Quantum Polling

Joan Vaccaro
Joe Spring
Anthony Chefles

PRA 75, 012333 (2007), quant-ph/0504161

~ Hillery et al. PLA 349 75 (2006), quant-ph/0505041
Introduction

~ small scale quantum processing

quantum data security

QKD – commercial...

other (incl. multiparty) protocols

- Quantum Fingerprinting
- Quantum Seals
- Authentication of Quantum Messages
- Quantum Broadcast Communication
- Quantum Anonymous Transmissions
- Quantum Exam
- Secret Sharing
Quantum Fingerprinting [Buhrman…PRL 87, 167902 (2003)]
- fingerprint: smaller string ~ uniquely identifies message.
- quantum fingerprints of classical messages are exp. smaller

Quantum Seals [Bechmann-Pasquinucci quant-ph/0303173]
- encode classical message in quantum state
  \(0 \rightarrow |0>|0>|f>, 1 \rightarrow |1>|1>|f>, \) order of bits is random, \(|f> = |0>+e^{i\phi}|1>\)
- easily read (majority vote) – can detect if message has been read

Authentication of Quantum Messages
[Barnum… quant-ph/0205128]
- allows Bob to check that message has not been altered
- e.g. distribute EPR pairs, use purity checking, teleport,…

Quantum Anonymous Transmissions
[Christandl… quant-ph/0409201]
- share GHZ state, pi phase, Hadamard, measure – announce,
- answer is mod 2. Can also share entanglement with “anon Bob”

Quantum Exam [Nguyen PLA 350, 174 (2006)]
- share GHZ states – local meas. gives shared random class. key
- use key to send common exam text and the individual answers.

Secret Sharing [Hillery…, PRA 59 1829 ;Cleve…PRL 83 648 (1999)]
Secret sharing

\((n,k)\) threshold scheme
- \(n\) shares
- need \(k\) pieces to reveal secret

Classical (2,2) threshold scheme:
- two secret numbers \(m, c\)
- encode as linear equation
  \[ y = m x + c \]

Quantum (2,2) threshold scheme

\[ \alpha |0\rangle + \beta |1\rangle \quad \mapsto \quad \alpha (|00\rangle + |11\rangle) + \beta (|01\rangle + |10\rangle) \]

\(k = 2, n = 2\)

Shamir, ACM 22, 612 (1979)

Cleve, Gottesman & Lo, PRL 83, 648 (1999)
Secret sharing

\((n,k)\) threshold scheme
- \(n\) shares
- need \(k\) pieces to reveal secret

Classical \((2,2)\) threshold scheme:
- two secret numbers \(m, c\)
- encode as linear equation
  \[ y = m x + c \]

Quantum \((2,2)\) threshold scheme

\[
\alpha |0\rangle + \beta |1\rangle \quad \mapsto \quad \alpha (|00\rangle + |11\rangle) + \beta (|01\rangle + |10\rangle)
\]

Cleve, Gottesman & Lo, PRL 83, 648 (1999)

Shamir, ACM 22, 612 (1979)
Secure survey

Estimate (or gift) $Q_1$ of each person is:
- private to each person
- nonbinding (receipt not nec.)

Net amount is known publicly

Distributed ballot state

$$|B_0\rangle = \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} |N-n\rangle_T |n\rangle_V$$

**Tallyman voting “booth”**

**$N$ “particles”**

$$\delta = \frac{2\pi}{N+1}$$
Secure survey

Estimate (or gift) \( Q_1 \) of each person is:
- private to each person
- nonbinding (receipt not nec.)

Net amount is known publicly

**Distributed ballot state**

\[
|B_0\rangle = \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} |N-n\rangle_T |n\rangle_V
\]

1\(^{st}\) person applies **local phase shift** \( \phi \)
for estimate \( Q_1 \) at voting booth

\[
\hat{N}|n\rangle_V = n|n\rangle_V
\]

\[
e^{i\phi \hat{N}}|n\rangle_V = e^{i\phi n}|n\rangle_V \quad \text{for } \phi = Q_1 \delta
\]

\[
\delta = \frac{2\pi}{N+1}
\]
Effect on ballot state:

\[ |B_1\rangle = e^{i(Q_1 \delta) \hat{N}} |B_0\rangle \]

\[ = \frac{1}{\sqrt{N + 1}} \sum_{n=0}^{N} e^{i(Q_1 \delta) n} |N - n\rangle_T |n\rangle_V \]

Partial traces:

\[ \hat{\rho}_T = \text{Tr}_V \left( |B_1\rangle \langle B_1| \right) \]
\[ = \frac{1}{N + 1} \sum_{n=0}^{N} |N - n\rangle \langle N - n| \]

\[ \hat{\rho}_V = \text{Tr}_T \left( |B_1\rangle \langle B_1| \right) \]
\[ = \frac{1}{N + 1} \sum_{n=0}^{N} |n\rangle \langle n| \]

Secrecy: phase value \( \phi \) is not available locally
.....after the $k^{th}$ person:

$$|B_k\rangle = e^{i(M\delta) \hat{N}} |B_0\rangle$$

$$= \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} e^{i(M\delta)n} |N-n\rangle_T |n\rangle_V$$

where $M = \sum_i Q_i$ is net amount

Global phase-state basis

$$|\theta_m\rangle = \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} e^{i(m\delta)n} |N-n\rangle_T |n\rangle_V$$

$$\langle \theta_m | \theta_n \rangle = \delta_{m,n}$$

$$|B_k\rangle \in \{ |\theta_m\rangle : m = 0,1, \ldots N \}$$

Global measurement yields $\theta^M_N$ and thus net amount $M$
Local attack – colluding to learn amounts offered:

Rewrite ballot state as:

\[ \sum_{n=0}^{N} \left| N - n \rightangle_{T} \left| n \rightangle_{V} = \int \left| -\theta \rightangle_{T} \left| \theta \rightangle_{V} \frac{d\theta}{2\pi} \]

\[ \sum_{n} e^{-in\theta} \left| N - n \rightangle_{T} \sum_{m} e^{im\theta} \left| m \rightangle_{V} \]

Imagine:
- **A** measures the phase angle \( \textit{locally} \) and finds \( \left| \theta \rightangle_{V} \)
  - value of \( \theta \) is random
- Subsequent amounts tendered accumulate \( \textit{locally} \):
  \[ \left| \theta \rightangle_{V} \rightarrow \left| \theta + M\delta \rightangle_{V} \]
- **C** then measures the phase angle

Collusion by **A** and **C** reveals net amount \( M \).

Detection: Tallyman detects attack by measuring total particle number (with prob. \( \sim 1 - 1/N \))
Defence - *multiparty ballot state*:

\[
|B_0\rangle = \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} |K(N-n)\rangle_T |n\rangle_V |n\rangle_V \cdots |n\rangle_V
\]

K booths: one for each person

\[
|B_k\rangle = \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} e^{i(M\delta)n} |K(N-n)\rangle_T |n\rangle_V |n\rangle_V \cdots |n\rangle_V
\]

Global Measurement in the \( |\theta_M\rangle \) basis yields \( \theta_M \) and thus net amount \( M \)
Secure voting

Vote of each person is:
- private, receipt-free
- limited to 1 vote
Tally of votes is known publicly

Use multiparty ballot state:

\[
| B_0 \rangle = \frac{1}{\sqrt{N + 1}} \sum_{n=0}^{N} |K(N-n)\rangle_T |n\rangle_V |n\rangle_V \cdots |n\rangle_V
\]

Vote: 
- ☒ “No” = zero phase shift
- ☒ “Yes” = phase shift of \( \delta \)

Problem: not restricted to 1 vote/person
Solution: use

- restricted voting system
- extra (trusted) electoral agent
Restricted voting system

Voter prepares qutrit pairs (basis $| -1 \rangle, | 0 \rangle, | 1 \rangle$)

$|"\text{No}"\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle |1\rangle + |-1\rangle |0\rangle \right)$

$|"\text{Yes}"\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle |1\rangle + |1\rangle |0\rangle \right)$

Extra (trusted) electoral agent

one qutrit is given to Tallyman,
other qutrit is given to a local Electoral Agent

Vote is recorded in ballot state using the local operation

$$\left| B_0 \right|\"X\"\rangle = \frac{1}{\sqrt{N + 1}} \sum_{n=0}^{N} \left| N - n \right>_T \left| n \right>_E \left| \"X\" \right\rangle$$
**Attack** – colluding by Tallyman and Electoral Agent to measure state of qutrit pairs

**Defence** – increase number of Electoral Agents

Example: triplet of qutrits

\[
\left| "\text{No}" \right> = \frac{1}{\sqrt{3}} \left( \left| -1 \right> \left| 0 \right> \left| 0 \right> + \left| 0 \right> \left| -1 \right> \left| 0 \right> + \left| 0 \right> \left| 0 \right> \left| -1 \right> \right)
\]

\[
\left| "\text{Yes}" \right> = \frac{1}{\sqrt{3}} \left( \left| 1 \right> \left| 0 \right> \left| 0 \right> + \left| 0 \right> \left| 1 \right> \left| 0 \right> + \left| 0 \right> \left| 0 \right> \left| 1 \right> \right)
\]

- **Tallyman**
- **2 Agents**

\[
\left| B_0 \right| "\text{X}" \right> = \frac{1}{\sqrt{N + 1}} \sum_{n=0}^{N} \left| 2(N - n) \right>_T \left| n \right>_E \left| n \right>_E \left| "\text{X}" \right>
\]

- **Tallyman**
- **2 Agents**

**Reduces** risk of collusion (all parties need to be involved)

**Reduces** information available to each Agent
Comparison

- **Classical scheme**
  
  Chaum’s secret ballot protocol unconditionally secure
  
  - uses blind signature and sender untraceability
  
  - share *one-time pads* between all pairs of voters

  **computational complexity:**
  
  \[ \text{distribute 1-time pads} = \frac{N(N-1)}{2} \]

- **Quantum scheme**

  computational complexity:
  
  distribute & collect ballot state to \( N \) voters

  \[ = 2N \]

  **order \( N \) speedup**

  **adv. is scalability!**
Summary

advocate small scale processing

secure survey
• multiparty ballot state
• each offer is anonymous

secure voting
• 1 vote per voter
• extra Electoral Agents
• receipt-free