The GGM PRF is a Weakly One-Way Family of Functions

Aloni Cohen[1] and Saleet Klein[2]

[1] MIT, Cambridge, MA, USA
aloni@mit.edu
[2] Tel Aviv University, Tel Aviv, Israel
saleetklein@mail.tau.ac.il

Abstract. We give the first demonstration of a cryptographic hardness property of the Goldreich-Goldwasser-Micali (GGM) pseudo-random function family when the secret key is exposed. We prove that for any constant $\epsilon > 0$, the GGM family is a $1/n^{2+\epsilon}$-weakly one-way family of functions, when the lengths of seeds, inputs, and outputs are equal. Namely, any efficient algorithm fails to invert GGM with probability at least $1/n^{2+\epsilon}$ – *even when given the secret key.* We additionally state a natural condition under which the GGM family is strongly one-way. Along the way, we prove a purely combinatorial lemma for 'GGM-like' functions, relating the size of the image of such functions to the statistical distance between certain 'sub-functions.'

1 Introduction

Pseudo-random functions are fundamental objects in cryptography, and theoretical computer science generally. A pseudo-random function ensemble is a collection of (efficient) functions $\mathcal{F} = \{f_s\}_{s \in \{0,1\}^*}$ indexed by a *secret key* $s \in \{0,1\}^*$ with the dual properties that (1) given the key s, f_s is efficiently computable and (2) without knowledge of the secret key, no probabilistic polynomial-time algorithm can distinguish between oracle access to a random function from the ensemble and access to a random oracle. The security property of pseudo-random functions depends on the absolute secrecy of the key, and no security is guaranteed when the secret key is revealed. Pseudo-random functions have found wide use in cryptography, often to derandomize algorithms to gain functionality while not compromising on security. This paradigm is found everywhere from private-key encryption and digital signatures [Gol04] to derandomizing obfuscated circuits [SW14]. Besides cryptography, pseudorandom functions have been used to show negative results in computational learning theory [Val84], and to demonstrate the inherent limits of using natural proofs to prove circuit lower-bounds [RR97].

The first construction of pseudo-random function families starting from any one-way functions came in 1986 by Goldreich, Goldwasser, and Micali [GGM86]. The GGM family is an important step in understanding the full power of one-way functions. Assuming only that a function is hard to invert, the construction amplifies the secrecy of a short random seed into an exponentially-long, randomly-accessible sequence of pseudo-random values. For about 10 years, this was the only known paradigm for constructing of pseudo-random functions, even from specific assumptions. Almost 30 years later, it remains the only generic approach to construct PRFs from any one-way function.

Almost three decades after its conception, we are continuing to discover surprising power specific to the GGM pseudo-random function family. The basic ideas of this construction were used in construction of broadcast encryption schemes in the early 90s [FN94]. More recently, Zhandry exhibited the first quantum-secure PRF by demonstrating that the (classical) GGM ensemble (instantiated with a quantum-secure pseudo-random generator) is secure even against quantum adversaries [Zha12]. In [BW13,BGI14,KPTZ13], the notion of constrained pseudo-random functions was introduced. The "constrained keys" for these PRFs allow a user to evaluate the function on special subsets of the domain while retaining pseudo-randomness elsewhere. The GGM ensemble (and modifications thereof) is a constrained PRF for the family of prefix-constraints (including point-puncturing), and is the only known non-trivial construction of constrained PRFs from one-way functions. This family of constraints is powerful enough to enable many known applications of these families for program obfuscation [SW14].

In this work, we give the first demonstration that the GGM family enjoys some measure of security even when the secret key is revealed to an attacker. In this setting, pseudo-random functions need not guarantee any security (even for constrained PRFs). Indeed, the Luby-Rackoff family of pseudo-random functions [LR88] are efficiently invertible given knowledge of the secret key. This suggests that we must examine *specific* constructions of pseudo-random functions. In this work, we ask the following question:

> *What security, if any, does the GGM ensemble provide when the secret key is known?*

A version of this question was posed and addressed by Goldreich in 2002[3] [Gol02]. Goldreich casts the question from the angle of correlation intractability. Informally, a function ensemble $\{f_s\}_{s\in\{0,1\}^*}$ is correlation intractable if – even given the function description s – it is computationally infeasible to find an input x such that x and $f_s(x)$ satisfy some "sparse" relation. Correlation intractability was formalized in [CGH04], which proved that no such family exists for $|x| \geq |s|$.

In [Gol02], Goldreich proves that the GGM ensemble is not correlation intractable, even for $|x| < |s|$, in a very strong sense. Goldreich constructs a pseudo-random generator $G^{(0)}$ which, when used to instantiate the GGM ensemble, allows an adversary with knowledge of the secret key s to efficiently find preimages of $x \in f_s^{-1}(0^n)$. This allows the inversion of f_s for a specific image 0^n, but not necessarily for random images.

[3] And posed much earlier by Micali and by Barak: see Acknowledgments of [Gol02].

1.1 Our contributions

In this work, we prove that the length-preserving[4] GGM ensemble is a weakly one-way family of functions. This means that any efficient algorithm $\mathcal{A}$ that – when given the secret key s – purports to invert GGM on random inputs must fail with some noticeable polynomial probability, with high probability over the keys s. Moreover, we prove that if either a random function in $\mathcal{F}_G$ is close in statistical distance to a permutation, or is "regular" in the sense that each image has a polynomially-bounded number of pre-images, length-preserving GGM ensemble is strongly one-way. Formally:

Theorem 1. *Let $\mathcal{F}_G = \{f_s\}_{s\in\{0,1\}^*}$ be the length-preserving GGM function ensemble with pseudo-random generator G, where $f_s : \{0,1\}^{|s|} \to \{0,1\}^{|s|}$. Then for every constant $\epsilon > 0$, $\mathcal{F}_G$ is a $1/n^{2+\epsilon}$–weakly one-way collection of functions. That is, for every probabilistic polynomial-time algorithm $\mathcal{A}$, for every constant $\epsilon > 0$, and all sufficiently large n's,*

$$\Pr_{\substack{s\leftarrow U^n\\ x\leftarrow U^n}}\left[\mathcal{A}(s, f_s(x)) \in f_s^{-1}(f_s(x))\right] < 1 - \frac{1}{n^{2+\epsilon}} \tag{1}$$

Theorem 2. *Let $\mathcal{F}_G$ be the GGM ensemble with pseudo-random generator G. $\mathcal{F}_G$ is a strongly one-way collection of functions if either of the following hold:*

(a) There exists a negligible $\mathsf{negl}(\cdot)$ such that for all sufficiently large n

$$\mathop{\mathbb{E}}_{s\leftarrow U^n}\Big[\mathrm{SD}\big(f_s(U^n),\ U^n\big)\Big] \le \mathsf{negl}(n) \tag{2}$$

(b) There exists a polynomial B such that for all sufficiently large n and for all $s, y \in \{0,1\}^n$

$$|f_s^{-1}(y)| \le B(n) \tag{3}$$

Remark 1. The conditions of Theorem 2 are very strong conditions. Whether a pseudo-random generator G exists which makes the induced GGM ensemble satisfy either condition is an interesting and open question. The possibility of such a generator is open even for the stronger requirement that for every seed s, f_s is a permutation.

In order to prove the above theorems, we establish the following purely combinatorial lemma.

Lemma 1. *Let $G : \{0,1\}^* \to \{0,1\}^*$ be any length doubling function (not necessarily pseudo-random), and let G_0, G_1, and $\mathcal{F}_G$ be constructed in the manner of GGM (see Definition 4). For every constant $\epsilon > 0$ and every $n \in \mathbb{N}$, either*

- *There exists $k \in [0, n-1]$ such that*

$$\mathop{\mathbb{E}}_{r\leftarrow f_{U^n}(U^k)}\Big[\mathrm{SD}\big(f_{G_0(r)}(U^n),\ f_{G_1(r)}(U^n)\big)\Big] \le 1 - \frac{1}{n^{2+\epsilon}} \tag{L.1}$$

[4] We consider only the case when seeds, inputs, and outputs are of the same lengths.

- *The expected size of the image of f_s is large:*

$$\mathop{\mathbb{E}}_{s \leftarrow U^n}\Big[\frac{|\mathsf{Img}(f_s)|}{2^n}\Big] > 1 - \frac{2}{n^{\epsilon/2}} \tag{L.2}$$

Informally, this lemma states that either:

- There is a level k such for a random node r on the kth level, the subtrees induced by the left child $G_0(r)$ and the right child $G_1(r)$ are not too dissimilar.
- The image of f_s is in expectation, very large subset of the co-domain.

The proof of the lemma involves a careful counting argument. Applying the lemma, we show that if an efficient algorithm successfully inverts GGM with random seeds and images uniformly sampled according to $f_s(U^n)$, then the same algorithm must also succeed when inputs are sampled uniformly according to U^n. This argument makes crucial use of statistical distance, posing a barrier towards proving strong one-wayness of GGM. Under the same supposition of a strong inverting algorithm, we violate the pseudo-randomness of the PRG underlying the GGM family, yielding a contradiction and proving the theorem.

Organization Section 2 provides preliminaries and some essential definitions. Section 3 proves Lemma 1, along with a reformulation that will be easier for us to use. Section 4 contains a statement and proof of an additional lemma that we require, while Section 5 contains a full proofs of the main theorems.

2 Preliminaries

2.1 Notation

For two strings a and b we denote by $a\|b$ their concatenation. For a bit string $x \in \{0,1\}^n$, we denote by $x[i]$ its i-th bit, and by $x[i:j]$ (for $i < j$) the sequence $x[i]\|x[i+1]\|\cdots\|x[j]$. We abbreviate 'probabilistic polynomial time' as 'PPT'.

For a probability distribution D, we use $\mathrm{Supp}(D)$ to denote the support of D. We write $x \leftarrow D$ to mean that x is a sample from the distribution D. By U^n, we denote the uniform distribution over $\{0,1\}^n$. For a probabilistic algorithm A, we let $A(x)$ denote a sample from the probability distribution induced over the outputs of A on input x, though we occasionally abuse notation and let $A(x)$ denote the distribution itself. For a function $f : X \to Y$ and a distribution D over X, we denote by $f(D)$ the distribution over Y induced by $(f(x))_{x \leftarrow D}$.

Definition 1 (Multiset). *A* multi-set *M over a set S is a function $M : S \to \mathbb{N}$. For each $s \in S$, we call $M(s)$ the* multiplicity *of s. We say $s \in M$ if $M(s) \geq 1$, and denote the* size *of M by $|M| = \sum_S M(s)$. For two multi-sets M and M' over S, we define their intersection $M \cap M'$ to be the multiset $(M \cap M')(s) = \min[M(s), M'(s)]$ containing each element with the smaller of the two multiplicities.*

2.2 Standard cryptographic notions, and the GGM ensemble

Definition 2 (One-way collection of functions; adapted from [Gol04]). *A collection of functions* $\{f_s : \{0,1\}^{|s|} \to \{0,1\}^*\}_{s \in \{0,1\}^*}$ *is called* strongly (w-weakly) one-way *if there exists a probabilistic polynomial-time algorithm* Eval *such that the following two conditions hold:*

- Efficiently computable: *On input* $s \in \{0,1\}^*$, *and* $x \in \{0,1\}^{|s|}$, *algorithm* Eval *always outputs* $f_s(x)$.
- Strongly one-way*: For every polynomial* $w(\cdot)$, *for every probabilistic polynomial-time algorithm* $\mathcal{A}$ *and all sufficiently large* n,

$$\Pr_{\substack{s \leftarrow U^n \\ x \leftarrow U^n}}[\mathcal{A}(s, f_s(x)) \in f_s^{-1}(f_s(x))] < \frac{1}{w(n)} \tag{4}$$

- w-Weakly one-way*: There exists a polynomial* $w(\cdot)$ *such that for every probabilistic polynomial-time algorithm* $\mathcal{A}$ *and all sufficiently large* n,

$$\Pr_{\substack{s \leftarrow U^n \\ x \leftarrow U^n}}[\mathcal{A}(s, f_s(x)) \in f_s^{-1}(f_s(x))] < 1 - \frac{1}{w(n)} \tag{5}$$

We emphasize that in weakly one-way definition there is a single polynomial w which bounds the success probability of every efficient adversary. Additionally, weakly one-way collections can be easily amplified to achieve (strong) one-way functions [Gol04].

Definition 3 (Pseudo-random generator). *An efficiently computable function* $G : \{0,1\}^n \to \{0,1\}^{2n}$ *is a (length-doubling)* pseudorandom generator*, if* $G(U^n)$ *is computationally indistinguishable from* U^{2n}*. Namely for any PPT* $\mathcal{D}$

$$\left| \Pr[\mathcal{D}(G(U^n)) = 1] - \Pr[\mathcal{D}(U^{2n}) = 1] \right| = \mathsf{negl}(n)$$

Definition 4 (GGM function ensemble [GGM86]). *Let* G *be a deterministic algorithm that expands inputs of length* n *into string of length* $2n$*. We denote by* $G_0(s)$ *the* $|s|$*-bit-long prefix of* $G(s)$*, and by* $G_1(s)$ *the* $|s|$*-bit-long suffix of* $G(s)$ *(i.e.,* $G(s) = G_0(s) \| G_1(s)$*. For every* $s \in \{0,1\}^n$ *(called the* seed*), we define a function* $f_s^{(G)} : \{0,1\}^n \to \{0,1\}^n$ *such that for every* $x \in \{0,1\}^n$,

$$f_s^{(G)}(x[1], \ldots, x[n]) = G_{x[n]}(\cdots(G_{x[2]}(G_{x[1]}(s))\cdots) \tag{6}$$

For any $n \in \mathbb{N}$*, we define* F_n *to be a random variable over* $\{f_s^{(G)}\}_{s \in \{0,1\}^n}$*. We call* $\mathcal{F}_G = \{F_n\}_{n \in \mathbb{N}}$ *the* GGM function ensemble with generator G.

The construction is easily generalized to the case when $|x| \neq n$*. Though we define the GGM function ensemble as the case when* $|x| = n$*, we will make use of the more general case. We will typically write* f_s *instead of* $f_s^{(G)}$.

The GGM construction may be interpreted as a binary tree, and we will use this view throughout. Starting from any length-doubling function $G : \{0,1\}^n \to \{0,1\}^{2n}$, a seed $s \in \{0,1\}^n$ can be viewed as recursively defining a binary tree with root s, and the given by $G_0(s)$ and $G_1(s)$.

Each node in the binary tree of the GGM function has an n-bit label, and we will be interested in the possible labels of a node's parent, namely the set $G_0^{-1}(x) \cup G_1^{-1}(x)$ for some $x \in \{0,1\}^n$. We will denote this set by $G_*^{-1}(x) := G_0^{-1}(x) \cup G_1^{-1}(x)$.

The following facts follow from [GGM86], or can be shown using essentially the same techniques.

Facts:

- If G is a pseudo-random generator, then $\mathcal{F}_G$ is a pseudo-random function family.
- The distribution $f_{U^n}(U^{\ell(n)})$ (sampled by evaluating $f_s(x)$ for uniform $s \leftarrow U^n$ and $x \leftarrow U^{\ell(n)}$) is computationally indistinguishable from U^n, for any polynomial $\ell(n)$.
- For a length-doubling PRG $G = (G_0, G_1)$, the distribution $G_U(U^n)$ (sampled by evaluating $G_b(x)$ for uniform $b \leftarrow U$ and $x \leftarrow U^n$) is computationally indistinguishable from U^n.

2.3 Statistical distance

For two probability distributions D and D' over some universe X, we denote their statistical distance $\mathrm{SD}(D, D')$:

$$\mathrm{SD}(D, D') := \frac{1}{2}\sum_{x \in X} |D(x) - D'(x)| = \max_{S \subseteq X} \sum_{x \in S} D(x) - D'(x)$$

For a collection of distributions $\{D(p)\}$ with some parameter p, and a distribution P over the parameter p, we write

$$(p, D(p))_P$$

to denote the distribution over pairs (p, x) induced by sampling $p \leftarrow P$ and subsequently $x \leftarrow D(p)$.[5] It follows from the definition of statistical distance that for distributions P, $D(P)$, and $D'(P)$ (see appendix):

$$\mathrm{SD}\left(\big(p, D(p)\big)_P, \big(p, D'(p)\big)_P\right) = \mathop{\mathbb{E}}_{p \leftarrow P}\left[\mathrm{SD}\big(D(p), D'(p)\big)\right] \tag{7}$$

The quantity $|\mathsf{Img}(f)|$ is related to the statistical distance between the uniform distribution U^n and the distribution $f(U^n)$. For any $f : \{0,1\}^n \to \{0,1\}^n$,

$$\mathrm{SD}(f(U^n), U^n) = 1 - \frac{|\mathsf{Img}(f)|}{2^n} \tag{8}$$

[5] For example, the distribution $(x, \mathsf{Bernoulli[x]})_{\mathsf{Uniform[0,1]}}$ is the distribution over (x, b) by drawing the parameter x uniformly from $[0,1]$, and subsequently taking a sample b from the Bernoulli distribution with parameter x.

This identity can be easily shown by expanding the definition of statistical distance, or by considering the histograms of the two distributions and a simple counting argument. See the appendix for a proof.

An additional fact about the statistical distance of GGM functions will be useful. For all $\ell < n$ and seeds s_0 and s_1:

$$\mathrm{SD}\big(f_{s_0}(U^\ell),\ f_{s_1}(U^\ell)\big) \geq \mathrm{SD}\big(f_{s_0}(U^n),\ f_{s_1}(U^n)\big) \tag{9}$$

This can be shown by expanding the definitions, or by considering the nature of the distributions. For GGM trees rooted at s, the distribution $f_s(U^\ell)$ corresponds to picking a uniform node on level ℓ of the tree. The GGM construction implies that if two internal nodes have the same label, then their subtrees exactly coincide. Thus, the fraction of nodes at level n that coincide on trees rooted at s_0 and s_1 is at least the fraction of nodes at level ℓ that coincide.

2.4 Rényi divergences

Similar to statistical distance, the Rényi divergence is a useful tool for relating the probability of some event under two distributions. Whereas the statistical distance yields an additive relation between the probabilities in two distributions, the Rényi divergence yields a multiplicative relation. The following is adapted from Section 2.3 of [BLL+15].

For any two discrete probability distributions P and Q such that $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$, we define the *Rényi divergence* (of order 2) by

$$R\left(P\|Q\right) = \left(\sum_{x\in\mathrm{Supp}(Q)} \frac{P(x)^2}{Q(x)}\right) \quad . \tag{10}$$

An important fact about Rényi divergence is that for an abitrary event $E \subseteq \mathrm{Supp}(Q)$

$$Q(E) \geq \frac{P(E)^2}{R\left(P\|Q\right)} \quad . \tag{11}$$

3 A combinatorial lemma

We prove the following lemma, which will be critical to establishing our main theorem. We emphasize that this lemma is purely combinatorial, and makes no use of computational assumptions.

Lemma 1. *Let $G : \{0,1\}^* \to \{0,1\}^*$ be any length doubling function (not necessarily pseudo-random), and let G_0, G_1, and $\mathcal{F}_G$ be defined as in Definition 4. For every constant $\epsilon > 0$ and every $n \in \mathbb{N}$, either*

- *There exists $k \in [0, n-1]$ such that*

$$\mathop{\mathbb{E}}_{r\leftarrow f_{U^n}(U^k)}\Big[\mathrm{SD}\big(f_{G_0(r)}(U^n),\ f_{G_1(r)}(U^n)\big)\Big] \leq 1 - \frac{1}{n^{2+\epsilon}} \tag{L.1}$$

– *The expected size of the image of f_s is large:*

$$\mathop{\mathbb{E}}_{s \leftarrow U^n}\Big[\frac{|\mathsf{Img}(f_s)|}{2^n}\Big] > 1 - \frac{2}{n^{\epsilon/2}} \tag{L.2}$$

Informally, this lemma states that either:

- There is a level k such that for a random node r on the kth level, the subtrees induced by the left child $G_0(r)$ and the right child $G_1(r)$ are not too dissimilar.
- The image of f_s is in expectation, a very large subset of the co-domain.

Before proving the lemma, we establish more useful versions of (L.1) and (L.2) which will be used when proving our main results. Firstly, (L.1) implies the following inequality:

$$\begin{aligned}
&\mathrm{SD}\Big(\big(G_0(r),\ f_{G_0(r)}(U^n)\big)_{r \leftarrow f_{U^n}(U^k)}\ ;\ \big(G_0(r),\ f_{G_1(r)}(U^n)\big)_{r \leftarrow f_{U^n}(U^k)}\Big)\\
&\leq \mathrm{SD}\Big(\big(r,\ f_{G_0(r)}(U^n)\big)_{r \leftarrow f_{U^n}(U^k)}\ ;\ \big(r,\ f_{G_1(r)}(U^n)\big)_{r \leftarrow f_{U^n}(U^k)}\Big)\\
&= \mathop{\mathbb{E}}_{r \leftarrow f_{U^n}(U^k)}\Big[\mathrm{SD}\Big(f_{G_0(r)}(U^n)\ ;\ f_{G_1(r)}(U^n)\Big)\Big] \qquad \text{by (7)}\\
&\leq 1 - \frac{1}{n^{2+\epsilon}} \qquad\qquad \text{(L.1*)}
\end{aligned}$$

The first inequality holds because a distinguisher (even unbounded) for the former pair of distributions implies there exists a distinguisher (with at least the same advantage) for the latter pair.[6]

(L.2) implies the following statistical distance bound:

$$\begin{aligned}
\mathrm{SD}\left(\big(s, f_s(U^n)\big)_{U^n}\ ;\ \big(U^n, U^n\big)\right) &= \mathop{\mathbb{E}}_{s \leftarrow U^n}\Big[\mathrm{SD}\big(f_s(U^n)\ ;\ U^n\big)\Big] \qquad \text{by (7)}\\
&= \mathop{\mathbb{E}}_{s \leftarrow U^n}\Big[1 - \frac{|\mathsf{Img}(f_s)|}{2^n}\Big] \qquad \text{by (8)}\\
&< \frac{2}{n^{\epsilon/2}} \qquad\qquad \text{(L.2*)}
\end{aligned}$$

Proof (Lemma 1). Fix $n \in \mathbb{N}$ and a seed $s \in \{0,1\}^n$. For every $k \in [0, n-1]$ and $v \in \{0,1\}^k$ (letting $\{0,1\}^0 = \{\varepsilon\}$, where ε is the empty string), we define two multi-sets over $\{0,1\}^n$ ('L' for 'leaves') which together contain all the leaves contained in the subtree with prefix v of the GGM tree rooted at s.

$$\begin{aligned}
L^s_{v,0} &= \{f_s(x) : x = v\|0\|\star\}_{\star \in \{0,1\}^{n-k-1}}\\
L^s_{v,1} &= \{f_s(x) : x = v\|1\|\star\}_{\star \in \{0,1\}^{n-k-1}}
\end{aligned} \tag{12}$$

[6] This essentially a data-processing inequality.

Define $I_v^s := L_{v,0}^s \cap L_{v,1}^s$ to be their intersection. Recall that for a multi-set M, $M(x)$ is the multiplicity of the element x in M. Expanding the definition of statistical distance:

$$\begin{aligned}
&\mathrm{SD}(f_{G_0(f_s(v))}(U^{n-k-1}) \;;\; f_{G_1(f_s(v))}(U^{n-k-1})) \\
&= \frac{1}{2^{n-k-1}} \cdot \max_{X \subseteq \{0,1\}^n} \sum_{x \in X} \Big(L_{v,0}^s(x) - L_{v,1}^s(x) \Big) \\
&= 1 - \frac{|I_v^s|}{2^{n-k-1}} \qquad (13)
\end{aligned}$$

Rearranging and using (9) with $\ell = n - k$, we have that

$$\frac{|I_v^s|}{2^{n-k-1}} \leq 1 - \mathrm{SD}\Big(f_{G_0(f_s(v))}(U^n) \;;\; f_{G_1(f_s(v))}(U^n) \Big) \qquad (14)$$

For each $v \in \{0,1\}^k$, we define a set B_v^s of "bad" inputs x to the function f_s. For each $y \in I_v^s$, there are at least $I_v^s(y)$-many distinct x_0 (respectively, x_1) such that $f_s(x_0) = y$ and $x_0 = v\|0\|\star$ begins with the prefix $v\|0$ (respectively, $v\|1$). Assign arbitrarily $I_v^s(y)$-many such x_0 and x_1 to the set B_v^s. By construction,

$$|B_v^s| = 2|I_v^s| \qquad (15)$$

Let $B^s = \bigcup_{k=0}^{n-1} \bigcup_{v \in \{0,1\}^k} B_v^s$, and let $Q^s := \{0,1\}^n \setminus B^s$.[7]

Observe that f_s is injective on Q^s. To see why, consider some $x \in Q^s$, and let $x' \neq x$ be such that $f_s(x) = f_s(x') = y$ if one exists. Suppose that the length of their common prefix $v = \mathsf{pre}(x, x')$ is maximal among all such x'. By the maximality of the prefix v, x must be in B_v^s.

Therefore,

$$|\mathsf{Img}(f_s)| \geq |Q^s| \qquad (16)$$

Claim. For $\epsilon > 0$, $n \in \mathbb{N}$, if (L.1) is false, then

$$\mathop{\mathbb{E}}_{s \leftarrow U^n}\Big[\frac{|B^s|}{2^n}\Big] < \frac{2}{n^{\epsilon/2}} \qquad (17)$$

Proved below, this claim implies (L.2), completing the proof.

$$\mathop{\mathbb{E}}_{s \leftarrow U^n}\Big[\frac{|\mathsf{Img}(f_s)|}{2^n}\Big] \geq \mathop{\mathbb{E}}_{s \leftarrow U^n}\Big[\frac{|Q^s|}{2^n}\Big] = 1 - \mathop{\mathbb{E}}_{s \leftarrow U^n}\Big[\frac{|B^s|}{2^n}\Big] > 1 - \frac{2}{n^{\epsilon/2}} \qquad (18)$$

Proof (Claim 3). Fix constant $\epsilon > 0$. Suppose (L.1) is false: for all $k \in [0, n-1]$,

$$\mathop{\mathbb{E}}_{r \leftarrow f_{U^n}(U^k)}\Big[\mathrm{SD}\Big(f_{G_0(r)}(U^n) \;;\; f_{G_1(r)}(U^n) \Big)\Big] > 1 - \frac{1}{n^{2+\epsilon}} \qquad (19)$$

By Markov's Inequality, for any $\tau > 0$:

$$\Pr_{r \leftarrow f_{U^n}(U^k)}\Big[1 - \mathrm{SD}\Big(f_{G_0(r)}(U^n) \;;\; f_{G_1(r)}(U^n) \Big) > \frac{\tau}{n^{2+\epsilon}}\Big] < \frac{1}{\tau} \qquad (20)$$

[7] 'Q' for 'good,' because G is our pseudo-random generator.

We can now bound the expected size of $|B^s|$ as follows.

$$\begin{aligned}
&\mathop{\mathbb{E}}_{s\leftarrow U^n}\left[\frac{|B^s|}{2^n}\right] && (21)\\
&= \Pr_{\substack{s\leftarrow U^n\\ x\leftarrow U^n}}[x\in B^s]\\
&\le \sum_{k=0}^{n-1}\sum_{v\in\{0,1\}^k}\Pr_{s,x}[x\in B^s_v] \qquad \text{by the definition of } B^s\\
&= \sum_{k=0}^{n-1}\Pr_{s,x}\left[x\in B^s_{x[1:k]}\right]\\
&\le \sum_{k=0}^{n-1} T\cdot\Pr_{s,x}\left(\frac{|B^s_{x[1:k]}|}{2^{n-k}}\le T\right)+\Pr_{s,x}\left(\frac{|B^s_{x[1:k]}|}{2^{n-k}}>T\right) \qquad \text{for any } 0\le T\le 1\\
&\le \sum_{k=0}^{n-1} T+\Pr_{s,x}\left(\frac{|I^s_{x[1:k]}|}{2^{n-k-1}}>T\right) \qquad \text{by (15)} && (22)
\end{aligned}$$

Purely to reduce clutter, for $r\in\{0,1\}^n$, let

$$\Delta(r)=1-\mathrm{SD}\Big(f_{G_0(r)}(U^n)\ ;\ f_{G_1(r)}(U^n)\Big) \tag{23}$$

Continuing the above series of inequalities, and then observing that the distribution over $f_s(x[1:k])$ is precisely $f_{U^n}(U^k)$:

$$\begin{aligned}
&\le \sum_{k=0}^{n-1}\Big(T+\Pr_{\substack{s\leftarrow U^n\\ x\leftarrow U^n}}\left[\Delta\left(f_s\left(x[1:k]\right)\right)>T\right]\Big) \qquad \text{by (14)}\\
&\le n\frac{\tau}{n^{2+\epsilon}}+n\frac{1}{\tau} \qquad \text{for } T=\frac{\tau}{n^{2+\epsilon}}, \text{ by (20)}\\
&= \frac{2}{n^{\epsilon/2}} \qquad \text{for } \tau=n^{1+\epsilon/2} && (24)
\end{aligned}$$

4 Breaking the PRG by inverting

Having established our combinatorial lemma, we now state and prove an additional lemma which will be used to establish our main theorems. Informally, this lemma states that any efficient algorithm $\mathcal{A}$ that can invert f_s on uniformly random values $y\in\{0,1\}^n$ can be used to distinguish outputs of the PRG G from random.

Lemma 2. *Let G and $\mathcal{F}_G$ be defined as in Definition 4. If there exists a PPT algorithm $\mathcal{A}$ and a polynomial $\alpha(n)$ such that for infinitely many $n\in\mathbb{N}$:*

$$\Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[\mathcal{A}(s,y)\in f_s^{-1}(y)]>\frac{1}{\alpha(n)} \tag{25}$$

Then there exists a PPT distinguisher $\mathcal{D}$, which for infinitely many $n \in \mathbb{N}$:

$$\left|\Pr\left[\mathcal{D}\left(G\left(U^n\right)\right) = 1\right] - \Pr\left[\mathcal{D}\left(U^{2n}\right) = 1\right]\right| \geq \left(\frac{1}{4\alpha(n)}\right)^5 - \mathsf{negl}(n) \tag{26}$$

Because G is assumed to be a pseudorandom generator, no such PPT distinguisher $\mathcal{D}$ can exist.

Notice that the distribution over (s, y) in Eq. (25) is not the same as in the (weakly) one-way function definition: in the lemma y is a uniformly random element of the co-domain, whereas in the definition of a one-way function y is distributed according to $f_s(U^n)$ – the image of a uniform pre-image under f_s.

Proof (Lemma 2). The distinguisher $\mathcal{D}$ is defined as follows:

```
**Input**  : PRG challenge $(y_0, y_1)$ which is a sample from either $G(U^n)$ or $U^{2n}$
**Output**: $b \in \{0,1\}$
Sample a seed $s \leftarrow U^n$ and a bit $b \leftarrow U$ uniformly at random;
Compute $x \leftarrow \mathcal{A}(s, y_b)$;
if $f_s(x) = y_b$ and $f_s(x \oplus 0^{n-1}1) = y_{1-b}$ then
  | Output 1;        ("PRG")
else
  | Output 0;        ("random")
end
```

Algorithm 1: The PRG distinguisher $\mathcal{D}$

Notice that if $\mathcal{D}$ outputs 1, then either (y_0, y_1) or (y_1, y_0) is in $\mathsf{Img}(G)$. If (y_0, y_1) was sampled uniformly from U^{2n}, then this happens with probability at most $2^{n+1}/2^{2n}$. Therefore,

$$\Pr[\mathcal{D}(y_0, y_1) = 1 \mid (y_0, y_1) \leftarrow U^{2n}] = \mathsf{negl}(n) \tag{27}$$

We prove that

$$\Pr[\mathcal{D}(y_0, y_1) = 1 \mid (y_0, y_1) \leftarrow G(U^n)] \geq \left(\frac{1}{4\alpha(n)}\right)^5 \tag{28}$$

At a very high level, the intuition is that for most $(y_0, y_1) \in \mathsf{Img}(G)$, there are not too many y_1' for which either $(y_0, y_1') \in \mathsf{Img}(G)$ or $(y_1', y_0) \in \mathsf{Img}(G)$ is true (similarly for y_0' and y_1). After arguing that $\mathcal{A}$ must invert even on such "thin" y's, the chance that $y_{1-b}' = y_{1-b}$ is significant. We now examine this argument in detail.

We define the function

$$\begin{aligned} G_* : \{0,1\} \times \{0,1\}^n &\rightarrow \{0,1\}^n \\ (b, y) &\mapsto G_b(y) \end{aligned}$$

Then $G_*^{-1}(y) := G_0^{-1}(y) \cup G_1^{-1}(y)$ is the set of all preimages of y under either G_0 or G_1, and $\mathsf{Img}(G_*) = \mathsf{Img}(G_0) \cup \mathsf{Img}(G_1)$ is the set of all n-bit strings in the image of either G_0 or G_1.

Definition 5 (θ-thin, θ-fat). *An element $y \in \{0,1\}^n$ is called* θ-thin *under G if $|G_*^{-1}(y)| \leq \theta$. Otherwise, it is called* θ-fat. *Define the sets:*

$$\begin{aligned} \mathsf{Thin}_\theta &:= \{y \in \{0,1\}^n \ : \ y \textit{ is } \theta\textit{-thin}\} \\ \mathsf{Fat}_\theta &:= \{0,1\}^n \setminus \mathsf{Thin}_\theta \end{aligned}$$

Observe that because each θ-fat y must have at least θ preimages, and the domain of G_* is of size 2^{n+1}:

$$|\mathsf{Fat}_\theta| \leq \frac{2^{n+1}}{\theta} \quad . \tag{29}$$

For any $\theta \in \{1, \ldots, 2^n\}$, we can lower bound the probability that the distinguisher $\mathcal{D}$ outputs 1 in case of getting a bespoke PRG input.

$$\begin{aligned} &\Pr[\mathcal{D}(G(U^n)) = 1] \\ &= \Pr_{\substack{s \leftarrow U^n, b \leftarrow U \\ (y_0,y_1) \leftarrow G(U^n)}} [\mathcal{A}(s, y_b) \in f_s^{-1}(y_b) \ \wedge \ \mathcal{A}(s, y_b) \oplus 0^{n-1}1 \in f_s^{-1}(y_{1-b})] && (30) \\ &\geq \Pr_{\substack{b \leftarrow U \\ (y_0,y_1) \leftarrow G(U^n)}} [y_b \in \mathsf{Thin}_\theta] \\ &\quad \cdot \Pr_{\substack{s \leftarrow U^n, b \leftarrow U \\ (y_0,y_1) \leftarrow G(U^n)}} [\mathcal{A}(s, y_b) \in f_s^{-1}(y_b) \ | \ y_b \in \mathsf{Thin}_\theta] \\ &\quad \cdot \Pr_{\substack{s \leftarrow U^n, b \leftarrow U \\ (y_0,y_1) \leftarrow G(U^n)}} [\mathcal{A}(s, y_b) \oplus 0^{n-1}1 \in f_s^{-1}(y_{1-b}) \mid \mathcal{A}(s, y_b) \in f_s^{-1}(y_b) \wedge \ y_b \in \mathsf{Thin}_\theta] \\ & && (31) \end{aligned}$$

Thus, it suffices to show that (31) is not negligible. We show that every term is not negligible.

The first term can be lower-bounded by

$$\Pr_{y \leftarrow G_U(U^n)} [y \in \mathsf{Thin}_\theta] \geq \frac{1}{2\alpha(n)} - \frac{1}{\theta} \tag{32}$$

This follows from (29) and the hypothesis (25) of the lemma (see appendix for full details).

The third term can be lower-bounded by:

$$\Pr_{\substack{s \leftarrow U^n, b \leftarrow U \\ (y_0,y_1) \leftarrow G(U^n)}} \left[\mathcal{A}(s, y_b) \oplus 0^{n-1}1 \in f_s^{-1}(y_{1-b}) \middle| \begin{matrix} \mathcal{A}(s, y_b) \in f_s^{-1}(y_b) \\ \wedge \ y_b \in \mathsf{Thin}_\theta \end{matrix} \right] \geq \frac{1}{\theta} \tag{33}$$

To see why, suppose that indeed $y_b \in \mathsf{Thin}_\theta$ and $\mathcal{A}(s, y_b) \in f_s^{-1}(y_b)$. Because y_b is θ-thin, there are at most θ-possible values of $y'_{1-b} := f_s(\mathcal{A}(s, y_b) \oplus 0^{n-1}1)$. The true y_{1-b} is hidden from the adversary's view, and takes each of the possible values with probability at least $1/\theta$. Thus the probability that $y_{1-b} = y'_{1-b}$ is as above.

The second term can be lower-bounded by:

$$\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow G_U(U^n)}} [\mathcal{A}(s, y) \in f_s^{-1}(y) \mid y \in \mathsf{Thin}_\theta] \geq \left(\frac{1}{4\alpha(n)} \right)^3 \tag{34}$$

See proof below. In the course of that argument, we set $\theta = 4\alpha(n)$

Finally, letting $\theta = 4\alpha(n)$ and putting it all together implies that

$$\Pr[\mathcal{D}(G(U^n)) = 1] > \left(\frac{1}{2\alpha(n)} - \frac{1}{\theta} \right) \cdot \left(\frac{1}{4\alpha(n)} \right)^3 \cdot \frac{1}{\theta} \tag{35}$$

$$\geq \left(\frac{1}{4\alpha(n)} \right)^5 \tag{36}$$

proving (28) and completing the proof of the lemma.

Proof (Inequality (34)*).* To prove the inequality we define the notion of q-good.

Definition 6 (q-good). *For any $q \in [0, 1]$, an element $y \in \{0, 1\}^n$ is called* q-good with respect to θ *if it is both θ-thin and $\mathcal{A}$ finds some preimage of y for a uniformly random seed s with probability at least q. Namely,*

$$\mathsf{Good}_q := \left\{ y \in \mathsf{Thin}_\theta \ : \ \Pr_{s \leftarrow U^n} [\mathcal{A}(s, y) \in f_s^{-1}(y)] > q \right\}$$

First, we show that[8]

$$\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow G_U(U^n)}} [\mathcal{A}(s, y) \in f_s^{-1}(y) \mid y \in \mathsf{Thin}_\theta]$$

$$\geq \Pr_{y \leftarrow G_U(U^n)} [y \in \mathsf{Good}_q \mid y \in \mathsf{Thin}_\theta] \quad \cdot \Pr_{\substack{s \leftarrow U^n \\ y \leftarrow G_U(U^n)}} [\mathcal{A}(s, y) \in f_s^{-1}(y) \mid y \in \mathsf{Good}_q]$$

$$\geq \frac{|\mathsf{Good}_q|}{\theta \mid \mathsf{Thin}_\theta|} \cdot q \tag{37}$$

This is follows from the following two observations:

- By definition of Good_q:

$$\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow G_U(U^n)}} [\mathcal{A}(s, y) \in f_s^{-1}(y) \mid y \in \mathsf{Good}_q] > q \tag{38}$$

- The distribution $y \leftarrow G_U(U^n)$ is equivalent to the distribution $(G_b(x))_{(b,x) \leftarrow U \times U^n}$. The number of pairs (b, x) such that $G_b(x) \in \mathsf{Good}_q$ is at least $|\mathsf{Good}_q|$, while

[8] Note that while it the trivial statement that $\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow U^n}} [\mathcal{A}(s, y) \in f_s^{-1}(y) \mid y \in \mathsf{Thin}_\theta] = \frac{|\mathsf{Good}_q|}{|\mathsf{Thin}_\theta|}$ is true, this is not the probability that we here bound.

the number of pairs (b, x) such that $G_b(x) \in \mathsf{Thin}_\theta$ is at most $\theta|\mathsf{Thin}_\theta|$. Therefore:

$$\begin{aligned}\Pr_{y \leftarrow G_U(U^n)}&[y \in \mathsf{Good}_q \mid y \in \mathsf{Thin}_\theta] \\ &= \Pr_{(b,x) \leftarrow U \times U^n}[G_b(x) \in \mathsf{Good}_q \mid G_b(x) \in \mathsf{Thin}_\theta] \\ &\geq \frac{1}{\theta} \cdot \frac{|\mathsf{Good}_q|}{|\mathsf{Thin}_\theta|}\end{aligned}$$

In the appendix, we show that

$$\frac{|\mathsf{Good}_q|}{|\mathsf{Thin}_\theta|} = \Pr_{s,y \leftarrow U^n}[y \in \mathsf{Good}_q | y \in \mathsf{Thin}_\theta] \geq \frac{1}{\alpha(n)} - \frac{2}{\theta} - q \tag{39}$$

Selecting $\theta = 4\alpha(n)$ and $q = 1/4\alpha(n)$, (37) is bounded below by

$$\begin{aligned}\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow G_U(U^n)}}[\mathcal{A}(s, y) \in f_s^{-1}(y) | y \in \mathsf{Thin}_\theta] &\geq \frac{|\mathsf{Good}_q|}{\theta|\mathsf{Thin}_\theta|} \cdot q \\ &\geq \left(\frac{1}{4\alpha(n)}\right)^3\end{aligned}$$

This completes the proof of (34).

5 The one-wayness of GGM

Using the two lemmata, we now restate and prove our two main theorems.

Theorem 1. *Let $\mathcal{F}_G$ be the GGM ensemble with pseudo-random generator G. Then for every constant $\epsilon > 0$, $\mathcal{F}_G$ is a $1/n^{2+\epsilon}$–weakly one-way collection of functions. That is, for every probabilistic polynomial-time algorithm $\mathcal{A}$, for every constant $\epsilon > 0$, and all sufficiently large n's,*

$$\Pr_{\substack{s \leftarrow U^n \\ x \leftarrow U^n}}[\mathcal{A}(s, f_s(x)) \in f_s^{-1}(f_s(x))] < 1 - \frac{1}{n^{2+\epsilon}} \tag{40}$$

Proof (Theorem 1). Fix a constant $\epsilon > 0$. We assume for contradiction that there exists a PPT $\mathcal{A}$ and an infinite sequence $I_\mathcal{A} = \{n_i\}_{i \in \mathbb{N}}$ such that for every $n \in I_\mathcal{A}$:

$$\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow f_s(U^n)}}[\mathcal{A}(s, y) \in f_s^{-1}(y)] > 1 - \frac{1}{n^{2+\epsilon}} \tag{41}$$

We will show that there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all sufficiently large $n \in I_\mathcal{A}$:

$$\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow U^n}}[\mathcal{A}(s, y) \in f_s^{-1}(y)] > \frac{1}{2n^{2+\epsilon/2}} - \mathsf{negl}(n) \tag{42}$$

That is, the same $\mathcal{A}$ that successfully inverts on random images with probability at least $1 - 1/n^{2+\epsilon}$ will also invert on uniformly random values $y \leftarrow U^n$. By Lemma 2, this suffices to prove the theorem.

Remark 2. While the proof of our two lemmata are much more technically involved than the proof that follows, the above statement is the conceptual heart of our result. It is, we think, quite surprising.

Apply Lemma 1 for $\epsilon' := \epsilon/2$. In the case that (L.2) is true, (42) follows immediately from (L.2*), observing that:

$$\begin{aligned}&\left| \Pr_{\substack{s \leftarrow U^n \\ y \leftarrow f_s(U^n)}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] - \Pr_{\substack{s \leftarrow U^n \\ y \leftarrow U^n}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] \right| \\ &\leq \mathrm{SD}\Big(\big(s, f_s(U^n)\big)_{s \leftarrow U^n} \ ; \ \big(U^n, U^n\big) \Big) < \frac{2}{n^{\epsilon/4}}\end{aligned}$$

In the case that (L.1) holds, we proceed by the following series of hybrids, making use of this fact alongside the pseudo-randomness of G.

$\mathbf{H_0}$**:** This is the weak one-way function security game. By assumption (41):

$$\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow f_s(U^n)}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] > 1 - \frac{1}{n^{2+\epsilon}} \tag{43}$$

$\mathbf{H_1}$**:** For every $k \in [0, n-1]$, the pseudo-randomness of the PRG implies that U^n and $G_0(f_{U^n}(U^k))$ are computationally indistinguishable.[9] In this hybrid, we pick s from the latter distribution instead of the former, using the k guaranteed by (L.1). This loses only a negligible amount in $\mathcal{A}$'s success probability.

$$\Pr_{\substack{r \leftarrow f_{U^n}(U^k) \\ s = G_0(r) \\ y \leftarrow f_s(U^n)}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] > 1 - \frac{1}{n^{2+\epsilon}} - \mathsf{negl}(n) \tag{44}$$

$\mathbf{H_2}$**:** In this hybrid, we use (L.1*) for $\epsilon' = \epsilon/2$ to switch from picking y from $f_s(U^n)$, to instead picking y from $f_{s_1}(U^n)$, where $s_1 = G_1(r)$ is the sibling of s under G:

$$\begin{aligned}&\left| \Pr_{\substack{r \leftarrow f_{U^n}(U^k) \\ (s,s_1)=G(r) \\ y \leftarrow f_s(U^n)}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] - \Pr_{\substack{r \leftarrow f_{U^n}(U^k), \\ (s,s_1)=G(r) \\ y \leftarrow f_{s_1}(U^n)}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] \right| \\ &\leq \mathrm{SD}\Big(\big(G_0(r), f_{G_0(r)}(U^n)\big)_{r \leftarrow f_{U^n}(U^k)} \ ; \ \big(G_0(r), f_{G_1(r)}(U^n)\big)_{r \leftarrow f_{U^n}(U^k)} \Big) \\ &\leq 1 - \frac{1}{n^{2+\epsilon/2}}\end{aligned}$$

[9] See the Facts about GGM in Section 2.

Therefore, for all sufficiently large $n \in I_{\mathcal{A}}$:

$$\Pr_{\substack{r \leftarrow f_{U^n}(U^k),\\ (s,s_1)=G(r)\\ y \leftarrow f_{s_1}(U^n)}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] > \frac{1}{2n^{2+\epsilon/2}} \tag{45}$$

H₃: In this hybrid, we use the pseudo-randomness of the PRG to sample sample s and s_1 independently (s_1 is now implicit). This is computationally indistinguishable by the same reasoning as hybrid H_1. This loses at most a negligible factor in $\mathcal{A}$'s success probability:

$$\Pr_{\substack{s \leftarrow U^n\\ y \leftarrow f_{U^n}(U^n)}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] > \frac{1}{2n^{2+\epsilon/2}} - \mathsf{negl}(n) \tag{46}$$

H₄: We again use the pseudo-randomness to sample y uniformly, losing only a negligible factor in $\mathcal{A}$'s success probability, establishing (42) and the theorem:

$$\Pr_{\substack{s \leftarrow U^n\\ y \leftarrow U^n}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] > \frac{1}{2n^{2+\epsilon/2}} - \mathsf{negl}(n) \tag{47}$$

Theorem 2. *Let $\mathcal{F}_G$ be the GGM ensemble with pseudo-random generator G. $\mathcal{F}_G$ is a strongly one-way collection of functions if either of the following hold:*

(a) There exists a negligible $\mathsf{negl}(\cdot)$ *such that for all sufficiently large n*

$$\mathop{\mathbb{E}}_{s \leftarrow U^n}\left[\mathrm{SD}\big(f_s(U^n),\ U^n\big)\right] \leq \mathsf{negl}(n) \tag{48}$$

(b) There exists a polynomial B such that for all sufficiently large n and for all $s, y \in \{0,1\}^n$

$$|f_s^{-1}(y)| \leq B(n) \tag{49}$$

Proof (Theorem 2). Suppose $\mathcal{F}_G$ satisfies one of the conditions of Theorem 2. Further suppose towards contradiction that there exists a probabilistic polynomial-time $\mathcal{A}$ and a polynomial $w(\cdot)$, such that for infinitely-many $n \in \mathbb{N}$

$$\Pr_{\substack{s \leftarrow U^n\\ x \leftarrow U^n}} [\mathcal{A}(s, f_s(x)) \in f_s^{-1}(f_s(x))] \geq \frac{1}{w(n)} \tag{50}$$

By Lemma 2, to derive a condtradiction it suffices to prove for some polynomial $\alpha(\cdot)$ related to w

$$\Pr_{\substack{s \leftarrow U^n\\ y \leftarrow U^n}} [\mathcal{A}(s,y) \in f_s^{-1}(y)] > \frac{1}{\alpha(n)} \tag{51}$$

Case (a) By assumption on $\mathbb{E}_s\left[\mathrm{SD}\big(f_s(U^n),\ U^n\big)\right]$ and Equation (7)

$$\mathrm{SD}\left((s, f_s(U_n))_{U_n}, (U_n, U_n)\right) \leq \mathsf{negl}(n) \tag{52}$$

It follows immediately that (51) holds for $1/\alpha(n) = 1/w(n) - 1/\mathsf{poly}(n)$, for any polynomial poly (e.g. for $1/\alpha(n) = 1/2w(n)$).

Case (b) For this case, we use the facts about Rényi divergence from the Preliminaries and follow that notation closely. Let $P = (s, f_s(U_n))_{s \leftarrow U_n}$ and $Q = (U_{2n})$ be probability distributions over $\{0,1\}^{2n}$.

Claim. $R\,(P\|Q) \leq B(n)^2$.

Proof (Claim 5).

$$\begin{aligned}
R\,(P\|Q) &= \sum_{(s,y)\in\{0,1\}^{2n}} \frac{P(s,y)^2}{Q(s,y)} \\
&= 2^{2n} \sum_{s,y} P(s,y)^2 \\
&= 2^{2n} \sum_{s,y} \left(\Pr_P[s] \cdot \Pr_P[y|s] \right)^2 \\
&= 2^{2n} \sum_{s,y} \left(\frac{1}{2^n} \cdot \Pr_P[y|s] \right)^2 \\
&= \sum_{s,y} \Pr_P[y|s]^2 \\
&= \sum_{s,y} \left(\frac{|f_s^{-1}(y)|}{2^n} \right)^2 \\
&\leq 2^{-2n} \sum_{s,y} B(n)^2 \\
&= B(n)^2
\end{aligned}$$

Let the event $E = \left\{ (s,y) \in \{0,1\}^{2n} : \Pr_{\mathcal{A}}[\mathcal{A}(s,y) \in f_s^{-1}(y)] > \frac{1}{2w(n)} \right\}$. By an averaging argument:

$$\begin{aligned}
\frac{1}{w(n)} &< \Pr_{(s,y)\leftarrow P}[\mathcal{A}(s,y) \in f_s^{-1}(y)] \\
&= \Pr_P[\mathcal{A}(s,y) \in f_s^{-1}(y) \ \wedge \ E] \\
&\quad + \Pr_P[\mathcal{A}(s,y) \in f_s^{-1}(y) \ \wedge \ \neg E] \\
&\leq \Pr_P[E] + \Pr[\mathcal{A}(s,y) \in f_s^{-1}(y) \mid \neg E] \\
&\leq P(E) + \frac{1}{2w(n)}
\end{aligned}$$

Using (11), we get that

$$P(E) > \frac{1}{2w(n)} \quad \Longrightarrow \quad Q(E) > \frac{1}{4w(n)^2 B(n)^2} \tag{53}$$

From the definition of event E, it follows that the condition in Equation (51) holds, completing the proof:

$$\Pr_{\substack{s \leftarrow U^n \\ y \leftarrow U^n}}[\mathcal{A}(s, y) \in f_s^{-1}(y)] > \frac{Q(E)}{2w(n)} > \frac{1}{8w(n)^3 B(n)^2} \tag{54}$$

6 Conclusion

In this work, we demonstrated that the Goldreich-Goldwasser-Micali pseudorandom function family is weakly one way. This is the first demonstration that the family maintains some cryptographic hardness even when the secret key is exposed.

Open questions Two interesting open questions suggest themselves.

1. Is GGM strongly one-way for all pseudorandom generators, or does there exist a generator for which the induced GGM ensemble can be inverted some non-negligible fraction of the time? A positive answer to this question would be very interesting and improve upon this work; a negative answer would be a spiritual successor to [Gol02].
2. In the absence of a positive answer to the above, do there exist pseudorandom generators for which the induced GGM ensemble is strongly one-way? In particular, do there exist generators that satisfy the requirements of Theorem 2?

Acknowledgments We would like to thank Shafi Goldwasser, Ran Canetti, and Alon Rosen for their encouragement throughout this project. We would additionally like to thank Justin Holmgren for discussions about the proof of Lemma 1, and Krzysztof Pietrzak, Nir Bitansky, and Adam Sealfon for their helpful helpful conversations.

This work was done in part while the authors were visiting the Simons Institute for the Theory of Computing, supported by the Simons Foundation and by the DIMACS/Simons Collaboration in Cryptography through NSF grant CNS-1523467. Aloni Cohen was supported by the NSF GRFP, along with NSF MACS - CNS-1413920, DARPA IBM - W911NF-15-C-0236, and Simons Investigator Award Agreement Dated 6-5-12. Saleet Klein was supported by ISF grant 1536/14, along with ISF grant 1523/14, and the Check Point Institute for Information Security.

References

BGI14. Elette Boyle, Shafi Goldwasser, and Ioana Ivan. Functional signatures and pseudorandom functions. In *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings*, pages 501–519, 2014.

BLL^{+}15. Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: using the rényi divergence rather than the statistical distance. In *Advances in Cryptology–ASIACRYPT 2015*, pages 3–24. Springer, 2015.

BW13. Dan Boneh and Brent Waters. Constrained pseudorandom functions and their applications. In *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II*, pages 280–300, 2013.

CGH04. Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *Journal of the ACM (JACM)*, 51(4):557–594, 2004.

FN94. Amos Fiat and Moni Naor. Broadcast encryption. In *Advances in CryptologyCRYPTO93*, pages 480–491. Springer, 1994.

GGM86. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

Gol02. Oded Goldreich. The ggm construction does not yield correlation intractable function ensembles. 2002.

Gol04. Oded Goldreich. *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2004.

KPTZ13. Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos, and Thomas Zacharias. Delegatable pseudorandom functions and applications. In *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, pages 669–684, 2013.

LR88. Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.

RR97. Alexander A. Razborov and Steven Rudich. Natural proofs. *J. Comput. Syst. Sci.*, 55(1):24–35, 1997.

SW14. Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 475–484, 2014.

Val84. Leslie G Valiant. A theory of the learnable. *Communications of the ACM*, 27(11):1134–1142, 1984.

Zha12. Mark Zhandry. How to construct quantum random functions. In *Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on*, pages 679–687. IEEE, 2012.

A Appendix

Proof of (7)*:*

$$\begin{aligned}
&\mathrm{SD}\left((p, D(p))_P, (p, D'(p))_P\right) \\
&= \frac{1}{2} \sum_{(p,x)\in \mathrm{Supp}(P)\times X} \left| \Pr_{(p,D(p))_P}(p,x) - \Pr_{(p,D'(p))_P}(p,x) \right| \\
&= \sum_{p\in \mathrm{Supp}(P)} \Pr_P(p) \cdot \frac{1}{2} \sum_{x\in X} \left| \Pr_{D(p)}(x) - \Pr_{D'(p)}(x) \right| \\
&= \sum_{p\in \mathrm{Supp}(P)} \Pr_P(p) \cdot \mathrm{SD}\left(D(p), D'(p)\right) \\
&= \mathop{\mathbb{E}}_{p\leftarrow P}\left[\mathrm{SD}\left(D(p), D'(p)\right)\right]
\end{aligned}$$

Proof of (8)*:*

$$\begin{aligned}
\mathrm{SD}(f(U^n), U^n) &= \frac{1}{2} \sum_{\alpha\in\{0,1\}^n} \Big| \Pr[f(U^n)=\alpha] - \Pr[U^n=\alpha] \Big| \\
&= \frac{1}{2} \sum_{\alpha} \left| \frac{|f^{-1}(\alpha)|}{2^n} - \frac{1}{2^n} \right| \\
&= \frac{1}{2}\Big(\sum_{\alpha\in \mathsf{Img}(f)} \left| \frac{|f^{-1}(\alpha)|}{2^n} - \frac{1}{2^n} \right| + \sum_{\alpha\notin \mathsf{Img}(f)} \frac{1}{2^n} \Big) \\
&= \frac{1}{2}\Big(1 - \frac{|\mathsf{Img}(f)|}{2^n} + 1 - \frac{|\mathsf{Img}(f)|}{2^n} \Big) \\
&= 1 - \frac{|\mathsf{Img}(f)|}{2^n}
\end{aligned}$$

Proof of (32)*:* Let $\mathsf{Fat}_\theta = \mathsf{Img}(G_*) \setminus \mathsf{Thin}_\theta$.

$$\begin{aligned}
\Pr_{y\leftarrow G_U(U^n)}[y \in \mathsf{Thin}] &= \frac{|\{(b,x) \ : \ G_b(x) \in \mathsf{Thin}_\theta\}|}{2^{n+1}} && (55) \\
&\geq \frac{|\mathsf{Thin}_\theta|}{2^{n+1}} && (56) \\
&= \frac{|\mathsf{Img}(G_*)| - |\mathsf{Fat}_\theta|}{2^{n+1}} && (57) \\
&\geq \frac{|\mathsf{Img}(G_*)| - 2^{n+1}/\theta}{2^{n+1}} && (58) \\
&\geq \frac{2^n/\alpha(n) - 2^{n+1}/\theta}{2^{n+1}} && (59) \\
&= 1/2\alpha(n) - 1/\theta && (60)
\end{aligned}$$

(58) follows from (29).

(59) is by the following bound:

$$\mathop{\mathbb{E}}_{s\in\{0,1\}^n}[\frac{|\mathsf{Img}(f_s)|}{2^n}] = \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[y \in \mathsf{Img}(f_s)] \geq \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[\mathcal{A}(s,y) \in f_s^{-1}(y)] \geq \frac{1}{\alpha(n)}$$

where, the last inequality is by the hypothesis (25) of the lemma. Thus, $\exists s$ such that $\frac{2^n}{\alpha(n)} \leq |\mathsf{Img} f_s| \leq |\mathsf{Img}(G_*)|$.

Proof of (39)*:*

$$\begin{aligned}
\frac{1}{\alpha(n)} &< \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[\mathcal{A}(s,y) \in f_s^{-1}(y)] \qquad \text{by (25)}\\
&= \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[\mathcal{A}(s,y) \in f_s^{-1}(y) \ \wedge \ y \in \mathsf{Thin}_\theta]\\
&\quad + \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[\mathcal{A}(s,y) \in f_s^{-1}(y) \ \wedge \ y \notin \mathsf{Thin}_\theta]\\
&\leq \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[\mathcal{A}(s,y) \in f_s^{-1}(y) \mid y \in \mathsf{Thin}_\theta] + \Pr_{y\leftarrow U^n}[y \notin \mathsf{Thin}_\theta]\\
&\leq \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[\mathcal{A}(s,y) \in f_s^{-1}(y) \mid y \in \mathsf{Thin}_\theta] + \frac{2}{\theta} \qquad \text{by (29)}\\
\Longrightarrow \ \frac{1}{\alpha(n)} - \frac{2}{\theta} &< \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[\mathcal{A}(s,y) \in f_s^{-1}(y) \mid y \in \mathsf{Thin}_\theta]\\
&= \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[y \in \mathsf{Good}_q \mid y \in \mathsf{Thin}_\theta]\\
&\qquad \cdot \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[A(s,y) \in f_s^{-1}(y) \mid y \in \mathsf{Good}_q]\\
&\quad + \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[y \notin \mathsf{Good}_q \mid y \in \mathsf{Thin}_\theta]\\
&\qquad \cdot \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[A(s,y) \in f_s^{-1}(y) \mid y \in \mathsf{Thin}_\theta \setminus \mathsf{Good}_q]\\
&\leq \Pr_{\substack{s\leftarrow U^n\\ y\leftarrow U^n}}[y \in \mathsf{Good}_q \mid y \in \mathsf{Thin}_\theta] + q
\end{aligned}$$

The final inequality is by the definition of $\mathsf{Thin}_\theta \setminus \mathsf{Good}_q$.

Proof of Claim 5:

$$\begin{aligned}
R\left(P\|Q\right) &= \sum_{(s,y)\in\{0,1\}^{2n}} \frac{P(s,y)^2}{Q(s,y)} \\
&= 2^{2n} \sum_{s,y} P(s,y)^2 \\
&= 2^{2n} \sum_{s,y} \left(\Pr_P[s] \cdot \Pr_P[y|s] \right)^2 \\
&= \sum_{s,y} \Pr_P[y|s]^2 \\
&= \sum_{s,y} \left(\frac{|f_s^{-1}(y)|}{2^n} \right)^2 \\
&\leq 2^{-2n} \sum_{s,y} B(n)^2 \\
&= B(n)^2
\end{aligned}$$