MTAT.07.003 Cryptology II
Spring 2010 / Exercise Session V

1. Recall that the message space of the ElGamal cryptosystem is a (t, ε_1)-DDH group $\mathbb{G}$. The latter is rather limiting, since normally one needs to encrypt n-bit messages and not the group elements. The simplified ElGamal cryptosystem is defined as follows:

   - Gen returns $\mathsf{sk} = x$ and $\mathsf{pk} = y = g^x$ for $x \xleftarrow{u} \mathbb{Z}_{|\mathbb{G}|}$;
   - $\mathsf{Enc}_{\mathsf{pk}}(m) = (g^k, h(y^k) \oplus m)$;
   - $\mathsf{Dec}_{\mathsf{sk}}(c_1, c_2) = c_2 \oplus h(c_1^x)$;

   where $h : \mathbb{G} \to \{0,1\}^n$ is a almost regular hash function. That is, the distribution $h(y)$ for $y \xleftarrow{u} \mathbb{G}$ is statistically ε_2-close to the uniform distribution over $\{0,1\}^n$. Prove that the simplified ElGamal cryptosystem is also IND-CPA secure and give the corresponding security bounds.

   Hint: Modify the security proof for the ElGamal cryptosystem to accommodate the change. Where do you need almost regularity?

   ($\star$) In practice, it is difficult if not impossible to define almost regular hash function $h : \mathbb{G} \to \{0,1\}^n$. Relax the security requirements even further so that the corresponding construction is also practical.

2. Prove the only non-trivial inclusion result for homological classification of public key cryptosystems. What about symmetric key cryptosystems?

   Theorem. Assume that $\pi(\cdot)$ is always a t_π-time predicate and it is always possible to obtain a sample from $\mathcal{M}_0$ in time t_m. If the cryptosystem $\mathcal{C}$ is (t, ε)-IND-CCA2 secure, then for all $(t - t_g - 2t_m)$-time adversaries $\mathcal{A}$:

   $$\mathsf{Adv}^{\mathsf{nm\text{-}cca2}}_{\mathcal{C}}(\mathcal{A}) \leq \varepsilon \ .$$

   Why does not a similar proof exists for IND-CCA1⇒NM-CCA1?

($\star$) In a fixed plaintext attack (FPA), an adversary has to fix the queried messages ahead of other interactions. Consequently, it might be possible to achieve a security goal against fixed plaintext attacks (CPA) that is infeasible against chosen ciphertext attacks. This separation manifests already if we consider indistinguishability as a security goal. Recall that a cryptosystem is (t, ε)-IND-FPA if for all t-time adversaries

$$\mathsf{Adv}^{\mathsf{ind\text{-}fpa}}(\mathcal{A}) = |\Pr[\mathcal{G}_0^{\mathcal{A}} = 1] - \Pr[\mathcal{G}_1^{\mathcal{A}} = 1]| \leq \varepsilon$$

where

$\mathcal{G}_0^{\mathcal{A}}$
$(m_0, m_1) \leftarrow \mathcal{A}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
return $\mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_0))$

$\mathcal{G}_1^{\mathcal{A}}$
$(m_0, m_1) \leftarrow \mathcal{A}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
return $\mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_1))$

(a) Prove that if the message space $\mathcal{M} = \{0,1\}$ then IND-FPA security implies IND-CPA security. Generalise the proof and show that IND-FPA security also implies IND-CPA security of encryption tuples

$$\overline{\mathsf{Enc}}_{\mathsf{pk}}(x_1,\ldots,x_n) = \big(\mathsf{Enc}_{\mathsf{pk}}(x_1),\ldots,\mathsf{Enc}_{\mathsf{pk}}(x_n)\big) \ .$$

(b) Give a corresponding construction that converts any IND-FPA secure encryption scheme to the IND-CPA secure encryption scheme. What is the corresponding overhead in communication and computation if we want to preserve the size of the message space?

(c) Prove that IND-FPA security still implies IND-CPA security for larger message spaces; however, the IND-CPA advantage can be $\mathrm{O}(|\mathcal{M}|)$ times larger than the IND-FPA advantage. What is the optimal trade-off point for construction given in (b).

(d) Finally, prove that the reduction result obtained in (c) is tight. For that, give a construction that takes in an IND-CPA secure cryptosystem and creates a new cryptosystem that is functional and IND-FPA secure but the IND-CPA advantage meets the bound derived in (d). If the bounds do not mach exactly, the reduction given in (c) might be non-optimal. Hence, it is important to study the relation between the upper and the lower bound on advantage obtained in (c) and (d).

3. Show that the Goldwasser-Micali cryptosystem is IND-CPA secure if the Quadratic Residuosity Problem is hard. All necessary concepts are defined below. The proof is similar to the analysis of the ElGamal cryptosystem.

Number theory. A prime p is a Blum prime if $p \equiv 3 \mod 4$. Let $N = pq$ where p, q are Blum primes. Then for each element $a \in \mathbb{Z}_N$, we can efficiently compute the Jacobi symbol $(\frac{a}{n})$. One can show that Jacobi symbols satisfies following equations

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\cdot\left(\frac{b}{n}\right) \qquad \text{and} \qquad \left(\frac{a^2}{n}\right) = 1 \ .$$

In the following, we also need a set

$$J_N(1) = \left\{x \in \mathbb{Z}_N : \left(\frac{x}{n}\right) = 1\right\} \ .$$

Finally, recall that an element b is a quadratic residue if there exists a such that $b = a^2 \mod N$. The set of quadratic residues is denoted by QR_N.

Quadratic residuosity problem. Let $\mathbb{P}_n$ denote uniform distribution over n-bit Blum primes. We say that the set of n-bit Blum primes is (t,ε)-secure with respect to quadratic residuosity problem if for all t-time adversaries $\mathcal{A}$:

$$\mathsf{Adv}^{\mathsf{qrp}}_{\mathbb{P}_n}(\mathcal{A}) = \left|\Pr\left[\mathcal{Q}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{Q}_0^{\mathcal{A}} = 1\right]\right| \leq \varepsilon$$

where

$$\begin{array}{ll} \mathcal{Q}_0^{\mathcal{A}} & \mathcal{Q}_1^{\mathcal{A}} \\ \left[\begin{array}{l} p, q \xleftarrow{u} \mathbb{P}(n) \\ N \leftarrow pq \\ x \xleftarrow{u} QR_N \\ \textbf{return } \mathcal{A}(x) \end{array}\right. & \left[\begin{array}{l} p, q \xleftarrow{u} \mathbb{P}(n) \\ N \leftarrow pq \\ x \xleftarrow{u} J_N \setminus QR_N \\ \textbf{return } \mathcal{A}(x) \end{array}\right. \end{array}$$

Goldwasser-Micali cryptosystem.

- **Key generation.** Sample primes $p, q \in \mathbb{P}(n)$ and choose quadratic non-residue $y \in J_N(1)$ modulo $N = pq$. Set $\mathsf{pk} = (N, y)$, $\mathsf{sk} = (p, q)$.
- **Encryption.** First choose a random $x \leftarrow \mathbb{Z}_N^*$ and then compute

$$\mathsf{Enc}_{\mathsf{pk}}(0) = x^2 \mod N \quad \text{and} \quad \mathsf{Enc}_{\mathsf{pk}}(1) = yx^2 \mod N.$$

- **Decryption.** Output 0 if the ciphertext c is quadratic residue and 1 otherwise. The latter is easy if the factorisation of N is known.

4. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public key cryptosystem and $\mathsf{Gen}^\circ, \mathsf{Enc}^\circ, \mathsf{Dec}^\circ)$ a symmetric key cryptosystem. Then we can define a hybrid cryptosystem.

   - **Key generation.** Run the key generation algorithm Gen and output the corresponding secret and public key pair $(\mathsf{sk}, \mathsf{pk})$.
   - **Encryption.** Given a message m, generate a session key $\mathsf{sk}^\circ \leftarrow \mathsf{Gen}^\circ$ and output a pair $c_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\mathsf{sk}_\circ)$ and $c_2 \leftarrow \mathsf{Enc}^\circ_{\mathsf{sk}^\circ}(m)$.
   - **Decryption.** To decrypt a ciphertext (c_1, c_2), first reconstruct the session key $\mathsf{sk}^\circ \leftarrow \mathsf{Dec}_{\mathsf{sk}}(c_1)$ and then recover $m \leftarrow \mathsf{Dec}^\circ_{\mathsf{sk}^\circ}(c_2)$.

   Analyse the IND-CPA security proof for the hybrid encryption scheme.

   (a) Note that the change in the first proof step does not require full IND-CPA security. Derive a minimal reasonable security condition for the public key encryption scheme so that the proof would still hold. A security condition is reasonable if it contains no explicit references to the symmetric cryptosystem and would be universal for all symmetric key cryptosystems. To achieve that, you might slightly change the construction of hybrid encryption scheme. Interpret the result.

   (b) Prove that the same proof construction can be used to shows that hybrid encryption scheme preserves IND-CCA1 security. Derive corresponding security guarantees. Generalise results of (a).

   ($\star$) Why cannot we use the same proof construction to show that hybrid preserves IND-CCA2 security? Give a separation that invalidates the first proof step and the entire claim about IND-CCA2 security. A separation is construction that takes in primitives needed in construct and then modifies them so that new primitives still satisfy the premises but the final claim does not hold, i.e., no proof can exist.

5. A cryptosystem is homomorphic if there exists an efficient multiplication operation defined over the ciphertext space $\mathcal{C}$ such that for any valid encryption $c_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)$ the distribution $c_1 \cdot \mathsf{Enc}_{\mathsf{pk}}(m_2)$ coincides with the distribution $\mathsf{Enc}_{\mathsf{pk}}(m_1 \otimes m_2)$, where $\otimes$ is a binary operation defined over the message space $\mathcal{M}$. Show that

   (a) the RSA cryptosystem is multiplicatively homomorphic;

   (b) the ElGamal cryptosystem is multiplicatively homomorphic;

   (c) the Goldwasser-Micali cryptosystem is XOR homomorphic;

6. Prove the following claims about public key cryptosystems

   (a) A homomorphic cryptosystem cannot be non-malleable.

   (b) NM-CPA security implies IND-CPA security.

   (c) NM-CCA1 security implies IND-CCA1 security.

   (d) NM-CCA2 security implies IND-CCA2 security.

($\star$) Show as many separations among the security properties of cryptosystem as you can. For example, show that there are IND-CPA secure cryptosystems that are not IND-CCA1 secure.