Towards quantum-based privacy and voting

Mário Ziman

Research Center for Quantum Information, Bratislava

http://www.quniverse.sk/

Collaborators:

Martina Bieliková, Mark Hillery, Vladimír Bužek
Program.

- Secret voting and privacy
- Anonymity in classical case
- Two schemes
- Mathematical formulation of the problem
- Quantum protocol
- Discussion
Quantum cryptography

- not completely serious viewpoint
  - uncertainty helps to secure the information
  - superposition helps to decrease the complexity
  - entanglement somehow helps

- quantum protocols
  - key distribution, coin tossing, bit commitment, oblivious transfer, pseudosignatures, secret sharing, etc.
Secret voting - definition

- **Security**
  - non-reusability = each voter can vote only once
  - eligibility = only legitimate users can vote
  - fairness = noone can learn intermediate result

- **Verifiability**
  - each voter can verify the correctness of the result
  - none of the voters is able to prove how he/she votes

- **Privacy**
  - votes are anonymous
Privacy and quantum

Motivation
- voting: input = N bits, but output = 1 bit (result)
- qubit state contains infinite information, but only one bit can be extracted
- idea: use single qubit as voting system
Classical proposals

- **anonymous broadcast**
  - problem: hide the identity of the sender
  - different scenarios: one-to-many, many-to-one, many-to-many
  - exists classical and quantum solutions

- **pseudosignatures**
Dining cryptographers problem

- three cryptographers, three dinners and one paid bill
- who has paid? one of cryptographers, or NSA?

- result = B₁ + B₂ + B₃
- payer Bⱼ = NOT [ bⱼ ]
- nonpayer Bⱼ = bⱼ

- result = 0 means NSA pays
- result = 1 means opposite

ONE-TO-MANY ANONYMOUS BROADCAST
Two scenarios

travelling-ballot scheme

distributed ballots scheme
Mathematical formulation

- initial (ballot) state $\Omega_0$
- votes of jth participant $U_k^{(j)}$, where $k \in X$
- collection of votes $\vec{v} = (k_1, \ldots, k_n)$
- voting map $\mathcal{V} : X \times \ldots \times X \rightarrow Y$
- election result $|\Omega_{\vec{v}}\rangle = U_{k_n} \cdots U_{k_1} |\Omega_0\rangle$
- privacy conditions
  
  $|\langle \Omega_{\vec{v}_1} | \Omega_{\vec{v}_2} \rangle| = 0$, iff $\mathcal{V}(\vec{v}_1) \neq \mathcal{V}(\vec{v}_2)$
  
  $|\langle \Omega_{\vec{v}_1} | \Omega_{\vec{v}_2} \rangle| = 1$, iff $\mathcal{V}(\vec{v}_1) = \mathcal{V}(\vec{v}_2)$

- in DS scheme $U_k^{(j)}$ commutes for different voters
Two voters “problem”

- Q: is qubit sufficient?
  - TS scheme NO, because three possible results
  - DS scheme NO, because the privacy conditions cannot be satisfied by any choice of voting operations, i.e.

\[ \Omega_{yes} \perp \Omega_{no} \perp \Omega_{?} \perp \Omega_{yes} \]

\[
|\Omega_{yes}\rangle = U_{yes} \otimes V_{yes} |\Omega_0\rangle \\
|\Omega_{no}\rangle = U_{no} \otimes V_{no} |\Omega_0\rangle \\
|\Omega_{?}\rangle = U_{yes} \otimes V_{no} |\Omega_0\rangle = U_{no} \otimes V_{yes} |\Omega_0\rangle
\]

- A: both schemes require use of qutrits
Useful property

- consider DS voting cryptosystem $\nu_1 = (\Omega_0, U_k^{(j)} = U_k)$
- define $\nu_2 = (U^\otimes n[\Omega_0], W_k = U_k U^\dagger)$
- both realize voting with the same properties

- consequence

  choice of identity as one of the voting operations

  $U_{no} = I$ \hspace{1cm} $U_{yes} = U$
DS scheme for two voters

- results
  \(|\Omega_0\rangle = |\Omega_0\rangle\)
  \(|\Omega_1\rangle = U \otimes I |\Omega_0\rangle = I \otimes U |\Omega_0\rangle\)
  \(|\Omega_2\rangle = U \otimes U |\Omega_0\rangle\)

- privacy
  \(\langle \Omega_j | \Omega_k \rangle = \delta_{jk}\)

- solution
  \(|\Omega_0\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)\)
  \(U = e^{i2\pi/3} |0\rangle\langle 0| + e^{i4\pi/3} |1\rangle\langle 1| + e^{i6\pi/3} |2\rangle\langle 2|\)
Three and more voters

- **DS scheme for three voters**
  - results 1
    \[ \ket{\Omega_{no}} = U \otimes I \otimes I \ket{\Omega_0} = \ldots = \ket{\Omega_0} \]
    \[ \ket{\Omega_{yes}} = I \otimes U \otimes U \ket{\Omega_0} = \ldots = U \otimes U \otimes U \ket{\Omega_0} \]
  - results 2
    \[ \ket{\Omega_0} = \ket{\Omega_0} \]
    \[ \ket{\Omega_1} = U \otimes I \otimes I \ket{\Omega_0} = I \otimes U \otimes I \ket{\Omega_0} = I \otimes I \otimes U \ket{\Omega_0} \]
    \[ \ket{\Omega_2} = I \otimes U \otimes U \ket{\Omega_0} = U \otimes I \otimes U \ket{\Omega_0} = U \otimes U \otimes I \ket{\Omega_0} \]
    \[ \ket{\Omega_3} = U \otimes U \otimes U \ket{\Omega_0} \]
  - privacy
    \[ \bra{\Omega_j} \Omega_k \rangle = \delta_{jk} \]

- **Our voting task = number of yes and no votes**
Solution in general

\[ |\Omega_0\rangle = \frac{1}{\sqrt{n+1}} \sum_{j=0}^{n} |j\rangle \otimes n \]

\[ U_{yes} = \sum_{k=0}^{n} e^{ik2\pi/(n+1)} |k\rangle \langle k| \]

\[ \langle \Omega_j | \Omega_k \rangle = \delta_{jk} \]

- application
  - determination of total amount of money among N people without revealing individual amounts
  - if x = amount of money then apply x-times yes operation
  - weakness of such voting cryptosystem
Consideration of other conditions

- non-reusability
  - each participant will receive three qudits:
    - two voting qudits $|\psi(\theta_{yes})\rangle$ $|\psi(\theta_{no})\rangle$
    - one ballot qudit (from shared state $|\Omega_0\rangle = \frac{1}{\sqrt{n+1}} \sum_{j=0}^{n} |j\rangle^{\otimes n}$)
  - voting:
    - choose “yes”, or “no” qudit, i.e. our system = (ballot qudit) x (voting qudit)
    - perform measurement with results $P_r = \sum_i |j + r\rangle \langle j + r| \otimes |j\rangle \langle j|$  
    - correcting transformation $V_r = I \otimes \sum_j |j + r\rangle \langle j|$  
  - result: $|\psi(\theta)\rangle = \frac{1}{\sqrt{d}} \sum_k e^{ik\theta} |k\rangle$  and $\theta_{yes} - \theta_{no} = 2\pi / d$

$$|\Omega_m\rangle = \frac{1}{\sqrt{d}} \sum_k e^{ik(m\theta_{yes}+(n-m)\theta_{no})} |k\rangle \otimes (2n)$$

- initial state distribution
Conclusion

- dining cryptographers realize one-to-many anonymous broadcast
- presented scheme realize “many-to-one” anonymous broadcast
- voting requires many-to-many anonymous broadcast
- both schemes can be used to perform the anonymous voting
- imperfect voting cryptosystem