Towards quantum-based privacy and voting

Mark Hillery[1], Mário Ziman[2,3], Vladimír Bužek[2,4], and Martina Bieliková[5]
[1] *Department of Physics, Hunter College of CUNY, 695 Park Avenue, New York, NY 10021, USA*
[2] *Research Center for Quantum Information, Slovak Academy of Sciences, Dúbravská cesta 9, 845 11 Bratislava, Slovakia*
[3] *Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic*
[4] *Abteilung Quantenphysik, Universität Ulm, 89069 Ulm, Germany and*
[5] Quniverse*, Líšśie údolie 116, 841 04 Bratislava, Slovakia*
(Dated: 26 April 2005)

The privacy of communicating participants is often of paramount importance, but in some situations it is an essential condition. A typical example is a fair (secret) voting. We analyze in detail communication privacy based on quantum resources, and we propose new quantum protocols. Possible generalizations that would lead to voting schemes are discussed.

Every day people have to make important decisions that should remain secret. Protecting the privacy of those decisions, if their results are to be communicated, can be a challenging problem. In this Letter we will consider a special instance of multi-party decision making. Consider a group of people who have to make a common decision, i.e. choosing one of several possible (prescribed) options. In many cases the fairest (democratic) way of making the decision is to *vote*. Reliable voting protocols should satisfy a number of conditions [1], three of which are: *i)* security, *ii)* verifiability, and *iii)* privacy. The security condition guarantees that all users can influence the result only by casting a *single* valid vote. That is, each voter can vote just once (non-reusability), only legitimate users can vote (eligibility) and no one can learn any intermediate result (fairness). The strongest version of the verifiability requirement is that each voter can verify the correctness of the result, however none of the voters is able to prove how he or she voted. This prevents vote buying.

A voting scheme satisfying all properties except the privacy condition is easy to implement. Privacy is related to the secrecy of the ballots, or equivalently to the anonymity of the voters. Ideally, no one should be able to tell how any of the voters voted. Such multi-party communication protocol is known as *secret*, or *anonymous voting*.

In the voting process the initial information I_i created by voters (their votes) is transformed into the final outcome corresponding to the information I_f. Usually I_i is much larger than I_f. The voting can be formalized as mapping $\mathcal{V} : X \times \ldots \times X \rightarrow Y$, where X, Y represent sets of individual voting options and a set of final results, respectively. The input/output information can be expressed in terms of the cardinalities of the sets X, Y, i.e. $I_i = N \log_2 |X|$ (N is the number of participants) and $I_f = \log_2 |Y|$. For example, N parliamentarians during a voting procedure create $I_i = N \log_2 3$ bits of information, given the choices: $X = \{accept, refuse, abstain\}$. However, the final result can be represented only by $I_f = \log_2 3$ bits with $Y = \{acceptance, refusal, undecided\}$.

Hiding the identity of the voters seems to be very difficult to achieve, because the information can often be traced back to its origin. In a public election the collected paper ballots are mixed in a ballot box, which could ensure the anonymity of a voter. However, the ballots could be marked in such a way that it is possible to identify the voters. Thus perfect privacy no longer holds. The first protocol to guarantee voting privacy (see Ref. [2]) was based on the so-called *MIX net machines*. Since then several secret voting protocols based on cryptographic primitives such as anonymous broadcast [2] or blind signatures [3, 4], have been proposed. Some of the properties of these protocols are even unconditionally secure, and others are guaranteed in the computational sense, i.e. they are based on one-way functions. David Chaum [5] suggested a solution of the so-called *dinning cryptographers problem* that can be used to implement a secret voting protocol. Let us briefly describe this procedure, which guarantees unconditionally the anonymity of the voters.

Three cryptographers are having a dinner in their favorite restaurant. After ordering their food, the waiter comes and informs them that someone has already paid for the dinner. The problem is to determine whether it has been paid for by one of them, or by someone else (for instance, by the NSA). The cryptographer who paid (if indeed one of dinning cryptographers took care of the bill) wants to remain anonymous. The three cryptographers can resolve the problem by using the following protocol: Each pair $\{j, k\}; (j, k = 1, 2, 3)$ of cryptographers toss a coin, i.e. they generate a random bit c_{jk}. The third cryptographer cannot see the result. Each cryptographer announces the logical (mod2) sum of the two bits he shares, i.e., the cryptographer k announces the value $s_k = \sum_{j \neq k} c_{jk}$, unless he is the one who paid for the dinner. The one who paid the bill announces the opposite value, i.e. $s_k = 1 + \sum_{j \neq k} c_{jk}$. If the dinner was paid by the NSA then $\sum_k s_k = 0$. If not, then $\sum_k s_k = 1$. The identity of the potential payer remains completely secret.

This protocol can be easily extended to an arbitrary number of users, and a slightly modified version can be used for voting. Each pair of voters shares a random integer (key) $c_{jk} \leq N$, where $c_{jk} = -c_{kj}$. Each voter chooses either $v_k = 0$ ("no") or $v_k = 1$ ("yes"). He broadcasts the message $s_k = v_k + \sum_{j \neq k} c_{jk}$. Because of $c_{jk} = -c_{kj}$ it is valid that $\sum_k s_k = \sum_k v_k$. Finally, each of the users can compute the sum and find out the total number of the "yes" votes. Let us note that all operations are modulo N. Privacy in this scheme is assured, but the protocol is not secure and cheating is easy. One cannot guarantee that voters will not "vote" an arbitrary number of times $v_k \leq N$, i.e. the result can be easily manipulated. However, there exists a modification that solves this problem and provides security based on the RSA protocol (for more details see Refs. [3, 5]).

We would now like to consider whether the paradigm and tools of quantum (information) theory and in particular, the quantum cryptography [6] can help us to implement tasks related to secret voting and maintaining the anonymity of the voters.

The first analysis of identity protection based on quantum protocols was performed by Christandl and Wehner (see Ref. [7]), who used generalized GHZ states to *anonymously broadcast* not only classical bits, but also qubits. Recently, Vaccaro et *al.* [8] proposed the first scheme for *quantum voting*, in which the quantum protocol is used to ensure the voter's privacy. A closely related problem of *anonymous oblivious transfer* has been studied in Ref. [9]. The privacy problem is relatively new even in the classical information theory. It seems (at least intuitively) that quantum systems may be more suitable and more efficient in achieving this goal.

Let us start with the analysis of the privacy and the voting problem in the framework of quantum theory. Our aim is to use quantum information to ensure the privacy. In principle, one can imagine two general schemes of the voting procedure: *i)* the distributed-ballots scheme (DB) and *ii)* the travelling-ballot scheme (TB). In the DB a voter obtains his own ballot, he or she performs voting operation and sends the ballot back. The TB is a scheme in which a single ballot/container is travelling (is sent) between voters and everyone performs the voting operation on the same physical system. Both, the DB and the TB scenarios can be formalized in the same way. Physically quantum voting is performed by transformations of some quantum system. Let us denote by Ω_0 the initial state of the system (the quantum ballot) and by $U_k^{(j)}$ a transformation performed by the jth user voting for the option $k \in X$. After the voting has concluded, the ballot is sent to the authority, who performs a measurement M on the ballot. The outcome of the measurement r is associated with the result of the voting, $r \in Y$. Let us denote by $\vec{v} = (k_1, \ldots, k_n)$ the particular collection of votes and by $\mathcal{V}(\vec{v}) \in Y$ the result of the process of voting. After the voting is completed the system is described by the state $|\Omega_{\vec{v}}\rangle = U_{k_n}^{(n)} \ldots U_{k_1}^{(1)} |\Omega_0\rangle$. The difference between these two schemes is that in the DB scheme we work with a composite system of N particles, and the operations for different users mutually commute.

In what follows we will assume that the initial state Ω_0 is pure and voting operations are represented by unitary maps. The privacy of votes is reflected by the following set of conditions

$$
\begin{aligned}
|\langle\Omega_{\vec{v}_1}|\Omega_{\vec{v}_2}\rangle| = 0, &\text{ iff } \mathcal{V}(\vec{v}_1) \neq \mathcal{V}(\vec{v}_2) \; ; \\
|\langle\Omega_{\vec{v}_1}|\Omega_{\vec{v}_2}\rangle| = 1, &\text{ iff } \mathcal{V}(\vec{v}_1) = \mathcal{V}(\vec{v}_2) \; .
\end{aligned} \tag{1}
$$

These conditions guarantee that finally only I_f bits of information is available and the identity of the voters is securely hidden. Our task is to find collections of voting operations $\{U_k^{(j)}\}$ and an initial state Ω_0 such that the above conditions are satisfied. In what follows we will simplify the task by assuming that each participant uses the same collection of operations, i.e. $U_k^{(j)} = U_k^{(j')} \equiv U_k$ for all j, j' and all k.

Let us start by analyzing the simplest case of two voters. In this case the privacy property does not make much sense, because after a public announcement of the result each voter can deduce how the other participant has voted. However, it can be of interest to some third party, particulary in the case of an *undecided* result, i.e. when votes do not coincide. Let us consider the TB scheme first. The set of possible results restricts from below the dimension of the required quantum system, i.e. $\dim \mathcal{H} \geq \log_2 I_f$, because this is the smallest quantum system containing I_f bits of information. In our case $Y = \{acceptance, refusal, undecided\}$ and consequently at least a qutrit is needed to perform the voting. Let us assume the state $|\Omega_0\rangle = |0\rangle$ and voting transformations $U_{no} = I$ and $U_{yes} = U$, where U is defined via transformations $|0\rangle \to |1\rangle \to |2\rangle \to |0\rangle$. It is easy to verify that Eqs. (1) are fulfilled, however this system does not guarantee the secrecy of votes. In the proposed protocol it is very easy to learn the actual state of the voting, i.e. the intermediate result. One way how to avoid this problem is to use an *authority* who prepares the initial state of the ballot and finally reads the result. The initial state is *unknown* to the voters, i.e. they cannot find out the intermediate result. Only the authority knows the basis in which the measurement must be performed. It requires a little algebra to find all states $|\Omega_0\rangle$, for which the voting operations U_{yes}, U_{no} (specified before) satisfy the system of equations (1).

In what follows we present a protocol with an honest (non-cheating) authority that utilizes entangled states: The authority prepares two qutrits that serve as a ballot in a maximally entangled state $|\Omega_0\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$. One of the qutrits is sent to the voters. Using the voting operation U_{yes} they produce mutually orthogonal states associated with mutually exclusive results of voting. In this way one can guarantee that intermediate measurements performed individually by voters who might want to learn an intermediate voting result provide no information about how the voting has progressed. The state of the particle seen by the voters is, at all times, simply a total mixture. Both of these protocols can be directly generalized to an arbitrary number of participants.

Next we shall again consider the case of two voters, but we shall analyze the DB scheme. Let us start with the assumption that each of the participants obtains a ballot represented by a single qubit. In the previous paragraph we have argued that the total system has to be at least three-dimensional. Although the system of two qubits is four-dimensional, the DB scheme allows the users to make only local voting operations, i.e. single-qubit unitary transformations. The question is, whether two qubits are sufficient to implement secret voting. Suppose that U_0, U_1 and V_0, V_1 are voting operations of the voters named U and V, respectively. Let us denote by $|\Omega_0\rangle$ the initial state of the two ballot qubits. The privacy conditions (1) yield the following system of equations

$$
\begin{aligned}
0 &= \langle\Omega_0|U_0^\dagger U_1 \otimes I|\Omega_0\rangle = \langle\Omega_0|I \otimes V_0^\dagger V_1|\Omega_0\rangle \; ; && (2)\\
1 &= \langle\Omega_0|U_0^\dagger U_1 \otimes V_1^\dagger V_0|\Omega_0\rangle \; ; && (3)\\
0 &= \langle\Omega_0|U_0^\dagger U_1 \otimes V_0^\dagger V_1|\Omega_0 \; ; && (4)\\
0 &= \langle\Omega_0|U_1^\dagger U_0 \otimes I|\Omega_0\rangle = \langle\Omega_0|I \otimes V_1^\dagger V_0|\Omega_0\rangle \; . && (5)
\end{aligned}
$$

Due to the fact that $U_0^\dagger U_1$ and $V_0^\dagger V_1$ are unitary single-qubit transformations, they can be expressed as $U_0^\dagger U_1 = I\cos\nu + i(\vec{m}\cdot\vec{\sigma})\sin\nu$ and $V_0^\dagger V_1 = I\cos\theta + i(\vec{n}\cdot\vec{\sigma})\sin\theta$. It also holds that $(U_0^\dagger U_1)^\dagger = U_1^\dagger U_0$ and $(V_0^\dagger V_1)^\dagger = V_1^\dagger V_0$. ¿From Eqs. (2) and (3) it follows that

$$
\cos\nu\cos\theta + \sin\nu\sin\theta\langle\Omega_0|\vec{n}\cdot\vec{\sigma}\otimes\vec{m}\cdot\vec{\sigma}|\Omega_0\rangle = 1 \, , \qquad (6)
$$

which together with Eq. (4) results in the condition $2\cos\nu\cos\theta = 1$. However, combining Eqs.(2) and (5) we find that $\cos\theta = 0$ and $\cos\nu = 0$. This is a contradiction and therefore two-dimensional systems are not sufficient to implement the DB scheme. One needs at least two qutrits. Note that in the DB scheme the fairness requirement holds, i.e. nobody can learn intermediate results.

To proceed further let us recall the following property. If the protocol $(|\Omega_0\rangle, \{U_k\})$ satisfies the privacy conditions, then so does the protocol $(|\Omega_0'\rangle, \{U_k'\})$, where $U_k' = U_k V$ and $|\Omega_0'\rangle = (V^{\otimes N})^\dagger|\Omega_0\rangle$. This means we can always choose $U_0 = I$, i.e. without the loss of generality we can assume that $U_{no} = I$ and $U_{yes} = U$. Applying the privacy conditions from Eq. (1) we obtain equations

$$
\begin{aligned}
\langle\Omega_0|U\otimes U|\Omega_0\rangle &= 0 \; ;\\
\langle\Omega_0|U\otimes I|\Omega_0\rangle &= 0 \; ;\\
\langle\Omega_0|I\otimes U|\Omega_0\rangle &= 0 \; ;\\
\langle\Omega_0|U^\dagger\otimes U|\Omega_0\rangle &= 1 \; . && (7)
\end{aligned}
$$

Our task is to find a solution of this set of equations. Because U is unitary, its eigenvalues are of the form $e^{i\eta_j}$ and $U = \sum_j e^{i\eta_j}|j\rangle\langle j|$, where $|j\rangle$ is the eigenvector corresponding to the eigenvalue $e^{i\eta_j}$. Let us consider the state $|\Omega_0\rangle = \sum_j |\alpha_j|^2|j\rangle\otimes|j\rangle$, where, again, $\{|j\rangle\}$ are eigenvectors of U. Using this Ansatz the above identities gives us the following equations $\sum_j |\alpha_j|^2 e^{i2\eta_j} = 0$, $\sum_j |\alpha_j|^2 e^{i\eta_j} = 0$, and $\sum_j |\alpha_j|^2 = 1$. The last of these equations is just the normalization condition for the state $|\Omega_0\rangle$, and is satisfied. We have already shown that a qubit is not a sufficient resource for quantum voting and larger dimensional systems have to be sent to both voters. Assuming $d = 3$ we find that the equations for parameters η_j, α_j have multiple solutions. Here, however, we will restrict ourselves to $|\alpha_j| = 1/\sqrt{d} = 1/\sqrt{3}$. The possible solutions then form a one-parameter set and among them is the following one

$$
\begin{aligned}
U &= e^{i2\pi/3}|0\rangle\langle 0| + e^{i4\pi/3}|1\rangle\langle 1| + e^{i6\pi/3}|2\rangle\langle 2| \; ;\\
|\Omega_0\rangle &= \frac{1}{\sqrt{3}}(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|2\rangle) \; . && (8)
\end{aligned}
$$

This solution (i.e., $U = \sum_k e^{i2k\pi/3}|k\rangle\langle k|$ and $|\Omega_0\rangle = \frac{1}{\sqrt{3}}\sum_k |k\rangle\otimes|k\rangle$) can be easily extended to an arbitrary number of participants. Let us suppose that there are N voters and the authority that distributes one qudit ($d > N$) to each voter. In accordance with the case of two voters let the authority prepare and distribute the state $|\Omega_0\rangle = \frac{1}{\sqrt{d}}\sum_j |j\rangle^{\otimes N}$. The voters will apply one of the two operations: either $U_{no} = I$, or $U_{yes} = U = \sum_k e^{ik2\pi/d}|k\rangle\langle k|$, depending on their decision. After performing the voting operations they send the qubits back to the authority, who now possesses the state $|\Omega_m\rangle = U^{\otimes m}\otimes I^{\otimes(N-m)}|\Omega_0\rangle = \sum_k e^{imk2\pi/d}|k\rangle^{\otimes N}$, where m is the number of voters who choose to vote "yes", i.e. the result of the voting. Note that this state contains no information about the particular voter, only the total number of "yes" votes is recorded. This guarantees the privacy of the individual votes. The distinguishability of different outcomes (different numbers of "yes" votes) is guaranteed by the orthogonality condition i.e. $\langle\Omega_m|\Omega_{m'}\rangle = \delta_{mm'}$.

This protocol protects the identity of the voters from a curious, but not malicious, authority and from other voters. We assume that the authority follows the protocol, but does whatever he can beyond this to determine the individual votes. In this case, because the state he receives contains no information about who voted how, he can do nothing. If, after the voing, a voter intercepts a particle from another voter, he will be able to learn nothing, because any subset of particles has a reduced density matrix proportional to the identity.

The protocol can also be used in the dinning-cryptographers problem. It has further uses as well. A simple generalization of the protocol can be used also for what was called in Ref. [8] an anonymous survey. Imagine that N people want to determine the total amount of money they have, but each individual does not want reveal how much money he or she has. These people use the same method, except that each person votes "yes" a number of times corresponding to the number of Euros (s)he has. In the resulting state, $|\Omega_m\rangle$, m will be equal to the total number of Euros, but the contributions of individual partners will be unknown. This is an example of quantum secure function evaluation [10, 11].

In a sense this voting protocol can be thought of as a generalization of the classical scheme. However, like its classical counterpart, it does not completely possess the properties of the security and the verifiability. In fact, we have focused our attention mainly on the un-traceability of voters (privacy). To achieve a completely secure voting scheme the protocol has to be improved. One of the security loopholes is the possibility for voters to vote more than once. This type of cheating, however, is not guaranteed to produce the desired result, because the states $|\Omega_m\rangle$ count only the number of "yes" votes modulo N. If too many voters vote "yes" too many times, the number m can become larger than N and because $|\Omega_m\rangle$ records the number of "yes" votes only modulo N, the final recorded number m could be small. In fact, even if there is a subset of cooperating voters it would be difficult to know what the effect of such cheating would be, and the voting process would become a strategic game.

In order to prevent voters from registering more than one vote (a complete non-reusability of ballots) we can proceed as follows: Besides the qudit from the state $|\Omega_0\rangle$ each of the participants receives two additional "voting" qudits, one in the state $|\psi(\theta_y)\rangle$ and the second one in the state $|\psi(\theta_n)\rangle$. These two qudits represent the "yes" and the "no" votes, respectively. Both of the states are of the form $|\psi(\theta)\rangle = \frac{1}{\sqrt{d}}\sum_k e^{ik\theta}|k\rangle$. Depending on his (her) choice the voter combines either $|\psi(\theta_y)\rangle$, or $|\psi(\theta_n)\rangle$, with the original ballot particle and performs a two-qudit measurement that is specified by a set of projectors $P_l = \sum_j |j+l\rangle\langle j+l| \otimes |j\rangle\langle j|$. Registering the outcome r the voter applies the operation $V_r = \sum_j |j+r\rangle\langle j|$ to the voting qudit and sends both (the ballot and the voting) qudits back to the authority. The remaining unused qudit must be kept, or destroyed in order to secure the privacy of the registered vote. The resulting two-qudit state that is sent to the authority is as follows: Assuming the vote "yes" we obtain $P_r(\frac{1}{\sqrt{d}}\sum_k |k\rangle|\psi(\theta_y)\rangle|k\rangle^{\otimes(N-1)}) = \frac{1}{d}\sum_k e^{i(k-r)\theta_y}|k\rangle|k-r\rangle|k\rangle^{\otimes(N-1)}$. After the "correcting" unitary operation V_r the $N+1$ qudits are in by the state $|\Omega_1\rangle = \frac{1}{\sqrt{d}}e^{-ir\theta_y}\sum_k e^{ik\theta_y}|k\rangle^{\otimes(N+1)}$, where the global phase is irrelevant. If $m_y = m$ the users voted "yes" and $m_n = N - m$ users voted "no", the authority gets back the state $|\Omega_m\rangle = \frac{1}{\sqrt{d}}\sum_k e^{ik(m_y\theta_y+m_n\theta_n)}|k\rangle^{\otimes 2N}$. Here the phase factor can be rewritten as follows $e^{ik(m_y\theta_y+m_n\theta_n)} = e^{ikm\Delta}e^{ikN\theta_n}$, where $\Delta = \theta_y - \theta_n$. We see that only if $\Delta = 2\pi/d$ the states $|\Omega_m\rangle$ are mutually orthogonal as is required.

If the authority is malicious as well as curious, one of the new security problem that arises is that of the *state identification*, i.e. verifying whether the initial ballot state is correct, and whether the voting states provided by the authority are also correct. The authority could cheat either by sending a ballot state that is a product state, so that each voter's particle is decoupled from all of the others, or by sending voting states that are different for each voter. In principle, if the authority is required to supply a large number of both kinds of states to the voters, they can verify the correctness of the states by performing state tomography. Another possibility, at least in regard to the ballot state, is for the voters to prepare that state by themselves. However, this is second option is somewhat restrictive, because it requires that participants (voters) have to meet as the same place (or they need quantum resources for a remote state preparation).

In summary, we have proposed new quantum protocols that guarantee the anonymity of participants in voting procedures and can be used in several complex communication tasks.

We would like to thank to Jan Bouda for his help with the literature on classical privacy and voting schemes. This work was supported by the National Science Foundation under grant PHY 0139692, by the European Union projects QGATES, QUPRODIS and CONQUEST, by the Slovak Academy of Sciences via the project CE-PI, by the project APVT-99-012304, and by the Alexander von Humboldt Foundation.

Note added: When this manuscript has been finished a paper by Vaccaro et al [8] has appeared where some of the issues discussed in the present paper have been studied as well.

[1] Bruce Schneier, *Applied Cryptography*, (Wiley, New York, 1996), page125.
[2] D. Chaum, Comm. ACM **24**, 464 (1981)
[3] J.N.E. Bos, *Practical Privacy*, (PhD thesis, Eindhoven University of Technology, ISBN 9061964059, 1992)
[4] B. Pfitzmann and M. Waidner, (Hildesheimer Informatik-Berichte, Institut für Informatik, Universität Hildesheim, ISSN 0941-3014, 1992)
[5] D. Chaum, Journal of Cryptography **1**, 65 (1988)
[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
[7] M. Christandl and S. Wehner, `quant-ph/0409201` (2004)
[8] J.A. Vaccaro, J. Spring, and A. Chefles, `quant-ph/0504161` (2005)
[9] J. Müller-Quade and H. Imai, *Anonymuos oblivious tranfer*, `cs.CR/0011004` (2000)
[10] H. Klauck, `quant-ph/0110038` (2001)
[11] C. Crepeau, D. Gottesman, and A. Smith, `quant-ph/0206138` (2002)