CS 276: Homework 2

Due Date: Sept. 13th, 2024 at 8:59pm via Gradescope

This problem is based on [CK16].

1 One-Way Functions

The security of a PRF is only guaranteed if the key is kept secret. However, [GGM86]'s PRF construction still retains some form of security (namely weak one-wayness) even if the key is leaked.

Definition 1.1 ([GGM86] Function Ensemble) *Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG, where $G_0(s)$ outputs the first n bits of $G(s)$ and $G_1(s)$ outputs the last n bits of $G(s)$.*

For any seed $s \in \{0,1\}^n$, and any input $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, let the function $f_s^G : \{0,1\}^n \to \{0,1\}^n$ be defined as follows:

$$f_s^G(x_1, \ldots, x_n) = G_{x_n}\Big(\ldots G_{x_2}\big(G_{x_1}(s)\big) \ldots \Big)$$

We sometimes write f_s^G as f_s.

Finally let us define the function ensemble $\mathcal{F}_G = \{f_s^G\}_{s \in \{0,1\}^n}$.

Definition 1.2 (One-Way Function Ensemble) *Let $\mathcal{F} = \{f_s\}_{s \in \{0,1\}^n}$ be a function ensemble where for every $s \in \{0,1\}^n$, f_s maps $\{0,1\}^n \to \{0,1\}^n$ and is efficiently computable.*

*$\mathcal{F}$ is **one-way** if for any efficient adversary $\mathcal{A}$,*

$$\Pr_{\substack{s \xleftarrow{\$} \{0,1\}^n \\ x \xleftarrow{\$} \{0,1\}^n}} \left[\mathcal{A}(s, f_s(x)) \in f_s^{-1}(f_s(x)) \right] \leq \mathsf{negl}(n)$$

Question: Prove that $\mathcal{F}_G$ is one-way, assuming conjecture 1.3 below.

Conjecture 1.3

$$\mathbb{E}_{s \xleftarrow{\$} \{0,1\}^n} \left[\frac{|\mathsf{Img}\,(f_s)\,|}{2^n} \right] \geq 1 - \mathsf{negl}(n)$$

Note: We do not know if this conjecture is true, but it is still possible to prove that $\mathcal{F}_G$ is *weakly* one-way without the conjecture.

If you're unsure how to get started, try assuming that f_s is one-to-one. This is a useful setting in which to build intuition.

Solution

1. Given any adversary $\mathcal{A}_{OWF}$ that attempts to invert f, we will construct an adversary $\mathcal{A}_{PRG}$ that attempts to distinguish the output of G from a uniformly random string.

   Construction of $\mathcal{A}_{PRG}$

   (a) Receive a string $y = (y^0, y^1) \in \{0,1\}^n \times \{0,1\}^n$ that is either $y = G(w)$, for $w \xleftarrow{\$} \{0,1\}^n$, or $y \xleftarrow{\$} \{0,1\}^{2n}$.
   (b) Sample $s \xleftarrow{\$} \{0,1\}^n$ and $b \xleftarrow{\$} \{0,1\}$.
   (c) Compute $x = \mathcal{A}_{OWF}(s, y^b)$. Compute $\tilde{x} = x \oplus 0^{n-1}||1$. In other words, $\tilde{x}$ is the same as x except the last bit is flipped.
   (d) Check whether $f_s(x) = y^b$ and $f_s(\tilde{x}) = y^{1-b}$. If both checks pass, then output 1 (guess "pseudorandom"). Otherwise, output 0 (guess "truly random").

2. Let us define some hybrids:

   - $\mathcal{H}_0(n)$:
     (a) Sample $y = (y^0, y^1) \xleftarrow{\$} \{0,1\}^n \times \{0,1\}^n$, $s \xleftarrow{\$} \{0,1\}^n$, $b \xleftarrow{\$} \{0,1\}$.
     (b) Compute $x = \mathcal{A}_{OWF}(s, y^b)$ and $\tilde{x} = x \oplus 0^{n-1}||1$.
     (c) Check whether $f_s(x) = y^b$ and $f_s(\tilde{x}) = y^{1-b}$. If so, then output 1. If not, then output 0.
   - $\mathcal{H}_1(n)$:
     (a) Sample $w \xleftarrow{\$} \{0,1\}^n$, $s \xleftarrow{\$} \{0,1\}^n$, $b \xleftarrow{\$} \{0,1\}$. Compute $y = (y^0, y^1) = G(w)$.
     (b) Compute $x = \mathcal{A}_{OWF}(s, y^b)$ and $\tilde{x} = x \oplus 0^{n-1}||1$.
     (c) Check whether $f_s(x) = y^b$ and $f_s(\tilde{x}) = y^{1-b}$. If so, then output 1. If not, then output 0.
   - $\mathcal{H}_2(n)$:
     (a) Sample $x \xleftarrow{\$} \{0,1\}^n$, $s \xleftarrow{\$} \{0,1\}^n$. Compute $b = x_n$ and $y^b = f_s(x)$.
     (b) Compute $x' = \mathcal{A}_{OWF}(s, y^b)$.
     (c) Check whether $f_s(x') = y^b$. If so, then output 1. If not, then output 0.

3. **Claim 1.4** $\Pr[\mathcal{H}_0(n) \to 1] = \mathsf{negl}(n)$.

   Proof. $\mathcal{H}_0(n) \to 1$ only if $f_s(x) = y^b$ and $f_s(\tilde{x}) = y^{1-b}$. However, this is only possible if (y^0, y^1) or (y^1, y^0) is in $\mathsf{Img}(G)$.

   Let $w = G_{x_{n-1}}\Big(\dots G_{x_2}\big(G_{x_1}(s)\big)\dots\Big)$. Then $f_s(x) = G_{x_n}(w)$ and $f_s(\tilde{x}) = G_{1-x_n}(w)$. If $f_s(x) = y^b$ and $f_s(\tilde{x}) = y^{1-b}$, then (y^0, y^1) or (y^1, y^0) is in $\mathsf{Img}(G)$.

Since $y \xleftarrow{\$} \{0,1\}^{2n}$, this occurs with negligible probability.

$$\begin{aligned}\Pr[\mathcal{H}_0(n) \to 1] &\leq \Pr_{y^0,y^1}[(y^0,y^1) \in \mathsf{Img}(G) \vee (y^1,y^0) \in \mathsf{Img}(G)] \\ &\leq \Pr_{y^0,y^1}[(y^0,y^1) \in \mathsf{Img}(G)] + \Pr_{y^0,y^1}[(y^1,y^0) \in \mathsf{Img}(G)] \\ &= 2 \cdot \frac{|\mathsf{Img}(G)|}{2^{2n}} \\ &\leq 2 \cdot \frac{2^n}{2^{2n}} = 2^{-n+1} \\ &= \mathsf{negl}(n)\end{aligned}$$

■

4. $\Pr[\mathcal{H}_1(n) \to 1] = \Pr[\mathcal{H}_0(n) \to 1] \pm \mathsf{negl}(n)$ by the PRG security of G. Therefore

$$\Pr[\mathcal{H}_1(n) \to 1] = \mathsf{negl}(n)$$

5. **Definitions:** Let $f_s^{(n-1)}$ take an input $x_{[n-1]} \in \{0,1\}^{n-1}$ and output

$$w = G_{x_{n-1}}\Big(\dots G_{x_2}(G_{x_1}(s))\dots\Big)$$

In other words $f_s^{(n-1)}$ applies the first $n-1$ stages of f_s. For a given x, let $w = f_s^{(n-1)}(x_{[n-1]})$ and $b = x_n$. Then $f_s(x) = G_b(w)$.

Next, let S be the set of (w,b)-pairs in $\{0,1\}^n \times \{0,1\}$ for which $|f_s^{-1}(G_b(w))| = 1$ and $w \in \mathsf{Img}(f_s^{(n-1)})$.

6. **Claim 1.5** *For any $(w,b) \in S$, the unique pre-image $x \in f_s^{-1}(G_b(w))$ also satisfies $w = f_s^{(n-1)}(x_{[n-1]})$.*

Proof. We know that there exists an $x'_{[n-1]}$ such that $w = f_s^{(n-1)}(x'_{[n-1]})$. If $x_{[n-1]} \neq x'_{[n-1]}$, then $f_s(x_{[n-1]}||b) = f_s(x'_{[n-1]}||b) = G_b(w)$, but $(x_{[n-1]}||b) \neq (x'_{[n-1]}||b)$. This would imply that $|f_s^{-1}(G_b(w))| \geq 2$, which is not true. ■

7. **Claim 1.6** *In $\mathcal{H}_1(n)$, if $(w,b) \in S$, then $f_s(x) = y^b$ automatically implies that $f_s(\tilde{x}) = y^{1-b}$.*

Proof. y^b has only one pre-image x, and if $f_s(x) = y^b$, then $\mathcal{A}_{OWF}$ has found this x-value. Furthermore this x-value satisfies: $w = f_s^{(n-1)}(x_{[n-1]})$. So $f_s(\tilde{x}) = G_{1-x_n}(w) = y^{1-b}$. ■

This implies that in $\mathcal{H}_1(n)$,

$$\Pr[f_s(x) = y^b | (w,b) \in S] = \Pr[f_s(x) = y^b \wedge f_s(\tilde{x}) = y^{1-b} | (w,b) \in S]$$

where $x \leftarrow \mathcal{A}_{OWF}(s, G_b(w))$.

8. **Claim 1.7** *In* $\mathcal{H}_1$*,* $\Pr_{w,s,b}[(w,b) \in S] = \frac{1}{2} - \mathsf{negl}(n)$*.*

   Proof. There is a one-to-one mapping between (w,b)-values in S and x-values for which $|f_s^{-1}(f_s(x))| = 1$ (lemma 1.11). Furthermore, $\Pr_{s,x}[|f_s^{-1}(f_s(x))| = 1] = 1 - \mathsf{negl}(n)$ (lemma 1.10). Then

$$\begin{aligned}\Pr_{w,s,b}[(w,b) \in S] &= \frac{\mathbb{E}_s\left[|S|\right]}{2^{n+1}} \\ &= \frac{1}{2} \cdot \frac{\mathbb{E}_s\left[|\{x \in \{0,1\}^n : |f_s^{-1}(f_s(x))| = 1\}|\right]}{2^n} \\ &= \frac{1}{2} \cdot \Pr_{s,x}[|f_s^{-1}(f_s(x))| = 1] \\ &= \frac{1}{2} - \mathsf{negl}'(n)\end{aligned}$$

   ■

9. **Claim 1.8** *In* $\mathcal{H}_1$*,* $\Pr[\mathcal{A}_{OWF}(s, y^b) \in f_s^{-1}(y^b) | (w,b) \in S] = \mathsf{negl}(n)$*.*

   Proof.

$$\begin{aligned}\Pr[\mathcal{H}_1(n) \to 1] &\geq \Pr[\mathcal{H}_1(n) \to 1 \wedge (w,b) \in S] \\ &= \Pr[(w,b) \in S] \cdot \Pr[\mathcal{H}_1(n) \to 1 | (w,b) \in S] \\ &\geq \frac{1}{2} \cdot \Pr[\mathcal{H}_1(n) \to 1 | (w,b) \in S] \pm \mathsf{negl}(n) \\ &= \frac{1}{2} \cdot \Pr[f_s(x) = y^b \wedge f_s(\tilde{x}) = y^{1-b} | (w,b) \in S] \pm \mathsf{negl}(n) \\ &\geq \frac{1}{2} \cdot \Pr[f_s(x) = y^b | (w,b) \in S] \pm \mathsf{negl}(n) \\ &= \frac{1}{2} \cdot \Pr[\mathcal{A}_{OWF}(s, y^b) \in f_s^{-1}(y^b) | (w,b) \in S] \pm \mathsf{negl}(n) \\ 2 \cdot \Pr[\mathcal{H}_1(n) \to 1] \pm \mathsf{negl}'(n) &\geq \Pr[\mathcal{A}_{OWF}(s, y^b) \in f_s^{-1}(y^b) | (w,b) \in S] \\ \mathsf{negl}''(n) &\geq \Pr[\mathcal{A}_{OWF}(s, y^b) \in f_s^{-1}(y^b) | (w,b) \in S]\end{aligned}$$

   In the last line, we used the fact that $\Pr[\mathcal{H}_1(n) \to 1]$ is negligible. ■

10. **Claim 1.9** *In* $\mathcal{H}_2$*, let* $w = f_s^{(n-1)}(x_{[n-1]})$ *and* $b = x_n$*. Then the distribution of* (w,b) *is statistically close to uniformly random over* S*.*

    Proof. Let us condition on $|f_s^{-1}(f_s(x))| = 1$. This occurs with overwhelming probability over (s,x) (lemma 1.10), so conditioning on this event changes the distribution of (w,b) by a negligible statistical distance.

    Now, x is uniformly random over $\{x : |f_s^{-1}(f_s(x))| = 1\}$. Each x-value maps to a unique $(w,b) \in S$, and every value in S is mapped to (lemma 1.11). Then (w,b) is uniformly random over S. ■

11. This implies that

$$\begin{aligned}\Pr[\mathcal{H}_2(n) \to 1] &= \Pr_{(w,b)\xleftarrow{\$}S}[\mathcal{A}_{OWF}(s, y^b) \in f_s^{-1}(y^b)] \pm \mathsf{negl}(n)\\ &= \Pr_{(w,b)\xleftarrow{\$}\{0,1\}^n\times\{0,1\}}[\mathcal{A}_{OWF}(s, y^b) \in f_s^{-1}(y^b) | (w,b) \xleftarrow{\$} S] \pm \mathsf{negl}(n)\\ &= \mathsf{negl}'(n)\end{aligned}$$

The last line uses the fact that $\Pr_{(w,b)\xleftarrow{\$}\{0,1\}^n\times\{0,1\}}[\mathcal{A}_{OWF}(s, y^b) \in f_s^{-1}(y^b) | (w,b) \xleftarrow{\$} S]$ is negligible.

12. $\mathcal{H}_2(n)$ is the one-way function ensemble security game for $\mathcal{F}$. We've shown that for any PPT adversary $\mathcal{A}_{OWF}$, the probability that $\mathcal{A}$ succeeds in the security game is negligible. Therefore, $\mathcal{F}$ is a secure one-way function ensemble.

1.1 Lemmas

Lemma 1.10 *With overwhelming probability over $s \xleftarrow{\$} \{0,1\}^n$ and $x \xleftarrow{\$} \{0,1\}^n$, $|f_s^{-1}(f_s(x))| = 1$.*

Proof. Let $\mathsf{thin}_s = \{y \in \{0,1\}^n : |f_s^{-1}(y)| = 1\}$, and let $\mathsf{fat}_s = \{y \in \{0,1\}^n : |f_s^{-1}(y)| \geq 2\}$. Then $|\mathsf{thin}_s| + |\mathsf{fat}_s| = |\mathsf{Img}(f_s)|$. Also,

$$\Pr_{s,x}[|f_s^{-1}(f_s(x))| = 1] = \mathbb{E}_{s\xleftarrow{\$}\{0,1\}^n}\left[\frac{|\mathsf{thin}_s|}{2^n}\right]$$

Next,

$$\begin{aligned}2^n &= \sum_{y\in\mathsf{Img}(f_s)} |f_s^{-1}(y)|\\ &= \sum_{y\in\mathsf{thin}_s} 1 + \sum_{y\in\mathsf{fat}_s} |f_s^{-1}(y)|\\ &\geq \sum_{y\in\mathsf{thin}_s} 1 + \sum_{y\in\mathsf{fat}_s} 2\\ &= |\mathsf{thin}_s| + 2\cdot|\mathsf{fat}_s|\\ &= |\mathsf{thin}_s| + 2\cdot(|\mathsf{Img}(f_s)| - |\mathsf{thin}_s|)\\ &= 2\cdot|\mathsf{Img}(f_s)| - |\mathsf{thin}_s|\end{aligned}$$

$$|\mathsf{Img}(f_s)| \leq \frac{1}{2}\cdot(2^n + |\mathsf{thin}_s|)$$

By conjecture 1.3,

$$
\begin{aligned}
1 - \mathsf{negl}(n) &\le \mathbb{E}_{s \xleftarrow{\$} \{0,1\}^n} \left[\frac{|\mathsf{Img}\,(f_s)\,|}{2^n} \right] \\
&\le \mathbb{E}_{s \xleftarrow{\$} \{0,1\}^n} \left[\frac{1}{2} \cdot (2^n + |\mathsf{thin}_s|) \right] \\
&= \frac{1}{2} + \frac{1}{2} \cdot \mathbb{E}_{s \xleftarrow{\$} \{0,1\}^n} \left[\frac{|\mathsf{thin}_s|}{2^n} \right] \\
1 - 2 \cdot \mathsf{negl}(n) &\le \mathbb{E}_{s \xleftarrow{\$} \{0,1\}^n} \left[\frac{|\mathsf{thin}_s|}{2^n} \right] \\
&\le \Pr_{s,x}[|f_s^{-1}(f_s(x))| = 1]
\end{aligned}
$$

$1 - 2 \cdot \mathsf{negl}(n)$ is overwhelming, and so is $\Pr_{s,x}[|f_s^{-1}(f_s(x))| = 1]$. ■

Lemma 1.11 *Given $x \in \{0,1\}^n$ for which $|f_s^{-1}(f_s(x))| = 1$, map*

$$x \to (w, b) = (f_s^{(n-1)}(x_{[n-1]}), x_n)$$

This is a one-to-one mapping between (w, b)-values in S and x-values for which $|f_s^{-1}(f_s(x))| = 1$.

Proof. If $|f_s^{-1}(f_s(x))| = 1$, then (w, b) is in S. This is because $w \in \mathsf{Img}(f_s^{(n-1)})$, and $|f_s^{-1}(G_b(w))| = |f_s^{-1}(f_s(x))| = 1$.

Next, every x for which $|f_s^{-1}(f_s(x))| = 1$ maps to a unique (w, b)-value. Otherwise, if there were two different x, x'-values that mapped to the same (w, b), then $f_s(x) = f_s(x')$, so $|f_s^{-1}(f_s(x))| \ge 2$.

Finally, every $(w, b) \in S$ is mapped to by an x for which $|f_s^{-1}(f_s(x))| = 1$. Since $(w, b) \in S$, there is a $x_{[n-1]} \in \{0,1\}^{n-1}$ such that $w = f_s^{(n-1)}(x_{[n-1]})$. If we let $x_n = b$, then $f_s(x) = G_b(w)$, and $|f_s^{-1}(f_s(x))| = |f_s^{-1}(G_b(w))| = 1$. ■

■

References

[CK16] Aloni Cohen and Saleet Klein. The GGM function family is weakly one-way. Cryptology ePrint Archive, Paper 2016/610, 2016.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792807, aug 1986.