Exercise Sheet #3

Advanced Cryptography 2021

Exercise 1 The Goldwasser-Micali Cryptosystem (midterm 2012)

Consider the group $\mathbf{Z}_n^*$. We recall that if m is an odd factor of n, then the Jacobi symbol $x \mapsto \left(\frac{x}{m}\right)$ is a group homomorphism from $\mathbf{Z}_n^*$ to $\{-1,+1\}$. I.e., $\left(\frac{xy \bmod n}{m}\right) = \left(\frac{x}{m}\right)\left(\frac{y}{m}\right)$. It further has the property that $\left(\frac{x}{mm'}\right) = \left(\frac{x}{m}\right)\left(\frac{x}{m'}\right)$. We consider that multiplication in $\mathbf{Z}_n$ and the computation of the above Jacobi symbol can each be done in $\mathcal{O}((\log n)^2)$.

Let s be a security parameter. We consider the following public-key cryptosystem.

Key Generation. Generate two different odd prime numbers p and q of bit size s, compute $n = pq$, and find some $z \in \mathbf{Z}_n^*$ such that $\left(\frac{z}{p}\right) = \left(\frac{z}{q}\right) = -1$. The public key is (n, z) and the secret key is p.

Encryption. To encrypt a bit $b \in \{0,1\}$, pick $r \in_U \mathbf{Z}_n^*$ and compute $c = r^2 z^b \bmod n$. The ciphertext is c.

Decryption. To decrypt c, compute $\left(\frac{c}{p}\right)$ and find b such that it equals $(-1)^b$. The plaintext is b.

This cryptosystem is known as the Goldwasser-Micali cryptosystem.

1. Show that the cryptosystem is correct. I.e., if the key generation gives (n, z) and p, if b is any bit, if the encryption of b with the key (n, z) produces c, then the decryption of c with the key p produces b.

2. Analyze the complexity of the three algorithms in terms of s.

3. Let $\mathcal{N}$ be the set of all n's which could be generated by the key generation algorithm. Let Fact be the problem in which an instance is specified by $n \in \mathcal{N}$ and the solution is the factoring of n.

   (a) Define the key recovery problem KR related to the cryptosystem. For this, specify clearly what is its set of instances and what is the solution of a given instance.

   (b) Show that the KR problem is equivalent to the Fact problem. Give the actual Turing reduction in both directions.

4. Let QR be the problem in which an instance is specified by a pair (n, c) in which $n \in \mathcal{N}$ and $\left(\frac{c}{n}\right) = 1$. The problem is to decide whether or not c is a quadratic residue in $\mathbf{Z}_n^*$.

(a) Define the decryption problem DP related to the cryptosystem. For this, specify clearly what is its set of instances and what is the solution of a given instance.

(b) Show that the DP problem is equivalent to the QR problem. Give the actual Turing reduction in both directions.

Exercise 2 The CPA-secure PKC from the deterministic PKC (HW 1, 2019)

We define the public key cryptosystem as a set $(\mathsf{Gen}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ with the message domain $\mathcal{M}$ where Gen, Enc and Dec are defined as follows:

- $\mathsf{Gen}(1^\lambda) = (sk, pk)$ is a probabilistic algorithm which takes the security parameter λ as input, and outputs the secret key sk and the public key pk.

- $\mathsf{Enc}(pk, m) = c$ is an algorithm which takes the public key pk and the message $m \in \mathcal{M}$ as input, and outputs ciphertext c.

- $\mathsf{Dec}(sk, c) = m$ is a deterministic algorithm which takes the secret key sk and the ciphertext c as input, and outputs the message m.

We say that $\mathcal{C}$ is a deterministic PKC if $\mathcal{C}.\mathsf{Enc}$ is a deterministic algorithm, and $\mathcal{C}$ is a probabilistic PKC if $\mathcal{C}.\mathsf{Enc}$ is a probabilistic algorithm.

Definition 1 (IND-CPA security) *Let $\mathcal{C}$ be a public key cryptosystem. Then, we say that the public key cryptosystem $\mathcal{C}$ is IND-CPA secure if*

$$\mathsf{Adv}^{\textsf{IND-CPA}}_{\mathcal{A},\mathcal{C}}(\lambda) = \left| \Pr\left[\textsf{IND-CPA}^{\mathcal{A}}_{\mathcal{C}}(0, \lambda) = 1\right] - \Pr\left[\textsf{IND-CPA}^{\mathcal{A}}_{\mathcal{C}}(1, \lambda) = 1\right] \right|$$

is a negligible function in λ for all probabilistic and polynomial time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ where $\textsf{IND-CPA}^{\mathcal{A}}_{\mathcal{C}}$ is defined as follows:

```
Game: $\textsf{IND-CPA}^{\mathcal{A}}_{\mathcal{C}}(b, \lambda)$
$sk, pk \leftarrow \mathsf{Gen}(1^\lambda)$
$m_0, m_1, s_1 \leftarrow \mathcal{A}_1(pk)$                    // $s_1$: State of $\mathcal{A}_1$
$c \leftarrow \mathcal{C}.\mathsf{Enc}(pk, m_b)$
$b' \leftarrow \mathcal{A}_2(c, s_1)$
return $b'$
```

Question 1. Prove that there is no IND-CPA-secure deterministic PKC.

Let $\mathcal{C}_1 = (\mathsf{Gen}_1, \mathcal{M}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ be a deterministic PKC which is secure against chosen plaintext decryption attacks. Then, we define a new PKC $\mathcal{C}_2 = (\mathsf{Gen}_2, \mathcal{M}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ with a group $\mathcal{M}_2 = \mathcal{M}_1$ (with additive notation below) as follows:

- $\mathsf{Gen}_2(1^\lambda)$

  1. Compute $(sk, pk) = \mathsf{Gen}_1(1^\lambda)$
  2. Return (sk, pk)

- $\mathsf{Enc}_2(pk, m)$

  1. Pick a random value r in $\mathcal{M}_2$ of same size as m

2. Compute $c = (c_1, c_2) = (\mathsf{Enc}_1(pk, m + r), \mathsf{Enc}_1(pk, r))$
3. Return c

- $\mathsf{Dec}_2(sk, c)$
  1. Separate c into two ciphertexts (c_1, c_2) encrypted with $\mathcal{C}_1$
  2. Return $\mathsf{Dec}_1(sk, c_1) - \mathsf{Dec}_1(sk, c_2)$

Question 2. Suppose that the message domain $\mathcal{M}_2 = \{0, 1\}^n$ with $\oplus$. Show that $\mathcal{C}_2$ is not IND-CPA-secure, i.e. show there is an adversary $\mathcal{A}$ whose advantage is not negligible.
Hint: Think about the neutral element

Definition 2 (IND-KPA security) *Let $\mathcal{C}$ be a public key cryptosystem. Then, we say that the public key cryptosystem $\mathcal{C}$ is IND-KPA secure if*

$$\mathsf{Adv}^{\mathit{IND\text{-}KPA}}_{\mathcal{A},\mathcal{C}}(\lambda) = \left| \Pr\left[\mathit{IND\text{-}KPA}^{\mathcal{A}}_{\mathcal{C}}(0, \lambda) = 1\right] - \Pr\left[\mathit{IND\text{-}KPA}^{\mathcal{A}}_{\mathcal{C}}(1, \lambda) = 1\right] \right|$$

is a negligible function in λ for all probabilistic and polynomial time algorithm $\mathcal{A}$ where $\mathit{IND\text{-}KPA}^{\mathcal{A}}_{\mathcal{C}}$ is defined as follows:

```
**Game:** $\mathit{IND\text{-}KPA}^{\mathcal{A}}_{\mathcal{C}}(b, \lambda)$
$sk, pk \leftarrow \mathsf{Gen}(1^\lambda)$
$m_0, m_1 \xleftarrow{\$} \mathcal{M} \times \mathcal{M}$
$c \leftarrow \mathcal{C}.\mathsf{Enc}(pk, m_b)$
$b' \leftarrow \mathcal{A}(pk, m_0, m_1, c)$
**return** $b'$
```

Question 3. Show that if $\mathcal{C}_1$ is the plain RSA, $\mathcal{C}_2$ is not IND-KPA-secure when $\mathcal{M}_2$ is a multiplicative group.