COL759 Assignment 1

Satyam Modi, Prashant Mishra

TOTAL POINTS

43 / 50

QUESTION 1

1 Q1 8 / 10

✓ **+ 2 pts** **Correct answer for |C| vs |M|**

+ 0 pts |K| vs |M| not attempted, or incorrect.

+ 2 pts |K| vs |M| attempted, but vague argument

+ 5 pts |K| vs |M| attempted, core idea is correct for the argument, but proof is incomplete/imprecise

✓ **+ 8 pts** **Correct proof**

+ 0 pts Not attempted/ Wrong Answer

- 1 pts For not explaining relation between perfect correctness and your answer.

- 2 Point adjustment

2 marks deducted for not describing the adversary properly.

Overall comments on submission:
- you seem to have the correct ideas, and enough mathematical maturity to express those ideas properly. However, the submission was difficult to read (for someone scoring 40+, I would expect the solutions to be cleaner). Please break down your proofs into claims/lemmas/theorems. Use proper math environments.
- In Q2, I couldn't understand why your reduction was playing the encryption security game. Discuss with me.

1 explain the adversary's strategy in full detail. What messages does the adversary send. You say "it can check for some message m" --- it should check for m0, m1 that it sends.

QUESTION 2

2 Q2 5 / 10

✓ **+ 2 pts** **Shannon OTP insecure**

+ 0 pts 2.2 not attempted/incorrect

+ 2 pts Correct reduction, analysis not included

+ 5 pts Correct reduction, partial analysis provided

+ 8 pts Correct reduction and analysis

✓ **+ 3 pts** **Partial proof, but no reduction described. Or reduction is playing the wrong security game.**

2 Please make your analysis a bit more readable from next time. It is difficult to verify the correctness.

3 B should be playing the PRG game, why is B sending m0, m1 to the PRG challenger?

QUESTION 3

3 Q3 15 / 15

+ 0 pts Incorrect calE' scheme. The proposed scheme either does not satisfy no.q.ss, or is closely related to \calE, and hence may not be KDM insecure.

✓ **+ 4 pts** **Correct \calE'**

+ 3 pts Partial proof of no.q.s.s. for \calE'

✓ **+ 7 pts** **Correct reduction and proof of no.q.s.s for \calE'**

✓ **+ 4 pts** **correct KDM attack**

QUESTION 4

4 Q4 15 / 15

✓ **+ 6 pts** **Hiding property - complete proof.**

+ 4 pts Hiding property - correct hybrids, incomplete reductions

+ 3 pts Hiding property - complete hybrids, but no reductions described.

+ 2 pts 4.1 Partially correct, incomplete analysis

+ 1 pts Hiding property - no reductions described.

✓ **+ 6 pts** **Binding property - correct proof**

+ **3 pts** Binding property - some missing steps/proof details

✓ **+ 3 pts 4.3: correct reasoning**

+ **1.5 pts** 4.3: partially correct reasoning.

+ **1 pts** only stated which property is violated, without proper justifiction

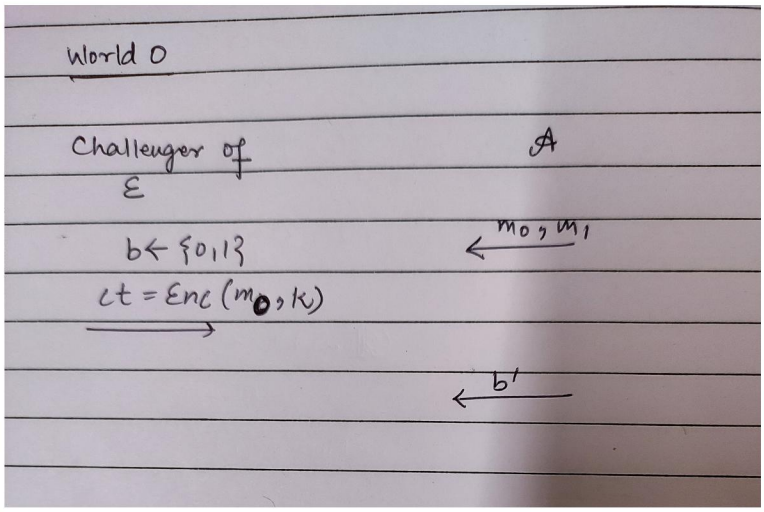
+ **0 pts** 4.3 unattempted/incorrect

4 there is no ciphertext in this game

1 Encryption Schemes with relaxed security

Solution : Given : Let E = (KeyGen, Enc, Dec) be an encryption scheme with message space M, key space K and ciphertext space C. For any adversary A , P [A wins the No-Query-Semantic-Security game] $\leq \frac{1}{2} + \epsilon$.

Here we will be considering an exponential time adversary A through out the solution which will be using the following strategy : If ciphertext ct is known to adversary ,it can check for some message m whether ct is an encryption of message m using some key k or not.



For World-0 let define some terminologies :

Let $S_0 = \{m_1 : Enc(m_1, k') = ct$ for some k' $\in$ K where "ct" is ciphertext of m_0 i.e., $Enc(m_0, k) = ct\}$

Let define an Event E_0 := the message m_1 is chosen such that there exists a key k_1 such that $E(m_1, k_1) = ct$.

Let define an Event E_0^c(complement of E_0) := There does not exists any key k_1 such that E(m_1, k_1) = ct for any given message m_1 .

P(E_0 | b=0) = Probability that m_1 is chosen randomly from message space M and it satisfy following condition i.e., $\exists$ k' $\in$ K such that $Enc(m_1, k')$ =ct

$\Rightarrow$ P(E_0 | b=0) = $\frac{|S_0|}{|M|}$ ..(1)

P(E_0^c | b=0) = Probability that m_1 is chosen randomly from message space M and it satisfy following condition i.e., there do not exist any k' $\in$ K such that Enc(m_1, k') = ct.
$\Rightarrow$ P(E_0^c | b=0) = 1- P(E_0 | b=0) = 1- $\frac{|S_0|}{|M|}$ ..(2)

P(b' =0 | E_0,b=0) = Probability that Adversary will predict b' =0 given that E_0 occur and m_0 is encrypted by Challenger = Probability that Adversary will output (b'=0) randomly = $\frac{1}{2}$. ..(3)

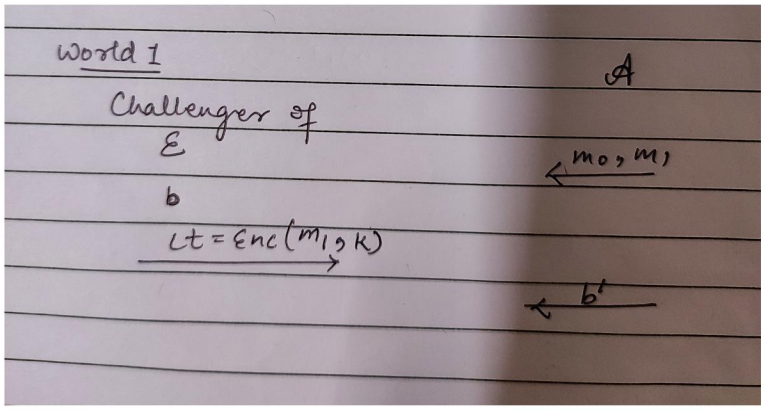
P(b' =0 | E_0^c,b=0) = Probability that Adversary will predict b' =0 given that E_0^c occur and m_0 is encrypted by Challenger =1.

In this case, since E_0^c holds, $\nexists$ any k' such that Enc(m_1,k') =ct in this case. So, the adversary A will simply output 0 with probability 1 as that is the only possibility.

P(b' = 0 | $b = 0$) = $P(b' = 0 \cap E_0 \mid b = 0) + P(b' = 0 \cap E_0^c \mid b = 0) = P(b' = 0 \mid E_0, b = 0) * P(E_0 \mid b = 0) + P(b' = 0 \mid E_0^c, b = 0) * P(E_0^c \mid b = 0)$ ..(5)

P(b' = 0 | $b = 0$) = $\frac{1}{2} * \frac{|S_0|}{|M|}$ +1*(1-$\frac{|S_0|}{|M|}$) = 1- $\frac{|S_0|}{2|M|} \geq 1 - \frac{|K|}{2|M|}$ ($|S_0| \leq |K|$) ..(6)

(As we have $|K|$ different keys then at most $|K|$ ciphertext can be matched to it i.e., $|S_0| \leq |K|$)



For World-1 let define some terminologies :

Let $S_1 = \{m_0 : Enc(m_0, k') = ct$ for some k' $\in$ K where "ct" is cipertext of m_1 i.e., Enc(m_1, k) = $ct\}$

Let define an Event E_1 := the message m_0 is chosen such that there exists a key k_0 such that $E(m_0, k_0) = ct$.

Let define an Event E_1^c(complement of E_1) := the message m_0 is such that there does not exists a key k_1 such that $E(m_1, k_1) = ct$.

P(E_1 | b=1) = Probability that m_0 is chosen randomly from message space M and it satisfy following condition i.e., $\exists$ k' $\in$ K such that Enc(m_0, k') =ct
$\Rightarrow$ P(E_1 | b=1) = $\frac{|S_1|}{|M|}$ ..(7)

P(E_1^c | b=1) = Probability that m_0 is chosen randomly from message space M and it satisfy following condition i.e., there do not exist any k' $\in$ K such that Enc(m_0, k') = ct.
$\Rightarrow$ P(E_1^c | b=1) = 1- P(E_1 | b=1) = 1- $\frac{|S_1|}{|M|}$ ..(8)

P(b' =1 | E_1,b=1) = Probability that Adversary will predict b' =1 given that E_1 occur and m_1 is encrypted by Challenger = Probability that Adversary will output (b') randomly = $\frac{1}{2}$. ..(9)

P(b' =1 | E_1^c,b=1) = Probability that Adversary will predict b' =1 given that E_1^c occur and m_1 is encrypted by Challenger =1.

In this case, since E_1^c holds, $\nexists$ any k' such that Enc(m_0,k') =ct in this case. So, the adversary A will simply output 1 with probability 1 as that is the only possibility.

P(b' = 1 | $b = 1$) = $P(b' = 1 \cap E_1 \mid b = 1) + P(b' = 1 \cap E_1^c \mid b = 1) = P(b' = 1 \mid E_1, b = 1) * P(E_1 \mid b = 1) + P(b' = 1 \mid E_1^c, b = 1) * P(E_1^c \mid b = 1)$ ..(11)

P(b' = 1 | $b = 1$) = $\frac{1}{2} * \frac{|S_1|}{|M|}$ +1*(1-$\frac{|S_1|}{|M|}$) = 1- $\frac{|S_1|}{2|M|} \geq 1 - \frac{|K|}{2|M|}$ ($|S_1| \leq |K|$) ..(12)

(As we have $|K|$ different keys then at most $|K|$ ciphertext can be matched to it i.e., $|S_1| \leq |K|$)

Let define total probability .

P [A wins the No-Query-Semantic-Security game] = P(b' = 0 | $b = 0) * P(b =$ 0) + $P(b' = 1 \mid b = 1) * P(b = 1)$. ..(13)

As we know that Challenger randomly choose b value for message encryption.

P(b = 0) = P (b = 1) = $\frac{1}{2}$. ..(14)

P [A wins the No-Query-Semantic-Security game] = $\frac{1}{2}$*{P(b' = 0 | $b = 0) +$ $P(b' = 1 \mid b = 1)\}$ ..(15)

Let substitute Equation 6 and Equation 12 value into Equation 15 :

P [A wins the No-Query-Semantic-Security game] = $\frac{1}{2}$*(1-$\frac{|S_0|}{2|M|} + 1 - \frac{|S_1|}{2|M|}$) $\geq \frac{1}{2}$*(1-$\frac{|K|}{2|M|} + 1 - \frac{|K|}{2|M|}$) $= 1 - \frac{|K|}{2|M|}$ ..(16)

Now as equation 13 will satisfy given condition i.e., P [A wins the No-Query-Semantic-Security game] $\leq \frac{1}{2} + \epsilon \Rightarrow 1 - \frac{|K|}{2|M|} \leq \frac{1}{2} + \epsilon \Rightarrow |K| \geq (1 - 2\epsilon)|M|$

Hence , Relation between $|K|$ and $|M|$ is $|K| \geq (1 - 2\epsilon)|M|$

Let now derive relation between $|C|$ and $|M|$.

Observation : We know that for any k $\in$ K , Enc(m_i,k) $\neq$ Enc(m_j,k) for i $\neq$ j.

Hence for each k $\in$ K, we get $|M|$ distinct ciphertext from each m $\in$ M as per above observation.

Hence we can conclude that $|C| \geq |M|$

1 Q1 8 / 10

✓ **+ 2 pts** **Correct answer for |C| vs |M|**

+ 0 pts |K| vs |M| not attempted, or incorrect.

+ 2 pts |K| vs |M| attempted, but vague argument

+ 5 pts |K| vs |M| attempted, core idea is correct for the argument, but proof is incomplete/imprecise

✓ **+ 8 pts** **Correct proof**

+ 0 pts Not attempted/ Wrong Answer

- 1 pts For not explaining relation between perfect correctness and your answer.

- 2 **Point adjustment**

2 marks deducted for not describing the adversary properly.

Overall comments on submission:
- you seem to have the correct ideas, and enough mathematical maturity to express those ideas properly. However, the submission was difficult to read (for someone scoring 40+, I would expect the solutions to be cleaner). Please break down your proofs into claims/lemmas/theorems. Use proper math environments.
- In Q2, I couldn't understand why your reduction was playing the encryption security game. Discuss with me.

1 explain the adversary's strategy in full detail. What messages does the adversary send. You say "it can check for some message m" --- it should check for m0, m1 that it sends.

2 Security against key recovery attacks

Solution : Given : Let E = (KeyGen, Enc, Dec) be an encryption scheme with message space M, key space K and ciphertext space C.

We define security game between Challenger and Adversary as follows:

Key-Recovery-Security

1.The challenger chooses a message m ← M, key k ← K and sends (m, Enc(m, k)) to the adversary.

2.The adversary sends its guess k , and wins the security game if k = k' .

We say that E is secure against key-recovery attacks if, for every prob. poly. time adversary A, there exists a negligible function μ(·) such that for all n,

Pr [A wins the Key-Recovery-Security game] $\leq \frac{1}{|K|}$ + μ(n). (1)

(a) Solution : Encryption Scheme for Shannon's One-Time Pad is such that given m ∈ M and k ∈ K then Enc(m,k)=m $\oplus k$.

Now as per Key-Recovery-Security game let show that Adversary can always win with probability 1 by giving following strategy.

As adversary will receiver (m,Enc(m,k)) = (m,m⊕ k) =(m,ct) form Challenger then he/she can easily recover key by doing following operation $\Rightarrow m \oplus ct = m \oplus (m \oplus k) = k$.

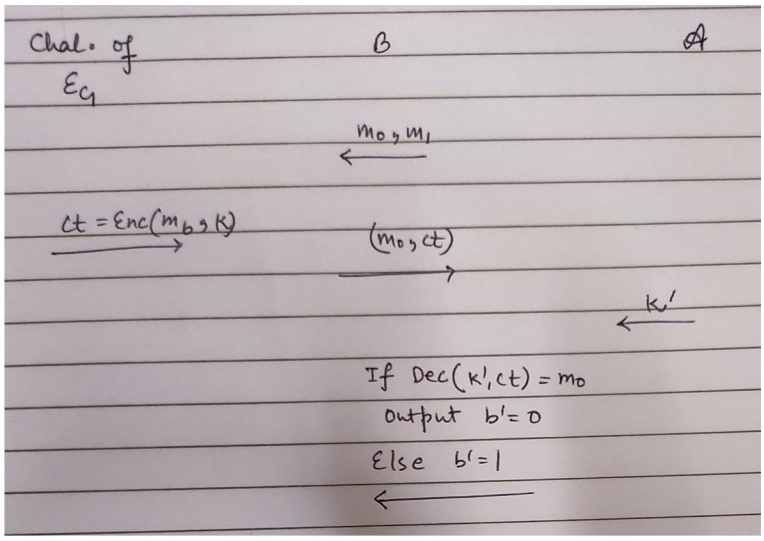
As Pr [A wins the Key-Recovery-Security game] = 1, this does not satisfy the given condition (1) of Key-Recovery-Security.

Hence , Shannon's One-Time Pad is not secure against key recovery attacks.

(b) Solution : Given : G : $\{0, 1\}^n \rightarrow \{0, 1\}^{100n}$ be a secure pseudorandom generator.

To show : the encryption scheme E_G (with key space K = $\{0, 1\}^n$and message space $M = \{0,1\}^{100n}$) satisfies Key-Recovery-Security, assuming G is a secure

PRG .



We will show that encryption scheme E_G is secure using construction method , let construct a game which include One challenger C , an Adversary B for encryption scheme of PRG G and Adversary A for encryption scheme E_G .

1. First B will send two messages m_0 and m_1 to challenger of E.

2. The challenger will send ciphertext ct=Enc(m_b,k) for some k $\in$ K and b $\in$ {0,1} such that ct=$m_b \oplus G(k)$.

3. Now B will send (m_0,ct) to A where ct is the same ciphertext which B has received from Challenger of E.

4. A will return a key k' $\in$ K to B.

5. Now B will check if G(k')$\oplus ct = m_0$, then it will output b' =0 else output b' = 1 where k' is key send by A in step 4 and ct is ciphertext receive by B at step 2 .

Let define Event E := The key k' send by A match with key k used by Challenger of E for encryption i.e., this condition hold G(k')$\oplus ct = m_0$

Let define Event E^c (E complement) as follows : The key k' send by A do not

match with key k used by Challenger of E for encryption i.e., this condition do not hold G(k')$\oplus ct = m_0$

let define : p = Pr [k=k'].

P(b'=0 | $E, b = 0$) = Probability that E occur (basically key predicted by A matches with key used by challanger) given that m_0 is encrypted by challenger = 1 . ..(1)

P(b'=0 | $E^c, b = 0$) =Probability that E^c occur given b(=0) = 0 . ..(2)

P(b' = 0 | $b = 0$) = $P(b' = 0 \wedge$ E | $b = 0) + P(b' = 0 \wedge$ E^c | $b = 0) = P(b' = 0$ | $E, b = 0) * P(E$ | $b = 0) + P(b' = 0$ | $E^c, b = 0) * P(E^c$ | $b = 0) = 1 * p + (1 - p) * 0 = p$ ..(3)

Let S$_0$ = $\{m_0 : Enc(m_0, k') = ct$ for some k' $\in$ K where "ct" is ciphertext of m_1 i.e., Enc(m$_1, k) = ct\}$

Let define an Event E_0 := the message m_0 is chosen such that there exists a key k_0 such that $E(m_0, k_0) = ct$ where ct is ciphertext of m_1 .

Let define an Event E_0^c(complement of E_0) := There does not exists any key k_0 such that E(m_0, k_0) = ct for any given message m_0 and where ct is ciphertext for m_1 .

let define p' = P(E_0 | $b = 0$) = $\frac{|S_0|}{|M|} \leq \frac{|K|}{|M|}$.
. This follows from the fact that for a given ciphertext ct, we can have maximum $|K|$ messages which can encrypt to ct through some key k.

P(b'=1 | $E_0, b = 1$) = Probability that E_0 occur (basically key predicted by A matches with key used by challanger) given that m_1 is encrypted by challenger = 1 . ..(4)

P(b'=1 | $E_0^c, b = 1$) =Probability that E^c occur given b(=1) = 0 . ..(5)

P(b' = 1 | $b = 1$) = $P(b' = 1 \wedge E_0$ | $b = 1) + P(b' = 0 \wedge E_0^c$ | $b = 0) = P(b' = 0$ |E$_0$,b=0)*P(E_0 | $b = 0) + P(b' = 0$ |E$_0^c$,b=0)*P(E_0^c | $b = 0) = p' * 0 + (1 - p') * 1 = 1 - p'$ ..(6)

Let calculate total probability .

Pr[A wins the No-Query-SS game] = P(b' = 0 | $b = 0) * P(b = 0) + P(b' = 1$ | $b = 1) * P(b = 1)$. ..(7)

As we know that Challenger randomly choose b value for message encryption.

P(b = 0) = P (b = 1) = $\frac{1}{2}$. ..(8)

Pr [A wins the No-Query-SS game] = $\frac{1}{2}$*{P(b' = 0 | $b = 0) + P(b' = 1 \mid b = 1)$} ..(9)

Let substitute Equation 3 and Equation 6 value into Equation 9 :

Pr [A wins the No-Query-SS game] = $\frac{1}{2}$(p + 1-p') $\leq \frac{1}{2}$ + μ(n). ..(10)

(Using the Semantic Secure Definition of)

Further solving we will get : p $\leq 2\mu(n)$ + p' $\leq 2\mu(n) + \frac{|K|}{|M|} = 2\mu(n) + \frac{2^n}{2^{100n}} \leq 2\mu(n) + \frac{1}{2^n}$. Since, $p \leq \frac{1}{|K|} + 2\mu(n)$, we have $\mathcal{E}_g$ satisfying the key-recovery security game.

2

2 Q2 5 / 10

✓ + 2 pts **Shannon OTP insecure**

+ 0 pts 2.2 not attempted/incorrect

+ 2 pts Correct reduction, analysis not included

+ 5 pts Correct reduction, partial analysis provided

+ 8 pts Correct reduction and analysis

✓ + 3 pts **Partial proof, but no reduction described. Or reduction is playing the wrong security game.**

2 Please make your analysis a bit more readable from next time. It is difficult to verify the correctness.

3 B should be playing the PRG game, why is B sending m0, m1 to the PRG challenger?

3 Bad Disk Encryption

We are given an encryption scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\{0,1\}^{\leq \ell}$ and key space $\{0,1\}^n$, where $\ell > n$ and $\mathcal{E}$ is semantically secure.
We define our encryption scheme $\mathcal{E}' = (\mathsf{KeyGen}, \mathsf{Enc}', \mathsf{Dec}')$ as follows:

$\underline{\mathsf{Enc}'(m,k)}$
If $|m| \geq n$ and $m[1:n] = k$:
  Output $0 \;||\; m[n+1:|m|]$
Else:
  Output $1 \;||\; \mathsf{Enc}(m,k)$

$\underline{\mathsf{Dec}'(ct,k)}$
If $ct[1] = 0$:
  Output $k \;||\; ct[2:|ct|]$
Else:
  Output $\mathsf{Dec}(ct[2:|ct|], k)$

Part(a) Proof for correctness

- **Case - I** When $|m| < n$, we have

$$\begin{aligned} ct = \mathsf{Enc}'(m,k) &= 1 \;||\; \mathsf{Enc}(m,k) \\ \mathsf{Dec}'(ct,k) &= \mathsf{Dec}(ct[2:|ct|], k) \\ &= \mathsf{Dec}(\mathsf{Enc}(m,k), k) \text{ where } ct[2:|ct|] = \mathsf{Enc}(m,k) \\ &= m \end{aligned}$$

- **Case - II** When $|m| \geq n$, we have

  Subpart(a) When $m[1:n] = k$

$$\begin{aligned} ct = \mathsf{Enc}'(m,k) &= 0 \;||\; m[n+1:|m|] \\ \mathsf{Dec}'(ct,k) &= k \;||\; ct[2:|ct|] \text{ since } ct[1] = 0 \end{aligned}$$

  Here, $k = m[1:n]$ and $ct[2:|ct|] = m[n+1:|m|]$ because of the way we encrypted the message m.

$$\begin{aligned} \mathsf{Dec}'(ct,k) &= m[1:n] \;||\; m[n+1:|m|] \\ &= m \end{aligned}$$

  Subpart(b) When $m[1:n]$!= k

$$\begin{aligned} ct = \mathsf{Enc}'(m,k) &= 1 \;||\; \mathsf{Enc}(m,k) \\ \mathsf{Dec}'(ct,k) &= \mathsf{Dec}(ct[2:|ct|], k) \\ &= \mathsf{Dec}(\mathsf{Enc}(m,k), k) \text{ where } ct[2:|ct|] = \mathsf{Enc}(m,k) \\ &= m \end{aligned}$$

  Proved

Part(b) Proof for semantic security of $\mathcal{E}'$

– For this, we assume that there is an adversary $\mathcal{A}$ that can break the semantic security of $\mathcal{E}'$ and then using $\mathcal{A}$, we produce another adversary $\mathcal{B}$ that breaks the semantic security $\mathcal{E}$.
Let p_0 and p_1 be the probability that adversary $\mathcal{A}$ outputs 0 in World 0 and World 1 of encryption scheme $\mathcal{E}'$. We formulate two worlds : World 0 and World 1 described as follows:

1. Adversary $\mathcal{B}$ sends m_0, m_1 to Challenger of $\mathcal{E}$.
2. Challenger of $\mathcal{E}$ sends $ct = \mathsf{Enc}'(m_b, k)$ where $b \leftarrow \{0, 1\}$
3. $\mathcal{B}$ forwards $ct' = 1 \mid\mid ct$ to the adversary $\mathcal{A}$ of $\mathcal{E}'$.
4. Now, $\mathcal{A}$ outputs b' which it forwards to $\mathcal{B}$.
5. $\mathcal{A}$ forwards b' to Challenger of $\mathcal{E}$.

  * **World**$_0$

    * Here, the adversary $\mathcal{B}$ chooses two messages m_0 and m_1 such that $|m_0| = |m_1| > n$ and sends to the challenger of $\mathcal{E}$. The challenger sends the ciphertext $ct = \mathsf{Enc}(m_0, k)$. After the adversary $\mathcal{B}$ receives the ciphertext ct, $\mathcal{B}$ sends $1 \mid\mid ct$ to adversary $\mathcal{A}$ (of encryption scheme $\mathcal{E}'$). The adversary $\mathcal{A}$ sends b' to adversary $\mathcal{B}$ which it forwards to challenger of $\mathcal{E}$. We find out $\Pr(b' = 0 | b = 0)$ as follows:
    1. $\Pr(b' = 0 \mid b = 0) = \Pr(b' = 0 \wedge m_0[1:n] = k \mid b = 0) + \Pr(b' = 0 \wedge m_0[1:n] \neq k \mid b = 0)$

    2. $\Pr(b' = 0 \wedge m_0[1{:}n] = k \mid b = 0) = \Pr(b' = 0 \mid m_0[1{:}n] = k, b = 0) \times \Pr(m_0[1:n] = k \mid b = 0) = \frac{1}{2^n}\Pr(b' = 0 \mid m_0[1:n] = k, b = 0) = \frac{1}{2^n}p$ where $p = \Pr(b' = 0 \mid m_0[1:n] = k, b = 0)$. Note that in this case probability of outputting 0 is not same as p_0 because the adversary $\mathcal{A}$ expects $0 \mid\mid m_0[n+1 : |m_0|]$ but it gets $1 \mid\mid \mathsf{Enc}(m_0, k)$. So, we assume that the probability of outputting 0 is some p in this case.

    3. $\Pr(b' = 0 \wedge m_0[1:n] \neq k \mid b = 0) = \Pr(b' = 0 \mid m_0[1{:}n] \neq k, b = 0) \times \Pr(m_0[1:n] \neq k \mid b = 0) = \frac{1}{2^n}\Pr(b' = 0 \mid m_0[1:n] \neq k, b = 0) = (1 - \frac{1}{2^n})p_0$

    4. $\Pr(b' = 0 \mid b = 0) = \frac{1}{2^n}p + (1 - \frac{1}{2^n})p_0$

– **World**$_1$

  – Here, the adversary $\mathcal{B}$ chooses two messages m_0 and m_1 such that $|m_0| = |m_1| > n$ and sends to the challenger of $\mathcal{E}$. The challenger sends the ciphertext $ct = \mathsf{Enc}(m_1, k)$. After the adversary $\mathcal{B}$ receives the ciphertext ct, $\mathcal{B}$ sends $1 \mid\mid ct$ to adversary $\mathcal{A}$ (of encryption scheme $\mathcal{E}'$). The adversary $\mathcal{A}$ sends b' to ad-

versary $\mathcal{B}$ which it forwards to challenger of $\mathcal{E}$. We find out $\Pr(b' = 0|b = 1)$ as follows:
1. $\Pr(b' = 0 \mid b = 1) = \Pr(b' = 0 \wedge m_1[1:n] = k \mid b = 1) + \Pr(b' = 0 \wedge m_1[1:n] \neq k \mid b = 1)$

2. $\Pr(b' = 0 \wedge m_1[1{:}n] = k \mid b = 1) = \Pr(b' = 0 \mid m_0[1{:}n] = k, b = 1) \times \Pr(m_1[1:n] = k \mid b = 1) = \frac{1}{2^n}\Pr(b' = 0 \mid m_1[1:n] = k, b = 1) = \frac{1}{2^n}p'$ where $p' = \Pr(b' = 0 \mid m_1[1:n] = k, b = 1)$. Note that in this case probability of outputting 0 is not same as p_0 because the adversary $\mathcal{A}$ expects $0 \mid\mid m_1[n+1:|m_0|]$ but it gets $1 \mid\mid \mathsf{Enc}(m_1, k)$. So, we assume that the probability of outputting 0 is some p' in this case.

3. $\Pr(b' = 0 \wedge m_1[1:n] \neq k \mid b = 1) = \Pr(b' = 0 \mid m_1[1{:}n] \neq k, b = 1) \times \Pr(m_1[1:n] \neq k \mid b = 1) = \frac{1}{2^n}\Pr(b' = 0 \mid m_1[1:n] \neq k, b = 1) = (1 - \frac{1}{2^n})p_1$

4. $\Pr(b' = 0 \mid b = 1) = \frac{1}{2^n}p' + (1 - \frac{1}{2^n})p_1$

Now, $|\Pr(b' = 0 \mid b = 0)$ - $\Pr(b' = 0 \mid b = 1)| = |\frac{1}{2^n}(p - p') + (1 - \frac{1}{2^n}) \times (p_0 - p_1)|$. Since, $|p_0 - p_1|$ is non-negligible and $\frac{1}{2^n}(p - p')$, $\frac{1}{2^n}(p_0 - p_1)$ are negligible. Thus, the overall expression is non-negligible. This proves that adversary B breaks the semantic security of $\mathcal{E}$.

But $\mathcal{E}$ is semantically secure, this proves that our assumption that $\mathcal{E}'$ is not semantically secure is false. This proves that $\mathcal{E}'$ is semantically secure.

Part(c) $\mathcal{E}'$ is not secure against KDM

- Here, we produce the adversary $\mathcal{A}$ which break the KDM security of $\mathcal{E}'$. $\mathcal{A}$ sends two messages m_0 and m_1 (distinct) to the challenger of the KDM security game of $\mathcal{E}'$. The ciphertext ct, adversary $\mathcal{A}$ receives is $\mathsf{Enc}'(k||m_b, k) = m_b$(Follows from our encryption algorithm). When adversary $\mathcal{A}$ receives ct, it compares ct with message m_0 and m_1 and outputs 0 if $ct = m_0$ and 1 if $ct = m_1$.

$$\begin{aligned}\Pr[\mathcal{A} \text{ wins}] &= \tfrac{1}{2}\Pr(b' = 0 \mid b = 0) + \tfrac{1}{2}\Pr(b' = 1 \mid b = 1)\\ &= \tfrac{1}{2} \times 1 + \tfrac{1}{2} \times 1\\ &= 1\end{aligned}$$

3 Q3 15 / 15

+ **0 pts** Incorrect calE' scheme. The proposed scheme either does not satisfy no.q.ss, or is closely related to \calE, and hence may not be KDM insecure.

✓ **+ 4 pts** **Correct \calE'**

+ **3 pts** Partial proof of no.q.s.s. for \calE'

✓ **+ 7 pts** **Correct reduction and proof of no.q.s.s for \calE'**

✓ **+ 4 pts** **correct KDM attack**

4 Bit Commitment Schemes from PRGs

- **1. Proof that the commitment scheme satisfies the hiding property.**

World 0
1. Adversary $\mathcal{A}$ sends m to Challenger.
2. Challenger sends $ct = G(k)$
3. $\mathcal{A}$ forwards b' to Challenger of $\mathcal{E}$.
$p_0 = \Pr(b' = 0)$

World 1
1. Adversary $\mathcal{A}$ sends m to Challenger.
2. Challenger sends $ct = m \oplus G(k)$
3. $\mathcal{A}$ forwards b' to Challenger of $\mathcal{E}$.
$p_1 = \Pr(b' = 0)$

Hybrid World
1. Adversary $\mathcal{A}$ sends m to Challenger.
2. Challenger chooses $r \leftarrow \{0,1\}^{3n}$ and sends $ct = m \oplus r$
3. $\mathcal{A}$ forwards b' to Challenger of $\mathcal{E}$.
$p_{hyb} = \Pr(b' = 0)$

We proceed by assuming that the commitment scheme is not secured against Hiding game and adversary $\mathcal{A}$ can break the hiding security of the scheme. i.e. $|p_0 - p_1| \geq \mu(n)$ for some non-negligible functions $\mu(n)$. This means either $p_0 - p_{hyb}$ is non-negligible or $p_{hyb} - p_1$ is non-negligible.

Thus, The reduction algorithm $\mathcal{B}$ interacts with the PRG challenger and the adversary $\mathcal{A}$. It chooses a uniformly random bit β (this bit decides whether it guesses $p_0 - p_{hyb}$ is non-negligible, or $p_{hyb} - p_1$ and does the following:

- If $\beta = 0$, the reduction algorithm guesses that $p_0 - p_{hyb}$ is non-negligible. We first prove that the ciphertext ct that the adversary $\mathcal{A}$ receives in the hybrid world is also random if r chosen is random. Let s_1 and s_2 be any random string from $\{0,1\}^{3n}$.
  $\Pr(ct = s_1) = \Pr(m \oplus r = s_1) = \Pr(r = m \oplus s_1)$
  $\Pr(ct = s_2) = \Pr(m \oplus r = s_2) = \Pr(r = m \oplus s_2)$
  Since, $\Pr(r = m \oplus s_1) = \Pr(r = m \oplus s_2) \implies \Pr(ct = s_1) = \Pr(ct = s_2)$.
  This proves that ciphertext ct being output in the hybrid world is also random(in distribution). Now, since the adversary $\mathcal{A}$ can distinguish between World 0 and Hybrid world, we know that the adversary $\mathcal{A}$ is able to distinguish between $G(k)$ and a random output r.

  The reduction algorithm $\mathcal{B}$ works as follows in this case:

1. The challenger of PRG G chooses $b \leftarrow \{0,1\}$ sends u_b to $\mathcal{B}$.
2. $\mathcal{B}$ forwards u_b to adversary $\mathcal{A}$.
3. $\mathcal{A}$ outputs b'.
4. $\mathcal{B}$ forwards b' to Challenger.

$\Pr(\mathcal{B} \text{ wins} \mid \beta = 0) = \frac{1}{2} \Pr(b' = 0 \mid b = 0) + \frac{1}{2} \Pr(b' = 1 \mid b = 1) = \frac{1}{2}p_0 + \frac{1}{2}(1 - p_{hyb})$.

– If $\beta = 1$, the reduction algorithm guesses that $p_{hyb} - p_1$ is non-negligible.

The reduction algorithm $\mathcal{B}$ works as follows in this case:
1. The challenger of PRG G chooses $b \leftarrow \{0,1\}$ sends u_b to $\mathcal{B}$.
2. $\mathcal{B}$ chooses some random message $m \leftarrow \{0,1\}^{3n}$ forwards $u_b \oplus m$ to adversary $\mathcal{A}$.
3. $\mathcal{A}$ outputs b'.
4. $\mathcal{B}$ forwards $1 - b'$ to Challenger.

The above algorithm works because the adversary $\mathcal{A}$ will be able to distinguish the case $b = 0$ and $b = 1$. When $b = 0$, $\mathcal{A}$ works as per world 1 and when $b = 1$, $\mathcal{A}$ works as per hybrid world. Since, the adversary is able to distinguish between World 1 and Hybrid world, it is able to distinguish between $G(k)$ and r.

$\Pr(\mathcal{B} \text{ wins} \mid \beta = 1) = \frac{1}{2} \Pr(\mathcal{B} \text{ outputs } 0 \mid b = 0) + \frac{1}{2} \Pr(\mathcal{B} \text{ outputs } 1 \mid b = 1) = \frac{1}{2} \Pr(b' = 1 \mid b = 0) + \frac{1}{2} \Pr(b' = 0 \mid b = 1) = \frac{1}{2}(1 - p_1) + \frac{1}{2}p_{hyb}$

$\Pr(\mathcal{B} \text{ wins}) = \Pr(\mathcal{B} \text{ wins} \wedge \beta = 0) + \Pr(\mathcal{B} \text{ wins} \wedge \beta = 1) = \frac{1}{2}(\frac{1}{2}p_0 + \frac{1}{2}(1 - p_{hyb})) + \frac{1}{2}(\frac{1}{2}(1 - p_1) + \frac{1}{2}p_{hyb}) = \frac{1}{2} + \frac{(p_0 - p_1)}{4}$.
Since, $p_0 - p_1$ is non-negligible, we have Pr($\mathcal{B}$ wins) - $\frac{1}{2}$ is non-negligible. This is a contradiction because $\mathcal{E}$ is semantically secure. Thus, our assumption that he commitment scheme is not secured against Hiding game is false.

- **2. Proof that the commitment scheme satisfies the binding property for any choice of G.**

  In the binding game, the challenger chooses the r-msg and sends to $\mathcal{A}$. Adversary sends the commitment com, with two openings op_0 and op_1. Adversary wins if CheckOpen(r-msg, com, op_0, 0) = CheckOpen(r-msg, com, op_1 , 1) = 1. In the given bit commitment scheme, when $b = 0$, we have com = $G(op_0)$ and when $b = 1$, we have com = $G(op_1) \oplus$ r-msg. For adversary to win, $G(op_1) \oplus$ r-msg = $G(op_0)$ must hold which can also be written as $G(op_1) \oplus G(op_0)$ = r-msg. Now, Pr(Adversary wins) = $\Pr(G(op_1) \oplus G(op_0) = \text{r-msg}) \leq (2^n.2^n)/2^{3n} = \frac{1}{2^n}$. This follows because $|G(K)| \leq 2^n$. Since, $\frac{1}{2^n}$ is negligible, we have Pr(Adversary wins) is negligible.

  3. When Commit-Rec simply outputs an empty message, and Commit-Send chooses r-msg, the binding property would break. This follows because now adversary is free to choose r-msg, op_0 and op_1 of his choice.

The adversary $\mathcal{A}$ simply chooses r-msg $= 0^{3n}$ and then randomly chooses op_0 and sets $op_1 = op_0$. In this case, $G(op_0) = G(op_1) = G(op_1) \oplus 0^{3n} = G(op_1) \oplus$ r-msg . Thus, the adversary wins with probability 1 in this case.

4 Q4 15 / 15

✓ **+ 6 pts** **Hiding property - complete proof.**

+ 4 pts Hiding property - correct hybrids, incomplete reductions

+ 3 pts Hiding property - complete hybrids, but no reductions described.

+ 2 pts 4.1 Partially correct, incomplete analysis

+ 1 pts Hiding property - no reductions described.

✓ **+ 6 pts** **Binding property - correct proof**

+ 3 pts Binding property - some missing steps/proof details

✓ **+ 3 pts** **4.3: correct reasoning**

+ 1.5 pts 4.3: partially correct reasoning.

+ 1 pts only stated which property is violated, without proper justifiction

+ 0 pts 4.3 unattempted/incorrect

4 there is no ciphertext in this game

Cryptography COL759 - Assignment 1

Satyam Kumar Modi (2019CS50448), Prashant Mishra (2019CS50506)

January 2022

Contents