The GGM Function Family is Weakly One-Way

Aloni Cohen and Saleet Klein

May 2025

Definition (Weak One-Way Function). *A function*

$$f : \{0,1\}^* \rightarrow \{0,1\}^*$$

is called weakly one-way *if it satisfies both of the following:*

1. *(**Efficiency**) There is a deterministic polynomial-time algorithm that on input x outputs $f(x)$.*
2. *(**Inversion Hardness**) There exists a polynomial $p(\cdot)$, such that for every probabilistic polynomial-time adversary A and for all sufficiently large $n \in \mathbb{N}$,*

$$\Pr_{x \leftarrow \{0,1\}^n}\big[A(1^n,\, f(x)) \in f^{-1}(f(x))\big] \;<\; 1 \;-\; \frac{1}{p(n)}.$$

Here the probability is over the uniform choice of $x \in \{0,1\}^n$ and the internal randomness of A.

Definition (Pseudo-random Generator). *An efficiently computable function*

$$G : \{0,1\}^n \;\longrightarrow\; \{0,1\}^{2n}$$

is called a (length-doubling) pseudorandom generator (PRG) *if the distribution $G(U_n)$ is computationally indistinguishable from the uniform distribution U_{2n}. In other words, for every probabilistic polynomial-time distinguisher D, there exists a negligible function $negl(\cdot)$ such that*

$$\Big|\Pr\big[D\big(G(U_n)\big) = 1\big] \;-\; \Pr\big[D(U_{2n}) = 1\big]\Big| \;\leq\; negl(n),$$

where the probabilities are taken over the choice of the uniform seeds and the internal randomness of D.

Theorem. *Let*

$$\big\{\, f_s : \{0,1\}^n \;\longrightarrow\; \{0,1\}^n \big\}_{s \in \{0,1\}^n}$$

be the length-preserving GGM function ensemble built from a pseudorandom generator G. Then for every constant $\varepsilon > 0$, GGM func. ensemble is a $(1 - 1/n^{2+\varepsilon})$-weakly one-way collection of functions.

Proposition (Input Switching Proposition)**.** *For every constant $\varepsilon > 0$ and sufficiently large $n \in \mathbb{N}$,*

$$\mathsf{Adv}_A\big(D_{\mathsf{owf}}\big) \ > \ 1 - \frac{1}{n^{2+\varepsilon}} \implies \mathsf{Adv}_A\big(D_{\mathsf{rand}}\big) \ > \ \frac{1}{\mathrm{poly}(n)}. \tag{12}$$

Claim. *For every $k \in \{0, \dots, n-1\}$,*

1. $D_{owf} \approx_c D_0^k$,
2. $D_1^k \approx_c D_{mix}$,
3. $D_{mix} \approx_c D_{rand}$.

Claim. *Let D_{owf}, D_0^k, D_1^k, D_{mix}, and D_{rand} be defined as above. For every constant $\varepsilon' > 0$ and every $n \in \mathbb{N}$, at least one of the following holds:*

1. *There exists $k^* \in \{0, 1, \dots, n-1\}$ such that*

$$SD\big(D_0^{k^*}, D_1^{k^*}\big) \ > \ 1 - \frac{1}{n^{2+\varepsilon}},$$

2.

$$SD\big(D_{owf}, D_{rand}\big) \ < \ \frac{2}{n^{\varepsilon'/2}}.$$

Lemma (Distinguishing Lemma)**.** *Let G be a pseudorandom generator for the corresponding GGM ensemble. For all PPT algorithms A and polynomials $\alpha(n)$, there exists a PPT distinguisher D such that for all $n \in \mathbb{N}$,*

$$\mathsf{Adv}_A\big(U_n \times U_n\big) \ \geq \ \frac{1}{\alpha(n)} \implies \big|\Pr\big[D\big(G(U_n)\big) = 1\big] - \Pr\big[D(U_{2n}) = 1\big]\big| \ \geq \ \left(\frac{1}{4\,\alpha(n)}\right)^5 - negl(n).$$