Cryptographic Protocols, day 4 exercises

Adrián Enríquez Ballester

February 22, 2022

1 Perfect security against key recovery

A Shannon cipher $\mathcal{E} = (E, D)$ defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ is perfectly secure against key recovery if $\forall k_0, k_1 \in \mathcal{K}$ and $\forall c \in \mathcal{C}$

$$Pr[E(k_0, m) = c] = Pr[E(k_1, m) = c]$$

where the probability runs over the choice of m, which is chosen uniformly at random in $\mathcal{M}$.

1.a Perfectly secure against key recovery does not imply perfectly secure

Consider the identity cipher $\mathcal{E} = (E, D)$ where $E(k, m) = m$ and $D(k, c) = c$, which is trivially a Shannon cipher because $\forall k \in \mathcal{K}$ and $\forall m \in \mathcal{M}$ we have

$$D(k, E(k, m)) = D(k, m) = m$$

This cipher is not perfectly secure in also a trivial way because it leaks everything about the message:

$$Pr[E(k, m) = c] = \begin{cases} 1, & \text{if } m = c \\ 0, & \text{otherwise} \end{cases}$$

$\forall m \in \mathcal{M}$ and $\forall c \in \mathcal{C}$, where the probability runs uniformly over the choice of k in $\mathcal{K}$.

At the same time, it is perfectly secure against key recovery because it does not use the provided key at all:

$$Pr[E(k, m) = c] = 1/|\mathcal{M}|$$

$\forall k \in \mathcal{K}$ and $\forall c \in \mathcal{C}$, being the probabilistic experiment at m, distributed uniformly in $\mathcal{M}$.

1.b Perfectly secure does not imply perfectly secure against key recovery

Consider this time a variant of the one-time-pad of size ℓ where the message space $\mathcal{M}$ does not contain the 0^ℓ element.

On the one hand, it still being perfectly secure because, given any message $m \in \mathcal{M}$ and any ciphertext $c \in \mathcal{C}$, there exists one single key $k \in \mathcal{K}$ such that $E(k, m) = c$, namely

$$k = m \oplus c$$

On the other hand, this cipher is not perfectly secure against key recovery because, once anyone observes a ciphertext, it is clear that the key which is the same as the ciphertext has not been used:

$$Pr[E(k, m) = c] = \begin{cases} 0, & \text{if } k = c \\ 1/\left|\mathcal{M}\right|, & \text{otherwise} \end{cases}$$

$\forall k \in \mathcal{K}$ and $\forall c \in \mathcal{C}$, with the probabilistic experiment at m distributed uniformly in $\mathcal{M}$.

This suggests that maybe an analogous version of the Shannon theorem for perfect security against key recovery could be stated when the message space is smaller than the key space.

1.c Both perfectly secure and perfectly secure against key recovery are compatible

We know that the one-time-pad cipher is perfectly secure. This means that $\forall m_0, m_1 \in \mathcal{M}$ and $\forall c \in \mathcal{C}$

$$Pr[E(k, m_0) = c] = Pr[E(k, m_1) = c]$$

where the probability runs over the choice of k, which is chosen uniformly at random in $\mathcal{K}$.

Given that the spaces $\mathcal{M}$ and $\mathcal{K}$ are the same and that the E function is symmetric due to the *xor* commutativity, we can transform the probabilistic experiment above to run over the message space $\mathcal{M}$ given two keys by swapping the function parameters while preserving the equality.

This turns out to be the condition for perfect security against key recovery also satisfied for the one-time-pad.

2 A wrong attempt of semantically secure RSA scheme

Consider the following public key encryption scheme $\mathcal{E} = (G, E, D)$:

- $G(\cdot)$: Same as RSA, namely given a (public) odd integer e, and a parameter size ℓ, generate p, q prime numbers of ℓ bits such that $gcd(e, p-1) = 1$, $gcd(e, q-1) = 1$.

  Compute $N = p \cdot q$, $\varphi(N) = (p-1) \cdot (q-1)$ and $d = e^{-1} \bmod \varphi(N)$.

  Output $pk = (N, e)$ as public key and $sk = (N, d)$ as private key.

  The message space is $\mathcal{M} = \mathbb{Z}_N^*$ and the ciphertext space is $\mathcal{C} = (\mathbb{Z}_N^*)^2$.

- $E(pk, m)$: Choose a random $x \in \mathbb{Z}_N^*$, define

$$c_1 = x^e \bmod N$$

  and

$$c_2 = x \cdot m \bmod N$$

  and output the ciphertext $c = (c_1, c_2)$.

- $D(sk, c)$: Compute $\widetilde{m} = c_2 / c_1^d \bmod N$ and output $\widetilde{m}$.

2.a It is a valid public key encryption scheme

Let $m \in \mathcal{M}$ be a message and $pk = (N, e)$, $sk = (N, d)$ the corresponding public and secret keys generated by G.

When performing an encryption for m as $E(pk, m)$, let x be the randomly chosen element from $\mathbb{Z}_N^*$, so the resulting ciphertext is

$$c = (x^e \bmod N, x \cdot m \bmod N)$$

Let us check that we can recover the original m:

$$D(sk, c) = \frac{x \cdot m}{(x^e)^d} \bmod N =$$

As $(x^a)^b = x^{a \cdot b \bmod \varphi(N)} \bmod N$, and $d = e^{-1} \bmod \varphi(N)$, the denominator reduces into x:

$$(x^e)^d \bmod N = x^{e \cdot e^{-1} \bmod \varphi(N)} \bmod N = x$$

so the whole expression becomes

$$D(sk, c) = \frac{x \cdot m}{x} \bmod N = m$$

and this means that

$$Pr[D(sk, E(pk, m)) = m] = 1$$

when m is randomly chosen from $\mathcal{M}$, because it already holds $\forall m \in \mathcal{M}$.

2.b It is not semantically secure

Consider an adversary $\mathcal{A}$ for the semantically secure attack game which receives $pk = (N, e)$ from the challenger, computes two different messages m_0, m_1 and sends them to the challenger.

The challenger replies with a ciphertext $c = (c_1, c_2)$ and $\mathcal{A}$ computes

$$x_i = c_2/m_i \bmod N$$

for each $i \in \{0, 1\}$.

By checking which one satisfies $x_i^e \bmod N = c_1$, it can be distinguished which one of m_0, m_1 has lead to the received ciphertext.

Note that, under this conditions, it is not possible to have two different $x_0, x_1 \in \mathbb{Z}_N^*$ such that $x_0^e = x_1^e$. Otherwise, it would contradict $(x^e)^d = x \bmod N \; \forall x \in \mathbb{Z}_N^*$, which is necessary for this scheme to work, so

$$SSAdv\,[\mathcal{A}, \mathcal{E}] = 1$$

$\mathcal{A}$ would be an efficient adversary (i.e. it performs the kind of operations that the challenger is also performing in an efficient way) with a far from negligible advantage in the game, so this scheme is not semantically secure.

3 A DDH-based public key encryption scheme for bits

Let $\mathbb{G}$ be a group of order q and g a generator of the group. Consider the following public key encryption scheme over message and ciphertext spaces $\mathcal{M} = \{0, 1\}$ and $\mathcal{C} = \mathbb{G}^2$.

- $G(\cdot)$: Chooses α at random in $\mathbb{Z}_q$ and defines $u = g^\alpha$. The public key is $pk = u$ and the secret key is $sk = \alpha$.
- $E(pk, m)$: First, it chooses a random $\beta \in \mathbb{Z}_q$ and defines $c_1 = g^\beta$. Now:
  - If $b = 0$, it defines $c_2 = u^\beta$.
  - If $b = 1$, it takes a random $\gamma \in \mathbb{Z}_q$, and defines $c_2 = g^\gamma$.

  The ciphertext is $c = (c_1, c_2)$.
- $D(sk, c)$: ?

3.a The decryption algorithm

Consider the decryption algorithm to be defined as follows:

$$D(\alpha, (c_1, c_2)) = \begin{cases} 0, & \text{if } c_1^\alpha = c_2 \\ 1, & \text{otherwise} \end{cases}$$

The criteria for assuming when the encryption algorithm has taken the branch corresponding to 0 is based on the fact that

$$c_1^\alpha = (g^\beta)^\alpha = (g^\alpha)^\beta = u^\beta = c_2$$

which will be the case when E is ciphering the bit 0 and not when ciphering the bit 1 unless, due to $\mathbb{G} = \langle g \rangle$ being a group of order q, the randomly chosen $\gamma \in \mathbb{G}$ has been exactly the element $\alpha \cdot \beta$. This leads to the decryption algorithm to output 0 when the original message was 1.

There is one element out of q that produces this failure and, as the choice is uniformly distributed, it will appear with probability $1/q$. This means that

$$Pr[D(sk, E(pk, b)) = b] = 1 - 1/q$$

which can be accepted by weakening the definition of public key encryption scheme and allowing it to fail with negligible probability.

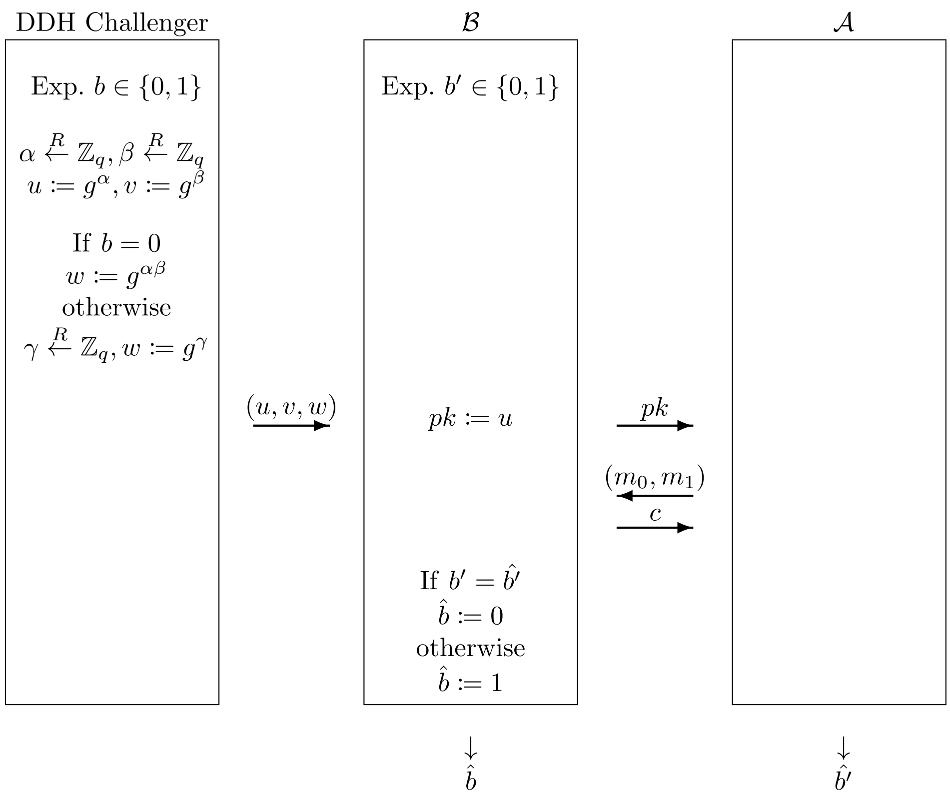
3.b The scheme is CPA-secure

Given an adversary $\mathcal{A}$ of the SS game, we can define an adversary $\mathcal{B}$ for the DDH game which plays also the role of challenger for $\mathcal{A}$ in the former game:

- The DDH challenger chooses α and β at random from $\mathbb{Z}_q$. It also computes $u = g^\alpha$ and $v = g^\beta$.
- If it is playing the DDH experiment $b = 0$, it defines $w = g^{\alpha\beta}$, otherwise it chooses a random γ from $\mathbb{Z}_q$ and defines $w = g^\gamma$.
- The DDH challenger sends the triple (u, v, w) to $\mathcal{B}$.
- $\mathcal{B}$ forwards u to $\mathcal{A}$ as the public key.
- $\mathcal{A}$ computes two messages m_0, m_1 and sends them to $\mathcal{B}$.
- $\mathcal{B}$ defines $c = E(u, m_{b'})$ and replies to $\mathcal{A}$ with it, being $b' \in \{0, 1\}$ the SS experiment being played. The encryption with E is done assuming v as g^β and w as u^β.
- $\mathcal{A}$ outputs $\hat{b'}$ as a guess for the SS experiment being played.
- $\mathcal{B}$ outputs $\hat{b}$ as a guess for the DDH experiment being played, where

$$\hat{b} = \begin{cases} 0, & \text{if } b' = \hat{b'} \\ 1, & \text{otherwise} \end{cases}$$

The explained game can be summarized with the following diagram:



On the one hand, being W_1^{DDH} the event of $\mathcal{B}$ outputting 1 at the DDH experiment 1, the ciphered messages sent to $\mathcal{A}$ are completely random because w itself is random, so we expect that its guess is also random, and also the guess of $\mathcal{B}$:

$$Pr\left[W_1^{DDH}\right] = 1/2$$

On the other hand, with W_0^{DDH} being the event of $\mathcal{B}$ outputting 1 at the DDH experiment 0, we can relate its probability with the SS experiments as follows:

$$\begin{aligned}
Pr\left[W_0^{DDH}\right] = Pr\left[\hat{b} = 1 | b = 0\right] = Pr\left[b' \neq \hat{b}' | b = 0\right] = \\
Pr\left[b' = 0\right] Pr\left[\hat{b}' = 1 | b' = 0\right] + Pr\left[b' = 1\right] Pr\left[\hat{b}' = 0 | b' = 1\right] = \\
1/2 \left(1 - Pr\left[\hat{b}' = 1 | b' = 1\right] + Pr\left[\hat{b}' = 1 | b' = 0\right]\right)
\end{aligned}$$

As W_i^{SS} is the event of $\mathcal{A}$ outputting 1 in the SS experiment i for $i \in \{0, 1\}$, we have

$$Pr\left[W_0^{DDH}\right] = 1/2 - 1/2\left(Pr\left[W_1^{SS}\right] - Pr\left[W_0^{SS}\right]\right)$$

and the adversaries corresponding advantages can be related as follows:

$$\begin{aligned} DDHAdv\left[\mathcal{B}, \mathcal{E}\right] = \left|Pr\left[W_1^{DDH}\right] - Pr\left[W_0^{DDH}\right]\right| \\ = 1/2\left|Pr\left[W_1^{SS}\right] - Pr\left[W_0^{SS}\right]\right| = 1/2 \cdot SSAdv\left[\mathcal{A}, \mathcal{E}\right] \end{aligned}$$

If the decissional Diffie-Hellman assumption holds for $\mathbb{G}$, then $DDHAdv\left[\mathcal{B}, \mathcal{E}\right]$ is negligible and, due to the relation between both advantages, $SSAdv\left[\mathcal{A}, \mathcal{E}\right]$ is also negligible, thus $\mathcal{E}$ is SS-secure.

Finally, we know by a theorem that if a public-key encryption scheme is semantically secure, then it is also CPA secure.