Anish Banerjee, Shankh Gupta **Problem Set - 3**
COL759: Cryptography October 2023

Problem 1: CPA with Very Weak Ciphertext Integrity

Solution:

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

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

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

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

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

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

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

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

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 $\mathcal{B} = |p_0 - p_{\mathsf{Hyb},0}|$

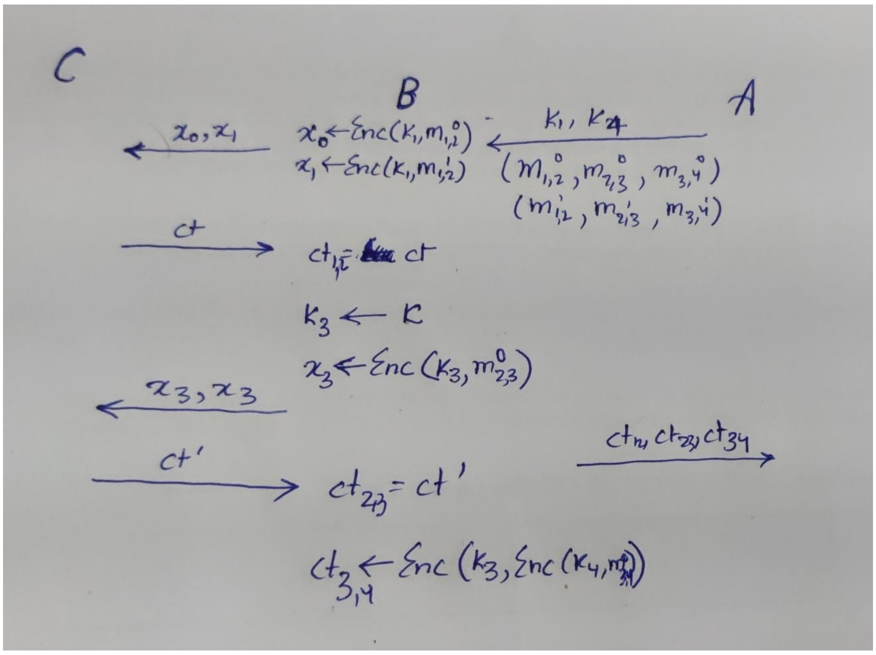

Figure 3: Reduction 1 for Problem 2

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 $\mathcal{B} = |p_{\mathsf{Hyb},0} - p_{\mathsf{Hyb},1}|$

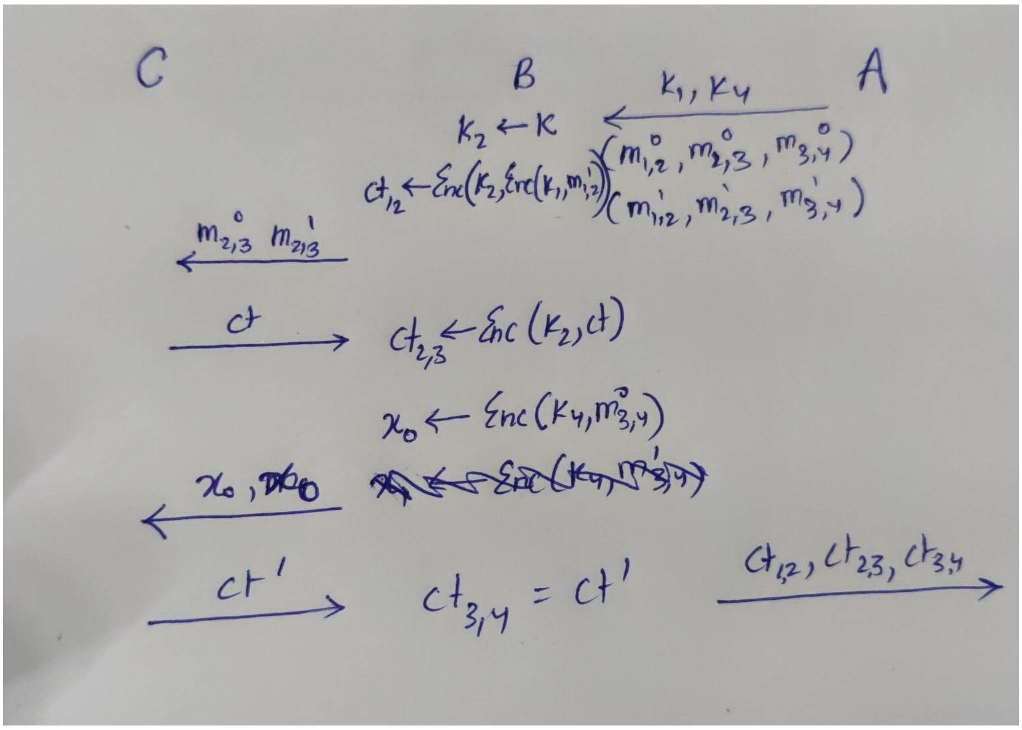

Figure 5: Reduction 2 for Problem 2

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 $\mathcal{B} = |p_{\mathsf{Hyb},1} - p_1|$

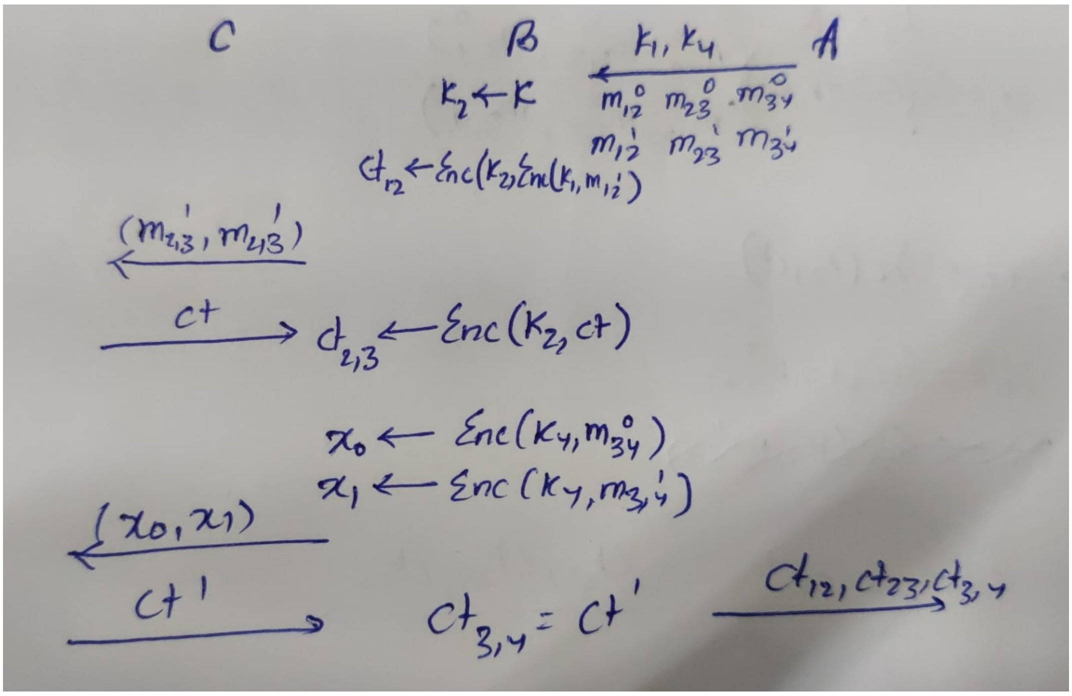

Figure 7: Reduction 3 for Problem 2

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:

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 decrupts to one of the previously queried messages: $\mathsf{Dec}(k, ct^*) \notin \{m_i\}$

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. The reduction simply forwards ct^* to the PT-INT challenger and wins with probability $|p_0 - p_{\mathsf{Hyb}}|$ □

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: Let the number of queries made by $\mathcal{A}$ be Q and the

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

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. $\square$

(b)

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

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

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.

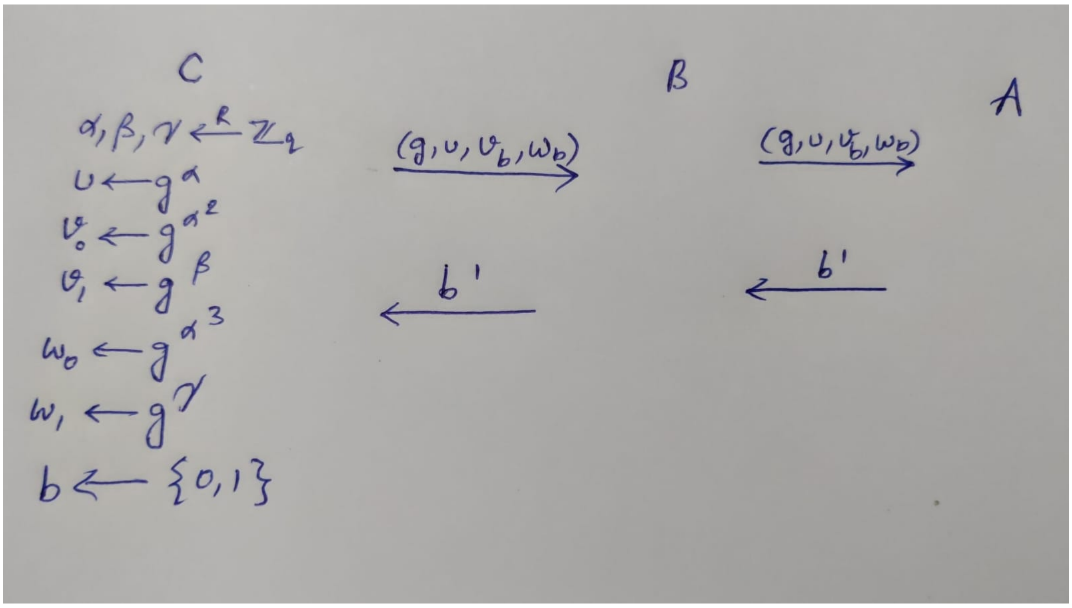

Figure 9: Reduction for Problem 5d

(d) Observe that the given distribution $\mathcal{D}_0$ is a modification of the DDH distibution

$$\mathcal{D}_0' = \{(g, g^a, g^b, g^{a \cdot b}) : g \leftarrow G, a, b \leftarrow \mathbb{Z}_p^*\}$$

where $b = a^2$. So, an Adversary which can distinguish between $\mathcal{D}_0'$ and $\mathcal{D}_1$ should also be able to distinguish between $\mathcal{D}_0$ and $\mathcal{D}_1$.

The reduction $\mathcal{B}$ simply forwards the message it receives from the challenger to $\mathcal{A}$ and forwards the output of $\mathcal{A}$ to $\mathcal{C}$ as showin in Fig. 9

(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:

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

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

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

  And computes the matrix:

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

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

Figure 10: Reduction for Problem 5e

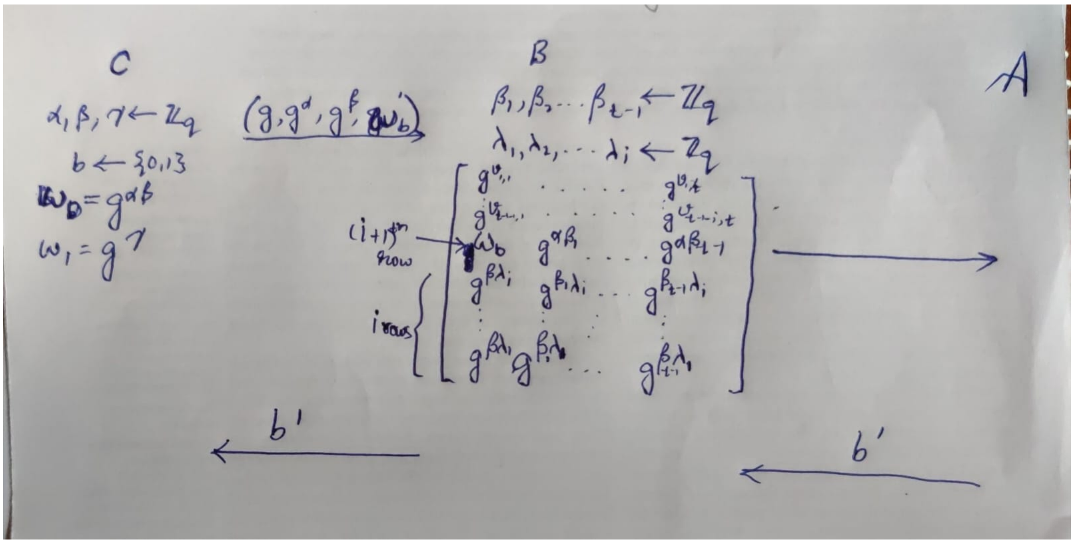

Figure 11: Reduction for Problem 5e

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

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

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

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

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

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

$\square$

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.