theorem]Claim

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

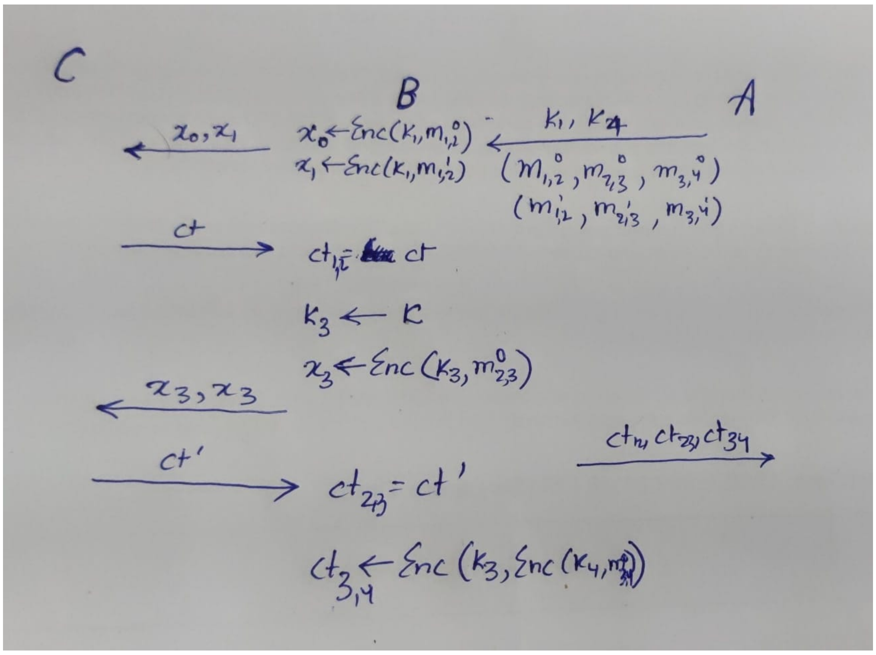

Figure 3: Reduction 1 for Problem 2

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

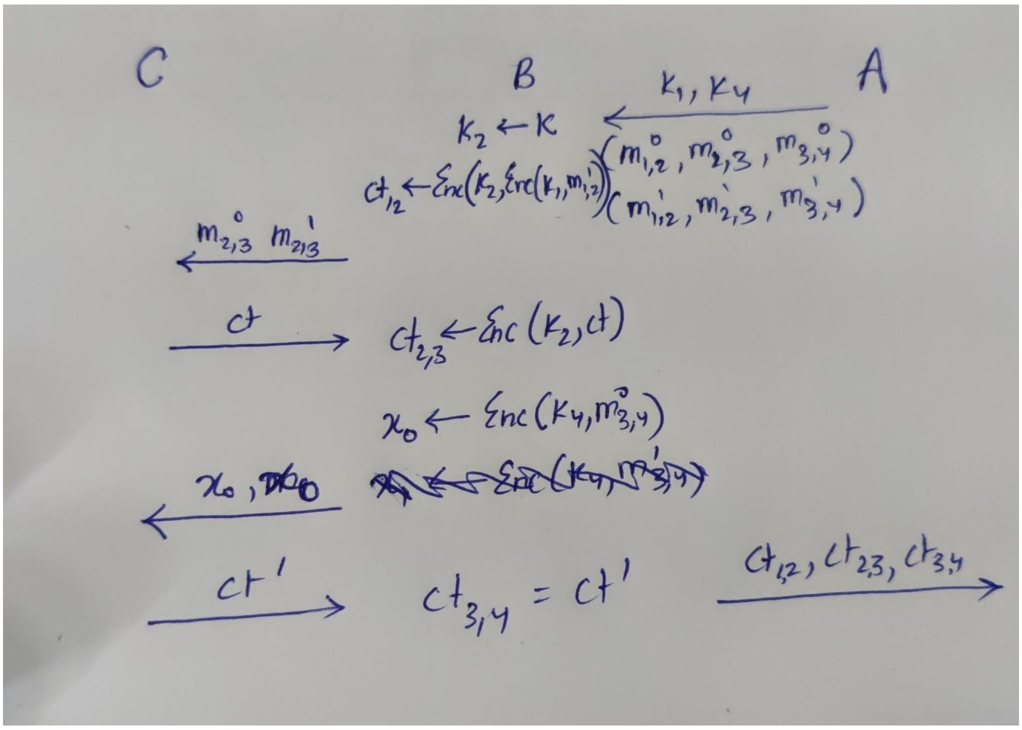

Figure 5: Reduction 2 for Problem 2

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

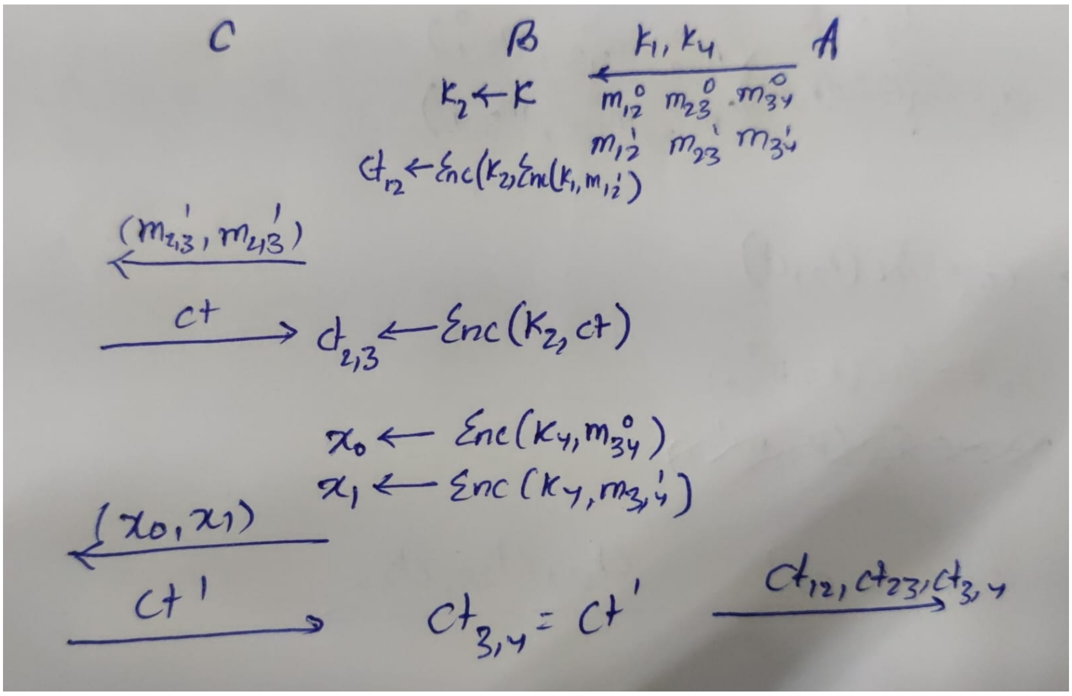

Figure 7: Reduction 3 for Problem 2

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:

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) 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.