Lecture 21

Committer

Receiver

* Commitments
* ZK Proof Systems

Want: 1. Committer cannot change its mind
2. Receiver does not learn anything about x

Opening Phase

Protocol

Motivation: Why do we want this?
A 3-col ZK proof

Prover

Verifier

commitment to colors of every vertex

random edge

open colors for endpoints
§ Examples of commitment schemes

**SCHEME 1**
Let $f$ be an OWF.
Let $B$ be its hardcore predicate.

$\text{Commit}(x)$: Committer picks $r \leftarrow \{0,1\}^k$

\[ \begin{array}{c}
\uparrow \\
\text{bit}
\end{array} \]

sends to receiver $(f(r), B(r) \oplus x) \overset{\equiv}{=} (C_1, C_2)$

$\text{Open}$: reveals $(x, r)$

$C_1 \equiv f(r)$, $C_2 \equiv B(r) \oplus x$

**SCHEME 2**
$\text{Setup}(1^k)$: Group $G$, generators $g, h$, order $q$ (DL is hard).

$\text{Commit}(x)$: Committer picks $r \leftarrow \mathbb{Z}_q$

\[ \begin{array}{c}
\uparrow \\
\in \mathbb{Z}_q
\end{array} \]

sends to receiver $g^x h^r = c$

$\text{Open}$: reveals $(x, r)$ Receiver checks $c = g^x h^r$

**DEF**
A non-interactive commitment scheme is a pair of protocols $(\text{Commit, Verify Open})$ s.t.

1. 1 bit
2. * $\text{Commit}(1^k, x)$ outputs $C$, open
3. * $\text{Verify Open}(C, x, open) \rightarrow \text{Accept/ Reject}$

**Properties**
- Comp. hiding: $\text{Commit}(1^k, 0) \approx \text{Commit}(1^k, 1)$
- Uncond. binding: No $C$, open0, open1 exist s.t.

\[ \text{Verify Open}(C, 0, \text{open}_0) \Rightarrow \text{Accept} \]
§ Analysis of scheme 1: hiding from hardcore bit binding from OWP

§ Analysis of scheme 2: No setup algo in def. (but easy fix)
  hiding: \( r \) is random \( \Rightarrow h^r \) is random
  as is \( g^x h^r = c \)

**Problem** → binding: not unconditional binding as we saw in class / chameleon hash

§ Is it possible to have both unconditional hiding and unconditional binding?

A. No. Tracy's argument

§ 2nd variant of commitment scheme

Is setup needed? If \( A \) is a poly-sized circuit, can hardwire \( \omega \) open \( \omega \) open for some \( C \)

So, there must be some input to \( A \) a.

that is not anticipated. How? either setup or potentially interaction

DEF

A commitment scheme consists of (Setup, Commit, Open) s.t.

* Setup \( (1^k) \) outputs a commitment key \( K \)

* Commit \( \text{protocol} \) is a protocol where the \( C \) (the committer's)
  input is \( (1^k, K, x) \) and the receiver's is \( (1^k, K), \) and the
  committer's output is the opening info and the receiver's is \( c \)
* Open is also a protocol. For uncond.

Comp. hiding: \( \forall (\text{p.p.t.}) \) receiver \( R^* \), \( R^* \) gets the same view from committer on input 0 as on input 1.

binding: \( \forall \) p.p.t. committer \( C^* \), Pr that, after running Commit, Receiver accepts both 0 \& 1 is negl.

\$ \text{ZK Proof example w/ Hamiltonian cycle (Hc)} \$ NP-complete problem

\( \text{graph } G = (V, E) \)

\( Hc : i_1, \ldots, i_n \) s.t. all distinct

\( (V_{i_j}, V_{i_{j+1}}) \in E \ \forall j \)

\( (V_{i_1}, V_{i_n}) \in E \)

\begin{align*}
\text{Prover} & & \text{Verifier} \\
\text{- Reorder vertices,} & & \\
\text{write down corresponding} & & \\
\text{edge matrix } M & & \\
\text{- Commit to every entry } & & b \in \{0,1\} \\
M_{i,j} \text{ of } M & & \leftarrow b \\
\text{commitment is } C_{i,j} & & \\
\text{If } b = 0, \text{ open all } C_{i,j} \text{'s show how it was permuted} & & \\
\text{If } b = 1, \text{ open entries corresponding to } Hc & &
\end{align*}
Analysis:

1. Completeness: if $G \in H_L$, $P \& V$ honest, $V$ accepts $\checkmark$

2. Soundness: $\frac{1}{2}$, $\forall p^*, \forall G \in H_L$ $\Pr[V$ accepts $] = \frac{1}{2}$

next lecture