

---

**Problem 1: CPA with Very Weak Ciphertext Integrity**

*Solution:*

## Problem 2 : Encryption Scheme with Threshold Decryption

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

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

Similarly, we can define the decryption:

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

**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  $(m_{1,2}^0, m_{2,3}^0, m_{3,4}^0)$  and  $(m_{1,2}^1, m_{2,3}^1, m_{3,4}^1)$ . Challenger samples  $b \leftarrow \{0, 1\}$ , computes  $\text{ct}_{1,2} \leftarrow \text{Enc} - \text{two}(k_1, k_2, m_{1,2}^b)$ ,  $\text{ct}_{2,3} \leftarrow \text{Enc} - \text{two}(k_2, k_3, m_{2,3}^b)$ ,  $\text{ct}_{3,4} \leftarrow \text{Enc} - \text{two}(k_3, k_4, m_{3,4}^b)$ .
- **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  $\text{ct} \leftarrow \text{Enc} - \text{two}(k_i, k_j, m)$  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  $(\text{Enc}, \text{Dec})$  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  $(m_{1,2}^0, m_{2,3}^0, m_{3,4}^0)$  and  $(m_{1,2}^1, m_{2,3}^1, m_{3,4}^1)$ . Challenger computes

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

and sends  $(\text{ct}_{1,2}, \text{ct}_{2,3}, \text{ct}_{3,4})$  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  $(m_{1,2}^0, m_{2,3}^0, m_{3,4}^0)$  and  $(m_{1,2}^1, m_{2,3}^1, m_{3,4}^1)$ . Challenger computes

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

and sends  $(\text{ct}_{1,2}, \text{ct}_{2,3}, \text{ct}_{3,4})$  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  $(m_{1,2}^0, m_{2,3}^0, m_{3,4}^0)$  and  $(m_{1,2}^1, m_{2,3}^1, m_{3,4}^1)$ . Challenger computes

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

and sends  $(\text{ct}_{1,2}, \text{ct}_{2,3}, \text{ct}_{3,4})$  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  $(m_{1,2}^0, m_{2,3}^0, m_{3,4}^0)$  and  $(m_{1,2}^1, m_{2,3}^1, m_{3,4}^1)$ . Challenger computes

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

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

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

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

Consider the reduction Fig. 2:

### Reduction

- $\mathcal{A}$  sends  $k_1, k_4$ , as well as challenge messages  $(m_{1,2}^0, m_{2,3}^0, m_{3,4}^0)$  and  $(m_{1,2}^1, m_{2,3}^1, m_{3,4}^1)$  to  $\mathcal{B}$
- $\mathcal{B}$  computes  $x_0 \leftarrow \text{Enc}(k_1, m_{1,2}^0), x_1 \leftarrow \text{Enc}(k_1, m_{1,2}^1)$  and sends them to the challenger  $\mathcal{C}$  for  $\mathcal{E}$  to obtain  $\text{ct} = \text{Enc}(k_2, \text{Enc}(k_1, m_{1,2}^b))$ .  $\mathcal{B}$  sets  $\text{ct}_{1,2} = \text{ct}$
- $\mathcal{B}$  samples  $k_3 \leftarrow \mathcal{K}$  and computes  $x_3 \leftarrow \text{Enc}(k_3, m_{2,3}^0)$ . He then sends  $(x_3, x_3)$  to  $\mathcal{C}$  to obtain  $\text{ct}' = \text{Enc}(k_2, \text{Enc}(k_3, m_{2,3}^0))$  and sets  $\text{ct}_{2,3} = \text{ct}'$
- Next,  $\mathcal{B}$  computes  $\text{ct}_{3,4} \leftarrow \text{Enc}(k_3, \text{Enc}(k_4, m_{3,4}^0))$
- $\mathcal{B}$  sends  $(\text{ct}_{1,2}, \text{ct}_{2,3}, \text{ct}_{3,4})$  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  $\mathcal{B} = |p_0 - p_{\text{Hyb},0}|$

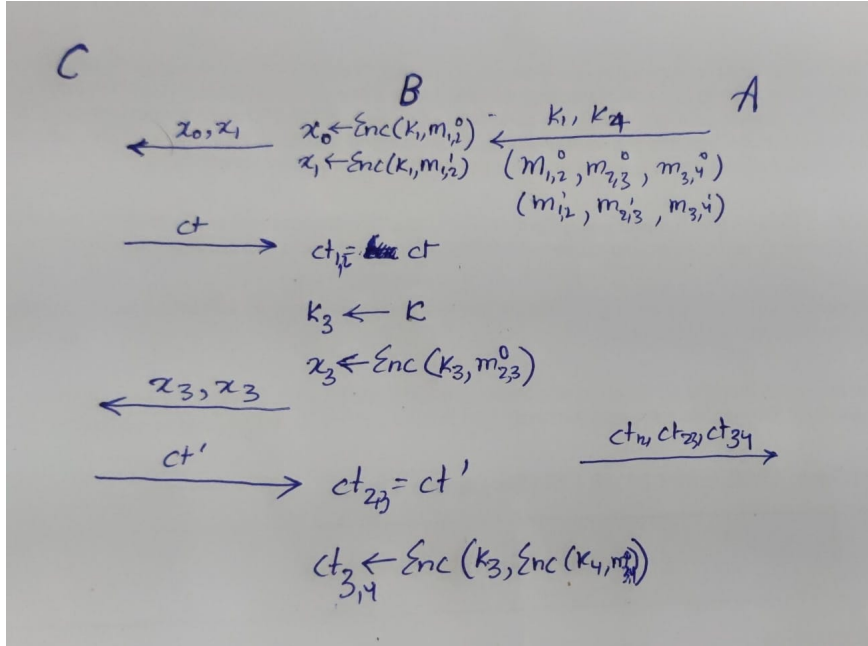


Figure 3: Reduction 1 for Problem 2

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

Consider the reduction Fig. 4:

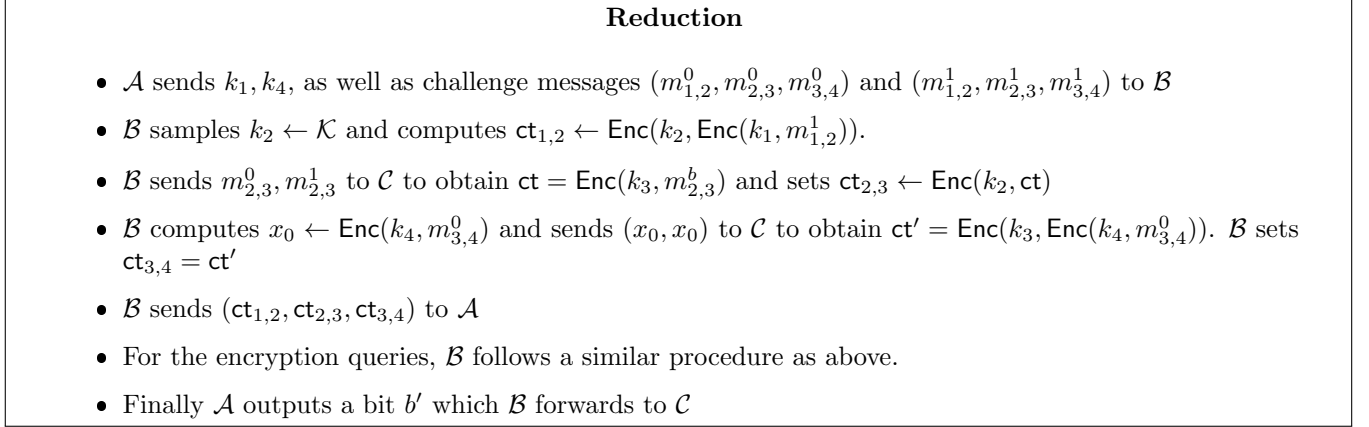


Figure 4: Reduction 2 for Problem 2

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

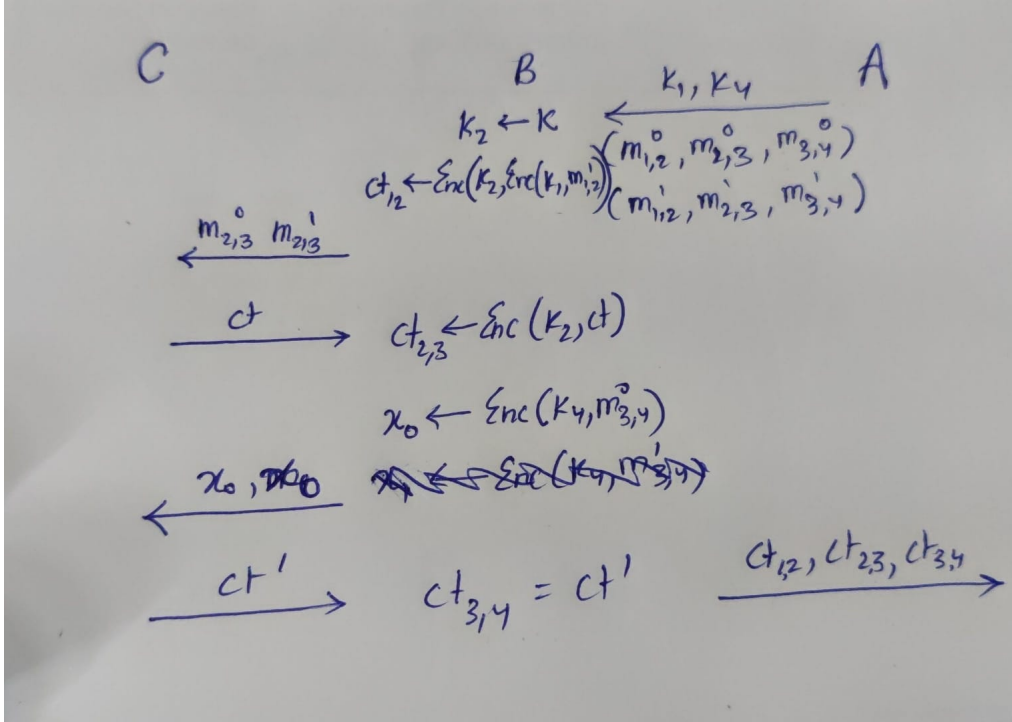


Figure 5: Reduction 2 for Problem 2

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

Consider the reduction:

#### Reduction

- $\mathcal{A}$  sends  $k_1, k_4$ , as well as challenge messages  $(m_{1,2}^0, m_{2,3}^0, m_{3,4}^0)$  and  $(m_{1,2}^1, m_{2,3}^1, m_{3,4}^1)$  to  $\mathcal{B}$
- $\mathcal{B}$  samples  $k_2 \leftarrow \mathcal{K}$  and computes  $\text{ct}_{1,2} \leftarrow \text{Enc}(k_2, \text{Enc}(k_1, m_{1,2}^1))$ .
- $\mathcal{B}$  sends  $m_{2,3}^1, m_{3,4}^1$  to  $\mathcal{C}$  to obtain  $\text{ct} = \text{Enc}(k_3, m_{2,3}^1)$  and sets  $\text{ct}_{2,3} \leftarrow \text{Enc}(k_2, \text{ct})$
- $\mathcal{B}$  computes  $x_0 \leftarrow \text{Enc}(k_4, m_{3,4}^0), x_1 \leftarrow \text{Enc}(k_4, m_{3,4}^1)$  and sends  $(x_0, x_1)$  to  $\mathcal{C}$  to obtain  $\text{ct}' = \text{Enc}(k_3, \text{Enc}(k_4, m_{3,4}^b))$ .  $\mathcal{B}$  sets  $\text{ct}_{3,4} = \text{ct}'$
- $\mathcal{B}$  sends  $(\text{ct}_{1,2}, \text{ct}_{2,3}, \text{ct}_{3,4})$  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  $\mathcal{B} = |p_{\text{Hyb},1} - p_1|$

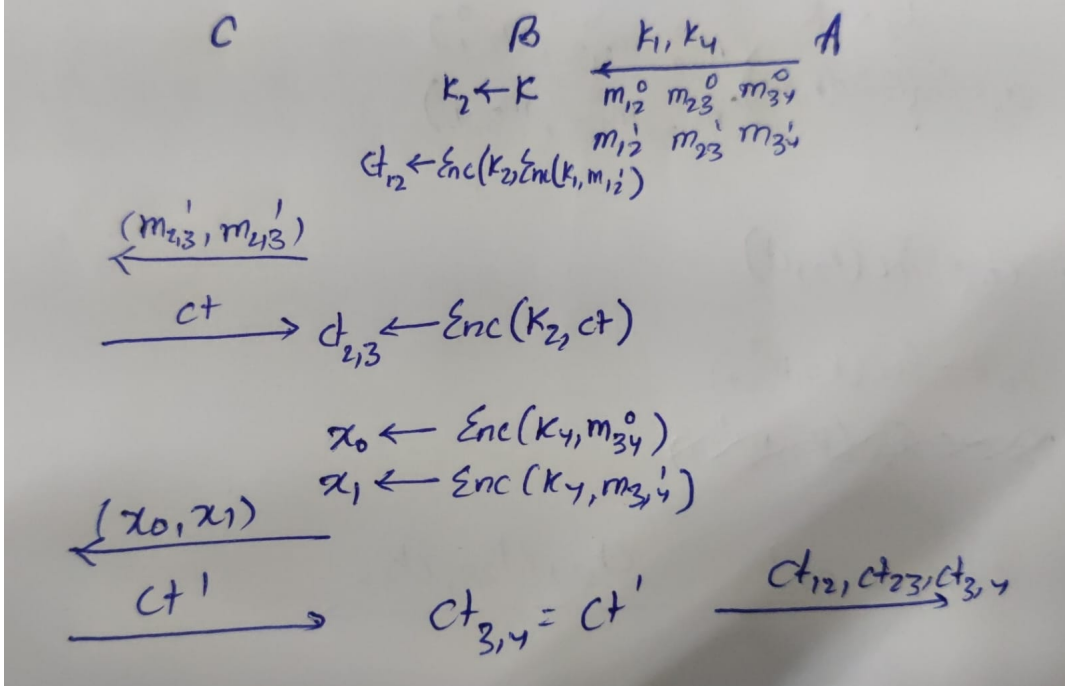


Figure 7: Reduction 3 for Problem 2

Thus from the above three claims, we can conclude that if  $(\text{Enc}, \text{Dec})$  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 Algorithm:

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

Taking modulo  $p$  on both sides:

$$ab \equiv 1 \pmod{p}$$

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

$$ab \equiv 1 \pmod{p} \quad ab' \equiv 1 \pmod{p}$$

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  $h(y) \equiv 0 \pmod{6}$ . Thus

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

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

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

$$a^{p-1} \equiv 1 \pmod{p}$$

*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

$$a \cdot i \equiv a \cdot j \pmod{p} \implies p|a(i - j) \implies i = j$$

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

$$a^{p-1} \equiv 1 \pmod{p}$$

□

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

$$a^{p-1} \equiv 1 \pmod{p}$$

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

$$a^{p-1-rq} \equiv 1 \pmod{p}$$

and hence  $a^s \equiv 1 \pmod{p}$ . But since  $s < r$ ,  $s$  must be 0.

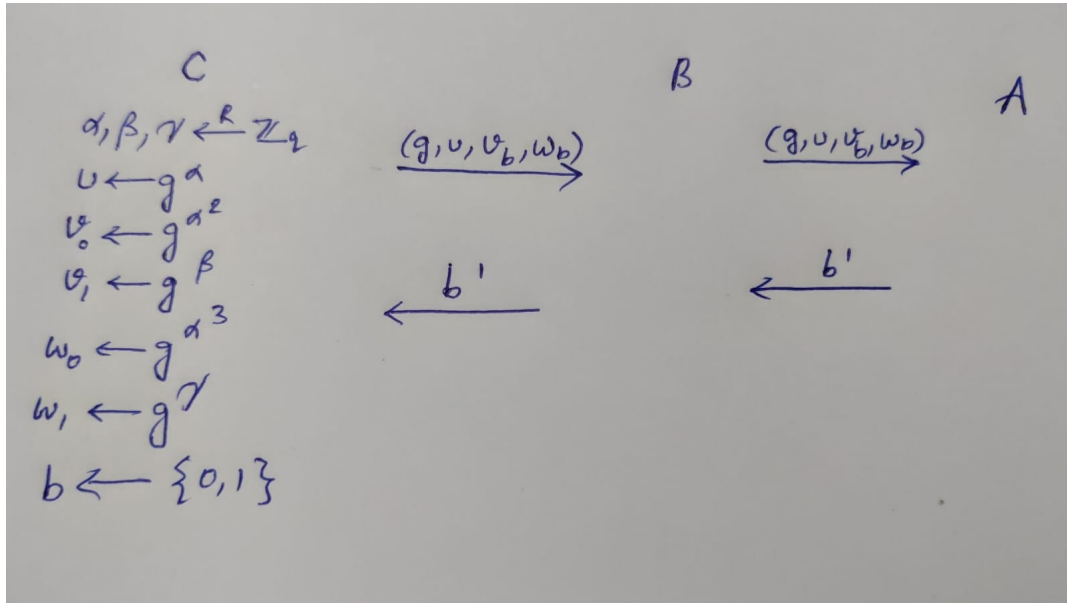


Figure 8: Reduction for Problem 5d

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

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

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 shown in Fig. 8

(e) TODO