MAMME FME **Codes and Cryptology**

Cryptography Part

Exam 18 December 2014

Choose three of the four exercises.

1. Show that computing square roots modulo $n = pq$ is as hard as computing square roots modulo n^2, where p, q are unknown prime numbers of the same size. To do it, consider the following steps:

   (a) Show than for any $\beta \in \mathbb{Z}_n$, and $y_1 \in \mathbb{Z}_n^\times$, $y_2 = y_1 + \beta n$ is a square in $\mathbb{Z}_{n^2}^\times$ if and only if y_1 is a square in $\mathbb{Z}_n^\times$.

   (b) Given a square root $x_1 \in \mathbb{Z}_n^\times$ of $y_1 \in \mathbb{Z}_n^\times$, show how to compute a square root of $y_2 = y_1 + \beta n \in \mathbb{Z}_{n^2}^\times$, of the form $x_2 = x_1 + \alpha n$.

   (c) Write a formal statement saying that $f_1 : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ such that $f_1(x) = x^2 \bmod n$ is a one-way function. Do the same for $f_2 : \mathbb{Z}_{n^2}^\times \to \mathbb{Z}_{n^2}^\times$ such that $f_2(x) = x^2 \bmod n^2$

   (d) Build a polynomial-time algorithm $\mathcal{A}_2$ that breaks the one-wayness of f_2 from any algorithm $\mathcal{A}_1$ that breaks the one-wayness of f_1, with at least the same success probability.

   (e) Show now a similar reduction working in the other direction.

2. Let $\mathcal{G}$ be a cyclic group of prime order q and let $g \in \mathcal{G}$ be a generator. Consider the following public key encryption scheme, where the secret key is a random pair $(x_1, x_2) \in \mathbb{Z}_q^2$, the public key is (g^{x_1}, g^{x_2}), and the encryptions of $m \in \mathcal{G}$ are $(g^{x_1 r_1}, g^{x_2 r_2}, m g^{r_1 + r_2})$, where $r_1, r_2 \in \mathbb{Z}_q$ are random.

   (a) Write the encryption algorithm in details.

   (b) Describe the decryption procedure.

   (c) Write a homomorphic property of the above encryption scheme.

   (d) Which security level do you think the scheme can achieve?

3. Let $\mathcal{G}$ be a cyclic group of prime order $q \approx 2^\lambda$ and let $g \in \mathcal{G}$ be a generator. The Computational Diffie-Hellman (CDH) problem in $\mathcal{G}$ consists in computing g^{xy} when given input (g, g^x, g^y), for random and independent $x, y \xleftarrow{R} \mathbb{Z}_q$.

   Suppose that $\mathcal{G}$ admits a bilinear pairing $e : \mathcal{G} \times \mathcal{G} \to \mathcal{G}_T$ for a group $\mathcal{G}_T$ with order q, generated by $e(g, g)$. Consider the following family of functions, parameterized by $A \in \mathcal{G}$: $\{f_A : \mathcal{G} \to \mathcal{G}_T\}_{A \in \mathcal{G}}$, where $f_A(B) = e(A, B)$.

   (a) Prove: assuming the hardness of the CDH problem, the family $\{f_A\}_{A \in \mathcal{G}}$ is a family of one-way functions (that is, for a random choice of $A \xleftarrow{R} \mathcal{G}$ and $T \xleftarrow{R} \mathcal{G}_T$, the probability to find $B \in \mathcal{G}$ such that $f_A(B) = T$ must be negligible in λ).

   (b) Describe the homomorphic properties of the one-way function f_A.

   (c) Analogously to what we saw in the course for the exponentiation one-way function, give a 3-moves zero-knowledge proof of knowledge protocol where a prover proves knowledge of $B \in \mathcal{G}$ such that $f_A(B) = T$, for public values $A \in \mathcal{G}$ and $T \in \mathcal{G}_T$. Sketch the proof for the security properties of this protocol.

   (d) Describe the protocols of a signature scheme constructed from the previous 3-moves zero-knowledge proof of knowledge protocol.

4. Let $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ be a set of 4 players, and consider the access structure defined by the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}, \{P_1, P_4\}, \{P_2, P_4\}\}$. The goal is to design a linear secret sharing scheme for Γ with the shortest possible shares.

   (a) Prove that it is **not** possible to realize this access structure in an ideal way, with a vector space secret sharing scheme, when secrets belong to the binary field $\mathbb{F}_2 = \{0, 1\}$.

   (b) In this case of binary secrets, describe the linear secret sharing scheme (vectors, shares...) that results from applying the general construction (based on dual access structures). What is the information rate of this scheme ?

   (c) Prove that there is an ideal (vector space) secret sharing scheme for Γ if we move to $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$ for $q > 2$ being a prime. [**Hint:** $q = 3$ and vectors with two components, for instance $\psi(D) = (1, 1)$, should be enough.]

   (d) Discuss the relation between Γ and a $(2, 4)$-threshold access structure; use this fact to give a modification of Shamir's threshold secret sharing scheme that realizes Γ when the secrets belong to $\mathbb{F}_q$ and $q > 4$.

(1) a) $\beta \in \mathbb{Z}_n$, $y_1 \in \mathbb{Z}_n^*$ $\Big\}$ $y_2 = y_1 + \beta n$

y_2 square in $\mathbb{Z}_{n^2}^*$ $\Leftrightarrow$ y_1 square in $\mathbb{Z}_n^*$

$\Rightarrow$ | $\exists \alpha \in \mathbb{Z}_{n^2}^*$ s.t. $\alpha^2 = y_1 + \beta n \pmod{n^2}$

Reducing mod n the previous expression:

$$\alpha^2 = y_1 \pmod{n}.$$

And then: y_1 is a square in $\mathbb{Z}_n^*$.

$\Leftarrow$ | $\exists \alpha' \in \mathbb{Z}_n^*$ s.t. $y_1 = \alpha'^2 \pmod{n}$.

Then: $y_2 = \alpha'^2 + \beta n \pmod{n^2}$.

Take: $\beta' = \frac{\beta}{2}$ and substitute in the previous expression:

$$y_2 = \alpha'^2 + 2\beta' n \pmod{n^2}$$
$$= (\alpha' + \beta' n)^2 \pmod{n^2}.$$

Which implies that y_2 is a square in $\mathbb{Z}_{n^2}^*$

$(\alpha' + \beta' n \neq 0 \pmod{n^2}$ otherwise $\alpha' \notin \mathbb{Z}_n^*)$

b) Given $x_1 \in \mathbb{Z}_n^\times$ s.t. $x_1^2 = y_1 \in \mathbb{Z}_n^\times$.

We want that: $x_2^2 = (x_1 + \alpha n)^2 = y_1 + \beta n = y_2 \pmod{n^2}$

Hence, $x_2^2 = x_1^2 + 2\alpha n \pmod{n^2}$

$= y_1 + \underbrace{2\alpha n}_{\beta} + \gamma n$

Take $\alpha = \frac{\beta}{2}$ and then.

$x_2 = x_1 + \frac{\beta}{2} n$ will be a square root of.

$y_1 + \beta n \in \mathbb{Z}_{n^2}^\times$.

c) Define $f_1 : \mathbb{Z}_n^\times \longrightarrow \mathbb{Z}_n^\times$

$x \longmapsto x^2$

then f_1 is one way because for any PPTM adversary A:

$$\Pr\left[A(1^n, y) \in f_1^{-1}(y) \mid \exists x \in \mathbb{Z}_n^\times \text{ s.t. } y = x^2 \bmod n\right] \in \text{negl}(n)$$

and f_1 is efficiently computable.

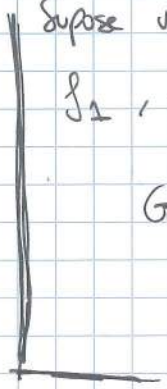
Define $f_2 : \mathbb{Z}_n^\times \longrightarrow \mathbb{Z}_n^\times$

$x \longmapsto x^2$.

then f_2 is efficiently computable and is one way because for any PPTM adversary A:

$$\Pr\left[A(1^n, y) \in f_2^{-1}(y) \mid \exists x \in \mathbb{Z}_n^\times \text{ s.t. } y = x^2 \bmod n^2\right] \in \text{negl}(n)$$

(d) Supose we have A_1 that breaks the one-wayness of f_1, that is:



Given $x^2 \in \mathbb{Z}_n^* \longmapsto x \in \mathbb{Z}_n^*$ (efficiently)

Now take $x^2 \in \mathbb{Z}_{n^2}^*$ (we don't know x).

1) Divide x^2 by n so that: $x^2 = r + \alpha \cdot n$, $\alpha \in \mathbb{Z}$, $r \in \mathbb{Z}_n^*$.
(Integer division) $(x^2 \in \mathbb{Z}_n^* \Rightarrow n \nmid x^2)$

2) Because x^2 was a square modulo n^2, $r = \bar{x}^2$ is a square mod n.
So we can apply A_1 and get (efficiently) $\bar{x}$

3) Finally built x as:

$$x = \bar{x} + \frac{\alpha n}{2} \pmod{n^2}.$$

→ This algorithm works because of step (b).

→ The success probability is the same because.

x square mod n^2 $\Rightarrow$ x square mod n

→ It's polynomial because all the aritmetic operations used and A_1 are polynomial.

e)

Now we get A_2 s.t:

$$x^2 \in \mathbb{Z}_{n^2}^{\times} \longrightarrow x \in \mathbb{Z}_{n^2}^{\times}$$

(efficiently)

We have now $x^2 \in \mathbb{Z}_n^{\times}$ and we want to compute $x \in \mathbb{Z}_n^{\times}$.

Define $y = x^2 \bmod n$

Consider $y \bmod n^2$ and add $\beta \in_R \mathbb{Z}_n$ s.t:

$$y + \beta n \bmod n^2$$

By (a) the previous expression is a square.

So we can apply A_2 and get $\alpha \in \mathbb{Z}_{n^2}^{\times}$ s.t.

$$\alpha^2 = y + \beta n \bmod n^2.$$

Divide α by n $\Rightarrow$ $\alpha = r + nk$

$$\Downarrow$$

$$\left[\alpha^2 = r^2 + 2nk \pmod{n^2}\right].$$

Then $\alpha \bmod n$ is the square root of y i.e x.

(2) (a) Take $G = \langle g \rangle$ prime order p.

$SK \leftarrow (x_1, x_2) \in_R \mathbb{Z}_q^2$.

$pk \leftarrow (g^{x_1}, g^{x_2})$.

~~$Enc_{(g^{x_1}, g^{x_2})} : G \times G \times G \longrightarrow G \times G \times G$~~

Given $m \in G$: $Enc_{(g^{x_1}, g^{x_2})} : G \times \mathbb{Z}_q \times \mathbb{Z}_q \longrightarrow G \times G \times G$

$$(m, r_1, r_2) \longmapsto (g^{x_1 r_1}, g^{x_2 r_2}, m g^{r_1 + r_2})$$

(b) $Dec_{(x_1, x_2)} : G \times G \times G \longrightarrow G$

$$(a, b, c) \longmapsto m'.$$

Compute x_1^{-1}, x_2^{-1} and then : $a^{x_1^{-1}}$, $b^{x_2^{-1}}$

Finally $m = \dfrac{c}{a^{x_1^{-1}} b^{x_2^{-1}}}$

If $a = g^{x_1 r_1}$, $b = g^{x_2 r_2}$, $c = m g^{r_1 + r_2}$ let's see that we can recover the message :

$$m' = \frac{c}{a^{x_1^{-1}} b^{x_2^{-1}}} = \frac{m g^{r_1 + r_2}}{\left(g^{x_1 r_1}\right)^{x_1^{-1}} \left(g^{x_2 r_2}\right)^{x_2^{-1}}} = \frac{m g^{r_1 + r_2}}{g^{x_1 x_1^{-1} r_1} g^{x_2 x_2^{-1} r_2}} =$$

$$= \frac{m \cancel{g^{r_1 + r_2}}}{\cancel{g^{r_1 + r_2}}} = m \quad \text{as we wanted.}$$

c) $Enc_{(g^{x_1}, g^{x_2})} : \mathbb{G} \times \mathbb{Z}_q \times \mathbb{Z}_q \longrightarrow \mathbb{G} \times \mathbb{G} \times \mathbb{G}$

$(m, r_1, r_2) \longmapsto (g^{x_1 r_1}, g^{x_2 r_2}, m g^{r_1 + r_2})$

Take $(m_1, r_1, r_2), (m_2, r_3, r_4) \in \mathbb{G} \times \mathbb{Z}_q \times \mathbb{Z}_q$

$(m_1, r_1, r_2) \circ (m_2, r_3, r_4) = (m_1 m_2, r_1 + r_3, r_2 + r_4) \xrightarrow{Enc}$

$\xrightarrow{Enc} \left(g^{x_1(r_1+r_3)}, g^{x_2(r_2+r_4)}, m_1 m_2 g^{r_1+r_2+r_3+r_4}\right) =$

$= \left(g^{x_1 r_1} g^{x_1 r_3}, g^{x_2 r_2} g^{x_2 r_4}, m_1 g^{r_1+r_3} m_2 g^{r_2+r_4}\right) =$

$= \left(g^{x_1 r_1}, g_2^{x_2 r_2}, m_1 g^{r_1+r_3}\right) \circ \left(g^{x_1 r_3}, g_2^{x_2 r_4}, m_2 g^{r_2+r_4}\right) =$

$= Enc_{(g^{x_1}, g^{x_2})}(m_1, r_1, r_2) \circ Enc_{(g^{x_1}, g^{x_2})}(m_2, r_3, r_4).$

d) - We can get ~~SE~~-OW because of CDH.

- [redacted]

- We can also get ~~SE~~-OW-CPA due to the randomness and CDH.

- But we cannot get ~~SE~~-OW-CCA because of the homomorphic properties.

- Due to the randomness included in the cypher function we can also get. ~~SE~~-LR.

1.

a) $y_2 = y_1 + \beta m$ is a square in $\mathbb{Z}_{m^2}^*$ $\Leftrightarrow$

$\exists\, a = a_1 + a_2 m \quad a_1, a_2 \in \mathbb{Z}_m^*$ st $a^2 = y_2 \Leftrightarrow$

$\Leftrightarrow \exists\, a = a_1 + a_2 m \quad a_1, a_2 \in \mathbb{Z}_m^*$ st $(a_1 + a_2 m)^2 = y_1 + \beta m \Leftrightarrow$

$\Leftrightarrow \exists\, a_1, a_2 \in \mathbb{Z}_m^*$ st $a_1^2 + 2a_1 a_2 m = y_1 + \beta m \Leftrightarrow$

$\Leftrightarrow a_1^2 \pmod m = y_1$ and $2a_1 a_2 + q \equiv \beta \mod m$

where $a_1^2 = qm + (a_1^2 \mod m)$

✓ As a_2 can be chosen to satisfy the 2nd equation then it is enough to have y_1 square in $\mathbb{Z}_m^*$

b) We want $y_2 = x_2^2 \pmod{m^2} \Rightarrow y_1 + \beta m = x_1^2 + 2\alpha x_1 m \pmod{m^2}$

$x_1^2 = qm + y_1$ by definition where $y_1 \in \mathbb{Z}_m^*$

$\Rightarrow \beta m = (q + 2\alpha x_1) m \mod m^2 \Rightarrow$

$\Rightarrow \beta = (q + 2\alpha x_1) \mod m \quad \beta \in \mathbb{Z}_m^*$

✓ So to compute α first compute $q = \frac{x_1^2 - y_1}{m}$

then as $\beta = (q + 2\alpha x_1) \mod m$

$\Rightarrow \alpha = \frac{\beta - q}{2x_1} \mod m$

c)

$f_1 : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ is a one way function if it is efficiently computable but,
$f_1(x) = x^2 \bmod n$

for any PPTM $\mathcal{A}$, $Pr[\mathcal{A}(\mathbb{Z}_n^\times, y)$ is a squareroot of y, for $x \in_R \mathbb{Z}_n^\times$ and $y \in_R \mathbb{Z}_n^\times] \in Negl(n)$

$f_2 : \mathbb{Z}_{n^2}^\times \to \mathbb{Z}_{n^2}^\times$ is a one way function if it is efficiently computable but,
$f_2(x) = x^2 \bmod n^2$

for any PPTM $\mathcal{A}$, $Pr[\mathcal{A}(\mathbb{Z}_{n^2}^\times, y)$ is a squareroot of y, for $x, y \in \mathbb{Z}_{n^2}^\times] \in Negl(n^2)$

d)

If $\mathcal{A}_1$ breaks f_1 ow with $Pr[\mathcal{A}_1 \text{ succeeds}] = \varepsilon$ then compute $\mathcal{A}_2(\mathbb{Z}_{n^2}^\times, y) = x$ as:

1. $y_1 = y \pmod n$ $\Theta(1)$ computing time
2. $x_1 = \mathcal{A}_1(\mathbb{Z}_n^\times, y_1)$ $Pr(\text{Succes}) = \varepsilon$ $\Theta(poly(n))$
3. $q = \dfrac{x_1^2 - y_1 \bmod n}{n}$ (fast computation at most $pol(n)$)
4. $\beta = \dfrac{y - y_1}{n} \bmod n$ $\Rightarrow$ f_1 is eff computable
5. $\alpha = \dfrac{\beta - q}{2x_1} \bmod n$
6. $x = \mathcal{A}_2(\mathbb{Z}_{n^2}^\times, y) = x_1 + \alpha n$

As steps 1, 3, 4, 5, 6 do not require too much computation time and are deterministic (always succeed, at least if the outcome of 2. is correct) then $Pr(\mathcal{A}_2 \text{ succeeds}) = \varepsilon$. Computational time $= \Theta(1) + 2\Theta(poly(n)) \in \Theta(poly(n))$

1.

e) If A_2 breaks ow of f_2 efficiently $\Rightarrow \Theta(\text{poly}(n))$, and $Pr(A_2 \text{ succeeds}) = \varepsilon$

then build A_1 as:

given $y \in \mathbb{Z}_n^*$

take y as an element of $\mathbb{Z}_{n^2}^*$

compute $x = A_2(\mathbb{Z}_{n^2}^*, y)$

take $x_1 = x \bmod n$

if $x^2 = y \bmod n^2$ then $x_1^2 = y \bmod n$

Not the right problem!

So, $Pr(A_1 \text{ succeeds}) = \varepsilon$ and computational time is $\Theta(1) + \Theta(\text{poly}(n)) = \Theta(\text{poly}(n))$

And we have a reduction

2.

a) Generate the key as follows

pick $x_1, x_2 \in \mathbb{Z}_q^*$ at random

$Sk = (x_1, x_2)$

generate and publish $(q, g, (g^{x_1}, g^{x_2}), G)$ pk

to encript

pick $r_1, r_2 \in \mathbb{Z}_q^*$ at random and compute

for a $pk = (y, z)$ and g the generator.

$Enc(m, pk, g, r_1, r_2) = (y^{r_1}, z^{r_2}, m \cdot g^{r_1+r_2})$ ✓

b) To decrypt follow (a, b, c)

$g^{r_1} = a^{+x_1^{-1}}$
$g^{r_2} = b^{+x_2^{-1}}$
} here Sk is used.

$m = c \cdot (g^{r_1} \cdot g^{r_2})^{-1}$

c) if $m_1, m_2 \in G$ are messages

then $Enc(m_1, pk, g, r_1, r_2) \cdot Enc(m_2, pk, g, r_3, r_4) =$

$= Enc(m_1 \cdot m_2, g, pk, \underbrace{r_1 + r_3}_{\tilde{r}_1}, \underbrace{r_2 + r_4}_{\tilde{r}_2})$

as $(y^{r_1} \cdot y^{r_3}, z^{r_2} \cdot z^{r_4}, m_1 \cdot m_2 \cdot g^{(r_1+r_2)} \cdot g^{(r_3+r_4)}) =$

✓ $(y^{\overbrace{r_1}^{\tilde{}}+r_3}, z^{\overbrace{r_2}^{\tilde{}}+r_4}, m_1 \cdot m_2 \cdot g^{\overbrace{r_1}^{\tilde{}}+r_3)+(\overbrace{r_2}^{\tilde{}}+r_4)})$.

d) Because of the homomorphic property it can not achieve IND - CPA ✓

However assuming CDH is hard ElGamal is OW-CPA

So as it is based on the same ideas I think this scheme is OW - CPA

In fact a reduction would be.

Given a CPA attacker against the OW of this scheme, A.

an attacker to ~~El Gamal~~ ~~DH CDH~~ B could be

Given ~~g, g^a, g^b~~ m_x and its encription $c_x = (pk, m_x) =$

$= (\tilde{g^r}, \tilde{y^r \cdot m_x})$

(✓) give as answer

$m_x = A(b, id, c \cdot)$ if g^x is also a generator this should work however I don't know which is the probability of this

so I cannot say this is a reduction.

8 -18/9,5/8 (8.5)

2. Let G be a cyclic group of prime order q and let $g \in G$ be a generator. Consider the following pk encryption scheme, where the secret key is a random pair $(x_1, x_2) \in \mathbb{Z}_q^2$, the public key is (g^{x_1}, g^{x_2}), and the encryptions of $m \in G$ are $(g^{x_1 r_1}, g^{x_2 r_2}, m g^{r_1+r_2})$, where $r_1, r_2 \in \mathbb{Z}_q$ are random.

a) Write the encryption algorithm in details.

$G = \langle g \rangle$, $M = G$, q prime $C = G \times G \times G$ $PK = G \times G$, $SK \in \mathbb{Z}_q^2$

KeyGen(ℓ)

$(x_1, x_2) \xleftarrow{\$} \mathbb{Z}_q^2$

$y \leftarrow (g^{x_1}, g^{x_2})$

$PK = y$, $SK = (x_1, x_2)$ ✓

Enc((G, q, g), y, m)

$(r_2, r_1) \xleftarrow{\$} \mathbb{Z}_q$

output $(g^{x_1 r_1}, g^{x_2 r_2}, g^{r_1+r_2} m)$

b) Describe the decryption procedure.

Dec((x_1, x_2), y, c)

$c = (c_1, c_2, c_3)$

compute $c_1' = c_1^{+x_1^{-1}}$, $c_2' = c_2^{+x_2^{-1}}$ ✗

output $c_3 c_1'^{-1} c_2'^{-1} = m$

c) Write a homomorphic property of the above encryption scheme.

$Enc(y, m_1) \cdot Enc(y, m_2) = (g^{x_1 r_1}, g^{x_2 r_2}, g^{r_1+r_2} m_1) \cdot (g^{x_1 r_1'}, g^{x_2 r_2'}, g^{r_1'+r_2'} m_2)$

$= (g^{x_1(r_1+r_1')}, g^{x_2(r_2+r_2')}, g^{(r_1+r_1')+(r_2+r_2')} m_1 m_2) \in Enc(e, m_1 m_2)$ ✓

$HomEval(c_1, c_2, (g^{x_1}, g^{x_2})) = c_1 c_2 (g^{x_1 r_1''}, g^{x_2 r_2''}, g^{r_1''+r_2''})$

$= (g^{x_1(r_1+r_1'+r_1'')}, g^{x_2(r_2+r_2'+r_2'')}, g^{(r_1+r_1'+r_1)+(r_2+r_2'+r_2'')})$

for r_1'' and r_2'' random in $\mathbb{Z}_q$

therefore $r_0' = r_1 + r_1' + r_1''$ is independent of r_1 and r_1'

and $r_0^2 = r_2 + r_2' + r_2''$ is independent of r_2 and r_2' ✓

d) Which security level do you think the scheme can achive?

Since it is homomorphic cannot achive the CCA

but it should achive the PKE-IND-CPA and PKE-OW-CPA

✓

1. (a) $\Rightarrow$ If $x_2^2 = y_1 + \beta n \bmod n^2$

$x_1^2 = y_1 \bmod n$ since $\beta n \equiv 0 \bmod n$

$\Downarrow$

$x^2 \equiv y_1 \bmod n$ ✓

$\Leftarrow$ If $y_1 = x^2 \bmod n$

$x^2 + \beta n \pmod n$

$\downarrow$ times n

$n y_1 = n x^2 + \beta n^2 \pmod{n^2}$ ✗

$\Downarrow$

$n x^2 = n y_1 + \beta n^2 \bmod n^2$

$\downarrow$ div by n

$x^2 = y_1 + \beta n \bmod n$ //

(b) $x_1^2 = y_1 \bmod n$

How to compute the square root $y_2 = y_1 + \beta n \bmod n^2$

of the form $x_2 = x_1 + \alpha n$

? $y_1 + \beta n \bmod n$

(c) $f_1\ Z_n^* \to Z_n^*$ $f_1(x) = x^2 \bmod n$ is a one way function because it is computable in polynomial time but the probability for all PPT A

$\Pr[Inv_{A,f}(y) \in f^{-1}(y)] \in negl(\ell)$

$\Pr[Inv(1^\ell, f(x)) = x] \in negl$ ← not negligible !!!

So given to A $y = x^2 \bmod n$ the probability of finding the preimage is negligible.

$f_2(x) = x^2 \bmod n^2$

The function is again polynomially computable and it is one way because

$\Pr[Inv(1^\ell, f(x)) = x] \in negl$.

where $f(x) = x^2 \bmod n^2$.

(d) If A_1 breaks the one-wayness of $f_1(x) = x^2 \bmod n$ we want to find A_2 breakup the one-wayness of $f_2(x) = x^2 \bmod n^2$.

we take $x^2 \bmod n^2$ and we sent it to A

A returns x_1 such that $f_1(x) = x^2 \bmod n$

so $x_2 = x_1 + \beta n$ is a square in Z_{n^2} by section (a).

(e) If A_2 breaks $f_2(x) = x^2 \bmod n^2$ and we have $f_1(x_1) = x_1^2 \bmod n$

We send to A_2 $x_1 + \beta n$ and ✓

by section (a) x_1 is a square root modulo n.

We have the same success probability since we are only running them once, and so if one gets right the other one must get the right answer as well.

(√)

2 (a) Key generation (sk, pk) : $G = \langle g \rangle$ with prime order p.

$sk = (x_1, x_2)$ where take $x_1, x_2 \in_R \mathbb{Z}_p$

$pk = (g^{x_1}, g^{x_2})$

Encryption: $c \leftarrow PKE.Enc(m, pk)$

compute $c_1 = (g^{x_1})^{r_1}$ $r_1 \leftarrow$ random $\in_R \mathbb{Z}_p$

compute $c_2 = (g^{x_2})^{r_2}$ $r_2 \leftarrow$ random $\in_R \mathbb{Z}_p$

compute $c_3 = m g^{r_1 + r_2}$

Define the ciphertext ~~$c = (c_1, c_2) \in G$~~

$c = (c_1, c_2, c_3) \in G^3$

(b) Decryption $m' \leftarrow PKE.Dec(C, sk)$ (x_1, x_2)

given a ciphertext

$c = (c_1, c_2, c_3)$ and the secret key (x_1, x_2)

$\tilde{m} = c_3 \cdot \left[c_1^{-x_1} \cdot c_2^{-x_2} \right]^{1/x_1 x_2}$

c) $Enc((g^{x_1}, g^{r_2}), m_1) \cdot Enc((g^{x_1}, g^{x_2}), m_2) =$

$= (g^{x_1 r_1}, g^{x_2 r_2}, m_1 g^{r_1 + r_2})(g^{x_1 r_3}, g^{x_2 r_4}, m_2 g^{r_3 + r_4}) =$

$= (g^{x(r_1 + r_3)}, g^{r_2(r_2 + r_4)}, m_1 m_2 g^{r_1 + r_2 + r_3 + r_4}) \in Enc(e, m_1, m_2)$

$HomEval((g^{x_1}, g^{x_2}), c_1, c_2) = c_1 c_2 (g^{x_1 r_5}, g^{x_2 r_6}, g^{r_5 + r_6})$

$= (g^{x_1 r}, g^{x_2 r'}, m_1 m_2 g^{r + r'})$

Therefore $r = r_1 + r_3 + r_5$ is independent of r_1 and r_3 and

$r' = r_2 + r_4 + r_6$ is independent of r_2 and r_4.

d) It can't get CCA security because of its homomorphic properties since it is the game defined for CCA security A is given $c \leftarrow Enc(pk, m_b)$ for either $b^* = 1$ or $b^* = 0$ and A has to guess which is the correct b.

But, due to homomorphic properties A can:

- compute $m' = m_0 \cdot \mu$ μ random and encrypt μ $c_\mu \leftarrow Enc(pk, \mu)$

Then $c' \leftarrow HomEval(pk, c_\epsilon, c_\mu)$

and using $O_{Dec}(c')$ A get m^*.

Now A only needs to compare m^* to m', if $m^* = m' \rightarrow b = 0$

else $\rightarrow b = 1$.

(2)

a) $G = \langle g \rangle$ of prime order q. This is public.

- Key generation:
  - Choose a random pair $(x_1, x_2) \in \mathbb{Z}_q^2$ (we can do it choosing $x_1, x_2 \in_R \mathbb{Z}_q$ independently)
  - Compute $g^{x_1} \in G$ and $g^{x_2} \in G$

  The secret key is (x_1, x_2) and the public one is (g^{x_1}, g^{x_2})

- Encryption: to encrypt a message $m \in G$
  - Choose $r_1, r_2 \in \mathbb{Z}_q$ at random
  - Compute $g^{x_1 r_1}$, $g^{x_2 r_2}$, $m \cdot g^{r_1 + r_2} \in G$

  The cipher text is $(g^{x_1 r_1}, g^{x_2 r_2}, m g^{r_1 + r_2})$

b) - Decryption: given the ciphertext $C = (C_1, C_2, C_3)$ and the secret key (x_1, x_2),

Compute $C_1^{x_2}$, $C_2^{x_1}$ and define $A = C_1^{x_2} \cdot C_2^{x_1}$

Compute $B = C_3^{-x_1 x_2}$

Compute $D = A \cdot B$

Compute the inverse of $x_1 x_2 \bmod q \to y$

Compute $D^{-y} \bmod q$

c) $\mathrm{Enc}(m_1) \odot \mathrm{Enc}(m_2) = (g^{x_1 (r_1 + r_1')}, g^{x_2 (r_2 + r_2')}, m m' \cdot g^{r_1 + r_1' + r_2 + r_2'})$

(componentwise operation; for some random $(r_1, r_2) \in \mathbb{Z}_q^2$; for some random $(r_1', r_2') \in \mathbb{Z}_q^2$)

$= \mathrm{Enc}(m'')$ where $m'' = m m'$

(for (r_1'', r_2'') random $\in \mathbb{Z}_q^2$) and $r_1'' = r_1 + r_1' \bmod q$

$r_2'' = r_2 + r_2' \bmod q$

(d) Because of the homomorphic property shown in (c), it will not be secure (in the sense of indistinguishability) against chosen ciphertext attacks.

↳ I can use the ~~oza~~ decryption oracle for $Enc(m_d \cdot m_b^*)$ and I can check if it is $m_d \cdot m_d$ or $m_d \cdot m_2$.

✓

However it ~~can~~ be secure against chosen plaintext attacks.

(V) ((Maybe PE ~~can~~ be PKE-OW-CPA secure under CDH assuption and PKE-IND-CPA secure under DDH assumption.))

It can be PKE-IND-CPA secure because it is not deterministic.

EXERCISE 1

a) $\forall \beta \in \mathbb{Z}_n$, $y_1 \in \mathbb{Z}_n^*$ $\quad y_2 = y_1 + \beta n$ is a square $\Leftrightarrow$ y_1 is a square in $\mathbb{Z}_n^*$ / in $\mathbb{Z}_{n^2}^*$

$\Rightarrow$ $\exists\, x_2 \in \mathbb{Z}_{n^2}^*$ s.t. $x_2^2 = y_2 = y_1 + \beta n \mod n^2 \Rightarrow$

$\Rightarrow x_2^2 = y_2 = y_1 \mod n$ ✓

then y_1 is a square ($(x_2)^2$) in $\mathbb{Z}_n^*$

$\Leftarrow$ y_1 is a square in $\mathbb{Z}_n^* \Rightarrow \exists\, x_1 \in \mathbb{Z}_n^*$ s.t. $x_1^2 = y_1 \mod n$

$\Rightarrow y_2 = y_1 + \beta n \mod n^2 \Leftrightarrow y_2 = x_1^2 + \beta n \mod n^2$ ✗ ✓

$\Rightarrow y_2 = (x_1 + \alpha n)^2$ s.t. $2\alpha = \beta \Rightarrow \alpha = \beta \cdot 2^{-1}$

$x_1^2 + 2\alpha n + \alpha^2 n^2 \to 0$

(since $2 \nmid n^2 = (pq)^2$, $p>2$, $q>2$, there exists 2^{-1})

and then y_2 is a square in $\mathbb{Z}_{n^2}$

b) $x_1 \in \mathbb{Z}_n^*$ s.t. $x_1^2 = y_1$ in $\mathbb{Z}_n^*$, show how to compute a square root of $y_2 = y_1 + \beta n \in \mathbb{Z}_{n^2}^*$ of the form $x_2 = x_1 + \alpha n$ (✓)

(the same procedure as the implication $\Leftarrow$)

$x_1^2 = y_1 \mod n \Rightarrow$ We want a square root x_2 of y_2 $(\Rightarrow x_2^2 = y_2)$

$y_2 = x_2^2 = (x_1 + \alpha n)^2 = x_1^2 + 2\alpha n + \alpha^2 n^2 = x_1^2 + 2\alpha n \mod n^2$

$\alpha^2 n^2 \to 0 \mod n^2$

then, since $x_1^2 = y_1 \mod n$ we get $2\alpha = \beta$ and then $\alpha = \beta \cdot 2^{-1}$

If x_1 is a square root of y_1, $x_2 = x_1 + \beta(2^{-1}) \cdot n$ is a square root of y_2

c) Write a formal statement saying that $f_1 : \mathbb{Z}_n^\times \longrightarrow \mathbb{Z}_n^\times$ such that $f_1(x) = x^2 \bmod n$ is one way function. The same for $f_2(x) = x^2 \bmod n^2$.

The function $f_1 : \mathbb{Z}_n^\times \longrightarrow \mathbb{Z}_n^\times$, $x \longmapsto x^2 \bmod n$ is efficiently computable,

it requires polynomial time. But for all PPTM A

✓ $\Pr\left[A(1^\ell, y) \in f_1^{-1}(y) \mid x \in \mathbb{Z}_n^\times,\ y \leftarrow x^2 \right) \in \text{negl}(\ell)$

the function $f_2 : \mathbb{Z}_n^\times \longrightarrow \mathbb{Z}_n^\times$, $x \longmapsto x^2 \bmod n^2$ is efficiently computable,
~~and~~
and for all PP turing machine A

✓ $\Pr\left(A(1^\ell, y) \in f_2^{-1}(y) \mid x \in \mathbb{Z}_{n^2},\ y \leftarrow x^2 \right) \in \text{negl}(\ell)$

d) Build a polynomial time algorithm A_2 that breaks one-wayness ~~function~~ of f_2 from any alg. A_1 that breaks the one-way of f_1.

✓ Suppose ~~we ha~~ there is an algorithm A_1 such that

$y \in \mathbb{Z}_n^\times \longrightarrow \boxed{A_1} \longrightarrow x \in \mathbb{Z}_n^\times$ s.t. $x^2 = y \bmod n$

~~we write~~ we write $y = y_1 + \beta n$ for some $y_1, \beta \in \mathbb{Z}_n^\times$

Then using A_1 compute x_1 s.t. $x_1^2 = y_1 \bmod n$.

(✓) Then write $x_2 = x_1 + 2^{-1}\beta n$ as in (b)

We have obtained ~~the~~ the ~~inverse of~~ value of $f_2^{-1}(y)$

This breaks one-wayness of f_2 with the same probability

EXERCISE 1

e) Show now a similar reduction working the other direction.

Suppose there exists A_2 s.t.

$$y \in \mathbb{Z}_{n^2} \longrightarrow \boxed{A_2} \longrightarrow x \in \mathbb{Z}_n \text{ s.t. } x^2 = y \bmod n^2.$$

Let $y \in \mathbb{Z}_{n^2}$ and $x \in \mathbb{Z}_{n^2}$ such that $x^2 = y \bmod n^2$

✓ for some $\beta \in \mathbb{Z}_n$ $y_1 = y - \beta n \Rightarrow$ * (By (a) since y is a square y_1 would be a square)

Take $y_1 = y - \beta n \bmod n^2$

$y_1 = y \bmod n \Rightarrow x^2 = y_1 \bmod n$.

✓

We have broken the one-wayness of f_1.

EXERCISE 2:

G cyclic group of prime order q. $G = \langle g \rangle$

a) ENCRYPTION ALGORITHM

Let G be a cyclic group of prime order q, and $G = \langle g \rangle$.

- Key generation: $(SK, PK) \leftarrow \Sigma.KG(1^k)$

✓ Take $(x_1, x_2) \in_R \mathbb{Z}_q^2$ the p

Compute (g^{x_1}, g^{x_2}).

$PK = (q, G, g, g^{x_1}, g^{x_2})$ and $SK = (x_1, x_2)$

output pk;

- $Enc(m, g^{x_1}, g^{x_2})$

✓ Take $(r_1, r_2) \in_R \mathbb{Z}_q^2$

output $(g^{x_1 r_1}, g^{x_2 r_2}, m g^{r_1 + r_2})$

b) DECRYPTION PROCEDURE $Dec(g^{x_1 r_1}, g^{x_2 r_2}, m \cdot g^{r_1 + r_2})$

$g_1 \leftarrow (g^{x_1 r_1})^{x_2}$

✓ $g_2 \leftarrow (g^{x_2 r_2})^{x_1}$

$k \leftarrow (x_1)^{-1} \cdot (x_2)^{-1}$

$\bar{g} \leftarrow (g_1 \cdot g_2)^k$

output $m \cdot g^{r_1 + r_2} \cdot (\bar{g})^{-1}$

$g_1 \cdot g_2 = g^{x_1 x_2 r_1} \cdot g^{x_1 x_2 r_2} = g^{x_1 x_2 (r_1 + r_2)}$

$(g_1 \cdot g_2)^k = \left(g^{x_1 x_2 (r_1 + r_2)}\right)^{(x_1 x_2)^{-1}} = g^{r_1 + r_2}$

$m \cdot g^{r_1 + r_2} \cdot g^{-(r_1 + r_2)} = m$

c) HOMOMORPHIC PROPERTY

$$Enc(m_1, g^{x_1}, g^{x_2}) \cdot Enc(m_2, g^{x_1}, g^{x_2}) = \left(g^{x_1 r_1^1}, g^{x_2 r_2^1}, m_1 g^{r_1' + r_2'}\right) \cdot \left(g^{x_1 r_1^2}, g^{x_2 r_2^2}, m_2 g^{r_1^2 + r_2^2}\right)$$

$$= \left(g^{x_1 (r_1' + r_2^2)}, g^{x_2 (r_2^1 + r_2^2)}, m_1 \cdot m_2 \cdot r^{(r_1' + r_1^2) + (r_2' + r_2^2)}\right) =$$

$$= Enc\left(m_1 \cdot m_2, g^{x_1}, g^{x_2}\right)$$

strongly homomorphic $Dec(sk, \cdot) : G^3 \to G^3$

?

d) SECURITY LEVEL

This scheme is not very secure. For instance is not secure against chosen ciphertext attacks.

If an adversary A can decipt $c_1 \to m_1$ for instance
$c_2 \to m_2$
then he can decipt
$c_1 \cdot c_2 \to m_1 \cdot m_2 \to$ (is a succesful attack).

(2)

$$\boxed{\text{KeyGen}} \longrightarrow (pk, sk) \in PK_l \times SK_l$$

$$pk \in PK_l,\ m \in M_l \mapsto \boxed{\text{Enc}} \longrightarrow c \in C_l$$

$$sk \in SK_l,\ c \in C_l \mapsto \boxed{\text{Dec}} \longrightarrow m' \in M_l \cup \{\perp\}$$

$pk : (g^{x_1}, g^{x_2})$

$sk : (x_1, x_2)$ $\quad x_1, x_2$ random

encryptions of M : $(g^{x_1 r_1}, g^{x_2 r_2}, M g^{r_1 + r_2})$ $\quad r_1, r_2$ random

(a)

~~Eg~~ Encryption:

Players: Alice & Bob. Alice transmits her public key (g^{x_1}, g^{x_2}) to Bob, and keeps the secret key (x_1, x_2) secret. Bob then wishes to send message M to Alice.

He first turns M into an integer m, such that $0 \leq m \leq n$ by using an agreed-upon reversible protocol (padding scheme). He then computes the ciphertext c corresponding to ~~$c \equiv m^e \pmod{n}$~~.

Bob then transmits c to Alice.

(b) Decryption : Alice can recover M from C by using her secret key $d = (x_1, x_2)$ via computing

$$M = C^d \pmod{n}$$

Given M, she can recover the original message by reversing the padding scheme.

(c) Strongly Homomorphic
Multiplicatively homomorphic

1.a) $\forall \beta \in \mathbb{Z}_n$

$y_1 \in \mathbb{Z}_n^*$

$y_2 = y_1 + \beta n$ is a square in $\mathbb{Z}_{n^2}^*$ $\iff$ y_1 is a square in $\mathbb{Z}_n^*$

? $\forall \beta \in \mathbb{Z}_n$, so $\beta \cdot n$ is not a square in $\mathbb{Z}_{n^2}$

So, we must prove

y_2 is a square in $\mathbb{Z}_{n^2}^*$

$\Updownarrow$

y_1 is a square in $\mathbb{Z}_n^*$

~~If y_1 is not a square in $\mathbb{Z}_n^*$~~

~~then y_1 can not be a square~~

1.b) $x_1 \in \mathbb{Z}_n^*$ (square root)

$y_1 \in \mathbb{Z}_n^*$

show how to compute a square root of $y_2 = y_1 + \beta n \in \mathbb{Z}_{n^2}^*$ of the form $x_2 = x_1 + \alpha n$

SR algorithm: $A(y_1) \longrightarrow x_1$

$A(y_2) \longrightarrow x_2$

We know that $y_2 = y_1 + \beta n$

So $A(y_1 + \beta n) \longrightarrow x_1 + \alpha n$

c) $f_1 : \mathbb{Z}_n^x \longrightarrow \mathbb{Z}_n^x \mid f_1(x) = x^2 \bmod n$

is a one way function:

$\Updownarrow$ $\forall \exists$ PPTM

$\varepsilon_1 = P_r\left[A_1(f_1(x)) \in f_1^{-1}(f_1(x)),\ x \leftarrow X\right] \in$ Negligible

$f_2 : \mathbb{Z}_{n^2}^x \longrightarrow \mathbb{Z}_{n^2}^x \mid f_2(x) = x^2 \bmod n^2$

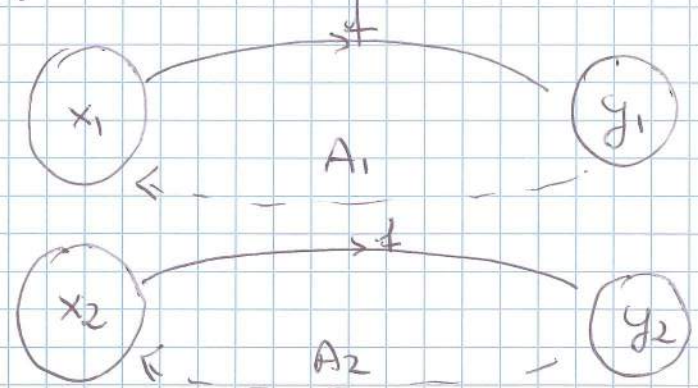
$\varepsilon_2 = P_r\left[A_2(f_2(x)) \in f_2^{-1}(f_2(x)),\ x \leftarrow X\right] \in$ Negli.

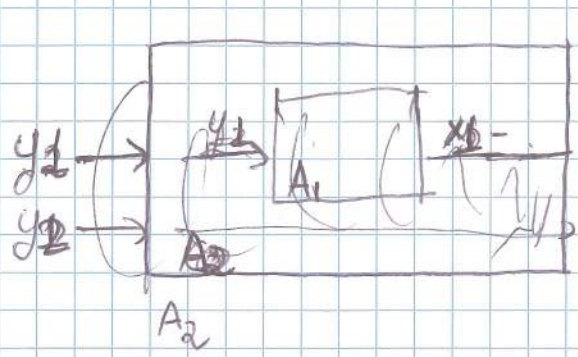
d) Imagine we have A_1 that gives $\in f_1^{-1}(f(x))$

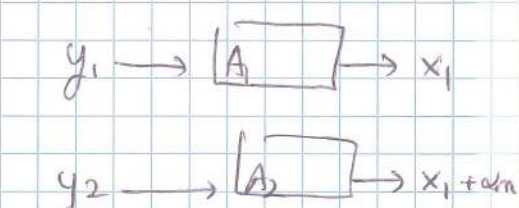
and e) To have the same success probability we must use only once A_1.

$A_1(y_1) = x_1$

$A_2(y_2) = x_2 = x_1 + \alpha n$







$A_2 = A_1(\ldots)$

$A_1(y_1) + \alpha n = x_1 + \alpha n$

$\|$ $\|$

$A_2(y_2) = x_2$

$\Downarrow$

$\varepsilon_1 = \varepsilon_2$

2. $g \in G$

SK: $(x_1, x_2) \in \mathbb{Z}_q^2$

PK: (g^{x_1}, g^{x_2})

Enc of m: $(g^{x_1 r_1}, g^{x_2 r_2}, m g^{r_1 + r_2})$ $r_1, r_2 \in \mathbb{Z}_q$ are random.

a) Key Gen (e)

(G, q, g)

$x_1, x_2 \leftarrow \mathbb{Z}_q^2$

$y_1, y_2 \leftarrow g^{x_1}, g^{x_2}$

output (x_1, x_2, y_1, y_2);

Enc (param, y_1, y_2, m)

$r_1, r_2 \leftarrow \mathbb{Z}_q$ $\quad c_1 = g^{x_1 r_1}$, $\quad c_2 = g^{x_2 r_2}$, $\quad c_3 = m g^{r_1 + r_2}$

output (c_1, c_2, c_3)

b) Dec (param, $x_1, x_2, (c_1, c_2, c_3)$):

output $\rightarrow$ m

$g^{x_1 r_1} \cdot (g^{x_2 r_2})^{-1}$

Dec: output $= \dfrac{c_3}{c_1^{+x_1} \cdot c_2^{+x_2}}$

$\dfrac{m g^{r_1 + r_2}}{g^{r_1} \cdot g^{r_2}} \equiv$ randomnes cancel out!!

The continuation of exercise 2.

MAMME. FME. UPC
Titulació

CODIS I CRIPTOGRAFIA
Assignatura

(3)

c) Homomorphic property: $output_A(g^{x_{1A}r_{1A}}, g^{x_{2A}r_{2A}}, m_A g^{r_{1A}+r_{2A}})$

Dec: (param, $x_1, x_2, c_1, c_2 c_3$) $output_B$ $(g^{x_{1B}r_B}, g^{x_{2B}r_{2B}}, m_B g^{r_{1B}+r_{2B}})$

$Dec(x_1, x_2, c_1, c_2, c_3) \overset{??}{=} Dec(x_{1A}, x_{2A}, c_{1A}, c_{2A}, c_{3A}) \cdot Dec(x_{1B}, x_{2B}, c_{1B}, c_{2B}, c_{3B})$

$$\frac{c_3}{c_1^{-x_1} \cdot c_2^{-x_2}} \overset{??}{=} \frac{c_{3A}}{c_{1A}^{-x_{1A}} c_{2A}^{-x_{2A}}} \cdot \frac{c_{3B}}{c_{1B}^{-x_{1B}} c_{2B}^{-x_{2B}}}$$

(??) ≡ if is true the homomorphic propertie of $\cdot$ is OK.

$\Leftrightarrow$ ~~$c_{3A} \cdot c_{3B}$~~

$g^{x_1 r_1} = c_1 = c_{1A} = c_{1B}$

$g^{x_2 r_2} = c_2 = c_{1A} = c_{1B}$

$c_3 = m_A \cdot m_B\, g^{2(r_1+r_2)}$

$c_{3A} = m_A\, g^{r_1+r_2}$

$c_{3B} = m_B\, g^{r_1+r_2}$

$\Big\} \; c_{3A} \cdot c_{3B} = m_B\, g^{2(r_1+r_2)}$

$c_{1A}^{-x_1} \cdot c_{1B}^{x_1} = c_1^2 = g^{2x_1 r_1}$ by the properties of the cyclic group, we can find $e \mid 2e = 1 \bmod q$ so I can write $g^{x_1 r_1}$ instead of $g^{2x_1 r_1}$.

The same for c_2^2. ⟹

Finally we obtain:

$$\frac{C_3}{C_1^{-x_1}\, C_2^{-x_2}} = \frac{C_{3A} \cdot C_{3B}}{C_{1A}^{-x_1}\, C_{2A}^{-x_2}\; C_{1B}^{-x_1}\; C_{1B}^{-x_2}}$$

Exercise (2)

(a) Encryption algorithm

Input: • a message $m \in M$

• a public key $pk = (y_1, y_2)$

• Pick $(r_1, r_2) \in \mathbb{Z}_q^2$ at random with a uniform distribution.

$c_1 := y_1^{r_1}$

$c_2 := y_2^{r_2}$

$c_3 := m \cdot \frac{c_1}{y_1}, \frac{c_2}{y_2}$

Send $c = (c_1, c_2, c_3)$

(b) Decryption procedure

Input: $(c_1, c_2, c_3) = c$

~~Public~~ key $sk = (g^{x_1}, g^{x_2})$

Secrete key $= (x_1, x_2)$

return $m := \frac{c_3 \cdot g^{x_1+x_2}}{c_1 \cdot c_2}$

prove of correctness:

$$\frac{c_3 g^{x_1+x_2}}{c_1 \cdot c_2} = \frac{m \cdot g^{r_1+r_2} g^{x_1} g^{x_2}}{g^{x_1 r_1} g^{x_2 r_2}} = \frac{m \cdot g^{r_1} g^{r_2}}{g^{r_1} g^{r_2}} = m$$

(c) $Enc(r_1, q_1, m_1) \cdot E(r_2, q_2, m_2) = (g^{x_1 r_1}, g^{x_2 r_2} m_1 \cdot g^{r_1+q_1})$.
$(g^{x_2 r_2}, g^{x_2 q_2}, m_2 \cdot g^{q_2+r_2}) = (g^{x_1(r_1+r_2)}, g^{x_2(q_1+q_2)}, m_1 m_2 g^{r_1+r_2+q_1+q_2})$

$\overset{\epsilon}{=} E(r_1+r_2, q_1+q_2, m_1 \cdot m_2)$.

It implies $Dec(C_1 \cdot C_2) = Dec(C_1) \cdot Dec(C_2)$.

(d) The code break against:

(i) Adversary A wants to decode any message with an oracle

(ii) Adversary A wants to decode an arbitrary message of his choice with the encoding of two differents messages.

proof. (i) Let m^* be the message to decrypt from a encoding C^*. We can write

$C^* = C_1^* \cdot C_2^*$

for appropriate non-empty $m_1^*, m_2^* \in M$.

Using the oracle, we find

$m_1^* = Dec(C_1^*)$

$m_2^* = Dec(C_2^*)$

We conclude $m^* = m_1^* \cdot m_2^*$.

(ii) Let (m_1^*, C_1^*) and (m_2^*, C_2^*) be the couples of messages whom A knows the encoding. We have

$Dec(C_1^* \cdot C_2^*) = m_1^* \cdot m_2^*$

So A can decode the new message $m_1^* m_2^*$.

(2) a) First we fix some notations for the keys

KeyGen(ℓ)

$(G, q, g) \leftarrow \text{InstGen}(\ell)$;

$x_1 \leftarrow \mathbb{Z}_q$;

$x_2 \leftarrow \mathbb{Z}_q$;

param $\leftarrow (G, q, g)$;

output $((g^{x_1}, g^{x_2}), (x_1, x_2))$; // we could also use $y_1 = g^{x_1}$, $y_2 = g^{x_2}$ as notation

Now the encryption

Enc(param, (g^{x_1}, g^{x_2}), m): // using ↑, this is also (param, (y_1, y_2), m)

$r_1 \leftarrow \mathbb{Z}_q$;

$r_2 \leftarrow \mathbb{Z}_q$;

output $(g^{r_1 r_2}, g^{x_2 r_2}, m g^{r_1 + r_2})$; // using ↑, this is also $(y_1^{r_1}, y_2^{r_2}, m g^{r_1 + r_2})$

b) The decryption would be as follows:

- we know $x_1, x_2 \in \mathbb{Z}_q$ (we can assume they are in $\mathbb{Z}_q^*$, otherwise $g^{x_i} = g$, not very good for security). Then we can compute $z_1, z_2 \in \mathbb{Z}_q$ s.t. $x_1 z_1 \equiv x_2 z_2 \equiv 1 \pmod q$
- On receiving (c_1, c_2, c_3), we compute $c_1^{z_1}$ and $c_2^{z_2}$, multiply them and divide c_3 by this product.

In details:

Dec(param, (x_1, x_2), (c_1, c_2, c_3)):

$z_1 \leftarrow x_1^{-1} \pmod q$

$z_2 \leftarrow x_2^{-1} \pmod q$

output $(c_1^{z_1} c_2^{z_2})^{-1} c_3$

c) We have $Enc(param, (y_1,y_2), m_1) Enc(param, (y_1,y_2), m_2)$

$\in Enc(param, (y_1,y_2), m_1 m_2)$ ✓

We'll write $Enc(m)$ for $Enc(param, (y_1,y_2), m)$ to lighten the notation from now on.

Write $Enc(m_1) = (g^{r_1 r_3}, g^{r_2 r_2}, m_1 g^{r_3 + r_2})$

$Enc(m_2) = (g^{r_1 r_1'}, g^{r_2 r_2'}, m_2 g^{r_1' + r_2})$

Then, if we choose r_3 and r_4 indepent from each other and independent from r_1, r_1' and r_2, r_2', then $r = r_1 + r_1' + r_3$ and $r' = r_2 + r_2' + r_4$ are respectively independent from them too. ✓ respectively

So $HomEval(param, (y_i,y_i), c_1, c_2) = c_1 c_2 \cdot (g^{r_1 r_3}, g^{r_2 r_4}, g^{r_3 + r_4})$ is the function that gives the strongly homomorphic property, since the probability distributions are the same.

d) Homomorphic properties suggest it cannot get the highest levels of security, indeed ✓ it is not IND-CCA secure.

To guess $b \in \{0,1\}$ from $(g^{r_1 r_1}, g^{r_2 r_2}, m_b g^{r_1 + r_2})$ (the classical IND-CCA game)

Compute $(1, 1, \mu)(c_1, c_2, c_3)$ with μ a message of your choice, decrypt $(c_1, c_2, \mu c_3)$ and compare the result to μm_0. Output '0' if it's the same and '1' otherwise.

✓ It seems like it could achieve IND-CPA.

(2) G order q

$sk \to (x_1, x_2) \in \mathbb{Z}_q^2$

$pk \to g^{x_1} g^{x_2}$

Enc. of m are $(g^{x_1 r_1}, g^{x_2 r_2}, m g^{r_1+r_2})$, $r_1, r_2 \in \mathbb{Z}_q$ at Random

a) Encription Algorithm

- Key generation

$(\{sk_i\}\{pk\}) \leftarrow [x_1, x_2] \in \mathbb{Z}_q^2, (g^{x_1} g^{x_2})$

$G = \langle g \rangle$ has a prime order q.

Take $x_1, x_2 \in_R \mathbb{Z}_q$ and compute $y_1 = g^{x_1}$, $y_2 = g^{x_2}$

- Encryption $c \leftarrow E(m, pk)$

(1) Choose $r_1, r_2 \in_R \mathbb{Z}_q$ at random and compute

~~$c_1 = g^{r_1}$ $c_2 = g^{r_2}$~~ $c = m g^{r_1+r_2}$

~~$f(x_1 r_1, x_2 r_2)$~~ $a = x_1 r_1$ ~~$b = x_2 r_2$~~

Output (a, b, c).

b) ~~$m = c \cdot g^{-(r_1+r_2)} \cdot g^{-(r_1+r_2)} \bmod q$~~

Output $m = c \cdot g^{-a} \cdot g^{-b} \bmod q$

Desc ~~(c_1, c_2, a, b)~~ (c, a, b)

$m = c \cdot g^{-a} g^{-b} \bmod q$

c) homomorphic property: ~~$f(mg, g^{x_1 r_1}, g^{x_2 r_2}, mg^{r_1+r_2})$~~

~~$f((x_1 x_2), (r_1 r_2))$~~ ~~$f(m, x_1 r_1, x_2 r_2)$~~

Gamal: $Enc(x, m_1) \cdot Enc(x, m_2) = (g^{r_1}, x^{r_1} m_1)(g^{r_2}, y^{r_2} m_2)$

- We have: $Enc(y, m_1) \cdot Enc(y, m_2) = (g^{x_1 r_1}, g^{x_2 r_2} m_1 g^{r_1+r_2}) \cdot (g^{x_3 r_3}, g^{x_4 r_4}, m_2 g^{r_3+r_4}) = (g^{x_1 r_1 + x_3 r_3}, g^{x_2 r_2 + x_4 r_4}, g^{r_1+r_2+r_3+r_4} m_1 \cdot m_2)$

✓

$\epsilon \neq Enc(e, m_1 m_2)$ $\quad Encr.\left(g^{n x_1 r_1}, g^{n x_2 r_2}, g^{n(r_1+r_2)} m\right)$

~~we have $(g^x g^y g^z m^n)$~~

~~$x = x_1 r_1 + x_2 r_2 + \ldots x_n r_n$~~

$y =$

d) This scheme is not secure.

we can ~~compute~~ known $r_1 r_2$ with CCA Game. ✓

if we have $g^s = g^r g^{xh}$

$g^{s'} = g^r g^{xh'}$

$g^{ss'} = g^{x(h-h')} \Rightarrow \frac{s-s'}{h-h'} = x$

We can ~~to~~ put a Hash function $g^s = Kg^{H(m,R)}$

(2)

a) Encryption: - Input: $g \in G$ of a cyclic group G

and the ~~public~~ secret key ~~(g^{x_1}, g^{x_2}) $(x_1, x_2) \in \mathbb{Z}_q^2$~~

- Choose at random $r_1, r_2 \in \mathbb{Z}_q$

- Encrypt the message $m \in G$ as

~~xxx~~ $c = m \cdot g^{r_1 + r_2}$.

~~Output~~ - Compute $a = g^{x_1 r_1}$, $b = g^{x_2 r_2}$

- Output (a, b, c).

b) Decryption: Given (a, b, c) and the ~~ph = (g, g^{x_1}, g^{x_2})~~

Output: $m = c \cdot g^{-a} \cdot g^{-b} \mod q$

c) Homomorphic property:

$Enc(pk, m_1) \cdot Enc(pk, m_2) = (g^{x_1 r_1^1}, g^{x_2 r_2^1}, m_1 g^{r_1^1 + r_2^1}) \cdot (g^{x_1 r_1^2}, g^{x_2 r_2^2}, m_2 g^{r_1^2 + r_2^2})$

$= (g^{x_1(r_1^1 + r_1^2)}, g^{x_2(r_2^1 + r_2^2)}, m_1 \cdot m_2 \cdot g^{(r_1^1 + r_2^1 + r_1^2 + r_2^2)})$

$\in$

$= Enc(pk, m_1 \cdot m_2)$.

d) The scheme can not achieve IND-CCA-security, because no homomorphic scheme can.

This is because CCA means the attacker A chooses two messages m_1 and m_2 and is given a ciphertext c_b for $b = 0$ or 1 (randomly chosen).

So A could call the oracle for an encryption of another message M to get an encryption of $m' = m_0 \cdot M$.

Let this encryption be $c' = \underbrace{Enc(m_0) \cdot Enc(M)}_{\text{homomorphic}} = c_0 \cdot c_M$

If $c_b = c'$ then $b = 0$, else it is 1.

But perhaps the scheme could be IND-CPA.

Given two ciphertexts $c_1 = (m_1 g^{r_1 + r_2})$ and $c_0 = (m_0 g^{r_1' + r_2'})$ and $m_b, b \in_R \{0, 1\}$ it is impossible for A to decide whether m_1 or m_0 has been encrypted.