Knowledge

APR 1

abhi shelat
EXECUTIONS

\[ \langle A(x), B(y) \rangle \sim \text{random variable.} \]

includes

\[
(x, r_A, z_A, M_A = (m_1, m_2, m_3, \ldots))
\]

\[
(y, r_B, z_B, M_B = (m_1, m_2, m_3, \ldots))
\]

\text{View}_A \langle A(x), B(y) \rangle = \text{part of this run}

\[
(x, r_A, z_A, M_A)
\]

“all strings seen by Alice during the protocol execution”
WHAT PROPERTIES SHOULD AN INTERACTIVE PROOF SYSTEM HAVE?
COMPLETENESS

FOR A LANGUAGE $L$, AND FOR ALL $x \in L$

$$\langle P(x, w), V(x) \rangle = 1$$

“INTERACTION WITH $V$ ACCEPTING THE PROOF”
COMPLETENESS

FOR A LANGUAGE \( L \), AND FOR ALL \( x \in L \)

\[ \Pr[\langle P(x, w), V(x) \rangle = 1] \]

“INTERACTION WITH \( V \) ACCEPTING THE PROOF”
COMPLETENESS

FOR A LANGUAGE $L$, AND FOR ALL $x \in L$

$\Pr[\langle P(x, w), V(x) \rangle = 1] = 1$

"INTERACTION WITH $V$ ACCEPTING THE PROOF"
COMPLETENESS

FOR A LANGUAGE $L$, AND FOR ALL $x \in L$

$$\Pr[\langle P(x, w), V(x) \rangle = 1] = 1 - \epsilon(|x|)$$

“INTERACTION WITH $V$ ACCEPTING
THE PROOF”
SOUNDNESS

“IF A STATEMENT IS FALSE, THEN NO PROVER SHOULD EVER BE ABLE TO CONVINCE THE VERIFIER THAT IT IS SO.”

FOR A LANGUAGE $L$, AND FOR ALL $x \notin L$, $\forall P^*$ (possibly unbounded)

$$\Pr[ \langle P^*(x), V(x) \rangle = 1 ] < \varepsilon(|x|)$$

WHERE $\varepsilon$ IS A NEGLIGIBLE FUNCTION
SOUNDNESS

“If a statement is false, then no prover should ever be able to convince the verifier that it is so.”

For a language $L$, and for all $x \notin L \forall P^*$

$$\Pr[ \langle P^*(x), V(x) \rangle = 1 ] < \epsilon(|x|)$$

Where $\epsilon$ is a negligible function
“After seeing a zero-knowledge proof, a verifier should be unable to accomplish any new tasks.”

\((P,V)\) is a zero-knowledge proof system for \(L\) if

\[
\forall V^* \exists \text{ ppt } S \text{ such that for all } x \in L
\]

\[
\{\text{View}_{V^*}(P(x,1^w) \leftrightarrow V^*(x))\}_n \approx \{S(1^n,x)\}_n
\]  \(1\)

If \(L \subseteq \text{BPP}\), then this condition is trivially true.

If \(L \not\subseteq \text{BPP}\), then this condition (1) must also hold for \(x \in L\).
When \( x \in L \), then \( S \) works. But if \( x \notin L \), then \( S \) fails.

\( \Rightarrow \) \( S \) can be used to decide the language \( L \).

\( \Rightarrow \) \( L \) is easily observed to be zero-knowledge.!!
GRAPH ISOMORPHISM

TWO GRAPHS ARE ISOMORPHIC IF THERE IS A WAY TO RELABEL THE NODES OF ONE SO THAT IT IS IDENTICAL TO THE OTHER
GIVEN TWO GRAPHS...

HOW CAN Alice CONVINCE Bob THAT THE TWO ARE ISOMORPHIC?
The better protocol involves Alice and Bob using two graphs $G_1$ and $G_2$.

**Alice**:
- Alice picks a permutation $\pi \leftarrow S_n$ of the set $\{1, 2, \ldots, n\}$.
- Alice computes $H := \pi(G_1)$.

**Bob**:
- Bob chooses $c \leftarrow \{1, 2\}$.
- Bob computes $G_c := \sigma(H)$, where $\sigma$ is another permutation of $\{1, 2, \ldots, n\}$.

**Security Condition**: $\mathcal{S}(n, G_1, G_2)$

1. Pick $c \leftarrow \{1, 2\}$.
2. Pick $\sigma$; compute $H$.
3. $H \in \pi(G_1)$.
4. Output $(H, c, \sigma)$. 
COMPLETENESS

Proof: if $G_1 \sim G_2$, then $I$ will always convince $V$. 
SOUNDNESS

Proof. If $G_1 \neq G_2$, then either $H \sim G_1$, $H \sim G_2$, or neither.

Thus for a given msg $H$, if a satisfactory 3rd msg for
out msg one challenge $C \in \{1,2\} \Rightarrow P$ succeeds w/prob. $\leq \frac{1}{2}$. 
We must exhibit an $S$ s.t. $\exists \text{ View}(P, V) \approx \{S\}$

$S(1^n, x)$

Repeat until success

1. pick $c, \sigma, \chi$.

2. Feed $c \lor \chi \lor \chi$. If on the first time, output $\chi$ and halt.

3. if $c^1 = c$, output $(\chi, c, \sigma)$.

\[ \rho \] be prob of non-absorbing. \[ E(\text{RUNTIME}) \cdot \rho \cdot 2 - \frac{1}{\rho} \cdot \rho \]
QUADRATIC EQUATIONS

\[ N = pq \]
\[ x^2 - 7 = 0 \mod N \]

PROVE THAT EQUATION HAS A SOLUTION
WITHOUT REVEALING THE SOLUTION!

**Alice** \((N, 7, x)\)

**Bob** \((N, 7)\)

**HINT:**
\[ r^2(x^2 - 7) = 0 \mod N \]
\[ r^2x^2 - r^27 = 0 \mod N \]
VERIFIER'S VIEW \( x^2 - 7 = 0 \mod N \)

Alice \((N, 7, x)\)

Bob \((N, 7)\)

\[ r \leftarrow \$ \]

\[ a = 7r^2 \]

\[ c \in \{0, 1\} \]

\[ z \]

\[ z^2 \cdot 7^{1-c} = a \]
\[ N = 35 = 5 \cdot 7 \quad \Rightarrow \quad x \equiv 14 \]

**Alice**

\( (35, 14) \)

\( r \leq 2 \)

\[ z = \begin{cases} 2 & \text{if } c = 0 \\ 2.7 & \text{if } c = 1 \end{cases} \]

**Bob**

\( (35, r) \)

\[ 4 \cdot 14 = 26 \]

\[ c = 0.13 \]

**Check**

\[ z \cdot q^{1-c} = 1 \]

\[ c = 0 \cdot 2^2 \cdot 14 = 2 \checkmark \]

\[ c = 1 \cdot 14^2 = 2 \checkmark \]
**VERIFIER’S VIEW**  \( x^2 - 7 = 0 \mod N \)

Alice \( (N, 7, x) \)

- \( r \leftarrow Z^*_N \)
- \( t \leftarrow r^2 \cdot 7 \)

Bob \( (N, 7) \)

\( c \leftarrow \{0, 1\} \)

\[ \text{CHECK } s^2 \cdot 7^{1-c} \equiv t \]

HOW TO GENERATE A “TRANSCRIPT” OF A PROOF:
NEW KIND OF PROOF
NON-ISOMORPHIC GRAPHS

Alice

determines if
$H \cong G_1$ or $G_2$
sends 1 or 2.

$H \leftarrow \Pi(G_1)$

or

$H \leftarrow \Pi(G_2)$

Bob

is $A \equiv B$??
3-COLORING OF A GRAPH

NP-COMPLETE