Specious Adversaries and Quantum Private Information Retrieval

QCrypt 2013

Ämin Baumeler[1] and Anne Broadbent[2]

[1]Faculty of Informatics
Università della Svizzera italiana, Lugano, Switzerland

[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

Private Information Retrieval

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

Oblivious Transfer:	Inf. th. security against server and client
PIR:	Inf. th. security against server
Private Query:	Relaxed security requirements

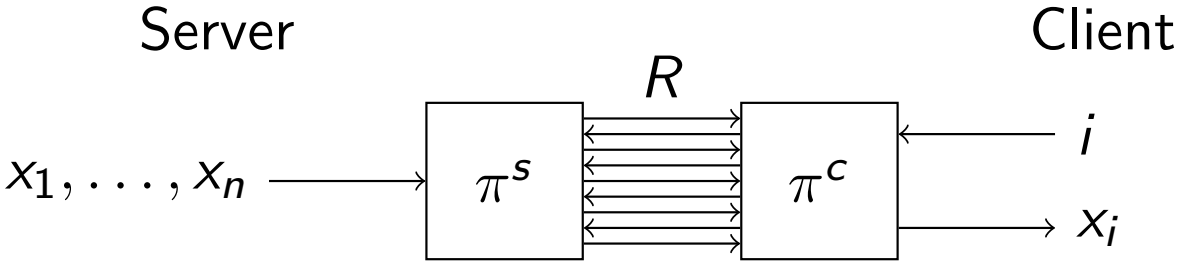
Protocol: ideal world and real world

Expression: PIR

[1] Maurer, Renner, *ICS 2011*, 2011.

Protocol: ideal world and real world

Expression: PIR

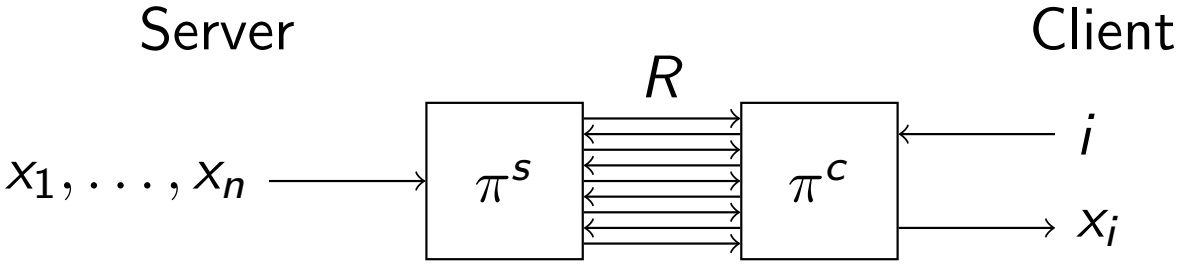


Expression:[1] $\pi^s \pi^c R$

[1] Maurer, Renner, *ICS 2011*, 2011.

Protocol: ideal world and real world

Expression: PIR



Expression:[1] $\pi^s \pi^c R$

Trivial protocol: Server sends database to client

[1] Maurer, Renner, *ICS 2011*, 2011.

Communication Complexity

Classical lower bond:[2]	$\Omega(n)$	honest-but-curious
Quantum lower bound:[3]	$\Omega(n)$	general

[2] Chor, Kushilevitz, Goldreich, Sudan, *Journal of the ACM, 45(6)*, 1998.
[3] Nayak, *FOCS'99*, 1999.
[4] Le Gall, *Theory of Computing, 8(1)*, 2012.

Communication Complexity

Classical lower bond:[2]	$\Omega(n)$	honest-but-curious
Quantum lower bound:[3]	$\Omega(n)$	general
Le Gall's protocol:[4]	$\mathcal{O}(\sqrt{n})$	"quantum" honest-but-curious

[2] Chor, Kushilevitz, Goldreich, Sudan, *Journal of the ACM, 45(6)*, 1998.
[3] Nayak, *FOCS'99*, 1999.
[4] Le Gall, *Theory of Computing, 8(1)*, 2012.

Communication Complexity

Classical lower bond:[2]	$\Omega(n)$	honest-but-curious
Quantum lower bound:[3]	$\Omega(n)$	general
Le Gall's protocol:[4]	$\mathcal{O}(\sqrt{n})$	"quantum" honest-but-curious
this work:	$\Omega(n)$	specious/purified adversaries

[2] Chor, Kushilevitz, Goldreich, Sudan, *Journal of the ACM, 45(6)*, 1998.
[3] Nayak, *FOCS'99*, 1999.
[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[5] adversary

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

[5] Dupuis, Nielsen, and Salvail, *CRYPTO10,*, 2010.

Specious[5] 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*.

[5] Dupuis, Nielsen, and Salvail, *CRYPTO10*,, 2010.

Specious[5] 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 $\hat{\pi}^s$:

$$\forall k \exists \mathcal{L}_k \quad \Delta(\pi_k^s \pi_k^c R, \mathcal{L}_k \hat{\pi}_k^s \pi_k^c R) \leq \gamma$$

[5] Dupuis, Nielsen, and Salvail, *CRYPTO10*,, 2010.

Specious[5] 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 $\hat{\pi}^s$:

$$\forall k \exists \mathcal{L}_k \quad \Delta(\pi_k^s \pi_k^c R, \mathcal{L}_k \hat{\pi}_k^s \pi_k^c R) \leq \gamma$$

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

[5] Dupuis, Nielsen, and Salvail, *CRYPTO10*,, 2010.

Requirements

Correctness:	$\Delta(\pi^s \pi^c R, \mathsf{PIR}) \leq \varepsilon$
Security (general):	$\forall \hat{\pi}^s \exists \sigma^s \quad \Delta(\hat{\pi}^s \pi^c R, \sigma^s \mathsf{PIR}) \leq \delta$
Security (specious):	$\forall \hat{\pi}^s \in \mathcal{S}\, \forall k\, \exists \sigma^s \quad \Delta(\hat{\pi}^s_k \pi^c_k R, \sigma^s \mathsf{PIR}) \leq \delta$

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: $(\mathbb{1} \otimes U^{1 \to i}) |\psi_{x,1}\rangle = |\psi_{x,i}\rangle$

Single message transmitted is a random access code.[6]

[6] Nayak, *FOCS'99*, 1999.

Conclusion

- QPIR secure against specious adversaries has communication complexity $\Omega(n)$
- Comparison between classical and quantum adversaries non-trivial

[7] Primo Levi, The periodic table, 1984.

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.*[7]

[7] Primo Levi, The periodic table, 1984.