## ☙ CS6222 Cryptography ❧

Topic: Construction of PRG from OWF | Date: Oct 22, 2024
Lecturer: Wei-Kai Lin (TA: Arup Sarker) | Scriber: Liran Li

---

# 1 Construction of PRG from OWF

Firstly we recall the leftover hash lemma:

**Theorem 1.** ***Leftover Hash Lemma***
*We have a family of hash functions $\mathbb{H} := \{h : \{0,1\}^n \to \{0,1\}^m\}$, the hash functions are pairwise independent, and we have a random variable $X \leftarrow \{0,1\}^n$, suppose the minimal entropy $H_\infty(X) \geq k$, then over the random space of $X$, $h \leftarrow \mathbb{H}$, 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 $\epsilon$-close to uniform distribution of $|h| + m$ bits, $|h|$ denotes the description length of the function $h$.*

**Note 2.** *Note that in the definition above, if $x = 0$, we will always have $M \odot x = 0$, which is a boundary case. We can define $M \odot x$ alternatively to be:*

$$M \odot x := \begin{cases} m \text{ (random)} & \text{if } x = 0 \\ M \odot x & \text{if } x \neq 0 \end{cases}$$

*and we define $h := (m, M)$.*

**Example 3.** We consider the example: $h := M \in \{0,1\}^{n \times m}$, a random matrix. If $M$ is squared matrix, it has a good chance to be invertible, given this $M \odot x$ is not likely to be close to uniform.

Also, we recall the definition of weak pseudo-entropy generators:

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

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

Now, we see how to construct PRG from PEG (Pseudo-Entropy Generator), we discuss the high level construction:

**Claim 5.** ***PEG $\Rightarrow$ PRG***
*Firstly we do* entropy equalization*:*

$$G(x_1, x_2, ..., x_m) := F(x_1) \| F(x_2) \| \cdots \| F(x_m)$$

*each $|x_i| = n$. Our goal is to have a minimal entropy version of PEG. Suppose $G$ is "strong PEG" (with respect to the minimal entropy), we define:*

$$g(x_1, ..., x_m) := G(x_1) \| G(x_2) \| \cdots \| G(x_m)$$

*observe that each $G(x_i) \approx_c Y_n'$, $H_\infty(Y_n) \geq k + \frac{1}{100n}$, we have after repetition:*

$$H_\infty(g) \geq m \cdot k + \frac{m}{100n} = m \cdot k + \frac{n}{100} \text{(if we take } m = n^2\text{)}$$

*for pseudo minimal entropy, and for the original construction we have $H_\infty \leq m \cdot k$. However, it is not the real construction yet, we use the hash functions:*

$$g(h_1, h_2, x_1, ..., x_m) \coloneqq h_1 \| h_2 \| h_1(G(x_1) \| G(x_2) \| \cdots \| G(x_m)) \| h_2(x_1 \| x_2 \| \cdots \| x_m)$$

*we want $h_1 : \{0,1\}^* \to \{0,1\}^{m \cdot k + n/200}$ and $h_2 : \{0,1\}^* \to \{0,1\}^{m \cdot (n-k) - n/400}$. We skipped some steps, note that knowing the number $k$ is crucial here, all the constructions above rely on the fact that we know $k$, otherwise, we have to try any $k \in \{1, ..., m\}$. Finally, after getting $k$, we have the PRG:*

$$g_1(x) \oplus g_2(x) \oplus \cdots \oplus g_k(x) \oplus \cdots \oplus g_n(x)$$

*which is pseudorandom based on the fact that just one $g_k$ is pseudorandom, by XOR trick, the whole function is pseudorandom.*

Given all the discussions above, the only remaining thing is to construct a PEG. Note that we want to get PEG from OWF.

**Definition 6. k-Regular One Way Function**
A *k-regular OWF* is a OWF such that for all $x \in \{0,1\}^n$, $|f^{-1}(f(x))| = 2^k$. (thinks of this as a $k$-to-1 mapping).

**Theorem 7.** *We have k-regular OWF implies $(n-k)$-PEG.*

*Proof.* Firstly we see the construction: suppose $f$ is $k$-regular OWF, then we construct $G$:

$$G(x, M, r) \coloneqq f(x) \| M \odot x \| M \| r \| r \odot x$$

where we have the matrix $M \in \{0,1\}^{k \times n}$, $|x| = n$, $M \odot x$ is $k$-bits, the output entropy of $f(x)$ is $H(f(x)) = n - k$. Entropy is still not clear yet, $M$ and $r$ are uniform, we don't know the situations of $M \odot x$ and $r \odot x$. Note that we have the hardcore $r \odot x$, even $x$ is mathematically determined, it could be hard to compute within polynomial time, thus $r \odot x$ can be the pseudo-entropy, we will prove this next time. □

## Acknowledgement

## References