

Problem 1: (Two truths and a lie)

a) Identify the lie.

i) Every HVZKP is secure against malicious verifiers with a different simulator.

ii) An IP with deterministic verifier can only exist for LNP.

iii) MVZKPs & LNP lie in minicrypt world.

+1 for correct answer

Solution: i) (HVZKP for GNI is an example)

b) Identify the lie.

i) Dig Sigs are public-key objects, but lie in minicrypt.

ii) RSA assumption holds $\Rightarrow$ factoring assumption holds.

iii) $\exists$ commitment schemes that are both perfect hiding & binding.

+1 for correct answer

Solution: ii) (this was class HW for you to prove).

Problem 2

a) RO $H: \{0,1\}^{n+1} \rightarrow \{0,1\}^n$

$\text{commit}(b; r) := H(b||r)$, for bit b & randomness $r \in \{0,1\}^n$.

Solution:

• It is computationally hiding: H is an RO, therefore

$$\text{commit}(0; r_0) = H(0||r_0)$$

$$\text{commit}(1; r_1) = H(1||r_1)$$

Given $\text{com}_b = \text{commit}(b; r_b)$ for $b \in \{0,1\}$, Adversary can only guess r_b w.p. $\frac{1}{2^n}$ & else, $H(b||r_b)$ looks random

$\Rightarrow \text{Commit}(0; r_0) \not\sim_c \text{Commit}(1; r_1)$

• Not perfect binding: with unbounded time, it is possible to brute-force & find r_1, r_2 s.t. $H(0||r_1) = H(1||r_2)$.

(+0.5) x 3 for each correct response
(+1) x 2 for comp hiding & comp binding proof

(+0.5) for perfect binding explanation

- It is **computationally binding**: Suppose $\mathcal{A}$ PPT that can find r_1, r_2 s.t. $\text{commit}(0; r_1) = \text{com} = \text{commit}(1; r_2)$

$\Rightarrow \mathcal{A}$ can find r_1, r_2 s.t. $H(0 || r_1) = H(1 || r_2)$
 $\Rightarrow \mathcal{A}$ can break collision resistance of RO H
 (which is a contradiction $\because$ RO is collision-resistant)

- b) $f: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ OWE.
 $\text{commit}(b; r) = (b \oplus r_1 \oplus \dots \oplus r_n, f(r))$ for bit b & randomness $r = r_1 || r_2 || \dots || r_n \in \{0,1\}^n$.

Solution:

- Not computationally hiding:**

Given OWE $g: \{0,1\}^n \rightarrow \{0,1\}^n$, consider $f: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ defined as:

$$f(x) := (g(x), \bigoplus_{i=1}^n x_i)$$

Then, show that f is a OWE (simple reduction)

For this f ,

$$\begin{aligned} \text{commit}(b; r) &= (b \oplus r_1 \oplus \dots \oplus r_n, f(r)) \\ &= (b \oplus (\bigoplus_{i=1}^n r_i), g(r), \bigoplus_{i=1}^n r_i) \end{aligned}$$

$\swarrow \searrow$
 XOR to recover b !

- Not computationally binding:** ($\Rightarrow$ not perfect binding)

Idea: f is OWE but need not be collision resistant.

f can be a OWE s.t. $\exists r, r'$ s.t. $\bigoplus_{i=1}^n r_i = \bigoplus_{i=1}^n r'_i \oplus 1$ & $f(r) = f(r')$
 which is feasible to find.

then

$$\begin{aligned} \text{commit}(0; r) &= (\bigoplus_{i=1}^n r_i \oplus 0, f(r)) \\ \text{commit}(1; r') &= (\bigoplus_{i=1}^n r'_i \oplus 1, f(r')) = (\bigoplus_{i=1}^n r_i, f(r)) \end{aligned} \quad \left. \vphantom{\begin{aligned} \text{commit}(0; r) \\ \text{commit}(1; r') \end{aligned}} \right\} \text{are equal.}$$

Take $f(x) = \begin{cases} g(x) & \text{if } \bigoplus_{i=1}^n x_i = 0 \\ g(x \oplus 0^{n-1} || 1) & \text{if } \bigoplus_{i=1}^n x_i = 1 \end{cases}$ for OWE g . (Recall this from mid-sem)
 (Prove it is one-way! Now, take $r \in \{0,1\}^n$ & set $r' = r \oplus 0^{n-1} || 1$)

(+0.5) x3
 for each
 correct
 response.

(+1) for
 comp hiding
 counterexample

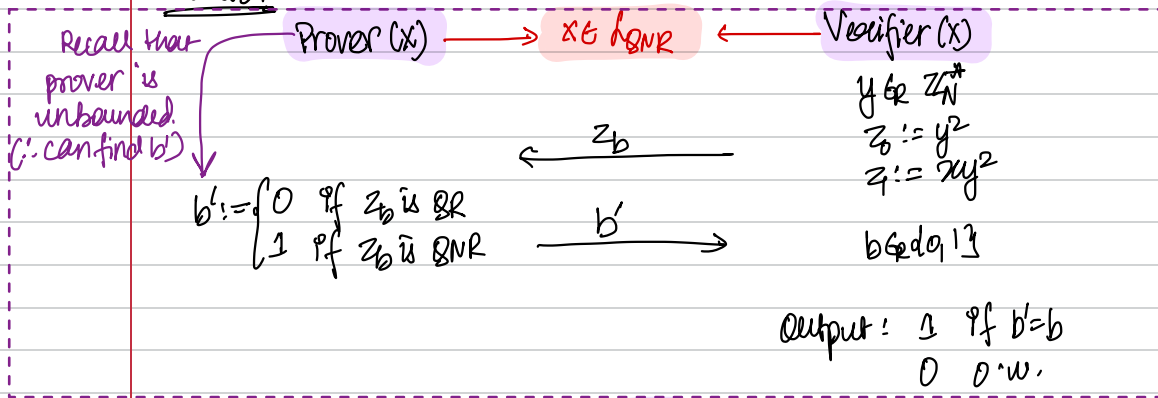
(+1.5) for
 comp binding
 counterexample.

Problem 3:

$L_{\text{QNR}} = \{ (N=pq, y) : \nexists x \in \mathbb{Z}_N^* \text{ s.t. } x^2 \equiv y \pmod{N} \}$

- Describe IP Π for L_{QNR} .
- Prove completeness and soundness of Π .
- Prove that Π is a ZKP.

Solution:



$\Pi = (P, V)$

Completeness: $x \in L_{\text{QNR}} \Rightarrow y^2$ is QR & xy^2 is QNR
Hence, for honest prover V accepts ($b'=b$) w.p. 1.

Soundness: $x \notin L_{\text{QNR}} \Rightarrow x$ is a QR
 $\Rightarrow y^2$ & xy^2 are both QR
 $\Rightarrow$ Even if P^* is unbounded, $b'=b$ only w.p. $1/2$.

HVZK:

$\text{Sim}(x)$:

- $b \in \{0, 1\}$
- Pick $y \in \mathbb{Z}_N^*$ set $z_b = x^b y^2$
- Output (b, z_b, b)

Easy to see $\text{View}_V(\langle P, V \rangle(x)) \equiv \text{Sim}(x) \quad \forall x \in L_{\text{QNR}}$.

+2 for correct protocol
+1

+1

+2 for correct simulator (partial privacy for decommitments)

Problem 4

$\text{Gen}(1^n)$: $G \rightarrow (G, q, g)$. RO $H: \{0,1\}^* \rightarrow \mathbb{Z}_q$

Generate $x \in \mathbb{Z}_q$ & compute $y = g^x$.

Output $pk = (G, q, g, y)$, $sk = (G, q, g, x)$

$\text{Sign}(sk, m)$: $k \in \mathbb{Z}_q$. $I = g^k$, $r = H(I, m)$, $s = (rx + k) \bmod q$

Output $\sigma = (r, s)$.

$\text{Verify}(pk, m, \sigma)$: output 1 iff $H(g^s \cdot y^{-r}, m) = r$

a) Same Gen , $\text{Sign}'(sk, m)$ picks $k \in \mathbb{Z}_q$, $r = H(m)$ & outputs $\sigma = (I = g^k, s := (rx + k) \bmod q)$

$\text{Verify}'(pk, m, \sigma = (I, s))$: generates $r = H(m)$ & outputs 1 iff $I = g^s \cdot y^{-r}$.

Solution: Recall that Mallory gets $pk = (G, q, g, y)$.

Mallory can pick $s \in \mathbb{Z}_q$, query RO on m to get r
output forgery $(m, \sigma = (I = g^s \cdot y^{-r}, s))$

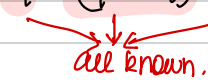
b) Suppose signing faulty & chooses dependent k_t in consecutively issued signatures. When signing m_0 , sign chooses uniform random $k_0 \in \mathbb{Z}_q$. But to sign m_0 , it sets $k_t = ak + b$ for some known a, b .

Adversary gets (m_0, σ_0) , (m_1, σ_1) & knows a, b, pk . Show it can recover sk .

Solution (sketch):

$$\sigma_0 = (r_0, s_0), \text{ where } s_0 = (r_0 x + k_0) \bmod q \rightarrow \textcircled{1}$$

$$\sigma_1 = (r_1, s_1), \text{ where } s_1 = (r_1 x + k_1) \bmod q \\ = (r_1 x + ak_0 + b) \bmod q \rightarrow \textcircled{2}$$

Solve for x : $\textcircled{1} \& \textcircled{2} \Rightarrow s_1 = (r_1 - ar_0)x + (as_0 + b) \bmod q$


(Recall geometric analogy of Schnorr discussed in class.
 $x \rightarrow$ slope $k \rightarrow$ intercept $(r, s) \rightarrow$ evaluation of line $xytk$ at random
 what the attack shows: if intercepts for 2 sig correlated $\rightarrow$ problem)

+2 for complete attack

+2 for complete attack.