Specious Adversaries and Quantum Private Information Retrieval
QCrypt 2013

Ämin Baumeler\textsuperscript{1} and Anne Broadbent\textsuperscript{2}

\textsuperscript{1}Faculty of Informatics
Università della Svizzera italiana, Lugano, Switzerland

\textsuperscript{2}Department of Combinatorics and Optimization &
Institute for Quantum Computing
University of Waterloo, Waterloo, Canada

August 8, 2013
Outline

• Private Information Retrieval
• Adversarial models
• Proof sketch
Results

- No-go: QPIR secure against specious/purified adversaries
- Quantum/classical adversary model comparison nontrivial
Private Information Retrieval

Server

\[ x_1, \ldots, x_n \]

PIR

Client

\[ i \]

\[ x_i \]
Private Information Retrieval

\[ x_1, \ldots, x_n \rightarrow PIR \rightarrow x_i \]

Server

Client

\( i \)

Oblivious Transfer: Inf. th. security against server and client
Private Information Retrieval

Oblivious Transfer: Inf. th. security against server and client

PIR: Inf. th. security against server
Private Information Retrieval

Server

$X_1, \ldots, X_n$

PIR

$\leftarrow i$

$\rightarrow X_i$

Client

Oblivious Transfer: Inf. th. security against server and client

PIR: Inf. th. security against server

Private Query: Relaxed security requirements
Protocol: ideal world and real world

$\pi_s \pi_c R x_1, \ldots, x_n \rightarrow PIR \leftarrow i \rightarrow x_i$

Expression: PIR

\[1\] Maurer, Renner, *ICS 2011*, 2011.
Protocol: ideal world and real world

Expression: PIR

Expression: $\pi^s \pi^c R$

---

$^{1}$Maurer, Renner, ICS 2011, 2011.
Protocol: ideal world and real world

Expression: PIR

Expression: $\pi^s \pi^c R$

Trivial protocol: Server sends database to client

$^1$Maurer, Renner, ICS 2011, 2011.
Communication Complexity

Classical lower bond: $\Omega(n)$ honest-but-curious
Quantum lower bound: $\Omega(n)$ general

---

## Communication Complexity

<table>
<thead>
<tr>
<th>Type</th>
<th>Lower Bound</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classical lower bond</td>
<td>$\Omega(n)$</td>
<td>honest-but-curious</td>
</tr>
<tr>
<td>Quantum lower bound</td>
<td>$\Omega(n)$</td>
<td>general</td>
</tr>
<tr>
<td>Le Gall’s protocol</td>
<td>$O(\sqrt{n})$</td>
<td>“quantum” honest-but-curious</td>
</tr>
</tbody>
</table>

---

Communication Complexity

Classical lower bond: \( 2 \Omega(n) \) honest-but-curious
Quantum lower bound: \( 3 \Omega(n) \) general
Le Gall’s protocol: \( O(\sqrt{n}) \) “quantum” honest-but-curious
this work: \( \Omega(n) \) specious/purified adversaries

---

\(^4\) Le Gall, *Theory of Computing, 8*(1), 2012.
Honest-but-curious adversary

Honest-but-curious
  honest: follow protocol
  curious: copy transcript
Honest-but-curious adversary

Honest-but-curious
  honest: follow protocol
  curious: copy transcript

“Quantum” honest-but-curious
  honest: follow protocol, to the extend of tracing-out
  curious: no-cloning theorem
Honest-but-curious adversary

Honest-but-curious
  honest: follow protocol
  curious: copy transcript

“Quantum” honest-but-curious
  honest: follow protocol, to the extend of tracing-out
  curious: no-cloning theorem

Audit point-of-view: pass audit at any step in the protocol
Specious\textsuperscript{5} adversary

Adversary can undo malicious actions at every step in the protocol.

\textsuperscript{5}Dupuis, Nielsen, and Salvail, \textit{CRYPTO10}, 2010.
Specious\textsuperscript{5} adversary

Adversary can undo malicious actions at every step in the protocol.

\textbf{specious} | 'spi\-ʃəs |

adjective
superficially plausible, but actually wrong: \textit{a specious argument}.
• misleading in appearance, especially misleadingly attractive: \textit{the music trade gives Golden Oldies a specious appearance of novelty.}

\textsuperscript{5}Dupuis, Nielsen, and Salvail, \textit{CRYPTO10}, 2010.
Specious adversary

Adversary can undo malicious actions at every step in the protocol.

**specious** | ˈspiːʃəs |
---|---
adjective
superficially plausible, but actually wrong: *a specious argument.*
- misleading in appearance, especially misleadingly attractive: *the music trade gives Golden Oldies a specious appearance of novelty.*

γ-specious adversary $\hat{\pi}^s$:

$$\forall k \exists L_k \quad \Delta(\pi^s_k \pi^c_k R, L_k \hat{\pi}^s_k \pi^c_k R) \leq \gamma$$

---

Specious\textsuperscript{5} adversary

Adversary can undo malicious actions at every step in the protocol.

\textbf{Specious}\textsuperscript{5} \textbf{adversary}

\begin{itemize}
  \item Adversary can undo malicious actions at every step in the protocol.
  \item Example: purified adversary $\bar{\pi}^s$
\end{itemize}

\textbf{specious} | 'spiːʃəs |
\textit{adjective}
superficially plausible, but actually wrong: \textit{a specious argument}.
\textbullet\ misdeading in appearance, especially misleadingly attractive: \textit{the music trade gives Golden Oldies a specious appearance of novelty}.

$\gamma$-specious adversary $\hat{\pi}^s$:
\[ \forall k \exists L_k \quad \Delta(\pi_k^s \pi_k^c R, L_k \hat{\pi}_k^s \pi_k^c R) \leq \gamma \]

\textbf{Example}: purified adversary $\bar{\pi}^s$

\textsuperscript{5}Dupuis, Nielsen, and Salvail, \textit{CRYPTO10}, 2010.
Requirements

Correctness: \( \Delta(\pi^s \pi^c R, \text{PIR}) \leq \varepsilon \)

Security (general): \( \forall \hat{\pi}^s \exists \sigma^s \Delta(\hat{\pi}^s \pi^c R, \sigma^s \text{PIR}) \leq \delta \)

Security (specious): \( \forall \hat{\pi}^s \in S \forall k \exists \sigma^s \Delta(\hat{\pi}^s_k \pi^c_k R, \sigma^s \text{PIR}) \leq \delta \)
Result (simplified)

Theorem:
Let $\pi^s \pi^c R$ be an $n$-bit QPIR protocol secure against specious servers. Then $\pi^s \pi^c R$ has communication complexity of at least $n$.

Proof sketch / reduction to RAC:\(^6\)

$|\psi_{x,i}\rangle$: global state at the end of pure protocol on input $x$ and $i$

1. Server runs purified protocol and simulates purified client with input 1
2. Server sends client’s part of $|\psi_{x,1}\rangle$ to client
3. Client runs local unitary: $\left(\mathds{1} \otimes U^{1 \rightarrow i}\right) |\psi_{x,1}\rangle = |\psi_{x,i}\rangle$

Single message transmitted is a random access code.\(^6\)

Conclusion

• QPIR secure against specious adversaries has communication complexity $\Omega(n)$

• Comparison between classical and quantum adversaries non-trivial

---

Conclusion

• QPIR secure against specious adversaries has communication complexity $\Omega(n)$

• Comparison between classical and quantum adversaries non-trivial

   I thought of another moral, more down to earth and concrete, . . . . The differences can be small, but they can lead to radically different consequences, like a railroad’s switch points; the chemist’s trade consists in good part in being aware of these differences, knowing them close up, and foreseeing their effects. And not only the chemist’s trade.\textsuperscript{7}

\textsuperscript{7}Primo Levi, The periodic table, 1984.