∾ CS6222 Cryptography ∾

Topic: Construction of PRG from OWF — Date: Oct 24, 2024
Lecturer: Wei-Kai Lin (TA: Arup Sarker) — Scriber: Nate Kimball and Alex Fetea

---

1 Construction of PEG from OWF

First, we recall the definition of a pairwise independent hash family and the Leftover Hash Lemma:

Definition 1. Pairwise Independent Hash Family
$\mathbb{H} = \{h : \{0,1\}^n \to \{0,1\}^n\}$ such that over random $h \leftarrow \mathbb{H}$:
$-\ \forall x \in \{0,1\}^n, h(x)$ is uniform in $\{0,1\}^m$
$-\ \forall x, x' \in \{0,1\}^n, h(x), h(x')$ are independent

Theorem 2. ***Leftover Hash Lemma***
Let $\mathbb{H} \coloneqq \{h : \{0,1\}^n \to \{0,1\}^m\}$ be a family of pairwise independent hash functions, and let $X \leftarrow \{0,1\}^n$ be a random variable with min-entropy $H_\infty(X) \geq k$. Then for $h \sim \mathbb{H}$ chosen uniformly at random, we have the following bound on the statistical distance:

$$SD[(h, h(X)), (h, U_m)] \leq \epsilon$$

if $m = k - 2\log(\frac{1}{\epsilon})$ for all $\epsilon > 0$, that is to say, $(h, h(X))$ is ϵ-close to the uniform distribution of $|h| + m$ bits, $|h|$ denotes the description length of the function h.

Recall the definition of an s-regular one-way function:

Definition 3. s-Regular One Way Function
An *s-regular OWF* is a OWF such that for all $x \in \{0,1\}^n$, $|f^{-1}(f(x))| = 2^{s(n)}$. (think of this as a s-to-1 mapping).

Also, recall the definition of a pseudo-entropy generator:

Definition 4. Pseudo-Entropy Generator
F is a *pseudo-entropy generator* if there exists $k = k(n)$ such that:

1. $H(F(U_n)) \leq k$.
2. There exists ensemble of distributions Y_n such that $H(Y_n) \geq k + \frac{1}{100n}$ and $\{F(U_n)\} \approx_c \{Y_n\}$.

Claim 5. ***OWF ⇒ PEG***
We will construct a PEG from an s-regular OWF, f, as follows:

$$F(x, M, r) \coloneqq f(x), M, r, M \odot x, r \odot x$$

where $f(x) \in \{0,1\}^n,\ M \in \{0,1\}^{(s+1)\times n},\ r \in \{0,1\}^n,\ M \odot x \in \{0,1\}^{s+1},\ r \odot x \in \{0,1\}$

so $H(f(x)) = n - s,\ H(M) = (s+1)n,\ H(r) = n,\ H(M \odot x) = ?, H(r \odot x) = ?$
For F to be a PEG, we want the entropy of $M \odot x$ and $r \odot x$ to be lower than if they were uniformly random, while still being computationally indistinguishable from uniform random strings.

First we will show that $r \odot x$ is at least somewhat determined given the remainder of the $F(x, M, r)$

Lemma 6. ***Low Real Entropy***
Given the following random variables:

$$X(x, M, r) \coloneqq (f(x), M, r, M \odot x),\ \ Z(x, M, r) \coloneqq r \odot x,\ \ Z' \coloneqq U_1$$

$F(U_n) = XZ$ *here* $n = |(x, M, r)|$ *instead of* $|f(x)|$
For some k, $H(F(U_n)) = H(XZ) = k$ *where* XZ *is the concatenation of* X *and* Z

Construct ensemble $Y_n = XZ'$
$H(Y_n) = H(XZ')$

we want to show that $H(Y_n) \geq k + \frac{1}{100n}$
Idea: given X, x *is unique, so* $r \odot x$ *must have less entropy then* U_1
Since f *is s-regular:*

$$T = f^{-1}(f(x)), |T| = 2^s$$

Since $M \odot x$ *is a pairwise independent hash:*

$$\forall x' \in T, x' \neq x, \Pr_M \left[M \odot x' = M \odot x\right] = \frac{1}{2^{s+1}}$$

because $\forall x.M \odot x$ *is uniform in* $\{0, 1\}^{s+1}$

We can get a bound on the uniqueness of x *given* X

$$\Pr_M \left[\exists x \in T \ \ s.t.\ \ M \odot x' = M \odot x\right] \leq \frac{1}{2^{s+1}} 2^s = \frac{1}{2} \quad \textit{by union bound}$$

the complement is

$$Pr\left[x \ \textit{is unique} \ |X\right] > \frac{1}{2}$$

if x *is unique, it determines* $x \odot r$ *decreasing entropy of* $Z|X$
$H(Z|X) \leq \frac{1}{2}$ *because there is at least* $\frac{1}{2}$ *probability that* x *is unique given* X*, in which case* $Z|X$ *can only take on one value and has entropy 0*
$H(Z'|X) = 1$ *by definition*
$H(Z|X) + \frac{1}{2} \leq H(Z'|X)$
$\Rightarrow H(XZ) + \frac{1}{2} \leq H(XZ')$ *by conditional entropy* $\forall$ *r.v.s* X, Z. $H(XZ) = H(X) + H(Z|X)$
$\therefore H(Y_n) \geq k + \frac{1}{100n}$

Lemma 7. ***High Pseudo Entropy***

$$\{F(U_n)\} \approx_c \{Y_n\},\ \ Y_n \ \textit{defined same as before}$$

$$(f(x), M, r, M \odot x, r \odot x) \approx_c (f(x), M, r, M \odot x, U_1)$$

Proof. Assume for the sake of contradiction, $\exists$ NUPPT A, poly p, s.t. for infinitely many n:

$$Pr\left[A(f(x), M, r, M \odot x) = r \odot x\right] \geq \frac{1}{2} + p(n)$$

This assertion is the negation of the lemma. We want to show that this implies f is not OWF, therefore the lemma must be true.

Our reduction won't have access to x, only $f(x)$, so how will we simulate $M \odot x$?
Idea: $|M \odot x| = s+1, M \odot x$ is necessarily not uniform, but $(M \odot x)[1...s - 2\log(n)]$ is uniform

$H_\infty(x|f(x)) = s$ because f is s-regular, so by the leftover hash lemma:

$$SD\left((M \odot x)[1...s - 2\log(n)], U_{s-2\log(n)}\right) \leq \frac{1}{n} = \epsilon$$

We can simulate $(f(x), M, r, (M \odot x)[1...s - 2\log(n)])$ by guessing uniformly randomly $(M \odot x)[1...s - 2\log(n)] \sim U_{s-2\log(n)}$

We have the following bound on the probability that $(M \odot x)[1...s - 2\log(n)]$ is supported, in other words, $(f(x), M, r, (M \odot x)[1...s - 2\log(n)])$ is valid, i.e. there exists an x and M that can produce that string:

$$SD(D, U) \leq \epsilon \implies Pr[x \in \sup(D)] \geq 1 - \epsilon$$

Since we have only $2\log(n) + 1$ bits of $M \odot x$ unknown, we can try all possible suffixes until a valid input is found in polynomial time.

We can construct the following reduction that inverts f:

$B(y = f(x)) :=$
  $M \leftarrow \{0,1\}^{(s+1)\times n}$
  $t_1 \leftarrow \{0,1\}^{s-2\log(n)}$
  for $t_2 \in \{0,1\}^{s-2\log(n)}$:
    $x' \leftarrow B_0(y, M, t = t_1 \| t_2)$ B_0 finds the preimage of $f(x)$ given M and $M \odot x$, it is defined below
    if $f(x') = y$, output x'

One of the values of $t_1 \| t_2$ should be a valid $M \odot x$, as proved before, so this reduction should return an element in the preimage with non-negligable probability, assuming B_0 inverts $f(x)$ given $M, M \odot x$ with non-negligable probability.

We will construct B_0 the same as was by Goldreich-Levin [GL89]. We will leave out some details and analysis, but they can be found in prior lectures or the original reduction.

$B(y, M, t) :=$
  $r_1, ..., r_m$ pairwise independent n-bit strings
  $g_1, ..., g_m$ pairwise independent bits
  for $i = 1...n$:
    for $j = 1...n$:
      $z_{ij} \leftarrow A(y, M, r_j \oplus e_i, t) \oplus g_j$ where e_i is the one-hot vector with $e_i[i] = 1$
      *the aim is that $A(y, M, r_j \oplus e_i, t) = x \odot (g \oplus e_i)$ and $g_j = x \odot r_j$
    $z_i \leftarrow \text{maj}(\{z_{ij}\}_{j=1...m})$

□

Acknowledgement

References

[GL89] Oded Goldreich and Leonid A. Levint. A hard-core predicate for all one-way functions. *Symposium on the Theory of Computing*, 1989.