The Singapore Protocol

Highly efficient quantum key distribution with minimal state tomography

BG Englert

phyebg@nus.edu.sg

National University of Singapore
Exchange Programmes @ NUS

NUS – CISEE Student Exchange Programme Awards
20 awards each academic year for students in the Commonwealth of Independent States (CIS) and Eastern Europe (EE: . . . , Poland, . . . )

EE Research Scientist Exchange Programme
Project-oriented exchange programme for full-time academic or research staff (mutual visits, 3 years)

More info at http://www.nus.edu.sg/iro
For enquiries contact Ms HAMIDAH Salleh <irohms@nus.edu.sg>
Quantumlah @

http://www.quantumlah.org

Postdoc position available January 2006
(pending approval of funding)
Collaborators and sponsors

D Kaszlikowski
J Řeháček
HK Ng & J Anders
KM Tin & CG Goh
WK Chua
SY Looi

Research supported by A*Star, DSTA, NUS, EU, Daimler Benz Foundation
Qubit tomography

Qubit state \( \rho = \frac{1}{2} (1 + \langle \vec{\sigma} \rangle \cdot \vec{\sigma}) \)

with Pauli vector operator \( \vec{\sigma} \)

Qubit tomography determines the 3 numbers that specify the Pauli vector \( \langle \vec{\sigma} \rangle = \text{tr} \{ \rho \vec{\sigma} \} \) from experimental probabilities, estimated from measured relative frequencies.
6-state POVM

\[ 1 = \frac{1 + \sigma_x}{6} + \frac{1 - \sigma_x}{6} + \frac{1 + \sigma_y}{6} + \frac{1 - \sigma_y}{6} + \frac{1 + \sigma_z}{6} + \frac{1 - \sigma_z}{6} \]

Redundant tomography: 6 probabilities determine the 3 parameters
4-state POVM

\[ 1 = \sum_{j=1}^{4} \frac{1 + \vec{t}_j \cdot \vec{\sigma}}{4} \]

**Minimal tomography:**

4 probabilities determine the 3 parameters
4-state POVM

\[
1 = \sum_{j=1}^{4} \frac{1 + \overrightarrow{t}_j \cdot \overrightarrow{\sigma}}{4}
\]

Minimal tomography:
4 probabilities determine the 3 parameters
4-state POVM

\[ 1 = \sum_{j=1}^{4} \frac{1 + t_j \cdot \vec{\sigma}}{4} \]

Minimal tomography:
4 probabilities determine the 3 parameters
4-state POVM

\[ 1 = \sum_{j=1}^{4} \frac{1 + \vec{t}_j \cdot \vec{\sigma}}{4} \]

**Minimal tomography:**
4 probabilities determine the 3 parameters
4-state POVM

\[ 1 = \sum_{j=1}^{4} \frac{1 + \vec{t}_j \cdot \vec{\sigma}}{4} \]

Minimal tomography:
4 probabilities determine the 3 parameters
4-state POVM

1 = \sum_{j=1}^{4} \frac{1 + \vec{t}_j \cdot \vec{\sigma}}{4}

Minimal tomography:
4 probabilities determine the 3 parameters
6-state Quantum Key Distribution

A qubit pair source emits singlets. Alice and Bob perform measurements on their respective qubits. The table below shows the probabilities of each measurement outcome. The mutual information is $\frac{1}{3}$ bits.
MQT protocol

MQT ≡ Minimal Qubit Tomography

But we don’t have efficient error correcting codes for such a channel — right now, that is
### 6-state protocol: Basis matching

<table>
<thead>
<tr>
<th></th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$\sigma_x$</td>
</tr>
<tr>
<td></td>
<td>+</td>
</tr>
<tr>
<td>$\sigma_x$</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
<tr>
<td>$\sigma_y$</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
<tr>
<td>$\sigma_z$</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
</tbody>
</table>

**total probability** $\frac{6}{18} + \frac{24}{36} = 1$
6-state protocol: Basis matching

<table>
<thead>
<tr>
<th></th>
<th>(\sigma_x)</th>
<th>(\sigma_y)</th>
<th>(\sigma_z)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(+)</td>
<td>0</td>
<td>1/18</td>
<td>+</td>
</tr>
<tr>
<td>(-)</td>
<td>1/18</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

\(\sigma_x\)

\(\sigma_y\)

\(\sigma_z\)

left with \(6/18 = 1/3\)
MQT protocol: Pairing

<table>
<thead>
<tr>
<th>Alice</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td>1/12</td>
<td>1/12</td>
<td>1/12</td>
</tr>
<tr>
<td>B</td>
<td>1/12</td>
<td>0</td>
<td>1/12</td>
<td>1/12</td>
</tr>
<tr>
<td>C</td>
<td>1/12</td>
<td>1/12</td>
<td>0</td>
<td>1/12</td>
</tr>
<tr>
<td>D</td>
<td>1/12</td>
<td>1/12</td>
<td>1/12</td>
<td>0</td>
</tr>
</tbody>
</table>

Bob

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1/12</td>
<td>1/12</td>
<td>1/12</td>
</tr>
<tr>
<td>1/12</td>
<td>0</td>
<td>1/12</td>
<td>1/12</td>
</tr>
<tr>
<td>1/12</td>
<td>1/12</td>
<td>0</td>
<td>1/12</td>
</tr>
<tr>
<td>1/12</td>
<td>1/12</td>
<td>1/12</td>
<td>0</td>
</tr>
</tbody>
</table>

Total probability

\[
\frac{4}{12} + \frac{8}{12} = 1
\]
### MQT protocol: Pairing

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td>0</td>
<td>1/12</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>1/12</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>0</td>
<td>1/12</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D</strong></td>
<td>1/12</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Left with only

\[
4/12 = 1/3
\]
MQT protocol: Pairing

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td></td>
<td>1/12</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>0</td>
<td>1/12</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>1/12</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>1/12</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Simple, yes, but not efficient:

Lost $\log_2 \frac{4}{3} - \frac{1}{3} = 0.415 - 0.333 = 0.082$ on the way

Can we do better?
MQT protocol: Key generation

[1]

Alice: A C D A B B C A D B …
Bob:  B A B C D C A B C D …

Alice chooses one letter at random: A
MQT protocol: Key generation

[2]  
A C D A B B C A D B ...  
Bob: B A B C D C A B C D ...  

She chooses two positions at random where this letter occurs and communicates the positions to Bob: 1 and 4
MQT protocol: Key generation

[3a]

Alice: A C D A B B C A D B ...
Bob:  B A B C D C A B C D ...

Bit conversion case

Bob has two different letters: B and C

He forms two 2-letter groups and decides at random which has value 0 and which has value 1:

\[
\begin{align*}
\text{AD} & = 0 \\
\text{BC} & = 1
\end{align*}
\]
MQT protocol: Key generation

[3b]

Alice: A C D A B B C A D B ...
Bob: B A B C D C A B C D ...

Bob communicates the groups to Alice.

\[
\begin{align*}
\text{AD} &= 0 \\
\text{BC} &= 1
\end{align*}
\]

Both know the group with her letter and add its value to the key sequence $\rightarrow 0$
MQT protocol: Key generation

[1’]

Alice: A C D A B B C A D B ...
Bob: B A B C D C A B C D ...

Alice chooses another letter at random: C
MQT protocol: Key generation

Alice: A C D A B B C A D B ... 
Bob: B A B C D C A B C D ... 

She chooses two positions at random where this letter occurs and communicates the positions to Bob: 2 and 7
MQT protocol: Key generation

[3c]

Alice: A C D A B B C A D B ...  
Bob: B A B C D C A B C D ...  

Recycle case
Bob has the same letter twice: A

He announces that this is the case – not telling, of course, which letter he got; both record their respective letters for later use:

Alice: ... C ...  
Bob: ... A ...
MQT protocol: Key generation

[Iteration step]

The sequences of recycled letters have the same statistical properties as the primary sequences. Alice and Bob repeat the whole story for the recycled sequences, thereby getting more key bits and new sequences of recycled letters. Then they do it again, and again, and again, . . .
MQT protocol: Yield

Alice \textit{AA} Bob \textit{BC, BD, CD, CB, DB, DC} \quad 6 \text{ of } 9

\textit{BB, CC, DD} \quad 3 \text{ of } 9

\( \frac{2}{3} \) probability for bit conversion, \( \frac{1}{3} \) for recycling

How many key bits for \( N \) letters?

\[ \frac{1}{2} \cdot \frac{2}{3} N + \frac{1}{4} \cdot \frac{2}{9} N + \frac{1}{8} \cdot \frac{2}{27} N + \cdots = \frac{2}{5} N \lesssim 0.415 N \]

- 33.3\% after 1 round
- 38.9\% after 2 rounds
- 39.8\% after 3 rounds
The tomographic element

Ideal source: \( \rho_{AB} = |s\rangle\langle s| \), projector on singlet

Real source: 
\[
\rho_{AB} = |s\rangle(1 - \epsilon)\langle s| + \frac{\epsilon}{4}
\]
admixture of unbiased noise

**Tomography**: Alice and Bob sacrifice some data to check whether they really get from the source what they should get

Other sources are not accepted
Complete tomography

1 qubit: $2^2 - 1 = 3$ parameters
$3 + 1 = 4$ probabilities

2 qubits: $2^4 - 1 = 15$ parameters
$15 + 1 = 4^2$ probabilities

3 qubits: $2^6 - 1 = 63$ parameters
$63 + 1 = 4^3$ probabilities

and so forth, . . . Alice and Bob have enough data – with no costly redundancy – for a complete characterization of the source output
Complete tomography

1 qubit: \(2^2 - 1 = 3\) parameters
\[3 + 1 = 4\] probabilities

2 qubits: \(2^4 - 1 = 15\) parameters
\[15 + 1 = 4^2\] probabilities

3 qubits: \(2^6 - 1 = 63\) parameters
\[63 + 1 = 4^3\] probabilities

and so forth, . . . Alice and Bob have enough data — with no costly redundancy — for a complete characterization of the source output
Complete tomography

1 qubit: \(2^2 - 1 = 3\) parameters
3 + 1 = 4 probabilities

2 qubits: \(2^4 - 1 = 15\) parameters
15 + 1 = 4^2 probabilities

3 qubits: \(2^6 - 1 = 63\) parameters
63 + 1 = 4^3 probabilities

and so forth, ... Alice and Bob have enough data – with no costly redundancy – for a complete characterization of the source output
Noise \equiv Eavesdropping

Eve prepares source state \( |S\rangle \), an entangled state of Alice&Bob’s qubits and the ancilla, such that

\[
\rho_{AB} = |S\rangle(1 - \epsilon)\langle S| + \frac{\epsilon}{4} = \text{tr}_{\text{ancilla}}\left\{ |S\rangle\langle S| \right\}
\]

**Unique choice:** \( |S\rangle = |s_{12}s_{34}\rangle\sqrt{1 - \epsilon} + |s_{13}s_{24}\rangle i\sqrt{\epsilon} \)

qubit 1: Alice  
qubit 2: Bob  
qubits 3,4: Eve’s ancilla
Effective quantum channels

Alice $\rightarrow$ Bob: noise level $\epsilon$
Alice $\rightarrow$ Eve: noise level $\eta$

$$\sqrt{\eta} = \sqrt{1 - \frac{3\epsilon}{4}} - \sqrt{\frac{3\epsilon}{4}}$$

- $\epsilon = 0$: $\eta = 1$
- $\epsilon = 2/3$: $\eta = 0$
Effective quantum channels

\[ \sqrt{\eta} = \sqrt{1 - \frac{3\epsilon}{4}} - \sqrt{\frac{3\epsilon}{4}} \]

- \( \epsilon = 0 \): \( \eta = 1 \)
- \( \epsilon = 2/3 \): \( \eta = 0 \)

Alice \rightarrow Bob: noise level \( \epsilon \)
Alice \rightarrow Eve: noise level \( \eta \)
Csiszár–Körner threshold

\[ \sqrt{\eta} = \sqrt{1 - \frac{3\epsilon}{4}} - \sqrt{\frac{3\epsilon}{4}} \]

or

\[ (1 - \frac{3}{2}\epsilon)^2 + (1 - \eta)^2 = 1 \]

Threshold for secure key generation by one-way communication is at cross-over point where

\[ \eta = \epsilon = \frac{1}{\frac{5}{2} + \sqrt{3}} = 0.2363 \]
The CK threshold for the 6-state protocol and the MQT protocol are the same.

Below the threshold the MQT protocol has the greater yield of “key bits per qubit sent”
Noise thresholds for key generation

1st round: 2 ancillas for each key bit
2nd round: 4 ancillas for each key bit
3rd round: 8 ancillas for each key bit

So, Eve’s job gets easier in every round

But, $\frac{3\epsilon}{4 - \epsilon} \rightarrow \left( \frac{3\epsilon}{4 - \epsilon} \right)^2$ in each recycling step, so that Alice and Bob have letter sequences of ever better quality

Who wins?
**Noise thresholds for key generation**

Incoherent attacks: Eve measures each ancilla separately

Coherent attacks: She measures them jointly

**Presently known threshold values of $\epsilon$**

<table>
<thead>
<tr>
<th>number of rounds</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>$\infty$</th>
</tr>
</thead>
<tbody>
<tr>
<td>incoh.</td>
<td>0.4087</td>
<td>0.4402</td>
<td>0.4739</td>
<td>0.5048</td>
<td>0.5839</td>
</tr>
<tr>
<td>coh.</td>
<td>0.2569</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

All of them are above the CK threshold at 0.2363
Conclusion

The Singapore protocol for quantum key distribution with minimal state tomography is the bestest of its kind.
## Collaborators and publications

<table>
<thead>
<tr>
<th>Collaborator</th>
<th>Publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>D Kaszlikowski</td>
<td>[1,3,4] quant-ph/0405084 min. qubit tomography</td>
</tr>
<tr>
<td></td>
<td>[2,4,5] physics/0409015 4-output ellipsometer</td>
</tr>
<tr>
<td></td>
<td>quant-ph/0504093 codes for key generation</td>
</tr>
<tr>
<td>J Řeháček</td>
<td>[1,3,4]</td>
</tr>
<tr>
<td>WK Chua</td>
<td>[4]</td>
</tr>
<tr>
<td>HK Ng &amp; J Anders</td>
<td>[2,4,5]</td>
</tr>
<tr>
<td>KM Tin &amp; CG Goh</td>
<td>[2]</td>
</tr>
<tr>
<td>SY Looi</td>
<td>[5]</td>
</tr>
</tbody>
</table>