Quantum Zero-Knowledge

Claude Crépeau

School of Computer Science
McGill University

joint work with
J. van de Graaf and A. Smith
Interactive Proofs
Interactive Proofs and Zero-Knowledge

∀x ∈ L \Pr( [A, B](x) = YES ) \approx 1
Let's try it!

Test Graph

Note: you can redraw a graph by Ctrl-clicking on it.
You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!

Note: you can redraw a graph by Ctrl-clicking on it.
Let's try it!

Note: you can redraw a graph by Ctrl-clicking on it.

Text taken from Cryptography, Theory and practice.
You will accept that the two graphs are isomorphic if the Test Graph was always isomorphic to the chosen graph.

Let's try it!

Note: you can redraw a graph by Ctrl-clicking on it.

Text taken from Cryptography, Theory and practice.
Interactive Proofs and Zero-Knowledge

\[ (G_0, G_1) \in \text{ISO} \]

\[ (G_0 = \pi(G_1)) \]

\[ G := \pi_0(G_0) \]

\[ \forall x \in L \ \Pr( [\text{Verifier}, \text{Oracle}](x) = \text{YES} ) = 1 \]
Interactive Proofs and Zero-Knowledge

$x \in L$

∀x ꔚ L  ∀Ø Pr( [Ø, Ø](x) = YES ) ≈ 0

NO!
Let's try it!

Note: you can redraw a graph by Ctrl-clicking on it.

Text taken from Cryptography, Theory and practice.
Let's try it!

Note: you can redraw a graph by Ctrl-clicking on it.

Text taken from Cryptography, Theory and practice.
Interactive Proofs and Zero-Knowledge

$(G_0, G_1) \not\in \text{ISO}$

$G \neq G_0$ or $G \neq G_1$

$G = \rho(G_c)\ ?$

$\forall x \in L \ \forall \theta \ \Pr( [\theta, G_c](x) = \text{YES} ) \leq \frac{1}{2}$
Interactive Proofs and Zero-Knowledge

$$(G_0, G_1) \notin \text{ISO}$$

$G \neq G_0$ or $G \neq G_1$

REPEAT k TIMES
and say "YES" only if all "YES"

$$\forall x \notin L \forall \rho \Pr([\rho, \text{??}](x) = \text{YES}) \leq \frac{1}{2^k}$$
Complexity and Arthur-Merlin Games
$P$-SPACE

$P$-Hierarchy

$= \bigcup_i \Sigma_i = \bigcup_i \Pi_i$
P-SPACE

IP

IP₄, IP₂, NP, BPP, IP₃, IP₅...

IP-Hierarchy

= Uᵢ IPᵢ
Arthur-Merlin GAMES
(Arthur-Morgane GAMES)

∀x∈L Pr( [A,B](x)=YES ) ≈ 1
Arthur-Merlin GAMES

\[
x \notin L
\]

\[
\begin{align*}
01100010101011010101010 & \\
00010101010111010101010 & \\
01011011010000101010101 & \\
01011011010000101010101 & \\
\end{align*}
\]

\[
\forall x \in L \forall y \Pr( [D,B](x) = \text{YES} ) \approx 0
\]
P-SPACE
AM[P]

...AMA AM NP BPP MA MAM ...

AM-Hierarchy

= \bigcup_i (AM)_i
AM-Hierarchy

\[ U_i (AM)^i \]
Interactive Proofs

\[ x \in L \]

\[ \forall x \in L \Pr( \left[\begin{array}{c} A \\ B \end{array}\right](x) = YES ) \approx 1 \]
P-SPACE
IP = AM[P]

...(AM)^k  IP_{2k}  NP  P

[Goldwasser-Sipser]

© Claude Crépeau 2003-2009
The entire IP hierarchy

IP = P-SPACE
Non-ISO ∈ IP_2 = AM
You will accept that the two graphs are isomorphic if the test graph was always isomorphic to the chosen graph.

Let's try it!

Graph A  Graph B

Test Graph

Note: you can redraw a graph by Ctrl-clicking on it.

Text taken from Cryptography, Theory and practice.
You will accept that the two graphs are isomorphic if the Test Graph is always isomorphic to the chosen graph.

Let's try it!

Note: you can redraw a graph by Ctrl-clicking on it.

Text taken from Cryptography, Theory and practice.
Let's try it!

Test Graph

Note: you can redraw a graph by Ctrl-clicking on it.

Text taken from Cryptography, Theory and Practice.
You will accept that the two graphs are isomorphic if the test graph was always isomorphic to the chosen graph.

Let's try it!

Note: you can redraw a graph by Ctrl-clicking on it.
Interactive Proofs

\((G_0, G_1) \in \text{Non-ISO} \quad (G_0 \neq \pi(G_1))\)

\[ G := \sigma(G_b) \]

\(c = b?\)

\[ \forall x \in L \Pr( [\hat{A}, \hat{B}](x) = \text{YES} ) = 1 \]
Interactive Proofs

\[(G_0, G_1) \notin \text{Non-ISO}\]

\[G \approx G_0 \text{ and } G \approx G_1\]

\[G := \sigma(G_b)\]

\[\forall x \notin L \ \forall \emptyset \ \Pr( [\emptyset, \hat{c}](x) = \text{YES} ) \leq \frac{1}{2}\]

NO!
Interactive Proofs

$$(G_0, G_1) \notin \text{Non-ISO}$$

$\Gamma_i \approx G_0 \text{ and } \Gamma_i \approx G_1$

$\Gamma_1, \Gamma_2, \ldots, \Gamma_k$

$C_1, C_2, \ldots, C_k$

$\Gamma_i := \sigma_i(G_{b_i})$

$c_i = b_i$ ?

REPEAT $k$ TIMES

and say "YES" only if all "YES"

$\forall x \notin L \forall \theta \ Pr( [\theta, \Gamma_i](x) = \text{YES} ) \leq \frac{1}{2^k}$

NO!
Quantum Interactive Proofs
The entire QIP hierarchy

[Watrous et al]
Zero-Knowledge
Zero-Knowledge

\[ x \in L \]

YES!
Zero-Knowledge

$x \in L$

Transferability of a proof.
Zero-Knowledge and Simulator

\[ \forall x \in L \quad \text{view}[\mathcal{A}, \mathcal{O}](x) = \mathcal{O}(x) \]
∀A ∈ C ∀x ∈ L view[\(A, D\)](x) = \(\emptyset(x)\)
Zero-Knowledge and Simulator

\[(G_0, G_1) \in \text{ISO} \quad (G_0 = \pi(G_1))\]

\[G := \pi_0(G_b)\]

\[\text{if } b = c \quad \text{then proceed}\]

\[\text{else restart}\]

\[\forall A, E \exists x \in L \quad \text{view}_{[A, E]}(x) = \varnothing(x)\]
The rewinding paradigm

**REPEAT k TIMES**

\[(G_0, G_1) \in \text{ISO} \]
\[(G_0 = \pi(G_1))\]

\[\rho = \pi_i\]

\[\forall A, B \exists \forall x \in L \text{ view}[A, B](x) = \emptyset(x)\]

**if** \(b_i = c_i\)
**then proceed**
**else rewind to** \(D_i\)

**D_i:** \(b_i\)

\[G_i := \pi_i(G_{b_i})\]
Auxiliary Input Zero-Knowledge

\[ \omega = \text{existing knowledge about } x \in L \]

\[ x \in L \]

\[ \text{YES !} \]
Auxiliary Input Zero-Knowledge

Contextual transferability of a proof.
Auxiliary Input Zero-Knowledge

∀ x ∈ L, ω  view[∀x ∈ L, ω](x) = θ(x, ω)
Auxiliary Input Zero-Knowledge

REPEAT k TIMES

\[ (G_0, G_1) \in \text{ISO} \]
\[ G_0 = \pi(G_1) \]

\[ D_i(\omega): b_i \]
\[ G_i := \pi_i(G_{b_i}) \]

if \( b_i = c_i \)
then proceed
else rewind to \( D_i(\omega) \)

\[ \forall x \in L, \omega \quad \text{view}[A, B(\omega)](x) = \bigotimes(x, \omega) \]

© Claude Crépeau 2003-2009
Quantum Zero-Knowledge
Auxiliary Q-Input Zero-Knowledge

$x \in L$

Leftover Q-input: $\rho'$

YES!
Auxiliary Q-Input Zero-Knowledge

Quantum-Contextual transferability of a proof.
Auxiliary Q-Input Zero-Knowledge

∀ x ∈ L, ρ ∀ view [DA, 0](ρ) (x) = O(x, ρ)
Quantum Zero-Knowledge: Formalizing the Model

messages:

1. $V_1(x)$
2. $P_1(x)$
3. $V_2(x)$
4. $P_2(x)$
5. $V_3(x)$
6. $P_4(x)$

Verifier’s qubits
Message qubits
Prover’s qubits

Output qubit
AUX qubits
Auxiliary Q-Input Zero-Knowledge

∀ ∈ 𝔽 ⊆ 𝕀 holds view\( \text{view}(\rho, \rho(x, i)) = \text{view}(\rho, x, i) \)
**REPEAT k TIMES**

\[(G_0, G_1) \in \text{ISO} \quad (G_0 = \pi(G_1))\]

**Auxiliary Q-Input Zero-Knowledge**

\[D_i(\rho): \quad b_i\]

\[G_i := \pi_i(G_{bi})\]

if \(b_i = c_i\)
then proceed
else rewind to \(D_i(\rho)\)

\[\forall \rho \in \text{poly}(|x|) \quad \text{view}[(A, B(\rho))(x, i)] = S(\rho, x, i)\]
$b_i = |0\rangle + |1\rangle$

$G_i := \pi_i(G_{bi})$

$(G_0, G_1) \in \text{ISO}$

$(G_0 = \pi(G_1))$

REPEAT $k$ TIMES

$c_i = |0\rangle + |1\rangle$

if $b_i = c_i$

without measuring $b_i$ nor $c_i$...

then proceed you may now measure $b_i$ and $c_i$...

else Apply transformation so that $b_i = c_i$ !!!

$\forall D \in \mathbb{D} \\forall \rho \\forall i \in \text{poly}(|x|)$ view $[A, D(\rho)](x, i) = \mathcal{S}(\rho, x, i)$
ISO ∈ Q ⊆ Z ⊆ K

etc
Conclusions
• Auxiliary Q-Input Zero-Knowledge is possible

• Natural ZK languages: Non-ISO & Cie ?
Quantum
Zero-Knowledge

Claude Crépeau

School of Computer Science
McGill University

joint work with
J. van de Graaf and A. Smith
Quantum Zero-Knowledge

Claude Crépeau

School of Computer Science
McGill University

joint work with
J. van de Graaf and A. Smith