Fundamentals of Cryptography — Handout 4.

Yu Yu

Theoretical Constructions of Pseudorandom Generators.

1 One-way functions and permutations

Definition 1 (one-way functions)**.** We say that function [1] $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ is a one-way function (ensemble) if

- (Easy-to-Compute). f can be computed by some algorithm in time $\mathsf{poly}(n)$.
- (Hard-to-Invert). For every PPT A, there exists a negligible function $\mathsf{negl}(\cdot)$ such that

$$\Pr_{x\leftarrow U_n,\ x'\leftarrow \mathsf{A}(1^n,f(x))}[f(x')=f(x)] \ \leq \ \mathsf{negl}(n).$$

  where the above probability is taken over the choice of x over U_n and the internal coins of A.

Quantitatively, we say that f is a $(t(n),\varepsilon(n))$-one-way function if no probabilistic A of running time $t(n)$ can invert the function with probability more than $\varepsilon(n)$.
Note: the above definition is a simplified version of the textbook, where the domain and ranges are arbitrary sets and we may need explicit sampling algorithms to sample a random element over the domain.

Definition 2 (one-way permutations)**.** A one-way permutation is a one-way function that is also a permutation at the same time.

The existence of one-way functions. We don't know if one-way functions exist but many people conjecture that they do, which implies N≠NP and is the foundation of modern cryptography. There are a few one-way function candidates:

1. (integer factorization). $f(x,y) = x\cdot y$ where x and y are random primes of the same length, and $\cdot$ denotes multiplication.
2. (subset-sum problem). $f(x_1,...,x_n,\mathcal{J}) = (x_1,...,x_n,\sum_{j\in\mathcal{J}} x_j)$, where all x_is are of length n, and $\mathcal{J}\subseteq\{1,...,n\}$.
3. (discrete logarithm). $f_p(x) = g^x \mod p$, where p is a prime (of length n) that defines the multiplicative cyclic group (section 7.3.2 of the KL book), g is the generator of the group.

[1] Recall that by function we're actually referring to a sequence of functions, i.e., $f \stackrel{\text{def}}{=} \{f_n : \{0,1\}^n \to \{0,1\}^{l(n)}\}_{n\in\mathbb{N}}$.

2 Hard-Core Predicates

Definition 3 (Hard-Core Predicates)**.** A polynomial-time computable predicate $h_c : \{0,1\}^n \to \{0,1\}$ is called a hard-core predicate of a function $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ if for every probabilistic polynomial-time algorithm A, there exists a negligible function negl such that

$$\Pr_{x \leftarrow U_n}[\mathsf{A}(f(x)) = h_c(x)] \;\leq\; \frac{1}{2} + \mathsf{negl}(n).$$

where the probability is taken over the uniform choice of $x \in \{0,1\}^n$ and the random coins of A.

Theorem 1 (Pseudorandom generators from any permutation with a hard-core predicate)**.** *If a permutation $f : \{0,1\}^n \to \{0,1\}^n$ has a hardcore predicate $h_c : \{0,1\}^n \to \{0,1\}$ (which implies that f is a one-way permutation, see Exercise 6.9 on KL). Then, function*

$$g(x) = (f(x), h_c(x))$$

is a one-way permutation from $\{0,1\}^n$ to $\{0,1\}^{n+1}$.

Proof. We will prove a more quantitative statement below: If h_c is a $(t(n),\varepsilon(n))$-hard-core predicate for f, i.e., for all probabilistic A of running time $t(n)$ we have

$$\Pr_{x \leftarrow U_n}[\mathsf{A}(f(x)) = h_c(x)] \;\leq\; \frac{1}{2} + \varepsilon(n).$$

Then, no distinguisher D of running time $t(n)/2$ can distinguish $(f(U_n), h_c(U_n))$ from $U_{n+1} = (f(U_n), U_1)$ with advantage more than $\varepsilon(n)$.
Suppose for contradiction that there exists deterministic[2] D of running time $t(n)/2$ such that

$$\Pr[\mathsf{D}(f(U_n), h_c(U_n)) = 1] \;-\; \Pr[\mathsf{D}(f(U_n), U_1) = 1] \;>\; \varepsilon(n)$$

As f is a permutation, fix any $f(x)$ the corresponding $h_c(x)$ is also fixed. We have

$$\begin{aligned} & \Pr[\mathsf{D}(f(U_n), h_c(U_n)) = 1] \;-\; \Pr[\mathsf{D}(f(U_n), U_1) = 1] \\ = \;& \frac{1}{2}\Big(\Pr[\mathsf{D}(f(U_n), h_c(U_n)) = 1] \;-\; \Pr[\mathsf{D}(f(U_n), h_c(U_n)\oplus 1) = 1] \Big) \;>\; \varepsilon(n) \end{aligned}$$

Since D outputs either 0 or 1, it follows that

$$\mathbb{E}_{x \leftarrow U_n}[\; \mathsf{D}(f(x), h_c(x)) - \mathsf{D}(f(x), h_c(x)\oplus 1) \;] \;>\; 2 \cdot \varepsilon(n) \tag{1}$$

Then, define algorithm A that on input $f(x)$, invokes $b_0 := \mathsf{D}(f(x), 0)$ and $b_1 := \mathsf{D}(f(x), 1)$, and outputs as the following.

$$\mathsf{A}(f(x)) = \begin{cases} 0, \text{ if } b_0 = 1, b_1 = 0 \\ 1, \text{ if } b_0 = 0, b_1 = 1 \\ U_1, \text{ otherwise } (b_0 = b_1) \end{cases}$$

We denote by

$$\begin{aligned} \mathcal{X}_{SUCC} &\stackrel{\text{def}}{=} \{x : \mathsf{D}(f(x), h_c(x)) - \mathsf{D}(f(x), h_c(x)\oplus 1) = 1\} \\ \mathcal{X}_{FAIL} &\stackrel{\text{def}}{=} \{x : \mathsf{D}(f(x), h_c(x)) - \mathsf{D}(f(x), h_c(x)\oplus 1) = -1\} \\ \mathcal{X}_{RAND} &\stackrel{\text{def}}{=} \{x : \mathsf{D}(f(x), h_c(x)) - \mathsf{D}(f(x), h_c(x)\oplus 1) = 0\} \end{aligned}$$

[2]For simplicity, here we only give the proof for deterministic D, you may want to think about how it extends to the probabilistic case.

where A guesses $h_c(x)$ successfully on input x from set $\mathcal{X}_{SUCC}$, fails on any x from $\mathcal{X}_{FAIL}$, and he tosses a fair coin on any x from $\mathcal{X}_{RAND}$. We also use shorthands $p_s \stackrel{\text{def}}{=} \Pr[U_n \in \mathcal{X}_{SUCC}]$, $p_f \stackrel{\text{def}}{=} \Pr[U_n \in \mathcal{X}_{FAIL}]$, $p_r \stackrel{\text{def}}{=} \Pr[U_n \in \mathcal{X}_{RAND}]$ and we recall $p_s + p_f + p_r = 1$. Now Equation (1) can be rewritten as:

$$p_s - p_f \ > \ 2 \cdot \varepsilon(n)$$

$$\begin{aligned}
\Pr[\mathsf{A}(f(U_n)) = h_c(U_n)] &= \Pr[U_n \in \mathcal{X}_{SUCC}] \cdot 1 \ + \ \Pr[U_n \in \mathcal{X}_{RAND}] \cdot \frac{1}{2} \\
&= p_s \ + \ \frac{p_r}{2} \\
&= \frac{p_s + p_f + p_r}{2} \ + \ \frac{p_s - p_f}{2} \ > \ \frac{1}{2} + \varepsilon(n)
\end{aligned}$$

which is a contradiction to the assumption and thus completes the proof. □

3 Hard-Core Predicates for Every One-way Function – the Goldreich-Levin Theorem

It was conjectured that every one-way function has a hard-core predicate, and this was proven by Goldreich and Levin in STOC 1989. In sections 6.3.2 and 6.3.3 the authors of KL book give a motivating proof for the simplified case, we will directly go for the full proof below.

Theorem 2 (Goldreich-Levin Theorem)**.** *Let $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a one-way function and define the padded one-way function*[3] *$f' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{l(n)} \times \{0,1\}^n$ as*

$$f'(x,r) \stackrel{def}{=} (f(x), r)$$

where $|x| = |r|$. Let $\mathsf{gl}(x,r) = \bigoplus_{i=1}^{n} x_i \cdot r_i \mod 2$. Then, gl is a hard-core predicate of f'.

Proof. Suppose that towards the contradiction that there exists a PPT A of running time t and a non-negligible function $\varepsilon(\cdot)$ such that

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n, r \xleftarrow{\$} \{0,1\}^n} [\ \mathsf{A}(f(x), r) = \mathsf{gl}(x,r)\ ] \geq \frac{1}{2} + \varepsilon(n) \tag{2}$$

Then, we will show next that there exists another PPT A' (who invokes A with running time $\mathsf{poly}(1/\varepsilon(n), n)$) such that

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\ \mathsf{A}'(f(x)) = x\ ] \geq \frac{\varepsilon^3(n)}{16n} \tag{3}$$

which is non-negligible (by the definition of $\varepsilon(\cdot)$) and thus concludes the theorem by reaching a contradiction. Now let's proceed to its proof.
First of all, Equation (2) implies that there exists a set $\mathcal{S}_n \subseteq \{0,1\}^n$ of size at least $\frac{\varepsilon(n)}{2} \cdot 2^n$ (i.e., $\Pr[U_n \in \mathcal{S}_n] \geq \frac{\varepsilon(n)}{2}$) such that for every $x \in \mathcal{S}_n$ it holds that

$$\Pr_{r \xleftarrow{\$} \{0,1\}^n} [\mathsf{A}(f(x), r) = \mathsf{gl}(x,r)] \ \geq \ \frac{1}{2} + \frac{\varepsilon(n)}{2}$$

[3] It is easy to see that f' is a one-way function iff f is.

the proof is simply (essentially Markov argument) by denoting $p \stackrel{\text{def}}{=} \Pr[U_n \in \mathcal{S}_n]$ we have

$$\frac{1}{2}+\varepsilon(n) \;\leq\; \Pr_{r\xleftarrow{\$}\{0,1\}^n}[\,\mathsf{A}(f(U_n),r)=\mathsf{gl}(U_n,r)\,] \;\leq\; p\times 1+(1-p)\times(\frac{1}{2}+\frac{\varepsilon(n)}{2}) \;\leq\; p+\frac{1}{2}+\frac{\varepsilon(n)}{2}$$

and thus $p \geq \frac{\varepsilon(n)}{2}$. Next, we are going to define an efficient A' that on input $y=f(x)$ and for every $x \in \mathcal{S}_n$, he inverts f (i.e., A outputs some x' s.t. $f(x')=f(x)$) with probability at least $\varepsilon(n)^2/8n$ (stated as Claim 2.1). Thus, overall he inverts f with probability

$$\Pr_{x\xleftarrow{\$}\{0,1\}^n}[\mathsf{A}'(f(x))=x] \;\geq\; \Pr[U_n\in\mathcal{S}_n]\cdot\frac{\varepsilon(n)^2}{8n} \;\geq\; \frac{\varepsilon(n)^3}{16n}$$

and thus completes the proof. □

THE INVERSION ALGORITHM A'. Let $\ell=\lceil\log(2n/\varepsilon(n)^2+1)\rceil$

1. Uniformly and independently sample $s^1,\ldots,s^\ell \stackrel{\$}{\leftarrow}\{0,1\}^n$, and $\sigma^1,\ldots,\sigma^\ell \stackrel{\$}{\leftarrow}\{0,1\}$, where each σ^i is a guess for $\mathsf{gl}(x,s^i)$.
2. For **every** non-empty subset $\mathcal{I}\subseteq\{1,\ldots,\ell\}$, let $r^{\mathcal{I}} \stackrel{\text{def}}{=} \bigoplus_{i\in\mathcal{I}} s^i$ and compute $\tau^{\mathcal{I}} := \bigoplus_{i\in\mathcal{I}}\sigma^i$ (which becomes a guess for $\mathsf{gl}(x,r^{\mathcal{I}})$ in the sense that it is correct if all the ℓ values of σ^i's are).
3. For every $j\in\{1,\ldots,n\}$, make a guess about the j^{th} bit of x, denoted by x_j, as follows:
   (a) For every non-empty subset $\mathcal{I}\subseteq\{1,...,\ell\}$, set $v_j^{\mathcal{I}} := \tau^{\mathcal{I}}\oplus\mathsf{A}(y,r^{\mathcal{I}}\oplus e_j)$, where
   $$e_j \stackrel{\text{def}}{=} \underbrace{0\cdots0}_{j-1}1\underbrace{0\cdots0}_{n-j} \;\in\{0,1\}^n$$
   (b) Do a majority voting on the candidate values $\{v_j^{\mathcal{I}} : \emptyset\neq\mathcal{I}\subseteq\{1,\cdots,\ell\}\}$ and let x'_j to be the majority bit of them.
4. Output $x'=x'_1\cdots x'_n$

Claim 2.1. *For every $x\in\mathcal{S}_n$,*

$$\Pr[\mathsf{A}'(f(x))=x]\geq\frac{\varepsilon(n)^2}{8n}$$

where the probability is taken over the internal random coins of A'.

Proof. Denote by $\mathcal{E}$ the event that all the guesses $\sigma^1,\ldots,\sigma^\ell$ equal to $\mathsf{gl}(x,s^1),\ldots,\mathsf{gl}(x,s^\ell)$ respectively, and we have

$$\Pr[\mathcal{E}]=2^{-\ell}=\frac{1}{2n/\varepsilon(n)^2+1} \;>\; \frac{\varepsilon(n)^2}{4n}\;.$$

We have that

$$\begin{aligned}
\Pr[x = x'] &= \Pr[x_1 \cdots x_n = x'_1 \cdots x'_n] \\
&\geq \Pr[\mathcal{E}] \cdot \Pr[x_1 \cdots x_n = x'_1 \cdots x'_n | \mathcal{E}] \\
&= \Pr[\mathcal{E}] \cdot \Pr[\neg \Big(x_1 \neq x'_1 \vee \cdots \vee x_n \neq x'_n \Big) | \mathcal{E}] \\
&\geq \Pr[\mathcal{E}] \cdot \left(1 - \sum_{j=1}^{n} \Pr[x_j \neq x'_j | \mathcal{E}]\right) \\
&\geq \frac{\varepsilon(n)^2}{4n} \cdot (1 - \frac{n}{2n}) \\
&= \frac{\varepsilon(n)^2}{8n}
\end{aligned}$$

where the second inequality is due to the union bound and the third inequality is due to Claim 2.2. □

Claim 2.2. *For every $x \in \mathcal{S}_n$, and every $j \in \{1, \cdots, n\}$, we have* $\Pr[x'_j \neq x_j \mid \mathcal{E}] \leq \frac{1}{2n}$.

Proof. Fix any $j \in \{1, \cdots, n\}$, we define 0-1 random variable $X^{\mathcal{I}}$ iff $\mathsf{A}(y, r^{\mathcal{I}} \oplus e_j) = \mathsf{gl}(x, r^{\mathcal{I}} \oplus e_j)$ Thus, , we have for every $\mathcal{I} \subseteq \{1, \cdots, \ell\}$

$$\mathbb{E}\left[X^{\mathcal{I}}\right] \geq \frac{1}{2} + \frac{\varepsilon(n)}{2}$$

and all the $X^{\mathcal{I}}$ are pairwise independent (i.e., for any $\mathcal{I}_1 \neq \mathcal{I}_2$, $X^{\mathcal{I}_1}$ and $X^{\mathcal{I}_2}$ are independent). Let $m = 2^\ell - 1 = 2n/\varepsilon(n)^2$ be number of all possible $X^{\mathcal{I}}$.

$$\begin{aligned}
\Pr[x'_j \neq x_j \mid \mathcal{E}] &= \Pr[\sum_{\mathcal{I}} X^{\mathcal{I}} \leq \frac{m}{2} \mid \mathcal{E}] \\
&= \Pr[\sum_{\mathcal{I}} X^{\mathcal{I}} \leq \frac{m}{2}] \\
&= \Pr[\sum_{\mathcal{I}} X^{\mathcal{I}} - \left(\frac{1}{2} + \frac{\varepsilon(n)}{2}\right) \cdot m \leq -\frac{\varepsilon(n)}{2} \cdot m] \\
&\leq \Pr[\left|\sum_{\mathcal{I}} X^{\mathcal{I}} - \left(\frac{1}{2} + \frac{\varepsilon(n)}{2}\right) \cdot m\right| \geq \frac{\varepsilon(n)}{2} \cdot m] \\
&\leq \frac{Var[\sum_{\mathcal{I}} X^{\mathcal{I}}]}{(\frac{\varepsilon(n)}{2} m)^2} = \frac{\sum_{\mathcal{I}} Var[X^{\mathcal{I}}]}{(\frac{\varepsilon(n)}{2} m)^2} \\
&\leq \frac{Var[X^{\mathcal{I}}]}{\frac{\varepsilon(n)^2}{4} m} \leq \frac{\frac{1}{4}}{\frac{\varepsilon(n)^2}{4} \frac{2n}{\varepsilon(n)^2}} = \frac{1}{2n}
\end{aligned}$$

where the second inequality is by Chebyshev, and the third inequality is due to that[4] for pairwise independent r.v.s $X_1, \ldots, X_m$

$$Var[\sum_{i=1}^{m} X_i] = \sum_{i=1}^{m} Var[X_i]$$

[4]Recall that $Var[X_i + X_j] = Var[X_i] + Var[X_j] - 2cov(X_i, X_j)$, where covariance $cov(X_i, X_j) = \mathbb{E}[X_i \cdot X_j] - \mathbb{E}[X_i] \cdot \mathbb{E}[X_j]$ which is zero if X_i and X_j are independent.

and third inequality is due to

$$Var[X^{\mathcal{I}}] = \mathbb{E}[(X^{\mathcal{I}})^2] - \mathbb{E}[X^{\mathcal{I}}]^2 = \mathbb{E}[X^{\mathcal{I}}] - \mathbb{E}[X^{\mathcal{I}}]^2 \leq \frac{1}{4}$$

□

Lemma 3 (Chebyshev's inequality.)**.** *Let Y be any random variable (taking real number values) with expectation μ and standard deviation σ (i.e., $Var[Y] = \sigma^2 = \mathbb{E}[(Y-\mu)^2]$). Then, for any $\delta > 0$ we have*

$$\Pr[\ |Y - \mu|\ \geq \delta\sigma]\ \leq\ 1/\delta^2$$

Summing up, combining Theorem 1 and 2 we get the corollary below:

Corollary 3.1. *One-way permutations imply pseudorandom generators.*

In fact, we know a more general statement below, which is one of the most founding pieces of modern cryptography. However, the proof will be much more involved and not suitable for presentation in a couple of lectures.

Theorem 4. *One-way functions imply pseudorandom generators.*

Homework 3. Exercises 6.1, 6.2, 6.4, 6.6 and the exercise below

Exercise 1 (Revisiting our proof for the Goldreich-Levin Theorem)**.** In fact, in our lecture we proved the following statement (which is slightly stronger than what we actually need with inferior bounds): assume there exists a PPT A of running time t and a non-negligible function $\varepsilon(\cdot)$ such that Equation (2) holds, then there exists another PPT A' of running time $\mathsf{poly}(1/\varepsilon(n), n)$ such that Equation (3) holds. Show that under the same assumption, there exists PPT A'' of running time $\mathsf{poly}(1/\varepsilon(n), n)$ such that

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n}[\ \mathsf{A}''(f(x)) \in f^{-1}(f(x))\ ] \geq \frac{\varepsilon(n)}{4} \tag{4}$$

Note that Equation (4) has better bounds than Equation (3) and it already suffices to prove the theorem.
hint: You just need to slightly adapt the proof to boost the inversion success probability using the fact that for any one-way function f, one can efficiently verify if some x' is a preimage of y under f or not, i.e. if $f(x') = y$ or not.

Proof. We know (as already proven) there exists $\mathcal{S}_n \subseteq \{0,1\}^n$ such that $\Pr[U_n \in \mathcal{S}_n] \geq \frac{\varepsilon(n)}{2}$) and for every $x \in \mathcal{S}_n$ it holds that

$$\Pr_{r \xleftarrow{\$} \{0,1\}^n}[\mathsf{A}(f(x), r) = \mathsf{gl}(x, r)]\ \geq\ \frac{1}{2} + \frac{\varepsilon(n)}{2}$$

The inversion algorithm A''. Let $\ell = \lceil \log(2n/\varepsilon(n)^2 + 1) \rceil$

Uniformly and independently sample $s^1, \ldots, s^\ell \xleftarrow{\$} \{0,1\}^n$. Let $\sigma^1 \ldots \sigma^\ell = 0^\ell$ (initialized to all zero), where each σ^i is a guess for $\mathsf{gl}(x, s^i)$.

1. For **every** non-empty subset $\mathcal{I} \subseteq \{1, \ldots, \ell\}$, let $r^{\mathcal{I}} \stackrel{\text{def}}{=} \bigoplus_{i \in \mathcal{I}} s^i$ and $\tau^{\mathcal{I}} := \bigoplus_{i \in \mathcal{I}} \sigma^i$ (which becomes a guess for $\mathsf{gl}(x, r^{\mathcal{I}})$ in the sense that it is correct if all the ℓ values of σ^i's are).

2. For every $j \in \{1, \ldots, n\}$, make a guess about the j^{th} bit of x, denoted by x_j, as follows:

   (a) For every non-empty subset $\mathcal{I} \subseteq \{1, ..., \ell\}$, set $v_j^{\mathcal{I}} := \tau^{\mathcal{I}} \oplus \mathsf{A}(y, r^{\mathcal{I}} \oplus e_j)$, where

   $$e_j \stackrel{\text{def}}{=} \underbrace{0 \cdots 0}_{j-1} 1 \underbrace{0 \cdots 0}_{n-j} \in \{0,1\}^n$$

   (b) Do a majority voting on the candidate values $\{v_j^{\mathcal{I}} : \emptyset \neq \mathcal{I} \subseteq \{1, \cdots, \ell\}\}$ and let x'_j to be the majority bit of them.

3. If $f(x') = f(x)$, output x' and terminate, otherwise, increment $\sigma^1 \ldots \sigma^\ell$ by 1 and repeat the above step 1 and step 2.

We have

$$\begin{aligned}
& \Pr_{x \stackrel{\$}{\leftarrow} \{0,1\}^n} [\ \mathsf{A}''(f(x)) \in f^{-1}(f(x))\ ] \\
\geq\ & \Pr_{x \stackrel{\$}{\leftarrow} \{0,1\}^n} [x \in \mathcal{S}_n] \cdot \min_{x \in \mathcal{S}_n} \{\Pr[\mathsf{A}''(f(x)) \in f^{-1}(f(x))]\} \\
\geq\ & \frac{\varepsilon(n)}{2} \cdot \min_{x \in \mathcal{S}_n} \{\Pr[x = x' | \text{ all } \sigma^i \text{ are correct guesses}]\} \\
\geq\ & \frac{\varepsilon(n)}{2} \cdot \frac{1}{2} = \frac{\varepsilon(n)}{2}
\end{aligned}$$

where note A'' may either return some $x' \neq x$ but satisfying $f(x') = f(x)$ (which is not a problem) or it will eventually reach the right guess values $\sigma^1 \ldots \sigma^\ell$ (for $\mathsf{gl}(x, s^1) \ldots \mathsf{gl}(x, s^\ell)$) on which it has success probability $1/2$ (see the original proof).

□