MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Security of Goldwasser-Micali cryptosystem). *Show that the Goldwasser-Micali cryptosystem is IND-CPA secure if the Quadratic Residuosity Problem is hard.*

Solution. Before we can give a corresponding proof we must define several concepts. Without them we cannot even define the Goldwasser-Micali cryptosystem.

QUADRATIC RESIDIOUCITY. 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 $\left(\frac{a}{n}\right)$. One can show that Jacobi symbols satisfies following conditions:

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

Also, 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. By the properties of Jacobi symbols all quadratic residues must be inside the following set

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

Moreover, it can be shown using the Chinese Reminder Theorem that the set of quadratic non-residues $J_N(1) \setminus QR_N$ is as big as the set of quadratic residues 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 $\mathcal{B}$ the advantage

$$\mathsf{Adv}^{\mathsf{qrp}}_{\mathbb{P}_n}(\mathcal{B}) = \left|\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] - \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right]\right| \leq \varepsilon$$

where the security games are defined as follows:

$$\begin{array}{ll} \mathcal{Q}_0^{\mathcal{B}} & \qquad \mathcal{Q}_1^{\mathcal{B}} \\ \left[\begin{array}{l} p, q \xleftarrow{u} \mathbb{P}(n) \\ N \leftarrow pq \\ x \xleftarrow{u} QR_N \\ \textbf{return } \mathcal{B}(x, N) \end{array}\right. & \qquad \left[\begin{array}{l} p, q \xleftarrow{u} \mathbb{P}(n) \\ N \leftarrow pq \\ x \xleftarrow{u} J_N(1) \setminus QR_N \\ \textbf{return } \mathcal{B}(x, N) \ . \end{array}\right. \end{array}$$

DEFINITION OF A CRYPTOSYSTEM. Goldwasser-Micali cryptosystem uses Blum primes and quadratic residuosity to encrypt bits using following algorithms.

- **Key generation.** Sample primes $p, q \in \mathbb{P}(n)$ and choose quadratic non-residue $y \in J_N(1)$ modulo $N = pq$. Use (N, y) as a public key pk and (p, q) as a private key sk.
- **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.

IND-CPA SECURITY. Recall that IND-CPA security is defined through the following security games:

$$
\begin{array}{ll}
\mathcal{G}_0 & \mathcal{G}_1 \\
\left[\begin{array}{l}
(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen} \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
\textbf{return } \mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_0))
\end{array}\right. &
\left[\begin{array}{l}
(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen} \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
\textbf{return } \mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_1))
\end{array}\right. .
\end{array}
$$

More precisely, a public key cryptosystem is (t, ε)-IND-CPA secure, if the advantage of any t-time adversary $\mathcal{A}$ against games $\mathcal{G}_0$ and $\mathcal{G}_1$ is bounded:

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

If we instantiate the IND-CPA security games for Goldwasser-Micali cryptosystem we get the following games:

$$
\begin{array}{ll}
\mathcal{G}_0 & \mathcal{G}_1 \\
\left[\begin{array}{l}
p, q \xleftarrow{u} \mathbb{P}_n \\
N \leftarrow pq \\
y \xleftarrow{u} J_N \setminus QR_N \\
\mathsf{pk} \leftarrow (N, y) \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
x \xleftarrow{u} \mathbb{Z}_N^* \\
\ \ \mathsf{if} \ \ m_0 = 0 \ \mathsf{then} \\
\ \ \left[\, c \leftarrow x^2 \bmod N \right. \\
\ \ \mathsf{else} \\
\ \ \left[\, c \leftarrow yx^2 \bmod N \right. \\
\textbf{return } \mathcal{A}(c)
\end{array}\right. &
\left[\begin{array}{l}
p, q \xleftarrow{u} \mathbb{P}_n \\
N \leftarrow pq \\
y \xleftarrow{u} J_N \setminus QR_N \\
\mathsf{pk} \leftarrow (N, y) \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
x \xleftarrow{u} \mathbb{Z}_N^* \\
\ \ \mathsf{if} \ \ m_1 = 0 \ \mathsf{then} \\
\ \ \left[\, c \leftarrow x^2 \bmod N \right. \\
\ \ \mathsf{else} \\
\ \ \left[\, c \leftarrow yx^2 \bmod N \right. \\
\textbf{return } \mathcal{A}(c)
\end{array}\right.
\end{array}
$$

Let us assume that there is an adversary $\mathcal{A}$ which breaks the IND-CPA security of Goldwasser-Micali cryptosystem. We will perform a reduction to the quadratic residuosity problem, by constructing an adversary $\mathcal{B}$. The adversary construction is presented below:

$$
\begin{array}{l}
\mathcal{B}(x, N) \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow (N, x) \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
\hat{x} \xleftarrow{u} \mathbb{Z}_N^* \\
b \xleftarrow{u} \{0, 1\} \\
\ \ \mathsf{if} \ \ m_b = 0 \ \mathsf{then} \\
\ \ \left[\, c \leftarrow \hat{x}^2 \bmod N \right. \\
\ \ \mathsf{else} \\
\ \ \left[\, c \leftarrow y\hat{x}^2 \bmod N \right. \\
\textbf{return } [b \stackrel{?}{=} \mathcal{A}(c)]
\end{array}\right.
\end{array}
$$

Note that the construction is valid, since the adversary $\mathcal{B}$ knows N and can therefore perform all the required operations. By inlining $\mathcal{B}$ into the games $\mathcal{Q}_0$ and $\mathcal{Q}_1$ defining the hardness of quadratic residuosity, we get the the following games:

$$
\begin{array}{ll}
\mathcal{Q}_0^{\mathcal{B}} & \mathcal{Q}_1^{\mathcal{B}} \\
\left[\begin{array}{l}
p, q \xleftarrow{u} \mathbb{P}(n) \\
N \leftarrow pq \\
x \xleftarrow{u} QR_N \\
\mathsf{pk} \leftarrow (N, x) \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
\hat{x} \xleftarrow{u} \mathbb{Z}_N^* \\
b \xleftarrow{u} \{0,1\} \\
\ \ \mathsf{if}\ \ m_b = 0\ \mathsf{then} \\
\ \ \left[\ c \leftarrow \hat{x}^2 \bmod N \right. \\
\ \ \mathsf{else} \\
\ \ \left[\ c \leftarrow x\hat{x}^2 \bmod N \right. \\
\mathbf{return}\ [\mathcal{A}(c) \stackrel{?}{=} b]
\end{array}\right.
&
\left[\begin{array}{l}
p, q \xleftarrow{u} \mathbb{P}(n) \\
N \leftarrow pq \\
x \xleftarrow{u} J_N \setminus QR_N \\
\mathsf{pk} \leftarrow (N, x) \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
\hat{x} \xleftarrow{u} \mathbb{Z}_N^* \\
b \xleftarrow{u} \{0,1\} \\
\ \ \mathsf{if}\ \ m_b = 0\ \mathsf{then} \\
\ \ \left[\ c \leftarrow \hat{x}^2 \bmod N \right. \\
\ \ \mathsf{else} \\
\ \ \left[\ c \leftarrow x\hat{x}^2 \bmod N \right. \\
\mathbf{return}\ [\mathcal{A}(c) \stackrel{?}{=} b]
\end{array}\right.
\end{array}
$$

Let us first compute the probability $\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right]$. For that note that $\hat{x}^2$ and $x\hat{x}^2$ are completely indistinguishable to the adversary. Since x is a quadratic residue, it can be written as $x = a^2 \bmod N$ for some $a \in \mathbb{Z}_N^*$ and thus $x\hat{x}^2 = (a\hat{x})^2 \bmod N$. Since $\hat{x}$ is generated uniformly randomly after a has been fixed, the element $a\hat{x}$ is a random element from $\mathbb{Z}_N^*$. Consequently, $\hat{x}^2$ and $x\hat{x}^2$ have the same distributions and we can further simplify the game:

$$
\begin{array}{l}
\mathcal{Q}_0^{\mathcal{B}} \\
\left[\begin{array}{l}
p, q \xleftarrow{u} \mathbb{P}(n) \\
N \leftarrow pq \\
x \xleftarrow{u} QR_N \\
\mathsf{pk} \leftarrow (N, x) \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
\hat{x} \xleftarrow{u} \mathbb{Z}_N^* \\
b \xleftarrow{u} \{0,1\} \\
c \leftarrow \hat{x}^2 \bmod N \\
\mathbf{return}\ [\mathcal{A}(c) \stackrel{?}{=} b]
\end{array}\right.
\end{array}
$$

As the adversary $\mathcal{A}$ receiver no information about b, the probability $\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] = \frac{1}{2}$.

Let us now analyse the game $\mathcal{Q}_1^{\mathcal{B}}$. The game returns 1 only if the adversary $\mathcal{A}$ guesses the bit b. Thus, we must split the game into two sub-games based on the value of b. When $b = 0$ the game $\mathcal{Q}_1^{\mathcal{B}}$ is equivalent to the game $\mathcal{G}_0^{\mathcal{A}}$ and when $b = 1$ the game $\mathcal{Q}_1^{\mathcal{B}}$ is equivalent to the game $\mathcal{G}_1^{\mathcal{A}}$. Consequently, we can express the success probability as follows:

$$
\begin{aligned}
\Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right] &= \Pr\left[b = 0\right] \cdot \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 0\right] + \Pr\left[b = 1\right] \cdot \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] \\
&= \frac{1}{2}\left(1 - \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right]\right) + \frac{1}{2} \cdot \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] \\
&= \frac{1}{2} + \frac{1}{2} \cdot \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] - \frac{1}{2} \cdot \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] \quad .
\end{aligned}
$$

As a result, we get a direct connection between the advantages of $\mathcal{A}$ and $\mathcal{B}$:

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{qrp}}_{\mathbb{P}_n}(\mathcal{B}) &= \left|\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] - \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right]\right| \\
&= \left|\frac{1}{2} - \frac{1}{2} - \frac{1}{2}\cdot\Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] + \frac{1}{2}\cdot\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right]\right| \\
&= \frac{1}{2}\cdot\left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| \\
&= \frac{1}{2}\cdot\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) \enspace .
\end{aligned}$$

To complete the proof, we must also find the relation between the running-times of $\mathcal{A}$ and $\mathcal{B}$. It is easy to see that the running-time of $\mathcal{B}$ is only by a constant c larger than the running-time $\mathcal{A}$. Consequently, the advantage of a $(t-c)$-time $\mathcal{A}$ adversary is bounded:

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) \le 2\cdot\mathsf{Adv}^{\mathsf{qrp}}_{\mathbb{P}_n}(\mathcal{B}) \le 2\varepsilon$$

and we have shown that Goldwasser-Micali cryptosystem is $(t-c, 2\varepsilon)$-IND-CPA secure given that the set of n-bit Blum integers is (t,ε)-secure with respect to the quadratic residuosity problem.