CS178 Assignment 1

Jonas Chen

January 21, 2025

Problem 1

> Show that any encryption scheme, say (Gen, Enc, Dec) satisfying one-time uniform ciphertext security can be converted into another encryption scheme (Gen′, Enc′, Dec′) with the following properties:
> - $(\text{Gen}', \text{Enc}', \text{Dec}')$ satisfies one-time uniform ciphertext security
> - The encryption algorithm Enc' is deterministic. Recall that Enc is allowed to be a probabilistic algorithm.

Solution

Recall that a probabilistic algorithm A can be written as $A(x, r)$ where x is in the input, and in addition the output of A depends on randomness r

Recall that an encryption scheme of the form (Gen, Enc, Dec) satisfies one-time uniform ciphertext security if $D_1 = D_2$ for all m where

$$D_1 = \{c \coloneqq \text{Enc}(k, m); k \leftarrow \text{Gen}(\lambda)\}$$

$$D_2 = \left\{c \overset{\$}{\leftarrow} C\right\}$$

for ciphertext space C, and $c \in C$.

Let (Gen, Enc, Dec) satisfy one-time uniform ciphertext security and allow $\text{Enc}(k, m, r)$ to be probabilistic.

Next perform the conversion: set $\text{Dec}' \coloneqq \text{Dec}$ and

convert $\text{Gen}(\lambda)$ to $\text{Gen}'(\lambda, r)$ and let r be sampled from the uniform distribution. If $\text{Gen}(\lambda)$ outputs k then $\text{Gen}'(\lambda, r)$ can generate $k \oplus r$ to guarantee that k is uniformly random (important for satisfying one-time uniform ciphertext security).

then convert $\text{Enc}(k, m, r)$ to $\text{Enc}'(k, m, r)$ where $\text{Enc}'(k, m, r) = k \oplus m$

We showed in class (in the proof that one-time pad satisfies uniform ciphertext security) that the an xor operation for any m and a k sampled from uniform distribution will produce a ciphertext distribution that is the uniform distribution. Therefore Enc' satisfies one-time uniform ciphertext security. Also, since k, m are determined before running Enc' it follows that Enc' is deterministic.

(note that we do not have to modify Dec since we don't have to guarantee that the new encryption scheme is correct)

Problem 2

> Suppose (Gen, Enc, Dec) and (Gen′, Enc′, Dec′) be two encryption schemes satisfying one-time uniform ciphertext security. We design a third encryption scheme, denoted by (Gen″, Enc″, Dec″).
> - $\mathrm{Gen}''(1^{2n})$: Run $\mathrm{Gen}(1^n)$ to generate key k_1. Run $\mathrm{Gen}'(1^n)$ to generate key k_2. Output the key $k = (k_1, k_2)$.
> - $\mathrm{Enc}''(k, m)$: on input $k = (k_1, k_2)$ and $m = (m_1, m_2) \in \{0,1\}^{2n}$, do the following: first run $\mathrm{Enc}(k_1, m_1)$ to obtain c_1. Next run $\mathrm{Enc}'(k_2, m_2)$ to obtain c_2. Output the ciphertext $c = (c_1, c_2)$.
> - $\mathrm{Dec}''(k, c)$: On input $k = (k_1, k_2)$ and ciphertext $c = (c_1, c_2)$, do the following: first run $\mathrm{Dec}(k_1, c_1)$ to obtain m_1. Next run $\mathrm{Enc}'(k_2, c_2)$ to obtain m_2. Output the recovered message $m = (m_1, m_2)$.
>
> Show that $(\mathrm{Gen}'', \mathrm{Enc}'', \mathrm{Dec}'')$ satisfies one-time uniform ciphertext security.

Solution

To show that $(\mathrm{Gen}'', \mathrm{Enc}'', \mathrm{Dec}'')$ satisfy one-time uniform ciphertext security, we need to show that $D_1 = D_2$ where $D_1 = \{(c_1, c_2) \coloneqq \mathrm{Enc}''((k_1, k_2), (m_1, m_2)); k_1 \leftarrow \mathrm{Gen}(1^n); k_2 = \mathrm{Gen}'(1^n)\}$ and $D_2 = \left\{(c_1, c_2) \overset{\$}{\leftarrow} C = \{0,1\}^{2n}\right\}$

$$\Pr[(c_1, c_2) = \mathrm{Enc}''((k_1, k_2), (m_1, m_2))] = \Pr[c_1 = \mathrm{Enc}(m_1, k_1)] \cdot \Pr[c_2 = \mathrm{Enc}'(m_2, k_2)] = \frac{1}{2^n} \cdot \frac{1}{2^n} = \frac{1}{2^{2n}}$$

where the first equality holds by definition, and second equality holds since (Gen, Enc, Dec) and (Gen′, Enc′, Dec′) satisfy one-time uniform ciphertext security. Therefore the ciphertext as defined in distribution D_1 is equivalent to sampling from uniform distribution over $\{0,1\}^{2n}$ since the probability for any particular ciphertext being that particular ciphertext is $\frac{1}{2^{2n}}$

Or, we could parameterize the sizes of $C_1 = \{0,1\}^{l_1}$, and $C_2 = \{0,1\}^{l_2}$ where $c_1 \in C_1, c_2 \in C_2$ i.e.

$$\Pr[(c_1, c_2) = \mathrm{Enc}''((k_1, k_2), (m_1, m_2))] = \Pr[c_1 = \mathrm{Enc}(m_1, k_1)] \cdot \Pr[c_2 = \mathrm{Enc}'(m_2, k_2)] = \frac{1}{2^{l_1}} \cdot \frac{1}{2^{l_2}} = \frac{1}{2^{l_1 + l_2}}$$

then $C = \{0,1\}^{l_1 + l_2}$ where $l_1 + l_2 = 2n$

(we assume that the () operator on messages and ciphertexts means the same as concatenation operator ||)

$\square$

Also apparently, the "hybrid technique" can also be used here:

Define distributions $D_{1.5}$ to be

$D_{1.5} = \{(c_1, c_2) \coloneqq (\mathrm{Enc}'(k_1, m_1), \mathrm{Enc}'(k_2, m_2)); k_1 \leftarrow \mathrm{Gen}(1^n); k_2 \leftarrow \mathrm{Gen}(1^n)\}$. Then we can easily see that $D_1 = D_{1.5}$ by definition of Enc'' and $D_{1.5} = D_2$ by the problem statement which states that $(\mathrm{Gen}', \mathrm{Enc}', \mathrm{Dec}')$ satisfies one-time uniform ciphertext security. Here we have $D_1 = D_{1.5} = D_2$ $\square$

Problem 3

> Consider the following encryption scheme (Gen, Enc, Dec):
> - $\text{Gen}(1^n)$ outputs $k = (k_1, k_2)$, where $k_1 \xleftarrow{\$} \{0,1\}^n, k_2 \xleftarrow{\$} \{0,1\}^n$
> - $\text{Enc}(k, m)$: on input a key $k, m \in \{0,1\}^n$, output $c = (c_1, c_2)$, where $c_1 = (k_1 \wedge m), c_2 = (k_2 \oplus m)$
> - $\text{Dec}(k, c)$: on input $k = (k_1, k_2), c = (c_1, c_2)$, output $k_2 \oplus c_2$ as the recovered message
>
> Show that there exists a message m such that the ciphertext distribution for this message is identical to the uniform distribution on $\{0,1\}^{2n}$.

Solution

set $m := k_1$ then $c_1 = k_1 \wedge k_1 = k_1$. Since k_1 is sampled from uniform distribution, then c_1 is sampled from uniform distribution. In class, we showed that c_2 is also sampled from uniform distribution. (one time pad achieves one time uniform security)

then (c_1, c_2) generated by Enc for this choice of m will be equivalent to be sampling from $\{0,1\}^{2n}$ uniformly (since both $c_1, c_2 \xleftarrow{\$} \{0,1\}^n$ as explained above)

(note: the problem statement is stated in a way which implies that $(c_1, c_2) \in \{0,1\}^{2n}$) $\square$

(Another possible choice is $m = 1^n = \underbrace{1...1}_{\text{n times}}$ since this choice of m results in $c_1 \xleftarrow{\$} \{0,1\}^n$, see the explanation in problem 4.)

The implication is that the encryption scheme does not satisfy uniform ciphertext security

Problem 4

Consider the following encryption scheme (Gen, Enc, Dec):

- $\text{Gen}(1^n)$ outputs $k = (k_1, k_2, k_3)$, where $k_1 \xleftarrow{\$} \{0,1\}^n, k_2 \xleftarrow{\$} \{0,1\}^n, k_3 \xleftarrow{\$} \{0,1\}^n$
- $\text{Enc}(k, m)$: on input a key $k = (k_1, k_2, k_3), m \in \{0,1\}^n$, output $c = (c_1, c_2, c_3)$, where $c_1 = (k_1 \wedge m), c_2 = (k_2 \vee m), c_3 = k_3 \oplus m$
- $\text{Dec}(k, c)$: on input $k = (k_1, k_2, k_3), c = (c_1, c_2, c_3)$, output $k_3 \oplus c_3$ as the recovered message

Show that there exists **no** message m such that the ciphertext distribution for this message is identical to the uniform distribution on $\{0,1\}^{3n}$.

Solution

On a high level, we need to show that for some fixed m that Enc's generation of c_1 and c_2 cannot be equivalent to sampling from uniform distribution over $\{0,1\}^n$ to generate c_1, c_2. (from class we know that c_3 when generated by Enc is equivalent to sampling from the uniform distribution over $\{0,1\}^n$) .

First, we can observe that in order for $c_1 = k_1 \wedge m$ to have distribution that is equal to uniform distribution, it is required that $m = 1...1$ (i.e. m must contain n $1'$s). Since k is sampled from uniform random dist, $\Pr[c_{1i} = 0] = \Pr[c_{1i} = 1] = 0.5$. If any bit of m_i is 0, then $\Pr[c_{1i} = 0] = 1$, which would violate condition for being uniformly random.

However, if $m = 1...1$ then $\Pr[c_2 = 1...1] = \Pr[k_2 \vee m = 1...1] = 1$, therefore c_2 cannot be sampled uniformly from $\{0,1\}^n$

Conversely, if $c_2 \xleftarrow{\$} \{0,1\}^n$ then it must be true that $m = 0...0$ (by similar logic). But then $\Pr[c_1 = 0...0] = 1$ and therefore c_1 cannot be chosen from uniform distribution $\{0,1\}^n$

To summarize, we have shown that $c_1 \xleftarrow{\$} \{0,1\}^n \Rightarrow c_2 \overset{\$}{\not\leftarrow} \{0,1\}^n$ and that $c_2 \xleftarrow{\$} \{0,1\}^n \Rightarrow c_1 \overset{\$}{\not\leftarrow} \{0,1\}^n$

Therefore, (c_1, c_2, c_3) is never sampled from the uniform distribution on $\{0,1\}^{3n}$ and therefore no m exists such that (c_1, c_2, c_3) is uniform. $\square$

This means encryption scheme does not satisfy uniform ciphertext security