Isaac Kim
CS 487
Professor Baldimtsi
Feb 19, 2023

## Homework 2

**1.1)** Consider an adversary A that picks messages $m_0 = 0^{4n}$, or all 0s message, and $m_1 = 0^{2n}||1^{2n}$. Given these messages, for any key $k$, $Enc(k, m_0)$ will have its first half equal to its second half, in fact, $Enc(k, m_0) = \mathrm{G}(k) \oplus \mathrm{G}(k)$. However, $Enc(k, m_1)$ will have its first half be the inverse of its second half. Then, when our adversary A gets a return ciphertext from the Challenger, it will only have to observe whether the two halves of the message are equal, or if $m_R = m_L$. Note that it doesn't matter what G($k$) is as A only cares about if the first half of the message equals the second half, or is the inverse of the second half. Then, for a random bit $b \in \{0, 1\}$ picked by the Challenger:

$$\text{Case 1, b = 0: Pr[A picks 0} \mid b = 0] = 1$$
$$\text{Case 2, b = 1: Pr[A picks 1} \mid b = 1] = 1$$

In both cases, the adversary knows exactly which message was encrypted. Then, $\Pr[\mathrm{Exp}_{A,\pi}(n) = 1] = (1)(\frac{1}{2})+(1)(\frac{1}{2}) = \frac{1}{2}+\frac{1}{2} > \frac{1}{2}+\mathrm{negl}(n)$. Hence, our encryption scheme is NOT EAV-secure.

**1.2)** The error in the reduction proof is in the analysis section. When $w$ is a truly random string, then Pr[A breaks EAV of $\pi$] $\neq \frac{1}{2}$, but rather Pr[A breaks EAV of $\pi$] $= \frac{1}{2} + p(n)$, for some non negligible value $p(n)$. This is because from part a), our adversary knows exactly which message was encrypted. Since our adversary only looks at whether the two halves of the ciphertext are equal or inverses of each other, it does not matter what $w$ is used to create the ciphertext. Then, Pr[D($r$)=1] $= \frac{1}{2} + p(n)$. The rest of the proof is unchanged; Pr[D($G(s)$)=1] $= \frac{1}{2} + p(n)$. Then,

$$|\Pr[\mathrm{D}(G(s))\text{=1] - }\Pr[\mathrm{D}(r)\text{=1]}| = |\tfrac{1}{2} + p(n) - \tfrac{1}{2} + p(n)| = 0 \leq \mathrm{negl}(n)$$

This value makes sense because this means that despite the fact that we assumed that our encryption scheme was *not* secure, we still arrived at the conclusion that our PRG *was* secure, which is exactly the scenario described in question 1.

**2.1)** Let G:$\{0, 1\}^{2n} \rightarrow \{0, 1\}^{4n}$ be a PRG (for every $n$). Let $n$ be even and $x \in \{0, 1\}^{2n}$ with $x = x_L||x_R$, where $x_L$ and $x_R$ are the left and right halves of $x$ respectively, let $s \in \{0, 1\}^n$. Note that $|s| = n$.
Given fact: If H:$\{0, 1\}^n \rightarrow \{0, 1\}^{4n}$ is a PRG, then G($s$) = H($s_1, s_2, ..., s_{\frac{n}{2}}$) is also a PRG, where $s_1, s_2, ..., s_{\frac{n}{2}}$ are the first $\frac{n}{2}$ bits of $s$. Some observations that we can make are:

$$\mathrm{G}(x) = \mathrm{H}(x_L)$$

Then, for all $s \in \{0, 1\}^n$,

$$\mathrm{G}_c(s) = \mathrm{G}(1^{|s|}||s) = \mathrm{G}(1^{|n|}||s)\text{= }\mathrm{H}(1^n)$$

Let D be our distinguisher for our PRG and $r \in \{0,1\}^{4n}$. By Kerckhoff's principle, D knows what $w = \mathrm{H}(1^n)$ is. Then, since for all $s \in \{0,1\}^n$, $\mathrm{G}_c(s) = \mathrm{H}(1^n)$, let $\mathrm{D}(\mathrm{G}_c(s)) = 1$ if and only if $\mathrm{G}_c(s) = w$. The probability that $r$ is picked at uniform random and is equal to $w$ is $\frac{1}{2^{4n}}$. Then,

$$|\Pr[\mathrm{D}(\mathrm{G}_c(s)){=}1] \text{ - } \Pr[\mathrm{D}(r){=}1]| = |1 - \tfrac{1}{2^{4n}}| > \mathrm{negl}(n)$$

Hence, $\mathrm{G}_c(s)$ is not a secure PRG.

**2.2)** Assume that $\mathrm{H} : \{0,1\}^n \to \{0,1\}^{2n}$ is a secure PRG, then prove that $\mathrm{G}(s_L||s_R) = s_L||\mathrm{H}(s_R)$ is also a secure PRG (where s = $s_L||s_R$ and $|s_L| = |s_R|$ (assume n is always even).

**a)** Contrapositive: If $\mathrm{G} = (s_L||\mathrm{H}(s_R))$ is not secure, then H is not secure.

**b)** By 2.2 a), this means that there exists some distinguisher $\mathrm{D}_G$ such that Pr[$\mathrm{D}_G$ breaks G] $= \frac{1}{2} + p(n)$ for some non negligible value $p(n)$. Let $\mathrm{D}_H$ be a distinguisher for H. Let $x \in \{0,1\}^{2n}$. The interaction between the two distinguishers goes as follows: $\mathrm{D}_H$ will send a message $w = w_L||w_R = x||x$ , $|w| = 4n$ to $\mathrm{D}_G$. Since $\mathrm{D}_G$ is a good distinguisher for G, $\mathrm{D}_G$ returns 1 if $x||x$ is a valid output of G, or $x||x = \mathrm{G}(s) = s_L||\mathrm{H}(s_R)$ with probability of $\frac{1}{2} + p(n)$. Then, if $\mathrm{D}_G$ returns 1, $\mathrm{D}_H$ will return 1, and knows that $x$ is a valid output of H with probability of $\frac{1}{2} + p(n)$, or Pr[$\mathrm{D}_H$ breaks H] $= \frac{1}{2} + p(n)$. Hence, $\mathrm{D}_H$ is a good distinguisher for H.

**c)** The probability of success of $\mathrm{D}_H$ will be the same as the probability of success for $\mathrm{D}_G$, since whenever $\mathrm{D}_G$ returns 1, $\mathrm{D}_H$ will also return 1.

**3.)** Let $F_k : \{0,1\}^n \to \{0,1\}^n$.

**a)** Show that $F_k^a(x) = F_k(0||x)||F_k(x||1)$, where || denotes string concatenation, is NOT a PRF.

An attacker A can query different strings and no matter what is returned from the Challenger, A has to only consider the first bit and the last bit since the first bit is always $F_k(0)$ and the last bit is always $F_k(1)$. If the first and last bits are equal to these values then A returns 1, otherwise, A returns 0, 1 signifying a valid output of $F_k^a$, and 0 a random string. Note that $F_k^a(x) = F_k(0||x)||F_k(x||1)$ and $F_k : \{0,1\}^n \to \{0,1\}^n$, $|F_k(0||x)||F_k(x||1)| = 2n$. Since the first bit and last bit stay the same (first bit is always $F_k(0)$ and the last bit is always $F_k(1)$), there are $2^{2n-2}$ strings where the first bit is $F_k(0)$ and the last bit is $F_k(1)$. Then, Pr[A returns 1 | $w \in \{0,1\}^n$ picked at uniform random] $= \frac{2^{2n-2}}{2^{2n}} = \frac{1}{4}$. Then,

Case 1: Pr[A($F_k^a(x)$)=1] = 1

Case 2: Pr[A($r$)=1] $= \frac{1}{4}$

Hence, |Pr[A($F_k^a(x)$)=1]-Pr[A($r$)=1] $= \frac{1}{4}| = 1 - \frac{1}{4} = \frac{3}{4} > \mathrm{negl}(n)$.

**b)** Since attacker A can query different messages, A can query messages $y, \bar{y}$, where $y \in \{0,1\}^n$, $\bar{y}$ is the inversion of $y$. Let $z_1, z_2$ be the outputs that A gets back after sending strings $y$ and $\bar{y}$ respectively. Note that $F_k^b(y) = F_k^b(\bar{y})$. Then, if $z_1 = z_2$, then A returns 1, meaning $z_1, z_2 \in F_k^b$, and otherwise 0, meaning that $z_1, z_2 \in \{0,1\}^n$ from uniform distribution. A however still returns 1 if $z_1, z_2 \in \{0,1\}^n$ uniform distribution and $z_1 = z_2$, which has a probability of $\frac{1}{2^n}$. Then,

Case 1: Pr[A($F_k^b(x)$)=1] = 1

Case 2: Pr[A($r$)=1] = $\frac{1}{2^n}$, where $r \in \{0,1\}^n$ uniform distribution

Hence, |Pr[A($F_k^b(x)$)=1]-Pr[A($r$)=1]| $= 1 - \frac{1}{2^n}$ >negl($n$).

**4.** The CPA game is one where an adversary $A$ interacts with a supposedly CPA-secure encryption scheme, and is allowed to query multiple messages of the same length, $m_0, m_1$ to this encryption scheme. A uniform bit $b \in \{0,1\}$ is chosen by the encryption scheme each time a message is queried, and the encryption scheme returns a ciphertext $c = \text{Enc}_k(m_b)$. $A$ then outputs a bit $b'$. The game is considered a win for $A$ if $b' = b$ and a loss otherwise. $A$ is still allowed to query messages if it likes after it outputs $b'$. If the difference between $A$ successfully determining whether a ciphertext came from the encryption scheme and a ciphertext being picked at uniform random is less than or equal to some negligible value, then the encryption scheme is CPA secure.

**a)** An adversary A can query messages $m_1, m_2$ to the Challenger, who sends back $c_1 = m_1 \oplus \text{G}(k) \oplus 1^{|2n|}$ and $c_2 = m_2 \oplus \text{G}(k) \oplus 1^{|2n|}$ or $c_1, c_2 \in \{0,1\}^{2n}$ uniform distribution. Then, A takes $w_1 = c_1 \oplus m_1 \oplus 1^{|2n|}$ and $w_2 = c_2 \oplus m_2 \oplus 1^{|2n|}$. If $w_1 = w_2$, A returns 1, meaning $w_1 = w_2 = \text{G}(k)$ for some $k$ and the Challenger is using the CPA scheme, and otherwise returns 0 meaning that $c_1, c_2 \in \{0,1\}^{2n}$ uniform distribution. However, A still returns 1 when $c_1, c_2 \in \{0,1\}^{2n}$ if $w_1 = w_2$, which has a probability of $\frac{1}{2^{2n}}$. Then,

Case 1: Pr[A returns 1 | $w_1 = w_2 = \text{G}(k)$] = 1

Case 2: Pr[A returns 1 | $c_1, c_2 \in \{0,1\}^{2n}$] = $\frac{1}{2^{2n}}$

Hence, |Pr[A returns 1 | $w_1 = w_2 = \text{G}(k)$] - Pr[A returns 1 | $c_1, c_2 \in \{0,1\}^{2n}$]| $= 1 - \frac{1}{2^{2n}}$ >negl($n$).

**b)** An adversary A can query messages $m_1, m_2$ to the Challenger, who sends back $c_1 = m_1 \oplus F_k(0^n)$ and $c_2 = m_2 \oplus F_k(0^n)$ respectively, or $c_1, c_2 \in \{0,1\}^n$ uniform distribution. Let $m_1 = m_2$. Since our random string in this CPA scheme is always $r = 0^n$, and therefore repeats, each key can only encrypt a message once. Then, our adversary A can just compare if $c_1 = c_2$, and returns 1 if they are equal, and 0 otherwise. A can still wrongly return 1 if $c_1 = c_2$ and $c_1, c_2 \in \{0,1\}^n$ uniform distribution, which has a probability of $\frac{1}{2^n}$. Then,

Case 1: Pr[A returns 1 | $c_1 = m_1 \oplus F_k(0^n) = c_2 = m_2 \oplus F_k(0^n)$] = 1

Case 2: Pr[A returns 1 | $c_1 = c_2$ and $c_1, c_2 \in \{0,1\}^n$] = $\frac{1}{2^n}$

Hence, |Pr[A returns 1 | $c_1 = m_1 \oplus F_k(0^n) = c_2 = m_2 \oplus F_k(0^n)$] - Pr[A returns 1 | $c_1 = c_2$ and $c_1, c_2 \in \{0,1\}^n$]| $= 1 - \frac{1}{2^n}$ >negl($n$).