Tutorial 2: Computational Secrecy and Pseudorandom Generators

Submission Guidelines All problems must be solved in class today. Searching on the internet for solutions is strictly discouraged.

1. Show that semantic security and security in the sense of indistinguishability of ciphertexts are equivalent.

A: We will show the equivalence in the presence of an eavesdropper for private key encryption schemes. Same equivalence holds even in the chosen plaintext attack model.

Let us first recall the definition of semantic security for an encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over message space $\mathcal{M}$. Semantic security in the presence of an eavesdropper is defined in terms of the following game, denoted SS, between a challenger and an adversray $\mathscr{A}$.

- Let D denote a distribution over $\mathcal{M}$ and let $f, h : \mathcal{M} \to \{0,1\}^*$, all specified by the adversary.
- The challenger picks $k \longleftarrow \mathsf{Gen}()$, $m \xleftarrow{\text{D}} \mathcal{M}$; picks a bit $\delta \xleftarrow{\text{U}} \{0,1\}$; if $\delta = 0$ set $c = \mathsf{Enc}(k, m)$, else set $c = \perp$ (indicating empty string). Send $h(m), c$ to $\mathscr{A}$.
- $\mathscr{A}$ returns a string $w \in \{0,1\}^*$.

$\mathscr{A}$'s advantage in the SS game is given by

$$\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{E},\mathscr{A}} = |\Pr[\mathscr{A}(h(m), c) = f(m) \mid \delta = 0] - \Pr[\mathscr{A}(h(m), c) = f(m) \mid \delta = 1]|$$

$\mathcal{E}$ is (ε, t) semantically secure or (ε, t) – SS-secure if for all t time adversaries $\mathscr{A}$, for all message distributions D and all functions $f, h : \mathcal{M} \to \{0,1\}^*$, $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{E},\mathscr{A}} \leq \varepsilon$.

IND-EAV-security implies SS-security. Let $\mathscr{A}$ be a SS adversary against $\mathcal{E}$ for a particular choice of message distribution D and functions f, h. Then we show how to build a $\mathsf{IND\text{-}CPA}$ adversary $\mathscr{B}$ using $\mathscr{A}$.

Description of $\mathscr{B}$:

- $\mathscr{B}$ picks two messages $m_0, m_1 \xleftarrow{\text{D}} \mathcal{M}$ and provides them to its challenger.
- The challenger picks $\beta \xleftarrow{\text{U}} \{0,1\}$, computes $c^* = \mathsf{Enc}(k, m)$ (where $k \longleftarrow \mathsf{Gen}()$ is chosen by the challenger when the game is setup) and provides c^* to $\mathscr{B}$.
- $\mathscr{B}$ computes $h(m_0)$ and sends $h(m_0), c^*$ to $\mathscr{A}$.
- $\mathscr{A}$ returns a string w to $\mathscr{B}$. If $w = f(m_0)$, then $\mathscr{B}$ sets $\beta' = 0$; else sets $\beta' = 1$ and returns β' to its challenger.

Now let us analyse the probability that $\mathscr{B}$ wins the $\mathsf{IND\text{-}CPA}$ game i.e., $\beta = \beta'$.

$$\begin{aligned}
\Pr[\beta = \beta'] &= \frac{1}{2}\left(\Pr[\beta = \beta' \mid \beta = 0] + \Pr[\beta = \beta' \mid \beta = 1]\right) \\
&= \frac{1}{2}\left(\Pr[\mathscr{A}(h(m_0), c^*) = f(m_0) | \beta = 0] + \Pr[\mathscr{A}(h(m_0), c^*) \neq f(m_0) | \beta = 1]\right) \\
&= \frac{1}{2}\left(\Pr[\mathscr{A}(h(m_0), c^*) = f(m_0) | \beta = 0] + 1 - \Pr[\mathscr{A}(h(m_0), c^*) = f(m_0) | \beta = 1]\right) \\
&= \frac{1}{2}\left(\Pr[\mathscr{A}(h(m_0), \mathsf{Enc}(k, m_\beta)) = f(m_0)] + 1 - \Pr[\mathscr{A}(h(m_0)) = f(m_0)]\right)
\end{aligned}$$

The last equality follows from the fact that c^* is completely independent of m_0 when $\beta = 1$ i.e., when c^* is an encryption of m_1. We have

$$\begin{aligned}\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{E},\mathscr{B}} &= |\Pr[beta = \beta'] - \frac{1}{2}| \\ &= \frac{1}{2}|\Pr[\mathscr{A}(h(m_0), \mathsf{Enc}(k, m_\beta)) = f(m_0)] - \Pr[\mathscr{A}(h(m_0)) \neq f(m_0)]| \\ &= \frac{1}{2}\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{E},\mathscr{A}}\end{aligned}$$

thus proving that (ε, t)-IND-CPA security implies (ε', t')-SS security with $\varepsilon' = 2\varepsilon$ and $t' = t - O(1)$ (assuming m_0, m_1 can be sampled in $O(1)$ time).

SS-security implies IND-EAV-security. Suppose that $\mathscr{B}$ is an IND-EAV adversary. We show how to build an ß adversary $\mathscr{A}$ using $\mathscr{B}$ for a particular choice of message distribution D and functions $f, h : \mathcal{M} \to \{0,1\}^*$. Note that we have the flexibility to choose the D, f and h here.

Description of $\mathscr{A}$:

- $\mathscr{A}$'s challenger picks a key $k \longleftarrow \mathsf{Gen}()$.
- $\mathscr{B}$ send two messages $m_0, m_1 \in \mathcal{M}$ to $\mathscr{A}$. $\mathscr{A}$ fixes distribution D such that $\Pr[M = m_0] = \Pr[M = m_1] = \frac{1}{2}$ for a random variable following D. Also, $\mathscr{A}$ defines f so that $f(m_0) = 0$ and $f(m_1) = 1$. It further chooses $h : \mathcal{M} \to \{0,1\}^*$ to be independent of f.
- $\mathscr{A}$'s challenger picks a message $m \xleftarrow{\text{D}} \mathcal{M}$, a bit $\delta \xleftarrow{\text{U}} \{0,1\}$; sets $c = \mathsf{Enc}(k, m)$ if $\delta = 0$ and otherwise sets $c = \perp$; sends $h(m), c$ to $\mathscr{A}$.
- If $c = \perp$, $\mathscr{A}$ returns a random bit $w \xleftarrow{\text{U}} \{0,1\}$ to its challenger and halts. Otherwise, $\mathscr{A}$ sends c to $\mathscr{B}$.
- $\mathscr{B}$ sends a guess β to $\mathscr{A}$. If $\beta = 0$, $\mathscr{A}$ sets $w = f(m_0) = 0$; otherwise, $\mathscr{A}$ sets $w = f(m_1) = 1$ and sends w to its challenger.

We have

$$\begin{aligned}&\Pr[\mathscr{A}(h(m), c) = f(m)] - \Pr[\mathscr{A}(h(m)) = f(m)] \\ &= \frac{1}{2}\left(\Pr[\mathscr{A}(h(m), c) = f(m) | m = m_0] + \Pr[\mathscr{A}(h(m), c) = f(m) | m = m_1]\right) \\ &\quad - \frac{1}{2}\left(\Pr[\mathscr{A}(h(m)) = f(m) | m = m_0] + \Pr[\mathscr{A}(h(m)) = f(m) | m = m_0]\right) \\ &= \frac{1}{2}\left(\Pr[\mathscr{A}(h(m_0), \mathsf{Enc}(k, m_0)) = 0] + \Pr[\mathscr{A}(h(m_1), \mathsf{Enc}(k, m_1)) = 1]\right) \\ &\quad - \frac{1}{2}\left(\Pr[\mathscr{A}(h(m_0)) = 0] + \Pr[\mathscr{A}(h(m_1)) = 1]\right) \\ &= \frac{1}{2}\Pr[\mathscr{B}(\mathsf{Enc}(k, m_0)) = 0] + \frac{1}{2}\Pr[\mathscr{B}(\mathsf{Enc}(k, m_1)) = 1] - \frac{1}{2}\left(\frac{1}{2} + \frac{1}{2}\right) \\ &= \Pr[\mathscr{B}(\mathsf{Enc}(k, m_\beta)) = \beta] - \frac{1}{2}\end{aligned}$$

thus implying

$$\begin{aligned}\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{E},\mathscr{A}} &= |\Pr[\mathscr{A}(h(m), c) = f(m)] - \Pr[\mathscr{A}(h(m)) = f(m)]| \\ &= |\Pr[\mathscr{B}(\mathsf{Enc}(k, m_\beta)) = \beta] - \frac{1}{2}| \\ &= \mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{E},\mathscr{B}}\end{aligned}$$

Therefore, (ε, t)-SS security implies (ε', t')-IND-CPA security with $\varepsilon' = \varepsilon$ and $t' = t - O(1)$

2. Let G be a PRF that stretches n-bit strings to $2n$-bit strings. For $s \in \{0,1\}^n$, write $G(s) = G_0(s) \| G_1(s)$, so that $G_0(s)$ represents the first n-bits of $G(s)$ and $G_1(s)$ represents the last n bits of $G(s)$. Define a new PRG G_0 that stretches n-bit strings to $4n$-bit strings as:

$$G'(s) = G(G_0(s)) \| G(G_1(s)).$$

Prove that if G is a secure PRG, then so is G'.

A: We show that (ε, t)-security of G implies (ε', t')-security of G' with $\varepsilon' \le 6\varepsilon$ and $t' = t - O(1)$. Suppose that $\mathscr{D}'$ is a distinguisher for G' in the PRG game. Let Game_0 denote the real PRG game for G where the challenger picks $\delta \xleftarrow{U} \{0,1\}$; if $\delta = 0$, picks $s \xleftarrow{U} \{0,1\}^n$, sets $r = G'(s)$; otherwise picks $r \xleftarrow{U} \{0,1\}^{4n}$ and sends r to $\mathscr{D}'$. $\mathscr{D}'$ returns a bit γ.

Define two games Game_1, Game_2, Game_3 with modified distributions of r when $\delta = 0$ as follows.

Game_1**:** When $\delta = 0$, challenger computes r as follows: pick random strings $t_1, t_2 \xleftarrow{U} \{0,1\}^n$; set $r = G(t_1) \| G(t_2)$.

Game_2**:** When $\delta = 0$, challenger picks $t_1 \xleftarrow{U} \{0,1\}^n$, $r_2 \xleftarrow{U} \{0,1\}^{2n}$ and sets $r \leftarrow G(t_1) \| r_2$.

Game_3**:** When $\delta = 0$, challenger picks $r \xleftarrow{U} \{0,1\}^{4n}$.

Let $\mathcal{E}_i$ denote the probability that $\mathscr{D}'$ returns 1 in Game_i for $i = 0,1,2,3$. Clearly, $2|\Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_3]| = \mathsf{Adv}^{\mathsf{PRG}}_{G',\mathscr{D}'}$ (we have seen this in class).

Lemma 1. $|\Pr[\mathcal{E}_{i-1}] - \Pr[\mathcal{E}_i]| \le \varepsilon$ *for* $i = 1,2,3$

Proof. We first show that $|\Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_1]| \le \varepsilon$. We construct a distinguisher $\mathscr{D}$ for G that leverages the ability of $\mathscr{D}'$ to distinguish between Game_0 and Game_1.

Description of $\mathscr{D}$:

- $\mathscr{D}$'s challenger picks $\beta \xleftarrow{U} \{0,1\}$. If $\beta = 0$, it picks $s \xleftarrow{U} \{0,1\}^n$ sets $w \longleftarrow G(s)$; otherwise w is sampled uniformly at random from $\{0,1\}^{2n}$ and sends w to $\mathscr{D}$.
- $\mathscr{D}$ picks a bit $\delta \xleftarrow{U} \{0,1\}$. When $\delta = 0$, it sets $r \longleftarrow G(w_1) \| G(w_2)$, where $w = w_1 \| w_2$ with $w_1, w_2 \in \{0,1\}^n$. Otherwise, if $\delta = 1$, $\mathscr{D}$ picks $r \xleftarrow{U} \{0,1\}^{4n}$ and sends r to $\mathscr{D}'$.
- $\mathscr{D}'$ returns a bit γ which is relayed by $\mathscr{D}$ to its challenger.

Observe that $\mathscr{D}$ simulates Game_0 when $\beta = 0$ (i.e., $w = G(s)$) and otherwise simulates Game_1 (when $w \xleftarrow{U} \{0,1\}^{2n}$). We therefore have

$$\begin{aligned}
\varepsilon &\ge \mathsf{Adv}^{\mathsf{PRG}}_{G,\mathscr{D}} \\
&= |\Pr[\mathscr{D}(w) = 1 | \beta = 0] - \Pr[\mathscr{D}(w) = 1 | \beta = 1]| \\
&= |\Pr[\mathscr{D}'(r) = 1 | \beta = 0] - \Pr[\mathscr{D}(r) = 1 | \beta = 1]| \\
&= |\Pr[\mathscr{D}'(r) = 1 \text{ in } \mathsf{Game}_0] - \Pr[\mathscr{D}(r) = 1 \text{ in } \mathsf{Game}_1]| \\
&= |\Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_1]|
\end{aligned}$$

Similarly, one can prove that $|\Pr[\mathcal{E}_1] - \Pr[\mathcal{E}_2]| \le \varepsilon$ and $|\Pr[\mathcal{E}_2] - \Pr[\mathcal{E}_3]| \le \varepsilon$. □

From the lemma it follows that

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{PRG}}_{G',\mathscr{D}'} &= 2|\Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_3]| \\
&\le 2(|\Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_1]| + |\Pr[\mathcal{E}_1] - \Pr[\mathcal{E}_2]| + |\Pr[\mathcal{E}_2] - \Pr[\mathcal{E}_3]| \\
&\le 6\varepsilon.
\end{aligned}$$

3. Suppose that G_1 and G_2 are PRGs defined from $\{0,1\}^n$ to $\{0,1\}^\ell$. Define a new PRG $G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\ell$, where $G(s_1, s_2) = G_1(s_1) \oplus G_2(s_2)$. Show that if either G_1 or G_2 is secure (we may not know which one is secure), then G is a secure PRG.

A: The idea is that if G_1 is secure then $G_1(s_1)$ will be indistinguishable from a random string of length ℓ. So, when added to $G_1(s_1) \oplus G_2(s_2)$ will be indistinguishable from random. Similar argument holds when G_2 is a secure PRG.

Suppose G_1 is (ε_1, t_1)-secure. It can be shown that G is (ε, t)-secure with $\varepsilon = \varepsilon_1$ and $t = t_1 - O(1)$ by constructing a distinguisher $\mathscr{D}_1$ for G_1 using a distinguisher $\mathscr{D}$ for G.

Description of $\mathscr{D}_1$:

- $\mathscr{D}_1$'s challenger picks $\beta \xleftarrow{U} \{0,1\}$. If $\beta = 0$, it picks $s \xleftarrow{U} \{0,1\}^n$ sets $w \longleftarrow G(s)$; otherwise w is sampled uniformly at random from $\{0,1\}^\ell$ and sends w to $\mathscr{D}$.
- $\mathscr{D}_1$ picks $s_2 \xleftarrow{U} \{0,1\}^n$, computes $t \longleftarrow w \oplus G_2(s_2)$ and sends t to $\mathscr{D}$.
- $\mathscr{D}$ returns a bit γ which is relayed by $\mathscr{D}_1$ to its challenger.

Note that w and hence t are uniformly distributed over $\{0,1\}^\ell$ when $\beta = 1$. Otherwise t is distributed as in the real game. We therefore have

$$\begin{aligned}
\varepsilon_1 &\geq \mathsf{Adv}^{\mathsf{PRG}}_{G_1,\mathscr{D}_1} \\
&= |\Pr[\mathscr{D}_1(w) = 1 | \beta = 0] - \Pr[\mathscr{D}_1(w) = 1 | \beta = 1]| \\
&= |\Pr[\mathscr{D}(t) = 1 | \beta = 0] - \Pr[\mathscr{D}(t) = 1 | \beta = 1]| \\
&= |\Pr[\mathscr{D}(G(s) \oplus G_2(s_2)) = 1 | s \xleftarrow{U} \{0,1\}^n] - \Pr[\mathscr{D}(t) = 1 | t \xleftarrow{U} \{0,1\}^\ell]| \\
&= \mathsf{Adv}^{\mathsf{PRG}}_{G,\mathscr{D}}
\end{aligned}$$

from which it follows that $\varepsilon = \varepsilon_1$ and the running time of $\mathscr{D}_1$ is $t_1 = t + O(1)$.

4. Let $G : \{0,1\}^n \to \{0,1\}^\ell$ be a PRG and let $\eta = 1/2^{\ell - n}$. Call G secure against *seed recovery* or (ε, t)-SR secure if any t-time adversary $\mathscr{A}$ has advantage at most ε in the following game: $\mathscr{A}$ receives $G(s)$ and returns a guess s' of s. Here, advantage $\mathsf{Adv}^{\mathsf{SR}}_{G,\mathscr{A}}$ is defined as $|\Pr[s = s'] - 1/2^n|$. Show that if G is an (ε', t')-PRG then it is (ε, t)-SR secure with $\varepsilon \leq \varepsilon' + \eta + 1/2^n$ and $t = t' + O(1)$.

A: Let $\mathscr{A}$ be a seed recovering adversary against G. We show how to build a distinguisher $\mathscr{D}$ for G.

Description of $\mathscr{D}$:

- From its challenger, $\mathscr{D}$ receives a string $r \in \{0,1\}^\ell$ which is either $G(s)$ for some $s \xleftarrow{U} \{0,1\}^n$ or uniformly distributed in $\{0,1\}^\ell$ according to some bit $\delta \xleftarrow{U} \{0,1\}$ being 0 or 1 respectively.
- $\mathscr{D}$ provides r to $\mathscr{A}$ and at the end of the seed recovery game, receives a string $s' \in \{0,1\}^n$ from $\mathscr{A}$.
- $\mathscr{D}$ now checks if $G(s') = r$; if so, returns 1 and otherwise returns 0.

Observe that when $r \xleftarrow{U} \{0,1\}^\ell$, $\mathscr{A}$'s guess is completely independent of r. There are 2^n possible values of s' and for a fixed s', there are 2^n possible outputs of G. So, the probability that $G(s') = r$ is precisely $2^n/2^\ell$ (since

r is uniformly distributed). We therefore have

$$\begin{aligned}
&\Pr[\mathscr{D}(r) = 1|\delta = 0] - \Pr[\mathscr{D}(r) = 1|\delta = 1] \\
&\quad = \Pr[\mathscr{A}(r) = s' \wedge s = s'] - \Pr[(\mathscr{A}(r) = s' \wedge G(s') = r)|r \xleftarrow{\mathrm{U}} \{0,1\}^\ell] \\
&\quad = \Pr[s' = s] - \sum_{s' \in \{0,1\}^n} \Pr[G(s') = r|\mathscr{A}(r) = s', r \xleftarrow{\mathrm{U}} \{0,1\}^\ell] \Pr[\mathscr{A}(r) = s'|r \xleftarrow{\mathrm{U}} \{0,1\}^\ell] \\
&\quad = \Pr[s' = s] - \sum_{s' \in \{0,1\}^n} \frac{2^n}{2^\ell} \frac{1}{2^n} \\
&\quad = \Pr[s' = s] - \frac{2^n}{2^\ell}
\end{aligned}$$

It now follows that

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{SR}}_{G,\mathscr{A}} &= \left|\Pr[s' = s'] - \frac{1}{2^n}\right| \\
&= \left|\Pr[\mathscr{D}(r) = 1|\delta = 0] - \Pr[\mathscr{D}(r) = 1|\delta = 1] + \frac{2^n}{2^\ell} - \frac{1}{2^n}\right| \\
&\leq |\Pr[\mathscr{D}(r) = 1|\delta = 0] - \Pr[\mathscr{D}(r) = 1|\delta = 1]| + \eta + \frac{1}{2^n} \\
&= \mathsf{Adv}^{\mathsf{PRG}}_{G,\mathscr{D}} + \eta + \frac{1}{2^n}.
\end{aligned}$$