Secure Identification Using Quantum Communication

Serge Fehr, Christian Schaffner (CWI Amsterdam, NL)
Ivan Damgård, Louis Salvail (University of Århus, DK)

Workshop: Practical Applications of New Research in Cryptography
Sabanci University, Turkey
Friday, April 18, 2008
Quantum Mechanics

\[ + \text{ basis} \]
\[ \begin{array}{c|c|c}
|0\rangle & |1\rangle \\
\hline
|0\rangle & + & \times \\
\hline
\end{array} \]

Measurements:
\[ + \text{ basis} \]
\[ \begin{array}{c|c|c}
|0\rangle & |1\rangle \\
\hline
\hline
|0\rangle & 0/1 & 0 \text{ with prob.} \\
\hline
\end{array} \]

Non-Classical Properties

\[ + \text{ basis} \]
\[ \begin{array}{c|c|c}
|0\rangle & |1\rangle \\
\hline
|0\rangle & + & \times \\
\hline
\end{array} \]

Measurements:
\[ \begin{array}{c|c|c|c}
|0\rangle & |1\rangle \\
\hline
\hline
0/1 & 0 & 0 \text{ with prob.} \\
\hline
\end{array} \]

Outline

- Quantum Mechanics
  - Quantum Key Distribution
  - Two-Party Setting
  - Secure Identification
  - Conclusion

Quantum Key Distribution (QKD)

Alice → Bob

Eve

- most studied in quantum cryptography
- 3-party scenario
- unconditional security against unrestricted eavesdroppers

QKD: Intuition

- quantum states are unknown to Eve, cannot copy them
- honest players can check whether Eve interfered
- then amplify their advantage

Commercial QKD-Products

- MagicQ (USA)
- idQuantique (Switzerland)
- SmartQuantum (France/USA)

only quantum communication, no quantum storage nor quantum computation required
Outline
- Quantum Mechanics
- Quantum Key Distribution
  - Two-Party Setting
  - Secure Identification
  - Conclusion

Two-Party Setting?
- Bit Commitment
- Oblivious Transfer
- Equality Test

Imp possibility Results
- Bit Commitment
- Oblivious Transfer
- Equality Test

Possible Assumptions
- bounded time $\Rightarrow$ classical cryptography, assumption-based
- noisy resources
- bounded memory

Classical Bounded-Storage Model
- long random string in the sky which players try to store
- a memory bound applies at a specified moment (string disappears)
- protocol for Oblivious Transfer
- memory size of honest players: $k$
- memory of dishonest players: $< k^2$
- tight bound [DM04]

Bounded-Quantum-Storage Model
- quantum memory bound applies at a specified moment
- besides that, players are unbounded (in time and space)
- honest players do not need quantum memory at all
- honest players: $0 \leq k$
- dishonest players: $< n/4 \leq k^2$
- unconditional security against quantum-memory bounded adversaries
Quantum Memory
(physics group of Eugene Polzik, Copenhagen (DK))
- 70% fidelity, few milliseconds, …
- technically very challenging

A Bit of History

Outline
- Quantum Mechanics
- Quantum Key Distribution
- Two-Party Setting
  - Secure Identification
  - Conclusion

Why Secure Identification?
I’m Alice my PIN is IMAB52 I want $25
Alright Alice, here you go.

Why Secure Identification?
I’m Alice my PIN is IMAB52 I want $25,000,000
Alright Alice, here you go.
Secure Evaluation of the Equality

- PIN-based identification scheme should be a secure evaluation of the equality function.
- A dishonest player can exclude only one possible password.

Quantum Identification Protocol

- Efficient gate $X^\dagger$.
- Two-univ hash fct $f(X) \oplus g(W)$.
- A dishonest player can only learn one $W'$.

Dishonest Alice

- $X = 1 1 0$, $W = 1 0$, $C(W) = + + + +$.
- $f(X) \oplus g(W')$, $w$ all different.
- Secure against unbounded Alice.

Unbounded Dishonest Bob

- $X = 0 1 1 1 0$, $W = 1 0$, $C(W) = + + + +$.
- $f(X) \oplus g(W')$.
- Completely insecure.

Restricted Dishonest Bob

- $X = 0 1 1 0$, $W = 1 0$, $C(W) = + + + +$.
- $f(X) \oplus g(W)$.
- After a lot of work: dishonest Bob can only learn one $W'$.

Properties of the Basic Scheme

- Efficient: $n$ qubits, 3 classical messages, honest players do not require quantum memory.
- Provably secure against:
  - Unbounded dishonest user Alice.
  - Dishonest server Bob with quantum memory < $n/11$.
  - Both have unbounded computing power and classical memory.
- Can be extended to tolerate noise, therefore implementable with current technology.
QUSEP Project:

Alice

Bob

Conclusion

- Intro to Quantum Mechanics
- Quantum Key Distribution
- Two-Party Quantum Cryptography
- PIN-Based Identification secure against quantum-memory bounded Adversaries

1-2 OT

Thanks to you!!

Quantum Cryptography is practical!!
(at least more than you thought)

Thanks to you!

Conclusion

- Quantum Cryptography is practical!!
(at least more than you thought)

Thanks to you!