the secret, the result of measurement of the qubit by D dealer is unambiguously defined by the results of measurements of the other qubits. Therefore, if the remaining n-1 members of the group, save for D dealer (in our case they are all members of the commission), jointly demonstrate the results of their measurements to all other members, then they have a possibility to determine the result of measurement made by D dealer. However, if at least one member of the group is lacking to comprise the n-1 number of participants, they are unable to restore the secret. In the simplest case of only three participants - dealer D and two members of the election commission M_1 and M_2 - and, for instance, the quantum measurement result $|100\rangle$ the value «1» of qubit measurement result of dealer D is computed according to the formula:

$$l_D = l_1 = l_2 \oplus l_3 \oplus 1 \quad (9)$$

In our case l_1 and l_2 are the results obtained in the course of qubit measurements by the members of the commission M_1 and M_2, respectively, and they have the value of «0». We generalize formula (9) for the purpose of the given scheme for all those and solely for those cases when the number of the participants who have chosen the circular basis equals $2(2k+1)$, where k is a whole non-negative number:

$$l_D = l_1 = l_2 \oplus l_3 \oplus ... \oplus l_n \oplus 1 \quad (10)$$

When the number of the group members who made the measurement in the circular basis equals $4k$, the formula below is correct:

$$l_D = l_1 = l_2 \oplus l_3 \oplus ... \oplus l_n \quad (11)$$

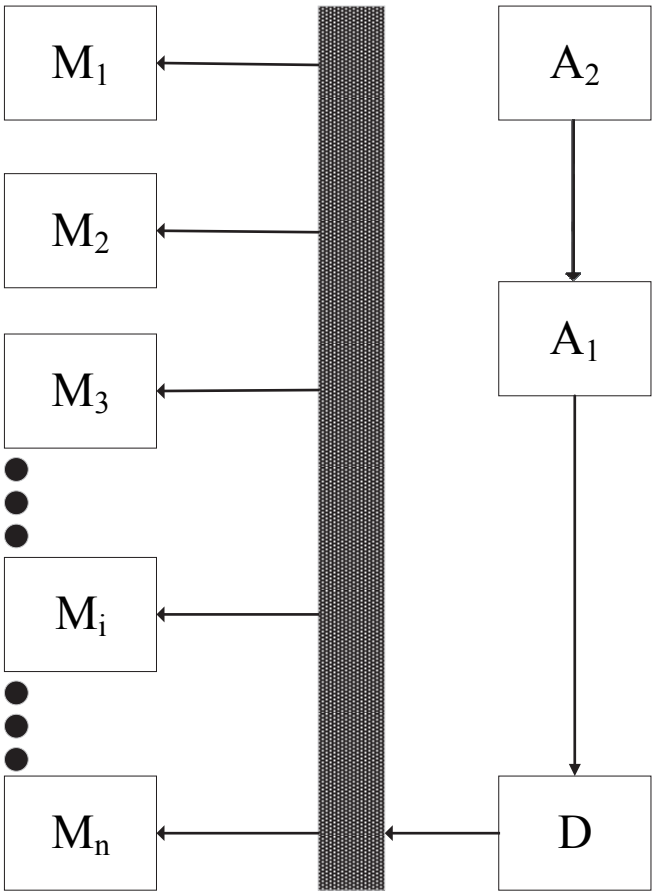

Fig. 2. Scheme of secret sharing among the election commission members. A_1 and A_2 are «Alice's» agents. D - «dealer», M_1, M_2… M_i, …M_n – members of the election commission.

Let us summarize the above and enumerate the steps required for the separation procedure to take place and for further restoration of the secret by the election commission members: a) a participant who is initially in possession of the secret (in our case it is dealer D) and who prepares n photons in GHZ state; b) the dealer leaves one photon with himself and sends the remaining photons of the GHZ state to n-1 participants of the secret sharing, i.e., to the members of the election commission. One qubit falls on each member of the commission; c) each participant of the secret sharing procedure selects, randomly and irrespective of the other members of the group, one measurement basis (out of two possible bases) of the quantum state of his photon – either diagonal or circular;

afterwards the quantum measurement is made, the measurement result and the information about the type of basis used for making the measurement are saved; d) steps a) - c) are reiterated as many times as necessary for ciphering the data received from Alice's agents A_1 and A_2; we note that the number of measurements will be at least two times as great as the number of classic data bits «0» and «1») – a half of the conducted measurements may not be usefully applied; e) then, after the d) step has been made, each member of the election commission sends a message to dealer D by a classic communication channel wherein he informs what basis was chosen for the measurement – either diagonal or circular; the dealer counts how many measurements were made in the circular basis and informs the election commission members either to the effect that the current round of measurements was useless (the case when the circular basis was chosen by an odd number of the participants) or that it is required to save the measurement results; besides, the information contains what the even number of measurements in the circular basis is multiple of: $2(2k+1)$ or $4k$, however, the k number proper is not revealed; the dealer will request a certain percentage of the measurement results in order to exercise control of interception – when there are about 50% of useless results of measurement it is possible to assert that there are no unauthorized actions of intruders but when a noticeably higher percentage of useless results has been recorded, (e.g., about 75%), there are grounds to suppose that there exist attempts to intercept and distort the information, whereby the results obtained after the latest safe data transfer are cancelled. Afterwards the election commission members can jointly restore the data obtained by them.

III. CONCLUSION

The scheme proposed in this paper makes use of quantum technologies while earlier, when describing the electronic voting systems based on secret sharing and bit commitment in the literature, such quantum technologies were not applied whereupon we may claim the engineering novelty of the solution described herein. In its turn, as it was stated above, the quantum cryptographic schemes have a certain advantage over the classical schemes (that do not make use of quantum technologies), in particular, they are characterized by a strong cryptography that is comparable with the unconditional security; also, as distinct from the classical cryptosystems, they enable to timely detect unauthorized bugging and, possibly, subsequent distortion of data in the communication channel.

REFERENCES

[1] B. A. Schoenmarkers, " Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting ," Lecture Notes in Computer Science, vol. 1666, pp. 148-164.

[2] N.P. Smart, Cryptography: An Introduction. McGraw Hill, 2002.

[3] T. Lunghi, J. Kaniewski, F. Bussieres, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner and H. Zbinden, "Experimental Bit Commitment Based on Quantum Communication and Special Relativity ," Physical Review Letters, vol. 111, 180504.

[4] L. Xiao, G.L. Long, F.G. Deng and J.W. Pan, "Efficient Multiparty Quantum-Secret-Sharing Schemes ," Physical Review A., vol. 69, 052307.