

Problem 1: $\Pi_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$ & $\Pi_2 = (\text{Gen}_2, \text{Enc}_2, \text{Dec}_2)$ are PKE schemes s.t. at least one is IND-CPA secure, but we don't know which one. Consider following constructions of "combiners" with $\text{Gen}(1^n)$: $(pk_1, sk_1) \leftarrow \text{Gen}_1(1^n)$, $(pk_2, sk_2) \leftarrow \text{Gen}_2(1^n)$ of: $((pk_1, pk_2), (sk_1, sk_2))$
 which of these is IND-CPA secure?

- $\text{Enc}(pk, m) := (\text{Enc}_1(pk_1, m), \text{Enc}_2(pk_2, m))$
- $\text{Enc}(pk, m) := \text{Enc}_1(pk_1, \text{Enc}_2(pk_2, m))$.
- $\text{Enc}(pk, m) := \text{Enc}_2(pk_2, \text{Enc}_1(pk_1, m))$.
- $\text{Enc}(pk, m) := (\text{Enc}_1(pk_1, r), \text{Enc}_2(pk_2, m \oplus r))$ for $r \leftarrow \{0, 1\}^{|m|}$.

Solution

a) Not secure. Eg. $\text{Enc}_1(pk_1, m) := m$ (Π_1 insecure) then clearly Π is insecure (even if Π_2 is IND-CPA secure)

b) (Thanks to Ravi for pointing out this attack)
 Not secure.

Eg. Π_2 is insecure and such that

$\text{Enc}_2(pk_2, m) : \begin{cases} \text{outputs } m \parallel 0 & \text{if first bit of } m \text{ is } 0 \\ \text{outputs } m & \text{otherwise.} \end{cases}$

Now, even if Π_1 is secure, for $m_0 = 0 \parallel m'$, $m_1 = 1 \parallel m'$ Evelyn gets $c_0 = \text{Enc}_1(pk_1, \text{Enc}_2(pk_2, m_0))$. $\because \text{Enc}_2(pk_2, m_0) \neq \text{Enc}_2(pk_2, m_1)$ are of different lengths, c_0 & c_1 are trivially distinguishable.

(Remark: this is because IND-CPA only holds when adversary sends two same-length messages. If the messages sent are of different length, CPA-attack is trivial.)

c) not secure. (Same reason as above)

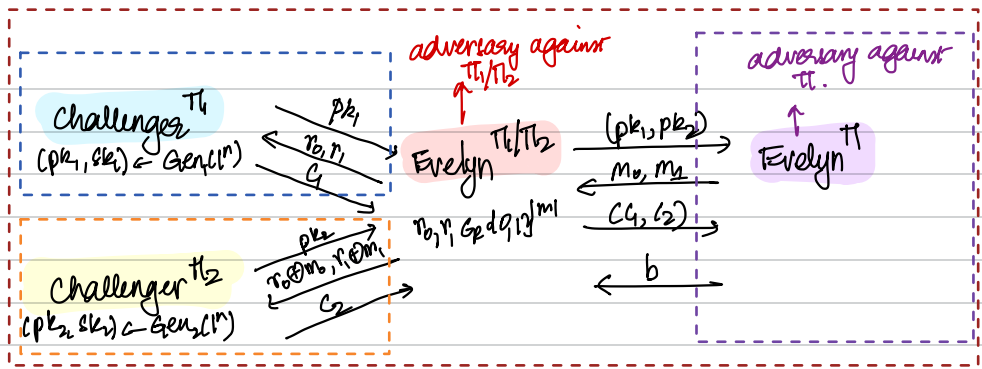
d) secure. (Giving complete explanation below, but a clear intuition was enough.)

To show: Π_1 IND-CPA-secure or Π_2 IND-CPA secure $\Rightarrow \Pi$ IND-CPA secure

$\therefore$ To show contradiction we show:

Π not IND-CPA secure $\Rightarrow \Pi_1$ & Π_2 both not IND-CPA secure.

For each part:
 +0.5
 for yes/no
 +0.5
 for correct
 intuitive
 explanation



Analyzing prob of breaking T_1 (symmetric argument for T_2):

$$\Pr[EvElyn^{T_1/T_2}(pk_1, c_1) = 1] - \Pr[EvElyn^{T_1/T_2}(pk_1, c_1) = 1]$$

$$c_1 \leftarrow Enc(pk_1, r_0) \quad c_1 \leftarrow Enc(pk_1, r_1)$$

$$= \left\{ \Pr[EvElyn^{T_1}(pk_1, pk_2, c_1, c_2) = 1] + \Pr[EvElyn^{T_1}(pk_1, pk_2, c_1, c_2) = 1] \right.$$

$$c_1 \leftarrow Enc(pk_1, r_0) \quad c_2 \leftarrow Enc(pk_2, m_0 \oplus r_0) \quad c_1 \leftarrow Enc(pk_1, r_1) \quad c_2 \leftarrow Enc(pk_2, m_1 \oplus r_1)$$

$$- \Pr[EvElyn^{T_1}(pk_1, pk_2, c_1, c_2) = 1] - \Pr[EvElyn^{T_1}(pk_1, pk_2, c_1, c_2) = 1]$$

$$c_1 \leftarrow Enc(pk_1, r_1) \quad c_2 \leftarrow Enc(pk_2, m_0 \oplus r_1) \quad c_1 \leftarrow Enc(pk_1, r_0) \quad c_2 \leftarrow Enc(pk_2, m_1 \oplus r_0)$$

(note that these two probabilities are same, hence cancel out)

$\therefore \textcircled{1}$ is exactly distinguishing prob of $EvElyn^{T_1}$, hence done. ①

Problem 2:

- $Gen'(1^n) = Gen(1^n)$; $Enc'(pk, m; r) := Enc(pk, m; G(r))$
- $Gen'(1^n) = Gen(1^n)$; $Enc'(pk, m; r) := Enc(pk, m; f_r(m))$
- $Gen'(1^n; f_{llk})$: generator $(pk, sk) \leftarrow Gen(1^n; f)$, output (pk_{llk}, sk)
 $Enc'(pk_{llk}, m) := Enc(pk, m; f_b(m))$.

Solution:

a) secure

$(G(\text{random}) \otimes_c \text{random}) \Rightarrow Enc(pk, m; G(\text{random})) \otimes_c Enc(pk, m; \text{random})$
 new security reduces to IND-CPA-security of T_1 .

b) secure

(similar reasoning as a), but with PRF instead of PRG)

+0.5 for correct yes/no
 +
 +0.5 for correct intuition

c) not secure

(Given K , PRF not secure. Also, deterministic $\Rightarrow$ not IND-CPA secure)

Problem 3:

a) $f_1(x) := f(x) \oplus x$

Solution: not secure.

Take $f(x_1 \| x_2) := g(x_2) \| 0^{n/2}$ for OWF g & $|x_1| = |x_2|$

(simple to show f is one-way)

But $f_1(x) = (g(x_2) \oplus x_1) \| x_2$, which is now easy to invert given $y = y_1 \| y_2$, inverse: $(y_1 \oplus g(y_2)) \| y_2$

b) $f_2(x) := y_1 \| y_2 \| \dots \| y_n$, where $y = y_1 \| y_2 \| \dots \| y_n := f(x)$

Solution: not secure.

(idea is to create a loophole to get easy inverse, based on last bit)

$$f(x_1 \| x_2) = \begin{cases} x_2 \| 0^{n/2} & \text{if } x_1 = 0^{n/2} \\ g(x_1) \| 0^{n/2-1} \| 1 & \text{o.w.} \end{cases}, \quad |x_1| = |x_2|, \quad g \text{ is a OWF}$$

f is OWF (reduce to one-wayness of g , $\therefore$ easy inverse case happens w.p. $1/2^{n/2}$, which is low.)

$$\begin{aligned} f_2(x_1 \| x_2) &= y_1 \| y_2 \| \dots \| y_n \\ &= y_1 \| y_2 \| \dots \| y_{n/2} \| 0^{n/2-1} \| 1, \text{ for } y_1 \| y_2 \| \dots \| y_{n/2} := f(x_1 \| x_2) \end{aligned}$$

can get inverse easily: $x = 0^{n/2} \| y_1 \| y_2 \| \dots \| y_{n/2}$

Problem 4:

1. $\text{Enc}(pk, m = m_1 \| m_2 \| \dots \| m_\ell) := \text{Enc}(pk, m_1) \| \dots \| \text{Enc}(pk, m_\ell)$

Solution (sketch)

Given $C_0 = C_1 \| C_2 \| \dots \| C_\ell$, you can query $C_2 \| C_1 \| C_3 \| \dots \| C_\ell$ to $\text{Dec}_{sk}(f)$

2. Enc(pk = (A, Aste), b): $r \in \mathbb{Z}_q^m$ encode b to $\hat{b}$ as $\hat{b} = b \cdot [q/2]$
 output: $C = (r^T A, r^T (Aste) + \hat{b})$

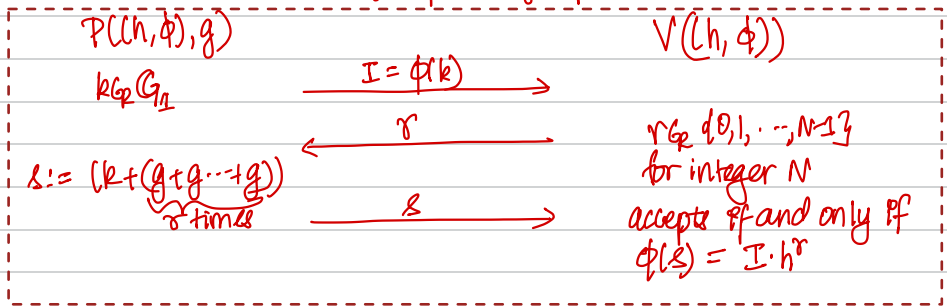
+2 for complete attack

Solution (Sketch):

Given $C_b = (r^T A, r^T (Aste) + b \cdot [q/2])$
 query Dec_{sk}(.) with $(r^T A, (r^T (Aste) + b \cdot [q/2] + r^T b)) \bmod q$
 will decrypt to (b).

Problem 5

$R_{hom} := \{(h, \phi), g\} \in (\underbrace{G_2 \times F}_{\text{multiplicative group}}) \times \underbrace{G_1}_{\text{additive group}} : \phi(g) = h\}$



a) completeness (simple to prove)

b) Special soundness

Solution (Sketch): Ext gets $(I, \sigma, s), (I, \sigma', s')$ for $r \neq r'$ s.t.
 (I, σ, s) and (I, σ', s') are both accepting transcripts,
 & gets statement (h, ϕ) .

$$\begin{aligned} \therefore I &= \phi(s) \cdot h^{-\sigma} = \phi(s') \cdot h^{-\sigma'} \\ \Rightarrow \phi(s) \cdot \phi(g)^{-\sigma} &= \phi(s') \cdot \phi(g)^{-\sigma'} \\ \Rightarrow \phi(s) \cdot \phi(g)^{\sigma} &= \phi(s') \cdot \phi(g)^{\sigma'} \Rightarrow \phi(s + \sigma' \cdot g) = \phi(s' + \sigma \cdot g) \\ \Rightarrow s + \sigma' \cdot g &= s' + \sigma \cdot g \quad (\because \phi \text{ is a bijection}) \\ \Rightarrow g &= (s - s') \cdot (\sigma - \sigma')^{-1} \quad (\sigma - \sigma' \neq 0 \because r \neq r') \end{aligned}$$

as long as inverse exists, can find g

+3 for class extractor & analysis

c) Zero knowledge

Solution (sketch):

$\text{Sim}(\text{Ch}, \phi)$: • Pick $r \in \{0, \dots, N-1\}$, $s \in \mathbb{G}_1$
output $(X = \phi(s) \cdot h^r, r, s)$

(Argument similar to Schnorr)

d) $R_{DH} := \{(\text{Ch}, u, v), x) \in \mathbb{G}^3 \times \mathbb{Z}_q : u = g^x \wedge v = h^x\}$

Solution (sketch):

$\phi: \mathbb{Z}_q \rightarrow \mathbb{G}^2$ defined as: $\phi(x) = (g^x, h^x)$
Prove ϕ is a group homomorphism. R_{hom} for ϕ is R_{DH}

Problem 6

$\text{Commit}^{\text{mult}}(m_1, m_2; r_1, r_2) := \text{Commit}(m_1; r_1) \parallel \text{Commit}(m_2; r_2)$
 $\text{Receive}^{\text{mult}}(\text{com}_1, \text{com}_2, m_1, m_2, r_1, r_2)$: output 1 if
Receive(com_1, m_1, r_1) = 1 and Receive(com_2, m_2, r_2) = 1
and 0, otherwise.

a) Computational hiding:

Solution (sketch):

$H_0: \text{Commit}(m_1; r_1) \parallel \text{Commit}(m_2; r_2)$ } → show indistinguishable by reducing to hiding of Π .
 $H_1: \text{Commit}(m'_1; r'_1) \parallel \text{Commit}(m_2; r_2)$ }
 $H_2: \text{Commit}(m'_1; r'_1) \parallel \text{Commit}(m'_2; r'_2)$ } ↓ reduction script

$H_0 \approx_c H_1 \wedge H_1 \approx_c H_2 \Rightarrow H_0 \approx_c H_2$ (can state & use transitivity)

b) Perfect binding

if perfect binding of Π^{mult} broken $\Rightarrow$ for $\text{com} = \text{com}_1 \parallel \text{com}_2$
 $\exists (m, r), (m', r') \neq$ and $\text{Receive}^{\text{mult}}(\text{com}, m, r) = 1$
& $\text{Receive}^{\text{mult}}(\text{com}, m', r') = 1$

+3 for correct analysis

$$\because m = m_1 || m_2 \neq m'_1 || m'_2 = m' \Rightarrow \underbrace{m_1 \neq m'_1}_{\substack{\downarrow \\ (m_1, r_1), (m'_1, r'_1) \text{ breaks perfect binding}}} \text{ or } \underbrace{m_2 \neq m'_2}_{\substack{\downarrow \\ (m_2, r_2), (m'_2, r'_2) \text{ breaks binding}}}$$

Problem 7:

- a) SDH: $\forall$ PPT $SqLogan$, $\nexists$ negl $s.t.$ $\forall n$:
 $\Pr_{\substack{(G, q, g) \leftarrow G(n) \\ a \in \mathbb{Z}_q}} [SqLogan(1^n, (G, q, g), g^a) = h : h = g^{a^2}] \leq \text{negl}(n).$

Show: SDH solver $\Rightarrow$ CDH solver

Solution (Sketch): (Thanks to Aditya for complete, clean attack!)

Challenger

$(G, q, g) \leftarrow G(n)$
 $a, b \in \mathbb{Z}_q$

g, g^a, g^b

Logan

(need to invoke $SqLogan$ on independent instances)

$r_1, r_2 \in \mathbb{Z}_q$

$g^{a^2 + r_1^2 + 2ar_1} = g^{(a+r_1)^2}$

$g^{b^2 + r_2^2 + 2br_2} = g^{(b+r_2)^2}$

$g^{a^2 + b^2 + 2ab} = g^{(a+b)^2}$

① $g + g^{a+r_1}$ (if wins)

② $g + g^{b+r_2}$ (if wins)

③ $g + g^{a+b}$ (if wins)

given these can find g^{ab} . Now, finding Sq root easy $\rightarrow$ can find g^{ab}

Analyze the prob. of winning to complete!
 (Notice that if you query g^a, g^b & g^{a+b} , these are correlated) & prob. analysis won't work. Important to invoke $SqLogan$ indep.)

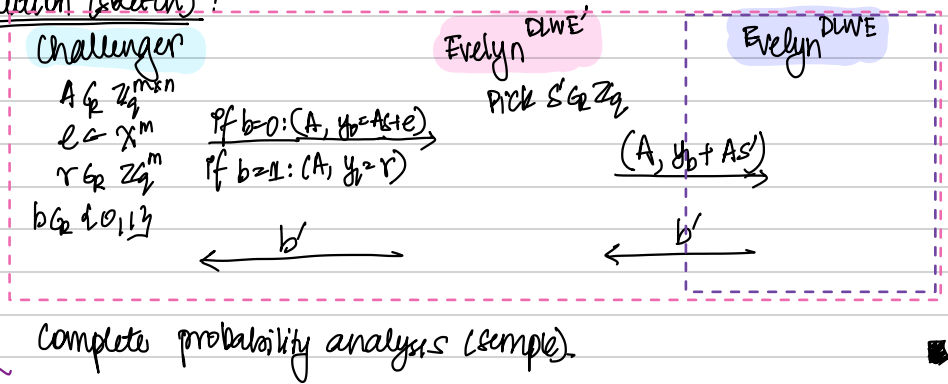
- b) DWE': $\forall$ SG $\mathbb{Z}_q^n$, $\nexists$ negl $s.t.$ $\forall n$

$$\left| \Pr_{\substack{A \in \mathbb{Z}_q^n \\ e \in \mathbb{Z}_q^m}} [Evelyn(A, Aste) = 1] - \Pr_{\substack{A \in \mathbb{Z}_q^n \\ r \in \mathbb{Z}_q^m}} [Evelyn(A, r) = 1] \right| \leq \text{negl}(n)$$

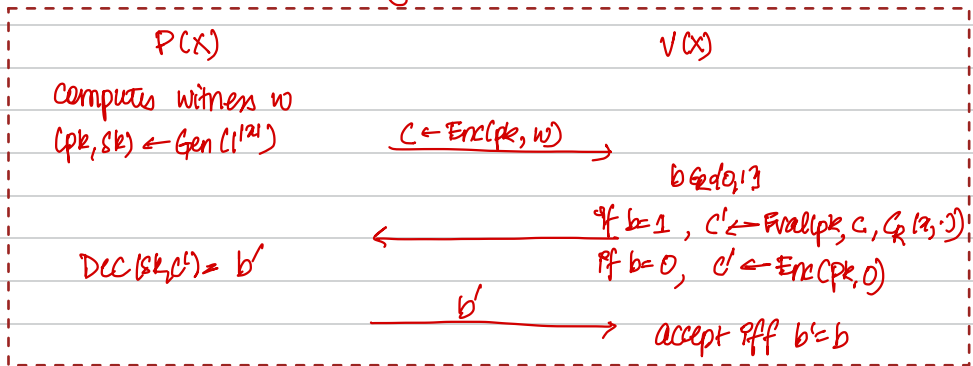
show: DLWE solver $\Rightarrow$ DLWE' solver.

Solution (Sketch):

+2.5 for complete attack
+0.5 for analysis.



Problem 8 ZKP for NP using FHE.



+0.5 for completeness
+0.5 for when perfect?

a) Perfect completeness $\rightarrow$ perfect only if underlying FHE has perfect correctness. (simple to show)

b) Soundness $\rightarrow$

idea: for $x \notin L$, $G(x, w) = 0 \neq w \Rightarrow \text{Dec}(sk, c') = 0$
 $\therefore$ only way P can win is by correctly guessing b which happens w.p. $1/2$

(to formally argue this, must use correctness of decryption)
 under evaluated ciphertexts

$\rightarrow$ this idea doesn't work (Soundness actually does not hold)

unless FHE satisfies:
 $\forall m, \forall f \in \mathcal{F}$
 for $(pk, sk) \leftarrow \text{Gen}(1^n)$

$$\begin{cases} c \leftarrow \text{Enc}(pk, m) \\ c' \leftarrow \text{Eval}(pk, c, f) \\ \text{o/p} : c' \end{cases}$$

$\approx_c$

$$\begin{cases} c' \leftarrow \text{Enc}(pk, m) \\ \text{o/p} : c' \end{cases}$$

- ① If this property doesn't hold the prover can respond with $b' = b$ w.s.p. 1 even if $x \notin L$!
- ② This property need not be satisfied by an FHE.

Example!

Take a secure FHE: $(\text{Gen}, \text{Enc}, \text{Dec}, \text{Eval})$

Construct: $(\text{Gen}' = \text{Gen}, \text{Enc}', \text{Dec}', \text{Eval}')$ as:

- $\text{Enc}'(pk, m) := 1 \parallel \text{Enc}(pk, m)$
- $\text{Eval}'(pk, c, f) := 0 \parallel \text{Eval}(pk, c, f)$
- $\text{Dec}'(sk, b'c) := \text{ignore first bit } b \text{ o/p } \text{Dec}(sk, c)$.

You can prove that this scheme will still be IND-CPA secure, satisfy both correctness & will have compactness, i.e. is an FHE. But clearly evaluated ciphertext is distinguishable from ciphertext output by Enc .

(Thanks to Tejeewar for the above explicit attack!)

c) Computational HVZK

(Solution sketch): idea is simulator (for $x \in L$) can pick

- C as $\text{Enc}(pk, \text{random})$
- $b \in \{0, 1\}$ if $b=1$ $c' \leftarrow \text{Eval}(pk, C, C_k(x, \cdot))$
 if $b=0$ $c' \leftarrow \text{Enc}(pk, 0)$
- outputs (C, c', b)

Use correctness of evaluation + IND-CPA security of Enc to argue computational indist of sim view from real view of V .

+2 for correct simulator
 +1 for correct analysis.