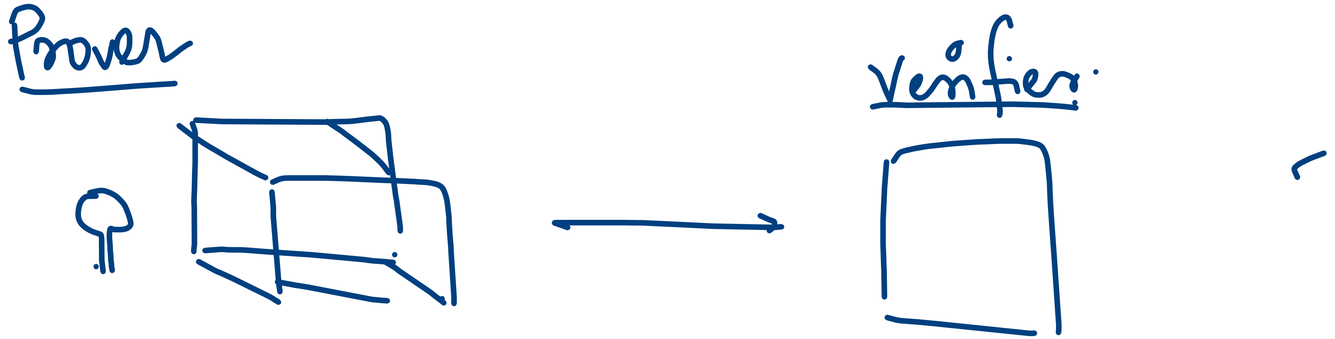
Commitment Scheme:

- Prover / (Sender).
- Verifier / (Receiver).



Commitment scheme is a tuple of three algorithms:

- $Gen(1^k) \to ck$
- $Commit(ck, m) \to (c, d)$
- $Open(ck, (c, d)) \to m$.

Hiding
- Computational
- Information theoretic

Binding
- Computational
- Information theoretic

$m_0, \quad m_1$

Hiding:

$C(m_0) \approx_c C(m_1)$.

RSA

$c = m^e \bmod N$

$m \in \mathbb{Z}_N^*$.

$c = m^e \bmod N$.

(d, m)

$c^d \bmod N \overset{?}{=} m$

$c = m^e \bmod N = (m')^{e'} \bmod N$.

One-way fn:

$$f : \{0,1\}^* \to \{0,1\}^*$$

$$\mu : \mathbb{N} \to \mathbb{R}.$$

$$x \leftarrow\$ \{0,1\}^n$$

$$\mu(n) \leq \frac{1}{p_0(n)} \quad \forall n \geq n_0$$

$$y = f(x)$$

$$\Pr\left[A(f(x)) \in f^{-1}(f(x))\right] \leq \text{negl}(n)$$

PRG: (Pseudo Random Generator).

$G: \{0,1\}^k \to \{0,1\}^*$.

1. Commitment Scheme.

$s \leftarrow \$ \{0,1\}^k$ $\quad$ $G: \{0,1\}^k \to \{0,1\}^{3k}$. $\quad$ Verifier

$r \leftarrow \$ \{0,1\}^{3k}$

$\xrightarrow[\text{Commit}]{x}$

if $b=0$
$x = G(s)$
if $b=1$
$x = G(s) \oplus r$
return x

$\xrightarrow[\text{Decommit}]{s}$

if $x = G(s)$ output 0.
if $x = G(s) \oplus r$ output 1.

$P_r[\text{Bad } r] \le \frac{1}{2^k}$ $\quad 2^{2k}$

s_1, s_2

$b=0\ x = G(s_1)$
$b=1\ x = G(s_2) \oplus r$

$\Rightarrow G(s_1) \oplus G(s_2) = r$.

Hard-Core predicate.

g is a one way fn.

$$g : \{0,1\}^n \to \{0,1\}^n$$

$$f : \{0,1\}^{2n} \to \{0,1\}^{2n}.$$

$$f(x,y) = (g(x), y).$$

$$hc : \{0,1\}^n \to \{0,1\}.$$

$$\Pr\left[A(f(x)) = hc(x)\right] \leq \frac{1}{2} + \text{negl}(n).$$

2. Commitment scheme from one-way permutation and hard-core predicate.

Prover

$r \leftarrow \$ \{0,1\}^n$

$c = f(r)$

$d = h(r) \oplus b$

$\xrightarrow{(c,d)}$ Commit

$\xrightarrow{r}$

Verifier

$V(f(r))$

$c \stackrel{?}{=} f(r)$

$b = d \oplus h(r)$

3) Discrete-log based Commitment Scheme.

(Pedersen Commitment Scheme).

Prover

$x \in \{0,1\}^{k-1}$

Verifier

Choose a prime q and generate a cyclic group G_q of order q where $|q| = k$

$q, h \leftarrow \$ G_q$

$\xleftarrow{q, h, a, G_q}$

$r \leftarrow \$ Z_q$

$c = g^x h^r$

$\xrightarrow{c}$ Commit

$\xrightarrow{(r, x)}$

$c \stackrel{?}{=} g^x h^r$

$c = g^x h^r = g^{x'} h^{r'}$

$g^x h^r = g^{x'} h^{r'}$

$\Rightarrow g^{x-x'} = h^{(r'-r)}$

$\Rightarrow \log_g h = (x-x')(r'-r)^{-1}$

$\Rightarrow g^{(x-x')(r'-r)^{-1}} = h$.

Information theoretic hiding.

$P_r[C = c] = \frac{1}{|Z_q|}$ where $h = g^\alpha$.

$P_r[g^x h^r = g^x g^{\alpha r} = c] \Rightarrow P_r[x + \alpha r = \beta]$

$= g^{x+\alpha r} = g^\beta] \Rightarrow P_r[r = \alpha^{-1}(\beta - x)] = \frac{1}{|Z_q|}$.

RSA-based assumption Commitment Scheme.

Prover $x \in \{0,1\}^{k-1}$

Verifier

k bit-primes p, q.

$N = pq$.

choose a prime $e > N$

(N, e, u) ←

$u \leftarrow\$ \mathbb{Z}_N^*$.

$r \leftarrow\$ \mathbb{Z}_N^*$.

$c = u^x r^e \bmod N$.

c — Commit →

(r, x) →

Check $c \stackrel{?}{=} u^x r^e \bmod N$.

Information theoretic hiding

Computational binding.