Anish Banerjee, Shankh Gupta
COL759: Cryptography

Problem Set - 3
October 2023

Problem 1: CPA with Very Weak Ciphertext Integrity

Solution: We define our encryption scheme $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$ as follows :

$$\mathsf{Enc}(k, m; r) = (r, F(k, r) \oplus m, F(k, m))$$

and

$$\mathsf{Dec}(k, \mathsf{ct}) = F(k, \mathsf{ct}_0) \oplus \mathsf{ct}_1$$

where $\mathsf{ct} = (\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{ct}_2)$.
Here, the key space $\mathcal{K} = \{0,1\}^n$ and message space $\mathcal{M} = \{0,1\}^n$, the random space $\mathcal{R} = \{0,1\}^n$ and the ciphertext space is $\mathcal{C} = \{0,1\}^{3n}$.

To prove the CPA security of $\mathcal{E}$, we will create the following Hybrid-World Structure :

World-b :

- The challenger $\mathcal{C}$ samples a key k and a random string r.
- The Adversary $\mathcal{A}$ sends polynomially many queries to the challenger. For each query (m_{i0}, m_{i1}), the challenger responds by sending $\mathsf{Enc}(k, m_{ib})$ to $\mathcal{A}$.
- Finally $\mathcal{A}$ sends a bit b' as its output to the challenger.

$$\text{Let } \Pr[b' = 0] = p_b.$$

Hybrid-World-b:

- The challenger $\mathcal{C}$ samples a key k and a random string r. It also samples a uniformly random function $f \leftarrow Func[\mathcal{X}, \mathcal{Y}]$ (where $\mathcal{X}, \mathcal{Y} = \{0,1\}^n$).
- The Adversary $\mathcal{A}$ sends polynomially many queries to the challenger. For each query (m_{i0}, m_{i1}), the challenger responds by sending $(r_i, f(r_i) \oplus m_{ib}, f(m_i))$ to $\mathcal{A}$.
- Finally $\mathcal{A}$ sends a bit b' as its output to the challenger.

$$\text{Let } \Pr[b' = 0] = p_{\mathsf{Hyb}-b}.$$

Claim 1: $p_{\mathsf{Hyb}-0} = p_{\mathsf{Hyb}-1}$

Proof. This follows from the fact that in the Hybrid-World-0 and Hybrid-World-1, $f(.)$ is sampled uniformly randomly and therefore using the security of Shannon's OTP, we can say that $p_{\mathsf{Hyb}-0} = p_{\mathsf{Hyb}-1}$. □

Claim 2: $|p_b - p_{\mathsf{Hyb}-b}|$ is negligible

Proof. We can show the contra-positive by creating a reduction $\mathcal{B}$ such that, if there exists a ppt. adversary $\mathcal{A}$ which can distinguish between p_b and $p_{\mathsf{Hyb}-b}$ with non-negligible probability, the using $\mathcal{A}$, the reduction $\mathcal{B}$ can break the PRF security with non-negligible advantage.
The reduction $\mathcal{B}$ works as follows :

- The reduction receives (m_{i0}, m_{i1}) from the adversary. It samples a $r_i \leftarrow \mathcal{R}$ and forwards r_i and m_{ib} one by one to the PRF challenger.
- The reduction receives y_i and z_i from the challenger. It then forwards $(r, y_i \oplus m_{ib}, z_i)$ to the adversary $\mathcal{A}$.
- Finally, the reduction receives b' from the advesary. It forwards b' to the PRF challenger.

If the PRF challenger chooses $F(k, \cdot)$ (i.e. psuedorandom), then that corresponds to World-b for the adversary $\mathcal{A}$ and it sends $b' = 0$ with probability p_b. On the other hand, if the challenger chooses $f(.)$ (i.e. truly random), then that corresponds to Hybrid-World-b for the adversary and it sends $b' = 1$ with probability $p_hyb - b$. So the winning advantage of the reduction $\mathcal{B}$ would then become :

$$\mathsf{PRFAdv}[\mathcal{B}, \mathcal{F}] = |p_b - p_{\mathsf{Hyb}-b}|$$

So, if $|p_b - p_{\mathsf{Hyb}-b}|$ is non-negligible, then our reduction $\mathcal{B}$ can win the PRF game with non-negligible advantage. Hence $|p_b - p_{\mathsf{Hyb}-b}|$ is negligible.
□

So using the above two claims, we can say that :

$$\mathsf{CPAAdv}[\mathcal{A}, \mathcal{E}] = |p_0 - p_1| = \epsilon$$

To prove the Very Weak Ciphertext Integrity of $\mathcal{E}$, we will setup two games as follows :

Game 0 :

- The challenger encrypts the messages using the encryption scheme $\mathcal{E}$.
- The adversary sends a ciphertext ct to the challenger. The adversary wins if ct is a valid ciphertext.

Let Pr[A wins Game 0] $= p_0$

Game 1 :

- The challenger encrypts the messages using the encryption scheme :

  $$\mathsf{Enc}(k, m) = (r, f(r) \oplus m, f(m))$$

  where f is a uniformly random function.
- The adversary sends a ciphertext ct to the challenger. The adversary wins if ct is a valid ciphertext.

Let Pr[A wins Game 1] $= p_1$

Claim 1: $p_1 = \epsilon$, where ϵ is negligible.

Proof. This is because f is a uniformly random function, therefore $\mathcal{A}$ can never predict the output of f on a new input which it hasn't seen before. So, at best, $\mathcal{A}$ can only predict the output with probability $\frac{1}{|\mathcal{Y}|}$, where $\mathcal{Y}$ is the output space. This probability is negligible as $|\mathcal{Y}| = 2^n$. □

Claim 2: $|p_0 - p_1|$ is negligible.

Proof. If the above claim is not true, i.e. if there exists an adversary $\mathcal{A}$ which can distinguish between game 0 and game 1, then we can create a reduction $\mathcal{B}$, such that $\mathcal{B}$ wins PRF game with non-negligible advantage using adversary $\mathcal{A}$.
The reduction $\mathcal{B}$ works as follows:

- The reduction encrypts messages by sampling $r \leftarrow \mathcal{R}$, and sending r and message m one by one to the PRF challenger. It receives y and z from the challenger and the encryption it calculates is : $(r, y \oplus m, z)$.
- It receives the encryption $\mathsf{ct} = (\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{ct}_2)$ from $\mathcal{A}$. It then sends ct_0 to $\mathcal{C}$ and gets y'. Then it sends $\mathsf{ct}_1 \oplus y'$ to $\mathcal{C}$ and gets z'.
- If $z' = \mathsf{ct}_2$ then $\mathcal{B}$ sends 0, else it sends 1 to the PRF challenger.

Here, the adversary sends a valid ciphertext ct to the reduction. If challenger chooses pseudorandom, then the ciphertext is of form : $(r, F(k, r) \oplus m, F(k, m))$, and the reduction guesses 0 with probability p_0 (because then $y' = F(k, r)$, $\mathsf{ct}_1 \oplus y' = m$ and $z' = F(k, m)$, which reduction compares with ct_2). Else if the challenger chooses truly random, then the reduction sends 1 with probability p_1. Hence

$$\mathsf{PRFAdv}[\mathcal{B}, \mathcal{F}] = |p_0 - p_1|$$

. This proves that $|p_0 - p_1|$ must be negligible. $\square$

Using the above two claims, we can say that p_0 is negligible, which implies that the winning probability of adversary in the Very Weak Ciphtertext Integrity game is negligible.

Problem 2 : Encryption Scheme with Threshold Decryption

Solution: Consider the following encryption scheme $\mathsf{Enc}-\mathsf{two}(k_i, k_j, m)$ defined as follows:

$$\mathsf{Enc}-\mathsf{two}(k_i,k_j,m) = \begin{cases} \mathsf{Enc}(k_2, \mathsf{Enc}(k_1, m)) & k_i = 1, k_j = 2 \\ \mathsf{Enc}(k_2, \mathsf{Enc}(k_3, m)) & k_i = 2, k_j = 3 \\ \mathsf{Enc}(k_3, \mathsf{Enc}(k_4, m)) & k_i = 3, k_j = 4 \end{cases}$$

Similarly, we can define the decryption:

$$\mathsf{Dec}-\mathsf{two}(k_i,k_j,\mathsf{ct}) = \begin{cases} \mathsf{Dec}(k_1, \mathsf{Dec}(k_2, \mathsf{ct})) & k_i = 1, k_j = 2 \\ \mathsf{Dec}(k_3, \mathsf{Dec}(k_2, \mathsf{ct})) & k_i = 2, k_j = 3 \\ \mathsf{Dec}(k_4, \mathsf{Dec}(k_3, \mathsf{ct})) & k_i = 3, k_j = 4 \end{cases}$$

Correctness: Correctness of the scheme can be checked easily

Security Game

- **Challenge Phase:** Challenger picks $k_2, k_3 \leftarrow \mathcal{K}$. The adversary sends keys k_1, k_4, as well as challenge messages $(m^0_{1,2}, m^0_{2,3}, m^0_{3,4})$ and $(m^1_{1,2}, m^1_{2,3}, m^1_{3,4})$. Challenger samples $b \leftarrow \{0,1\}$, computes $\mathsf{ct}_{1,2} \leftarrow \mathsf{Enc}-\mathsf{two}(k_1, k_2, m^b_{1,2}), \mathsf{ct}_{2,3} \leftarrow \mathsf{Enc}-\mathsf{two}(k_2, k_3, m^b_{2,3}), \mathsf{ct}_{3,4} \leftarrow \mathsf{Enc}-\mathsf{two}(k_3, k_4, m^b_{3,4})$.
- **Encryption Queries:** The adversary can make polynomially many encryption queries. Each query consists of a message m and an index-pair $\{i,j\} \in \{\{1,2\},\{2,3\},\{3,4\}\}$. The challenger computes $\mathsf{ct} \leftarrow \mathsf{Enc}-\mathsf{two}(k_i, k_j, m)$ and sends to the adversary.
- **Guess:** Finally, the adversary sends its guess b' and wins if $b = b'$.

Figure 1: Security Game for Problem 2

Security: If $(\mathsf{Enc}, \mathsf{Dec})$ is CPA secure, then no p.p.t. adversary has non-negligible advantage in the security game defined above.

The proof is by a hybrid argument. Consider the following worlds which differ in only the challenge phase with respect to the above security game.

World 0

- Challenger picks $k_2, k_3 \leftarrow \mathcal{K}$. The adversary sends keys k_1, k_4, as well as challenge messages $(m^0_{1,2}, m^0_{2,3}, m^0_{3,4})$ and $(m^1_{1,2}, m^1_{2,3}, m^1_{3,4})$. Challenger computes

  $$\mathsf{ct}_{1,2} \leftarrow \mathsf{Enc-two}(k_1, k_2, m^0_{1,2}), \mathsf{ct}_{2,3} \leftarrow \mathsf{Enc-two}(k_2, k_3, m^0_{2,3}), \mathsf{ct}_{3,4} \leftarrow \mathsf{Enc-two}(k_3, k_4, m^0_{3,4})$$

  and sends $(\mathsf{ct}_{1,2}, \mathsf{ct}_{2,3}, ct_{3,4})$ to the adversary.

Hybrid World 0

- Challenger picks $k_2, k_3 \leftarrow \mathcal{K}$. The adversary sends keys k_1, k_4, as well as challenge messages $(m^0_{1,2}, m^0_{2,3}, m^0_{3,4})$ and $(m^1_{1,2}, m^1_{2,3}, m^1_{3,4})$. Challenger computes

  $$\mathsf{ct}_{1,2} \leftarrow \mathsf{Enc-two}(k_1, k_2, m^1_{1,2}), \mathsf{ct}_{2,3} \leftarrow \mathsf{Enc-two}(k_2, k_3, m^0_{2,3}), \mathsf{ct}_{3,4} \leftarrow \mathsf{Enc-two}(k_3, k_4, m^0_{3,4})$$

  and sends $(\mathsf{ct}_{1,2}, \mathsf{ct}_{2,3}, ct_{3,4})$ to the adversary.

Hybrid World 1

- Challenger picks $k_2, k_3 \leftarrow \mathcal{K}$. The adversary sends keys k_1, k_4, as well as challenge messages $(m^0_{1,2}, m^0_{2,3}, m^0_{3,4})$ and $(m^1_{1,2}, m^1_{2,3}, m^1_{3,4})$. Challenger computes

  $$\mathsf{ct}_{1,2} \leftarrow \mathsf{Enc-two}(k_1, k_2, m^1_{1,2}), \mathsf{ct}_{2,3} \leftarrow \mathsf{Enc-two}(k_2, k_3, m^1_{2,3}), \mathsf{ct}_{3,4} \leftarrow \mathsf{Enc-two}(k_3, k_4, m^0_{3,4})$$

  and sends $(\mathsf{ct}_{1,2}, \mathsf{ct}_{2,3}, ct_{3,4})$ to the adversary.

World 1

- Challenger picks $k_2, k_3 \leftarrow \mathcal{K}$. The adversary sends keys k_1, k_4, as well as challenge messages $(m^0_{1,2}, m^0_{2,3}, m^0_{3,4})$ and $(m^1_{1,2}, m^1_{2,3}, m^1_{3,4})$. Challenger computes

  $$\mathsf{ct}_{1,2} \leftarrow \mathsf{Enc-two}(k_1, k_2, m^1_{1,2}), \mathsf{ct}_{2,3} \leftarrow \mathsf{Enc-two}(k_2, k_3, m^1_{2,3}), \mathsf{ct}_{3,4} \leftarrow \mathsf{Enc-two}(k_3, k_4, m^1_{3,4})$$

  and sends $(\mathsf{ct}_{1,2}, \mathsf{ct}_{2,3}, ct_{3,4})$ to the adversary.

In subsequent worlds, the number of encryptions for $b = 1$ increases. Let $p_0, p_{\mathsf{Hyb},0}, p_{\mathsf{Hyb},1}, p_1$ be the probabilities that the adversary outputs 0 in the above worlds.

Claim: If there exists an adversary $\mathcal{A}$ for which $|p_0 - p_{\mathsf{Hyb},0}|$ is non-negligible then there exists an adversary $\mathcal{B}$ which breaks the CPA security of $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$ with advantage $|p_0 - p_{\mathsf{Hyb},0}|$

Consider the reduction Fig. 2:

Reduction

- $\mathcal{A}$ sends k_1, k_4, as well as challenge messages $(m^0_{1,2}, m^0_{2,3}, m^0_{3,4})$ and $(m^1_{1,2}, m^1_{2,3}, m^1_{3,4})$ to $\mathcal{B}$
- $\mathcal{B}$ computes $x_0 \leftarrow \mathsf{Enc}(k_1, m^0_{1,2}), x_1 \leftarrow \mathsf{Enc}(k_1, m^1_{1,2})$ and sends them to the challenger $\mathcal{C}$ for $\mathcal{E}$ to obtain $\mathsf{ct} = \mathsf{Enc}(k_2, \mathsf{Enc}(k_1, m^b_{1,2}))$. $\mathcal{B}$ sets $\mathsf{ct}_{1,2} = \mathsf{ct}$
- $\mathcal{B}$ samples $k_3 \leftarrow \mathcal{K}$ and computes $x_3 \leftarrow \mathsf{Enc}(k_3, m^0_{2,3})$. He then sends (x_3, x_3) to $\mathcal{C}$ to obtain $\mathsf{ct}' = \mathsf{Enc}(k_2, \mathsf{Enc}(k_3, m^0_{2,3}))$ and sets $\mathsf{ct}_{2,3} = \mathsf{ct}'$
- Next, $\mathcal{B}$ computes $\mathsf{ct}_{3,4} \leftarrow \mathsf{Enc}(k_3, \mathsf{Enc}(k_4, m^0_{3,4}))$
- $\mathcal{B}$ sends $(\mathsf{ct}_{1,2}, \mathsf{ct}_{2,3}, \mathsf{ct}_{3,4})$ to $\mathcal{A}$
- For the encryption queries, $\mathcal{B}$ follows a similar procedure as above.
- Finally $\mathcal{A}$ outputs a bit b' which $\mathcal{B}$ forwards to $\mathcal{C}$

Figure 2: Reduction 1 for Problem 2

If $\mathcal{C}$ chooses b to be 0 then the above reduction corresponds to World 0 while if he chooses 1, then it corresponds to Hybrid World 0. So the CPA advantage of $\mathcal{B} = |p_0 - p_{\mathsf{Hyb},0}|$

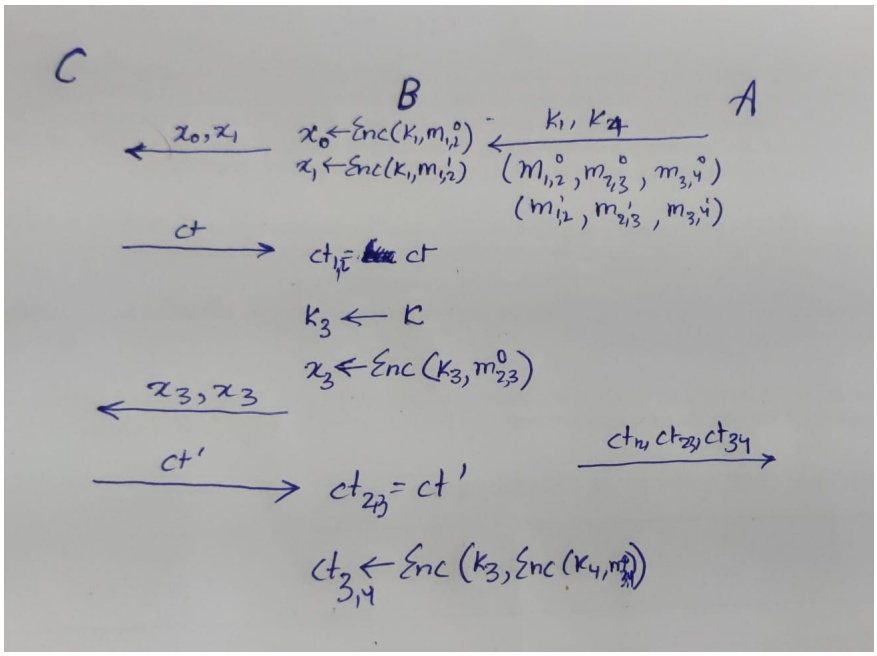

Figure 3: Reduction 1 for Problem 2

Claim: If there exists an adversary $\mathcal{A}$ for which $|p_{\mathsf{Hyb},0} - p_{\mathsf{Hyb},1}|$ is non-negligible then there exists an adversary $\mathcal{B}$ which breaks the CPA security of $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$ with advantage $|p_{\mathsf{Hyb},0} - p_{\mathsf{Hyb},1}|$

Consider the reduction Fig. 4:

Reduction

- $\mathcal{A}$ sends k_1, k_4, as well as challenge messages $(m^0_{1,2}, m^0_{2,3}, m^0_{3,4})$ and $(m^1_{1,2}, m^1_{2,3}, m^1_{3,4})$ to $\mathcal{B}$
- $\mathcal{B}$ samples $k_2 \leftarrow \mathcal{K}$ and computes $\mathsf{ct}_{1,2} \leftarrow \mathsf{Enc}(k_2, \mathsf{Enc}(k_1, m^1_{1,2}))$.
- $\mathcal{B}$ sends $m^0_{2,3}, m^1_{2,3}$ to $\mathcal{C}$ to obtain $\mathsf{ct} = \mathsf{Enc}(k_3, m^b_{2,3})$ and sets $\mathsf{ct}_{2,3} \leftarrow \mathsf{Enc}(k_2, \mathsf{ct})$
- $\mathcal{B}$ computes $x_0 \leftarrow \mathsf{Enc}(k_4, m^0_{3,4})$ and sends (x_0, x_0) to $\mathcal{C}$ to obtain $\mathsf{ct}' = \mathsf{Enc}(k_3, \mathsf{Enc}(k_4, m^0_{3,4}))$. $\mathcal{B}$ sets $\mathsf{ct}_{3,4} = \mathsf{ct}'$
- $\mathcal{B}$ sends $(\mathsf{ct}_{1,2}, \mathsf{ct}_{2,3}, \mathsf{ct}_{3,4})$ to $\mathcal{A}$
- For the encryption queries, $\mathcal{B}$ follows a similar procedure as above.
- Finally $\mathcal{A}$ outputs a bit b' which $\mathcal{B}$ forwards to $\mathcal{C}$

Figure 4: Reduction 2 for Problem 2

If $\mathcal{C}$ chooses b to be 0 then the above reduction corresponds to Hybrid World 0 while if he chooses 1, then it corresponds to Hybrid World 1. So the CPA advantage of $\mathcal{B} = |p_{\mathsf{Hyb},0} - p_{\mathsf{Hyb},1}|$

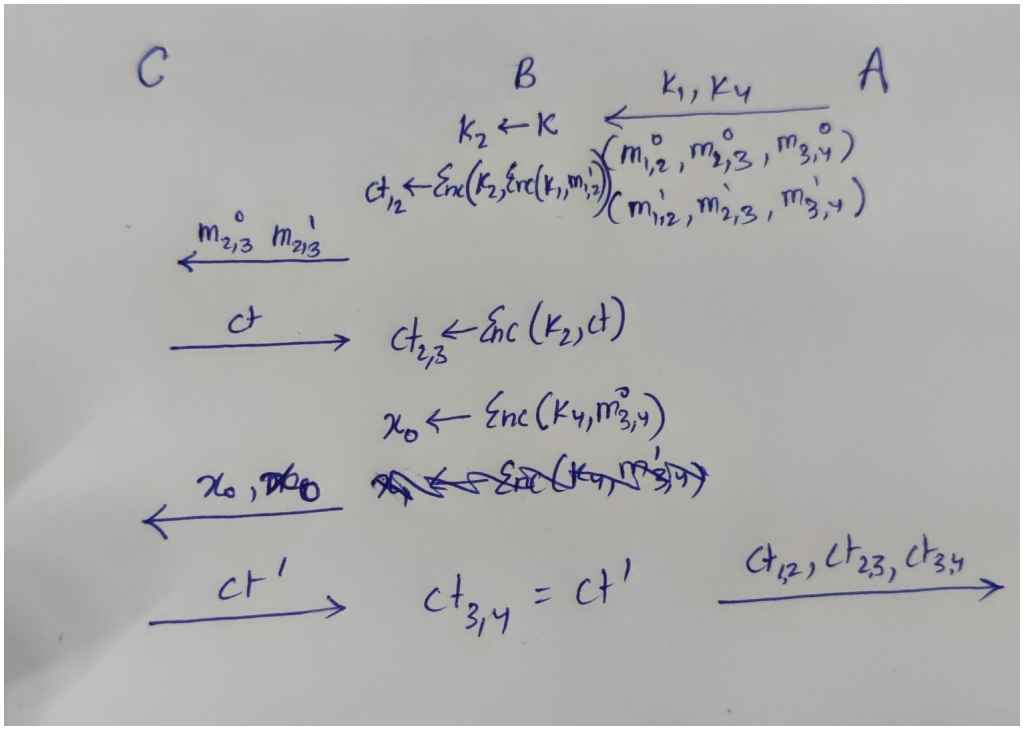

Figure 5: Reduction 2 for Problem 2

Claim: If there exists an adversary $\mathcal{A}$ for which $|p_{\mathsf{Hyb},1} - p_1|$ is non-negligible then there exists an adversary $\mathcal{B}$ which breaks the CPA security of $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$ with advantage $|p_{\mathsf{Hyb},1} - p_1|$

Consider the reduction:

Reduction

- $\mathcal{A}$ sends k_1, k_4, as well as challenge messages $(m^0_{1,2}, m^0_{2,3}, m^0_{3,4})$ and $(m^1_{1,2}, m^1_{2,3}, m^1_{3,4})$ to $\mathcal{B}$
- $\mathcal{B}$ samples $k_2 \leftarrow \mathcal{K}$ and computes $\mathsf{ct}_{1,2} \leftarrow \mathsf{Enc}(k_2, \mathsf{Enc}(k_1, m^1_{1,2}))$.
- $\mathcal{B}$ sends $m^1_{2,3}, m^1_{2,3}$ to $\mathcal{C}$ to obtain $\mathsf{ct} = \mathsf{Enc}(k_3, m^1_{2,3})$ and sets $\mathsf{ct}_{2,3} \leftarrow \mathsf{Enc}(k_2, \mathsf{ct})$
- $\mathcal{B}$ computes $x_0 \leftarrow \mathsf{Enc}(k_4, m^0_{3,4}), x_1 \leftarrow \mathsf{Enc}(k_4, m^1_{3,4})$ and sends (x_0, x_1) to $\mathcal{C}$ to obtain $\mathsf{ct}' = \mathsf{Enc}(k_3, \mathsf{Enc}(k_4, m^b_{3,4}))$. $\mathcal{B}$ sets $\mathsf{ct}_{3,4} = \mathsf{ct}'$
- $\mathcal{B}$ sends $(\mathsf{ct}_{1,2}, \mathsf{ct}_{2,3}, \mathsf{ct}_{3,4})$ to $\mathcal{A}$
- For the encryption queries, $\mathcal{B}$ follows a similar procedure as above.
- Finally $\mathcal{A}$ outputs a bit b' which $\mathcal{B}$ forwards to $\mathcal{C}$

Figure 6: Reduction 3 for Problem 2

If $\mathcal{C}$ chooses b to be 0 then the above reduction corresponds to Hybrid World 1 while if he chooses 1, then it corresponds to World 1. So the CPA advantage of $\mathcal{B} = |p_{\mathsf{Hyb},1} - p_1|$

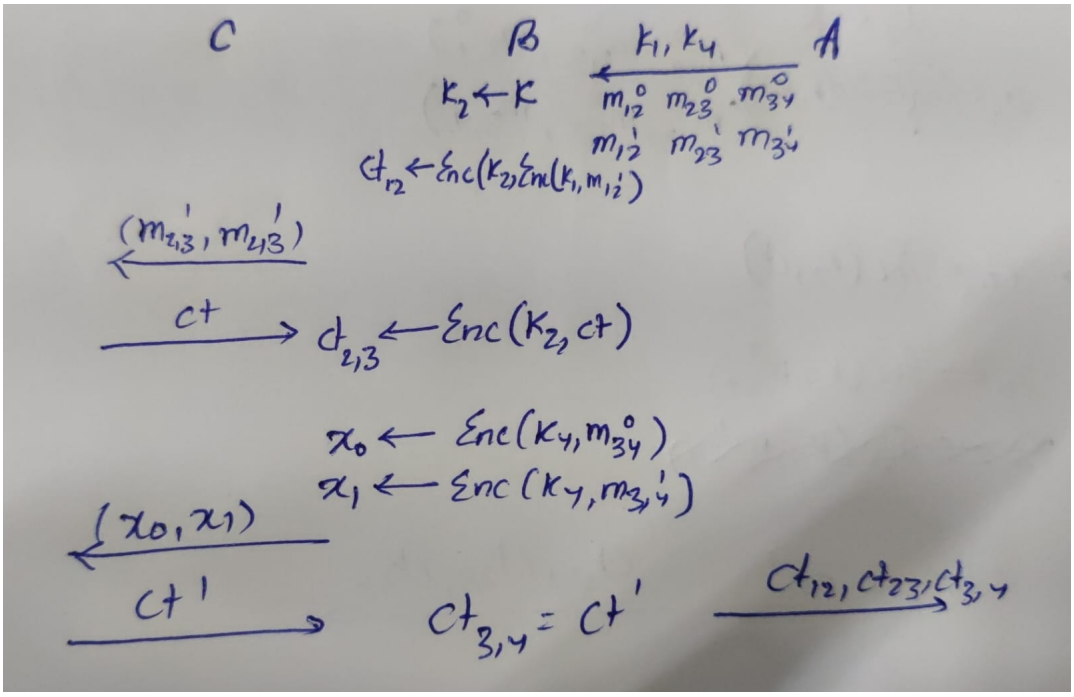

Figure 7: Reduction 3 for Problem 2

Thus from the above three claims, we can conclude that if $(\mathsf{Enc}, \mathsf{Dec})$ is CPA secure, then no p.p.t. adversary has non-negligible advantage in the security game defined above.

Problem 3 : One-time secure MACs, and Upgrading One-Time MACs to Many-Time MACs

Solution:

(a) We construct the following One-Query Unconditionally Secure MAC scheme $\mathcal{I} = (\mathsf{Sign}, \mathsf{Verify})$:

$$\mathsf{Sign}(k, m) = (m \wedge k_1) \vee k_2$$

and

$$\mathsf{Verify}(k, m, \sigma) = \begin{cases} 1 & \text{if } \sigma = (m \wedge k_1) \vee k_2 \\ 0 & \text{Otherwise} \end{cases}$$

where $k = (k_1, k_2)$ is sampled from keyspace $\mathcal{K} = \{0,1\}^{2n}$ (k_1 and k_2 are n bits each). Also the signature space is $\{0,1\}^n$.

Claim : The winning probability of an computationally unbounded adversary $\mathcal{A}$ is bounded by $\frac{1}{2^n}$, and hence is negligible.

Proof. On getting the signature of some message $m \in \mathcal{M}$, the adversary knows m, σ and n but doesn't know (k_1, k_2). So if the adversary enumerates all such possible pairs of (k_1, k_2) which satisfies this equation, then there are about 2^n such pairs.
To prove this, consider the i^{th} bit of message m (m_i) and corresponding bit in σ (σ_i). Also take i^{th} bits of k_1 and k_2 as a_1 and a_2.
Case 1: $m_i = 0$ and $\sigma_i = 0$
Possibilities: for $a_1 = 0$, a_2 can only be 0 and for $a_1 = 1$, a_2 can be only 0. (2 pairs of (k_1, k_2))
Case 2: $m_i = 0$ and $\sigma_i = 1$
Possibilities: for $a_1 = 0$, a_2 can only be 1 and for $a_1 = 1$, a_2 can be only 1. (2 pairs of (k_1, k_2))
Case 3: $m_i = 1$ and $\sigma_i = 1$
Possibilities: for $a_1 = 0$, a_2 can only be 1 and for $a_1 = 1$, a_2 can be both 0 and 1. (3 pairs of (k_1, k_2))
Case 4: $m_i = 1$ and $\sigma_i = 0$
Possibilities: for $a_1 = 0$, a_2 can only be 0 and for $a_1 = 1$, there is no possible value of a_2. (1 pair of (k_1, k_2))
So overall there are 2^n expected number of pairs of k_1 and k_2 satisfying our equation.

Now if the adversary wants to send forgery σ' of some different message m', such that $\sigma' = (k_{i1} \wedge m') \vee k_{i2}$, where k_{i1} is some choice of key k_1 by $\mathcal{A}$ and k_{i2} is the corresponding key k_2 which satisfies $\sigma = (m \wedge k_{i1}) \vee k_{i2}$. But for different choices of k_{i1}, the corresponding σ' is different. So there are 2^n different equally likely choices of σ' which the adversary can send as forgery out of which only one is correct.
□

Hence our one-query Unconditionally Secure MAC is secure even against an unbounded adversary.

(b) To prove the security of our MAC scheme $\mathcal{I} = (\mathsf{Sign}, \mathsf{Verify})$, we setup the following games :

Game 0: This is the usual MAC security game.

- **Setup Phase :** Challenger chooses a PRF key $k = (k_1, k_2)$ where $k_1 \epsilon \mathcal{K}_1$ and $k_2 \epsilon \mathcal{K}_2$.
- **Query Phase :** Adversary sends polynomially many queries. For the i^{th} query m_i, the challenger chooses a random string $r_i \leftarrow \mathcal{X}$ and sends $\sigma_i = \mathsf{Sign}(k, m_i; r_i)$ to the adversary.
- **Forgery :** Finally, the adversary outputs (m^*, σ^*) such that $(m^*, \sigma^*) \neq (m_i, \sigma_i)$ for all i.

Let the winning probability of Adversary $\mathcal{A}$ in Game 0 be p_0.

Game 1: This is similar to previous game except the PRF is replaced by a uniformly random function.

- **Setup Phase :** Challenger chooses a PRF key $k = (k_1, k_2)$ where $k_1 \epsilon \mathcal{K}_1$ and $k_2 \epsilon \mathcal{K}_2$. It also samples a unifromly random function $f \leftarrow Func[\mathcal{X}, \mathcal{T}]$.
- **Query Phase :** Adversary sends polynomially many queries. For the i^{th} query m_i, the challenger chooses a random string $r_i \leftarrow \mathcal{X}$ and sends $\sigma_i = (r, \mathsf{Sign}_1(k_1, m_i) \oplus f(r_i))$ to the adversary.
- **Forgery :** Finally, the adversary outputs (m^*, σ^*) such that $(m^*, \sigma^*) \neq (m_i, \sigma_i)$ for all i.

Let the winning probability of Adversary $\mathcal{A}$ in Game 1 be p_1.

Game 2: This is similar to previous game except the signature is replaced by a uniformly random function.

- **Setup Phase :** Challenger chooses a PRF key $k = (k_1, k_2)$ where $k_1 \epsilon \mathcal{K}_1$ and $k_2 \epsilon \mathcal{K}_2$. It also samples two uniformly random functions $f \leftarrow Func[\mathcal{X}, \mathcal{T}]$ and $f' \leftarrow Func[\mathcal{M}, \mathcal{T}]$.
- **Query Phase :** Adversary sends polynomially many queries. For the i^{th} query m_i, the challenger chooses a random string $r_i \leftarrow \mathcal{X}$ and sends $\sigma_i = (r, f'(m_i) \oplus f(r_i))$ to the adversary.
- **Forgery :** Finally, the adversary outputs (m^*, σ^*) such that $(m^*, \sigma^*) \neq (m_i, \sigma_i)$ for all i.

Let the winning probability of Adversary $\mathcal{A}$ in Game 2 be p_2.

Claim 1: $p_2 = \epsilon$, where ϵ is a negligible function.
Proof: This is because f and f' are truly random functions and the adversary can never predict the output of these functions at some input (Using Shannon's security). It can only guess the output with a probability of $\frac{1}{|\mathcal{T}|}$. So the value of p_2 is negligible.

Claim 2: $|p_1 - p_0|$ is negligible.
Proof: This follows from the security of the PRF function. Suppose there exists an adversary $\mathcal{A}$ that can distinguish between the two games (i.e. $|p_1 - p_0|$ is non-negligible), then we can construct a reduction $\mathcal{B}$ which uses this adversary to win the PRF game with non-negligible advantage. The reduction works as follows:

- It samples $r_i \leftarrow \mathcal{X}$ for the i^{th} query. It sends this to the PRF challenger and receives y_i.
- It then sends $(r_i, y_i \oplus \mathsf{Sign}_1(k_1, m))$ to the adversary. The adversary finally outputs a forgery (m^*, σ^*), where $\sigma^* = (\sigma_0^*, \sigma_1^*)$
- The reduction then sends a final query σ_0^* to the PRF challenger and receives y^*. If $y^* = \sigma_1^* \oplus \mathsf{Sign}_1(k_1, m^*)$ then the reduction sends 1, else it sends 0.

If the PRF challenger chooses pseudorandom, then the reduction will output 0 with a probability of p_0 else if the PRF challenger chooses completely random function, then the reduction sends 1 with probability p_1.
Hence the $\mathsf{PRFAdv}[\mathcal{B}, \mathcal{F}] = |p_0 - p_1|$, which is negligible.

Claim 3: $|p_2 - p_1|$ is also negligible.
Proof: Suppose in game 1, the adversary sends a forgery as (m^*, σ^*). We can then write p_1 as follows:
$p_1 = \Pr[\text{A wins game 1 and A also knows } \mathsf{Sign}_1(k_1, m^*)] +$
$\Pr[\text{A wins game 1 and A doesn't know } \mathsf{Sign}_1(k_1, m^*)]$
The second case (A wins game 1 but A doesn't know $\mathsf{Sign}_1(k_1, m^*)$) is equivalent to game 2, since A doesn't was not able to compute the function, σ_1 behaves as a random function for the adversary. So we can write :

$$|p_1 - p_2| = \Pr[\text{A wins game 1 and A also knows } \mathsf{Sign}_1(k_1, m^*)]$$

and from this ,

$$|p_1 - p_2| \leq \Pr[\text{A knows } \mathsf{Sign}_1(k_1, m^*)]$$

Now we can say that the above term is negligible using one-query security of σ_1. This is because in all the queries of the adversary, we sent the signature as $f(r) \oplus \sigma_1$ where $f(r)$ is some truly random function. Using Shannon's OTP security, we can say that $f(r) \oplus \sigma_1$ is also completely random to the adversary. So the probability that adversary sends $\mathsf{Sign}_1(k_1, m^*)$ without knowing the signature of any other message $m \epsilon \mathcal{M}$ is negligible because σ_1 is one-query secure.

Hence using all the above three claims, we can say that p_0 is negligible and hence our MAC scheme $\mathcal{I}$ is secure.

Problem 4 : CCA Security v/s Authenticated Encryption

Solution:

(a) Here we need to show that CCA+PT-INT $\implies$ CT-INT. Intuitively, this is true because if an adversary breaks CT-INT, he produces a ciphertext of (1) a previously queried message or (2) a new message. If (1) happens then CCA breaks and if (2) happens then PT-INT breaks.

Let $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme that follows CCA and PT-INT. We will show that it satisfies CT-INT. Consider the following worlds:

World 0:

This is the CT-INT game

Hybrid Word

This is the CT-INT game but the ct^* given as output by the adversary decripts to one of the previously queried messages: $\mathsf{Dec}(k, \mathsf{ct}^*) \in \{m_i\}$

Let p_0 and p_{Hyb} be the winning probabilities of the adversary in World 0 and Hybrid World respectively.

Claim: If there exists an adversary for which $|p_0 - p_{\mathsf{Hyb}}|$ is non-negligible then there exists a reduction $\mathcal{B}$ which breaks the PT-INT of $\mathcal{E}$

Proof. Indeed, if p_0 and p_{Hyb} are far apart then the probability that the output ct^* given by $\mathcal{A}$ decrypts to a message different from the queried messages is non-negligible. This is sufficient to break PT-INT. The reduction simply forwards ct^* and wins with probability $|p_0 - p_{\mathsf{Hyb}}|$ $\square$

Claim: If there exists an adversary for which p_{Hyb} is non-negligible then there exists a reduction $\mathcal{B}$ which breaks the CCA security of $\mathcal{E}$

Proof. Consider the following reduction:

Reduction

- $\mathcal{A}$ sends m_i to $\mathcal{B}$
- $\mathcal{B}$ samples $m \leftarrow \mathcal{M}$ and sends encryption query (m_i, m) to CCA challenger $\mathcal{C}$
- $\mathcal{C}$ replies with ct_i which $\mathcal{B}$ forwards to $\mathcal{A}$
- Finally, $\mathcal{A}$ outputs ct^* which $\mathcal{B}$ forwards to $\mathcal{C}$ for decryption. If the output is $\perp$, $\mathcal{B}$ outputs 1 otherwise it outputs 0

Figure 8: Reduction for Problem 4a

Let the number of queries made by $\mathcal{A}$ be Q and the message space be $\mathcal{M}$.

Now, if the challenger chooses $b = 0$ then it is the same as the CT-INT game.

$$\Pr[b' = 0 | b = 0] = p_{\mathsf{Hyb}}$$

If challenger choose $b = 1$ then for all its queries, $\mathcal{A}$ gets the encryption of a random message m. The probability of outputing 0 here will be bounded by the probability that $m \in \{m_i\}$ which is

$$\Pr[\exists m_i : m = m_i] \leq \frac{Q}{|\mathcal{M}|}$$

Thus,

$$\Pr[b' = 0 | b = 1] \leq \frac{Q}{|\mathcal{M}|}$$

$$\mathsf{CCAAdv}[\mathcal{B}, \mathcal{C}] \geq p_{\mathsf{Hyb}} - \frac{Q}{|\mathcal{M}|}$$

Which is non-negligible assuming $\mathcal{M}$ to be superpolynomial. □

(b) We use **Strong PRP**[1] P_s as the cryptographic primitive in our scheme $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$.

$$\mathsf{Enc}(k, m) := \{r \leftarrow \mathcal{R}, \mathsf{ct} \leftarrow P_s(k, (m, r)), \text{Output } \mathsf{ct}\}$$
$$\mathsf{Dec}(k, \mathsf{ct}) := \{(m, r) = P_s^{-1}(k, \mathsf{ct}), \text{Output } m\}$$

Observe that if the ciphertexts are tampered with, they will still get decrypted to some message m' since the decryption algorithm never outputs abort. Hence, this scheme **doesn't satisfy plaintext integrity**.

Claim: $\mathcal{E}$ is CCA secure

Proof. We will show the CCA security of our encryption scheme using hybrid worlds as follows:

World-b

- This is the usual CCA game. The challenger samples a key $k \leftarrow \mathcal{K}$, a bit $b \leftarrow \{0, 1\}$ and a random string $r \leftarrow \mathcal{R}$.
- For the i^{th} Encryption query of the adversary (m_{i0}, m_{i1}), the challenger forwards $\mathsf{Enc}(k, m_{ib})$ to the adversary.
- For the j^{th} Decryption query of the adversary (ct_j), the challenger calculates $(m_j, r_j) \leftarrow \mathsf{Dec}(k, \mathsf{ct}_j)$ and sends m_j to the adversary.
- After polynomially many queries, the adversary finally outputs its guess bit b'.

$$\text{Let } \Pr[b' = 0] = p_b$$

Hybrid-World-b

- This is the usual CCA game except know the challenger uses purely random permutations. The challenger samples a bit $b \leftarrow \{0, 1\}$, a random string $r \leftarrow \mathcal{R}$ and a uniformly random permutation $f \leftarrow Perm[\mathcal{M}]$.
- For the i^{th} Encryption query of the adversary (m_{i0}, m_{i1}), the challenger forwards $f(m_{ib}||r)$ to the adversary.
- For the j^{th} Decryption query of the adversary (ct_j), the challenger computes $(m_j, r_j) \leftarrow f^{-1}(\mathsf{ct}_j)$ and forwards m_j to the adversary.
- After polynomially many queries, the adversary finally outputs its guess bit b'.

$$\text{Let } \Pr[b' = 0] = p_{\mathsf{Hyb}\_b}$$

[1] This can be created by using a 4-round Luby-Rakoff Construction. A strong PRP is secure against inversion queries too

Claim 1: $p_{\mathsf{Hyb\_0}} = p_{\mathsf{Hyb\_1}}$.
Proof: This follows from the fact that the challenger uses a purely random permutation $f(.)$ to calculate the encryption. So, using Shannon's security, the adversary cannot distinguish between the two hybrid worlds even by knowing the previous encryption and decryption queries.

Claim 2: $|p_{\mathsf{Hyb}\_b} - p_b|$ is negligible.
Proof: Suppose that there exists an adversary $\mathcal{A}$ that can distinguish between World-b and Hybrid-world-b. We can then create a reduction $\mathcal{B}$ such that it breaks the strong PRP security with non-negligible advantage using the adversary $\mathcal{A}$.
The reduction works as follows:

- The reduction takes all the encryption queries from the adversary and forwards them to the PRP challenger as forward queries. It then forwards the replies from the challenger back to the adversary.
- Similarly, the reduction takes all the decryption queries from the adversary and forwards them to the PRP challenger as inversion queries. It then forwards the replies from the challenger back to the adversary.
- After polynomially many queries, the adversary $\mathcal{A}$ sends a bit b' to the reduction. The reduction sends the bit b' as its guess to the strong PRP challenger.

Here if the PRP challenger chooses to send psuedorandom permutations, then that corresponds to World-b for the adversary and it sends $b' = 0$ with a probability of p_b. On the other hand, if the PRP challenger sends truly random permutations that correspond to Hybrid-World-b for the adversary and it sends $b' = 1$ with a probability of p_1.
The $\mathsf{PRPAdv}[\mathcal{B}, P_s] = |p_{\mathsf{Hyb}\_b} - p_b|$. Hence $|p_{\mathsf{Hyb}\_b} - p_b|$ must be negligible.

Using the above two claims, we can say that $|p_0 - p_1|$ is negligible and hence our encryption scheme is CCA secure.

□

Problem 5: Modular Arithmetic and Basic Group Theory

Solution:

(a) Since a and p are coprime, by the Extended Euclid's Agorithm:

$$ab + py = \gcd(a, p) = 1$$

Taking modulo p on both sides:

$$ab \mod p = 1$$

Where $b \in \mathbb{Z}_p$ (If not then by the division algorithm $b = qp + b', b' < p$. So, we can replace b with b')

Now suppose there exist $b, b' \in \mathbb{Z}_p$ such that

$$ab = 1 \mod p \qquad ab' = 1 \mod p$$

Then by definition of mod, $p|a(b - b')$. So $b - b' = 0$ since a and $b - b'$ will be coprime to p. Hence b is unique.

(b) Consider $h(y) = y^2 + y$ and $n = 6$. For 3 values of y viz. $2, 3, 5$, we have $h(y) = 0 \mod 6$. Thus

$$|\{y \in \mathbb{Z}_6 : y^2 + y = 0 \mod 6\}| = 3 > 2$$

(c) For this part, we will use Fermat's Little Theorem.

Theorem 1 (Fermat's Little Theorem)**.** *For any prime number p and $a \in \mathbb{Z}$*

$$a^{p-1} = 1 \mod p$$

Proof. We use the following observation:

Observation: Let $a \in \mathbb{Z}_p^*$. Consider the set $S_a = \{a \cdot i : i \in \mathbb{Z}_p^*\}$. Then $S_a = \mathbb{Z}_p^*$.

Otherwise, suppose there exist $i, j \in \mathbb{Z}_p^*$ such that

$$a \cdot i \mod p = a \cdot j \mod p \implies p|a(i - j) \implies i = j$$

Now consider the product of all elements of S_a

$$\prod_{a_i \in S_a} a_i = \prod_{i=1}^{p-1} a \cdot i = a^{p-1} \prod_{i \in \mathbb{Z}_p^*} i$$

Since $S_a = \mathbb{Z}_p^*$, the products on both sides must be the same. Hence

$$a^{p-1} = 1 \mod p$$

□

Let $a \in \mathbb{Z}_p$ and $r = \mathsf{ord}(a)$. Then $a^r = 1 \mod p$. By Fermat's Little Theorem:

$$a^{p-1} = 1 \mod p$$

Suppose by the division algorithm, $p - 1 = rq + s$, $s < r$. Since $a^{p-1} = 1 \mod p$ and $a^r = 1 \mod p$,

$$a^{p-1-rq} = 1 \mod p$$

and hence $a^s = 1 \mod p$. But since $s < r$, s must be 0.

Reduction

- The challenger samples $\alpha, \beta, \gamma \leftarrow \mathbb{Z}_q, b \leftarrow \{0,1\}$ and calculates $u = g^{\alpha}, v_0 = g^{\alpha^2}, v_1 = g^{\beta}, w_0 = g^{\alpha^3}, w_1 = g^{\gamma}$ and sends (g, u, v_b, w_b) to $\mathcal{B}$
- $\mathcal{B}$ samples $\delta \leftarrow \mathbb{Z}_q$ and sends $(g, u, v_b g^{\delta}, w_b u^{\delta})$ to $\mathcal{A}$
- $\mathcal{A}$ returns a bit b' which $\mathcal{B}$ forwards to $\mathcal{C}$

Figure 9: Reduction for Problem 5d

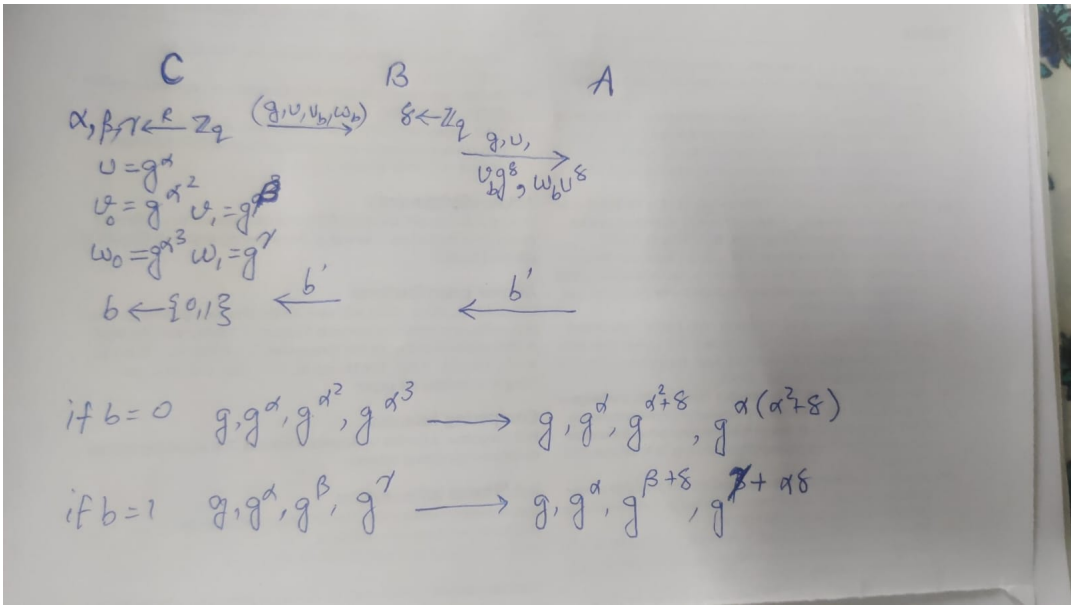

Figure 10: Reduction for Problem 5d

(d) The reduction works as Fig. 9

If $b = 0$ $\mathcal{A}$ gets $(g, g^{\alpha}, g^{\alpha^2+\delta}, g^{\alpha(\alpha^2+\delta)})$ which is of the form $(g, g^{\alpha}, g^{\beta'}, g^{\alpha\beta'})$ since δ is chosen at random. Hence the distribution reduces to the DDH distribution $\mathcal{D}' = \{(g, g^{\alpha}, g^{\beta}, g^{\alpha\beta}) : \alpha, \beta, \gamma \leftarrow \mathbb{Z}_q\}$

If $b = 1$ $\mathcal{A}$ gets $(g, g^{\alpha}, g^{\beta+\delta}, g^{\gamma+\alpha\delta})$ which is of the form $(g, g^{\alpha}, g^{\beta'}, g^{\gamma'})$ since β, δ are chosen at random.

(e) Let S_i denote the set of matrices $M \in \mathbb{Z}_q^{t \times t}$ where the last i rows are of the form

$$\lambda_j(v_1 \dots v_t), \qquad j \in [i], (v_1 \dots v_t) \leftarrow \mathbb{Z}_q^t, \lambda_j \leftarrow \mathbb{Z}_q$$

and the remaining rows have elements sampled at random from $\mathbb{Z}_q$. In other words, last i rows are random multiples of some tuple (chosen at random) and remaining rows are drawn at random. Observe that $S_n = \mathsf{Rank}_1[t, q]$ and $S_1 = \mathbb{Z}_q^{t \times t}$.

The proof proceedes by a sequence of n hybrid worlds:

Hybrid World i:

The Challenger samples from the distribution

$$\mathcal{D}'_i = \{(g, g^{\mathbf{M}}) : g \leftarrow G, \mathbf{M} \leftarrow S_i\}$$

Observe that Hybrid World 1 corresponds to sampling from $\mathcal{D}_1$ and Hybrid World n corresponds to sampling from $\mathcal{D}_0$ specified in the question. Let p_i be the probability of the Adversary outputting 0 in the above Hybrids.

Claim: If there exists an adversary $\mathcal{A}$ such that $|p_i - p_{i+1}|$ is non-negligible then there exists an adversary $\mathcal{B}$ which solves the DDH problem for group G.

Proof. Consider the following reduction:

Reduction

- $\mathcal{C}$ samples $b \leftarrow \{0,1\}$ and $g \leftarrow G$. He calculates g^α, g^β and $w_0 = g^{\alpha\cdot\beta}, w_1 = g^\gamma$ where $\alpha, \beta, \gamma \leftarrow \mathbb{Z}_q$ and sends $(g, g^\alpha, g^\beta, w_b)$ th $\mathcal{B}$
- $\mathcal{B}$ samples the following:

$$\beta_1, \beta_2, \ldots \beta_{t-1} \leftarrow \mathbb{Z}_q$$

$$\lambda_1, \lambda_2, \ldots \lambda_i \leftarrow \mathbb{Z}_q$$

$$v_{i,j} \leftarrow \mathbb{Z}_q \qquad 1 \le i \le t-i-1, 1 \le j \le t$$

And computes the matrix:

$$\begin{bmatrix} g^{v_{1,1}} & g^{v_{1,2}} & \ldots & g^{v_{1,t}} \\ \vdots & \vdots & \ddots & \vdots \\ g^{v_{t-i-1,1}} & g^{v_{t-i-1,2}} & \ldots & g^{v_{t-i-1,t}} \\ w_b & g^{\alpha\beta_1} & \ldots & g^{\alpha\beta_{t-1}} \\ g^{\lambda_i\beta} & g^{\lambda_i\beta_1} & \ldots & g^{\lambda_i\beta_{t-1}} \\ \vdots & \vdots & \ddots & \vdots \\ g^{\lambda_1\beta} & g^{\lambda_1\beta_1} & \ldots & g^{\lambda_1\beta_{t-1}} \end{bmatrix}$$

And sends it to $\mathcal{A}$

- $\mathcal{A}$ responds with a bit b' which $\mathcal{B}$ forwards to $\mathcal{C}$

Figure 11: Reduction for Problem 5e

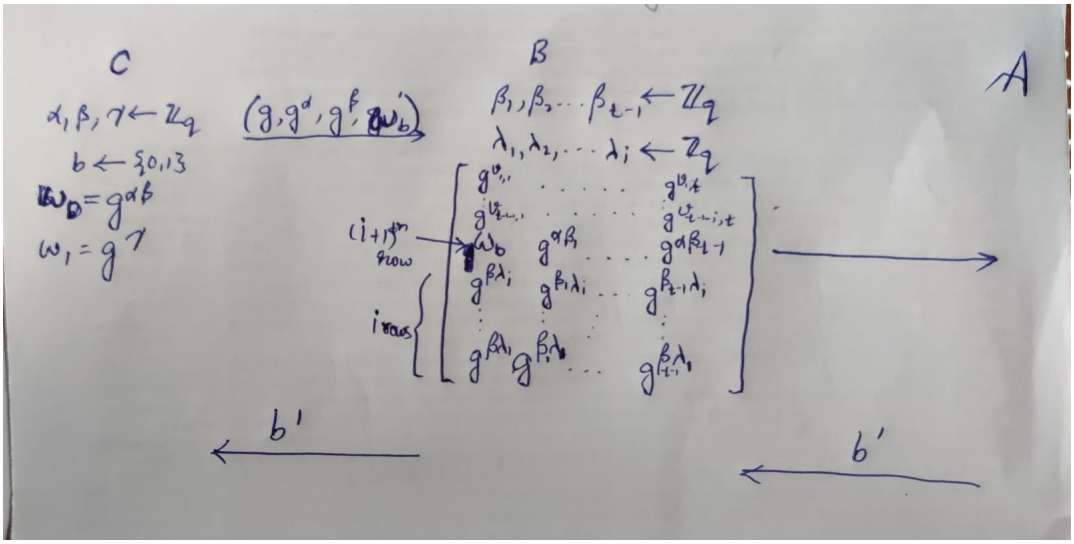

Figure 12: Reduction for Problem 5e

Observe that if $b = 0$ then it corresponds to Hybrid World $i+1$ and if $b = 1$ then it corresponds to Hybrid World i. This is because the matrix

$$\begin{bmatrix} v_{1,1} & v_{1,2} & \ldots & v_{1,t} \\ \vdots & \vdots & \ddots & \vdots \\ v_{t-i-1,1} & v_{t-i-1,2} & \ldots & v_{t-i-1,t} \\ \alpha\beta & \alpha\beta_1 & \ldots & \alpha\beta_{t-1} \\ \lambda_i\beta & \lambda_i\beta_1 & \ldots & \lambda_i\beta_{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1\beta & \lambda_1\beta_1 & \ldots & \lambda_1\beta_{t-1} \end{bmatrix}$$

Has the last $i+1$ rows as the multiple of the tuple $(\beta, \beta_1, \beta_2 \dots \beta_{t-1})$ while

$$\begin{bmatrix} v_{1,1} & v_{1,2} & \dots & v_{1,t} \\ \vdots & \vdots & \ddots & \vdots \\ v_{t-i-1,1} & v_{t-i-1,2} & \dots & v_{t-i-1,t} \\ \gamma & \alpha\beta_1 & \dots & \alpha\beta_{t-1} \\ \lambda_i\beta & \lambda_i\beta_1 & \dots & \lambda_i\beta_{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1\beta & \lambda_1\beta_1 & \dots & \lambda_1\beta_{t-1} \end{bmatrix}$$

Has the last i rows as the multiple of the tuple $(\beta, \beta_1, \beta_2 \dots \beta_{t-1})$. Hence,

$$\mathsf{DDHAdv}[\mathcal{B}, \mathcal{C}] = |p_i - p_{i+1}|$$

□

Therefore we observe that the hybrid worlds are computationally indistinguishable. Assuming that the DDH problem is hard on G,

$$|p_1 - p_n| \leq \sum_{i=1}^{n-1} |p_i - p_{i+1}|$$

Which is negligible assuming $|p_i - p_{i+1}|$ is negligible. So, $\mathcal{D}_0$ and $\mathcal{D}_1$ are computationally indistinguishable.