HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

23/10/2023. Homework for Lecture 7.

Exercise 1. Let $\Pi = (Gen, Enc, Dec)$ be a computationally secure encryption scheme. We consider the following experiment:

- Alice produces a random secret key k for the security parameter n,
  $k \leftarrow Gen(1^n)$
- Alice produces a random open messages $m = x_1 \ldots x_n$ of length n bits (with the uniform distribution, i.e., each message can be chosen with the probability $1/2^n$)
- Alice computes an encrypted message $e = Enc(m, k)$
- Adversary obtains the encrypted message e and one more bits that is equal to the parity of all bits of the open message, i.e., $x_1 \oplus x_2 \oplus \ldots \oplus x_n$, and tries to guess x_n,
  $j \leftarrow Adv(1^n, e)$.

The success of Adversary is defined as

$$\mathbf{success} = \begin{cases} 1, & \text{if } j = x_n \\ 0, & \text{otherwise.} \end{cases}$$

Prove that for every poly-time computable algorithm Adv

$$|\text{Prob}[\mathbf{success} = 1] - 1/2|$$

is a negligibly small function.

Exercise 2. Let $\Pi = (Gen, Enc, Dec)$ be a computationally secure encryption scheme. We consider the following experiment:

- Alice produces a random secret key k for the security parameter n,
  $k \leftarrow Gen(1^n)$
- Alice produces a random open messages $m = x_1 \ldots x_n$ of length n bits (with the uniform distribution, i.e., each message can be chosen with the probability $1/2^n$)
- Alice computes an encrypted message $e = Enc(m, k)$
- Adversary obtains the encrypted message e, and tries to guess $x_1 x_2$,
  $j \leftarrow Adv(1^n, e)$, where $j \in \{00, 01, 10, 11\}$.

The success of Adversary is defined as

$$\mathbf{success} = \begin{cases} 1, & \text{if } j = x_1 x_2 \\ 0, & \text{otherwise.} \end{cases}$$

Prove that for every poly-time computable algorithm Adv

$$|\text{Prob}[\mathbf{success} = 1] - 1/4|$$

is a negligibly small function.

Exercise 3. Using the theorem on *semantic security* give a new proof of the fact that for every computationally secure encryption scheme $\Pi = (Gen, Enc, Dec)$, in each of the attacks 2-4 discussed in the class, for every Adversary computable in polynomial time,

the probability of success differs from $1/2$ by only a negligibly small function.

Exercise 4. Find an integer number g such that the sequence

$$g \mod 17,\ g^2 \mod 17,\ g^3 \mod 17, \ldots$$

covers the entire set $\{1, 2, \ldots, 16\}$.