On Derandomizing Yao's Weak-to-Strong OWF Construction

Chris Brzuska, Geoffroy Couteau, Pihla Karanko, Felix Rohrbach

On Derandomizing Yao's Weak-to-Strong OWF Construction

Chris Brzuska[1(✉)], Geoffroy Couteau[2], Pihla Karanko[1], and Felix Rohrbach[3]

[1] Aalto University, Espoo, Finland
{chris.brzuska,pihla.karanko}@aalto.fi
[2] IRIF, CNRS, Paris, France
geoffroy.couteau@ens.fr
[3] TU Darmstadt, Darmstadt, Germany
felix.rohrbach@cryptoplexity.de

Abstract. The celebrated result of Yao (Yao, FOCS'82) shows that concatenating $n \cdot p(n)$ copies of a weak one-way function (OWF) f, which can be inverted with probability $1 - \frac{1}{p(n)}$, suffices to construct a strong OWF g, showing that weak and strong OWFs are black-box equivalent. This direct product theorem for hardness amplification of OWFs has been very influential. However, the construction of Yao is not *security-preserving*, i.e., the input to g needs to be much larger than the input to f. Understanding whether a larger input is inherent is a long-standing open question.

In this work, we explore necessary features of constructions which achieve short input length by proving the following: for any *direct product* construction of a strong OWF g from a weak OWF f, which can be inverted with probability $1 - \frac{1}{p(n)}$, the input size of g must grow as $\Omega(p(n))$. By direct product construction, we refer to any construction with the following structure: the construction g executes some arbitrary pre-processing function (independent of f) on its input, obtaining a vector $(y_1, \cdots, y_l)$, and outputs $f(y_1), \cdots, f(y_l)$. Note that Yao's construction is obtained by setting the pre-processing to be the identity. Our result generalizes to functions g with post-processing, as long as the post-processing function is not too lossy. Thus, in essence, any weak-to-strong OWF hardness amplification must either (1) be very far from security-preserving, (2) use adaptivity, or (3) must be very far from a *direct-product* structure (in the sense of having a very lossy post-processing of the outputs of f).

On a technical level, we use ideas from lower bounds for secret-sharing to prove the impossibility of derandomizing Yao in a black-box way. Our results are in line with Goldreich, Impagliazzo, Levin, Venkatesan, and Zuckerman (FOCS 1990) who derandomize Yao's construction for *regular* weak OWFs by evaluating the OWF along a random walk on an expander graph—the construction is adaptive, since it alternates steps on the expander graph with evaluations of the weak OWF.

1 Introduction

In this work, we continue the study of constructions of strong one-way functions (OWFs) from weak OWFs. The classical weak-to-strong hardness amplification

K. Nissim and B. Waters (Eds.): TCC 2021, LNCS 13043, pp. 429–456, 2021.
https://doi.org/10.1007/978-3-030-90453-1_15

technique, due to Yao [40], uses direct product amplification which is not security preserving[1]. Our main result shows that the increase in the input size is inherent for *direct product* constructions. Namely, any direct product black-box construction of a strong OWF from a $(1 - 1/p(n))$-weak OWF must have input length at least $\Omega(p(n))$.

Weak and Strong OWFs. An $\alpha(n)$-secure OWF $f : \{0,1\}^n \mapsto \{0,1\}$ is an efficiently computable function such that any probabilistic polynomial-time adversaries $\mathcal{A}$ can invert f with probability at most $\alpha(n)$. When α is a negligible function, we say that f is a *strong* OWF; when $\alpha(n) = 1-1/p(n)$ for a polynomial p, we say that f is a *weak* OWF. The seminal work of Yao [40] shows that weak OWFs imply strong OWFs, via a standard *direct product* hardness amplification: given a weak OWF f, define $g(x_1, ..., x_l) = f(x_1)||...||f(x_l)$. Then, Yao proved that g is a strong OWF for $l > |x_i|\, p(|x_i|)$.

Adaptive vs. Non-adaptive Construction. In this paper we study *non-adaptive* weak-to-strong OWF constructions, that is, constructions where the calls to the weak OWF can be made in parallel. I.e., a strong OWF construction g that makes calls to a weak OWF f is called *non-adaptive* if g's calls to f only depend on g's input, but not on the output of f on any of these inputs. Yao's construction is a simple, non-adaptive construction where each call to f is an independent chunk of the input. In general, non-adaptive constructions can make correlated calls to f though.

We say that a construction is *adaptive*, if the output of (at least) one call to f is used to determine the input to another f call. That is, adaptive constructions cannot compute all calls to f in parallel. For the toy constructions on the right, g_1 is non-adaptive (it does not matter whether g_1 computes $f(x)$ or $f(x+1)$ first) and g_2 is adaptive (g_2 must make the inner f call first).

$$g_1(x) := f(x)||f(x+1)$$
$$g_2(x) := f(f(x))$$

On the (in)efficiency of Yao's Construction. The construction of Yao is generic: it turns an *arbitrary* weak OWF f into a strong OWF g and just depends on the hardness of f. In addition, g has an appealing simple direct-product structure. In turn, g is suboptimal w.r.t. its computational complexity:

1. g makes a *large number of calls* to the underlying weak OWF, and
2. g is *not security preserving*, in that the input length of g is polynomially larger than the input length of f.

Many celebrated cryptographic reductions are similarly not security-preserving and have a high number of calls—the HILL construction of pseudorandom generator from any OWF being perhaps one of the most well-known examples [14].

[1] In a security-preserving construction, the input length of the strong OWF is linear in that of the weak OWF.

In beautiful works, a decade ago, Haitner, Reingold, Vadhan and Zheng [13,36] developed rich tools for computational entropy, and improved the original n^8 seed length by HILL to $\mathcal{O}(n^3)$, where n is the input length of the OWF—since further improvements seem extremely hard to obtain, it is natural to ask whether large lower bounds on the input size are inherent.

In a seminal result [19], Impagliazzo and Rudich [19] formalize the notions of *black-box* constructions/reductions, and develop methods to establish their limitations. Informally, a (fully) black-box construction of a primitive C from a primitive P treats both P and any adversary $\mathcal{A}$ against P in a black-box way. Following this breakthrough result, a long line of work (see [6,8,9,23,24, 26,27,38]) has been devoted to proving limitations on the *efficiency* of black-box reductions. Our work continues this successful line of work.

To our knowledge, three previous works study black-box limitations on the efficiency of Yao's construction. Lin, Trevisan, and Wee [24] address the first of the two limitations above: they show that any fully black-box construction of an $\varepsilon(n)$-secure OWF from a $(1-\delta(n))$-secure OWF f must make at least $q = \Omega((1/\delta)\cdot\log(1/\varepsilon))$ calls to f. They also show that fully black-box construction cannot be perfectly security-preserving: if f has input size n, the input size of the strong OWF must be at least $n+\Omega(\log 1/\varepsilon)-O(\log q)$. The work of [26] showed that *non-adaptive* fully black-box construction (i.e., a construction where all the calls to f are made in parallel) cannot amplify security beyond $\mathsf{poly}(n)$ if the algorithm implementing the reduction has constant depth, and its size is below $2^{\mathsf{poly}(n)}$. Eventually, the work of [27] extended the results of [24] to the weakly black-box setting with bounded non-uniformity.

1.1 On Security-Preserving Amplification of Weak OWFs

The above result leaves open one of the most intriguing limitations of Yao's construction: the fact that it causes a polynomial blowup in the input size. While [24] shows that *some* blowup in the input size is available, it leaves a huge gap: starting with a $(1-1/p(n))$-secure OWF f with input length n, Yao's construction requires an input size $n^2\cdot p(n)$ to build *any* strong OWF, while the result of [24] only shows that to build an *extremely strong* OWF, say a $2^{-\mu\cdot n}$-secure OWF (for some constant μ), one needs input size at least $(1+\mu)\cdot n-\log p$.

In a sense, the proof of [24] cannot do much better, because it also applies to the setting of *regular* one-way functions (where outputs have the same number of preimages), and rules out even *adaptive* fully black-box reductions. However, in this setting, it is actually known that we can do much better than Yao's construction and obtain an almost security-preserving construction, if we start from a regular weak OWF, and use adaptivity. Indeed, the work of [10] provides precisely such a construction, using random walks on expander graphs.

This leaves us in between two extremes: on the one hand, Yao's construction is non-adaptive (hence optimally parallelizable: if one starts with a parallelizable weak OWF, one ends up with a parallelizable strong OWF), extremely simple (it has a straightforward direct product structure) and works for arbitrary OWFs; however, it is not security-preserving. On the other hand, the construction of Goldreich, Impagliazzo, Levin, Venkatesan, and Zuckerman [10] is almost

security-preserving, but is considerably more involved, requires adaptive calls, and works only for regular OWFs. Improving this state of affair is a long-standing and intriguing open problem.

1.2 Our Contribution

In this work, we make progress on this problem. Specifically, we show that any relativizing *direct product* black-box construction of strong OWF from a $(1 - 1/p(n))$-secure OWF cannot be security preserving, in a strong sense: it requires an input length of at least $\Omega(p(n))$. While this still leaves a gap with respect to Yao's construction, which has input length $O(n^2 \cdot p(n))$, this gap vanishes asymptotically when p grows. By *direct product* construction, we mean a construction g of strong OWF with the following structure: on input x, $g(x)$ outputs $(f(y_1), \cdots, f(y_\ell))$, where f is the weak OWF, and $(y_1, \cdots, y_\ell)$ are computed from x arbitrarily, but without calling f (we call the mapping from x to $(y_1, \cdots, y_\ell)$ the *pre-processing*). This is a natural generalization of *Yao-style* constructions of strong OWFs (we recover Yao's construction by letting the pre-processing be the identity function). Furthermore, our result generalizes to the setting where some post-processing (independent of f) is applied to the outputs $(f(y_1), \cdots, f(y_\ell))$, whenever this post-processing is *not too lossy*: we prove that whenever each output of the post-processing has at most polynomially many preimages, the same $\Omega(p(n))$ input length bound holds. We summarize the results in the following informal theorem:

Theorem 1. *Let f be a $(1 - 1/p(n))$-secure OWF (a weak OWF). Let g be any non-adaptive construction, with not-too-compressing post-processing, of input length $< cp(n)$, for certain constant c. Then, it is impossible to prove, in a relativizing fully black-box way, that g is a strong OWF.*

Observe that if we could generalize our result to arbitrary (f-independent) post-processing functions, the above would capture all non-adaptive constructions. Hence, in essence, our result says the following: any (fully black-box) construction of strong OWF from a weak OWF must either (1) be very far from security preserving, or (2) use adaptivity, or (3) compute a highly non-injective function of the outputs of the non-adaptive calls (i.e., be very far from a "direct product" structure).

1.3 Relation to Correlated-Product and Correlated-Input Security

Usually, parallel concatenation of cryptographic primitives on *independent* inputs preserves security. For example, if f and g are one-way functions, then so is $(x_1, x_2) \mapsto (f(x_1), g(x_2))$. However, things might potentially change radically when x_1 and x_2 are not sampled independently, but are instead *correlated*, e.g., sampled jointly from a high min-entropy source. Variants of this problem have been studied on many occasions in cryptography, and have profound connections to the feasibility of cryptography with weak sources of randomness,

leakage-resilient cryptography, related-key attacks, or deterministic encryption (to name a few); see e.g. [39] for discussions on cryptography with correlated sources. In addition, security for correlated inputs has proven to be a very useful assumption by itself: one-wayness under correlated product (i.e., one-wayness of $f(x_1), \cdots, f(x_k)$ for $(x_1, \cdots, x_k)$ sampled from a joint distribution) has been used to build CCA secure cryptosystems [16,30], and correlated-input secure hash functions have found numerous applications such as OT extension [22], trapdoor hash function [7], constrained pseudorandom functions [1], password-based login [12], and many more.

A general and natural question to ask is: which type of constructions *preserve* hardness, when the inputs are jointly sampled from a high min-entropy source, rather than being sampled independently? This is a fundamental question in itself, because this setting occurs in real-life use of standard cryptographic construction (when they are misused, when the source of randomness is imperfect, or when the adversary has access to some leakage on the inputs), but also due to the many applications outlined above.

It is well-known that not all constructions will preserve security under correlated inputs. For example, even though the map $x \mapsto x^e \bmod n$ is believed to be one-way when n is a product of two large safe primes (this is the RSA assumption), the extended euclidean algorithm provides an efficient inverter for the map $x \mapsto (x^{e_1}, x^{e_2}) \bmod n$ whenever $\gcd(e_1, e_2) = 1$ (this example is taken from [16]). Hence, there are specific functions f_i (here, $f_i : x \mapsto x^{e_i}$) and specific correlations of the inputs (here, the equality correlation: the same input x is used for all functions) such that correlated-product security breaks down. However, this leaves open the possibility that some specific input correlations preserve correlated-product security (for example, this is the case when the correlated-inputs are indistinguishable from random, e.g. when sampled as the output of a PRG), or that some specific functions maintain correlated-product security for general correlations.

Our results can be cast in the context of correlated-product security: we show that even though Yao's construction of OWF, which is a very natural and seminal construction, is provably secure (with a black-box proof) when used with random and independent inputs, it breaks down for *any possible correlated source*, whenever the entropy of the source is below $p(n)$. This provides a natural example of a construction, from a weak OWF f, where correlated-product security cannot be generically shown to hold (in a black-box way) for *arbitrary* sources, unless they contain enough entropy such that all of the correlated inputs can have independent entropy. In contrast, [30] shows that when f is instantiated as a *lossy trapdoor function*, then $f(x_1), \cdots, f(x_k)$ is one-way for correlated inputs $(x_1, \cdots, x_k)$, and [16] shows that assuming OWFs, there *exists* a correlated-product secure function. Our results provide a partial complementary perspective to this line of work.

Comparison to [39]. Wichs [39] also studies, among other questions, the one-wayness of constructions of the form $(f(x_1), \cdots, f(x_k))$ for inputs $(x_1, \cdots, x_k)$ sampled from a correlated source. Our results are incomparable: we show that

for a *generic weak OWF* f, and for any *fixed* distribution over the inputs $(x_1, \cdots, x_k)$ with $o(k)$ bits of entropy, the one-wayness of $f(x_1), \cdots, f(x_k)$ does not follow from that of f in a black-box way. In contrast, [39] shows that for an *arbitrary function* f, there is no black-box reduction (to any standard hardness assumption) of one-wayness of $(f(x_1), \cdots, f(x_k))$ when the x_i can come from *arbitrarily correlated distributions*, even with high per-input entropy. That is, [39] handles a considerably larger class of constructions and reductions to many possible assumptions, but only rules out a much more stringent security notion (where one-wayness must hold even when the input distributions are not fixed a priori and can be correlated arbitrarily).

1.4 Related Works

We already pointed out to numerous related works on bounding the efficiency of black-box reductions [6,8,9,23,24,26,27,38], including some specifically targeting hardness amplifications of one-way functions, and related works on correlated-product security. Besides, our black-box separations use some established tools (in addition to key new technical insights, which we cover afterwards) such as the two-oracle technique of [17,32] where one oracle implements the base primitive and the second oracle breaks all constructions built from this primitive. We use Borel-Cantelli style technique from [28] to extract a single oracle from a distribution of random oracles analogously to the seminal work on black-box separations by Impagliazzo and Rudich [19].

Hardness amplification of functions, via direct products and related constructions, have a rich and dense history, which goes well beyond one-way functions and is too vast to be covered here. In particular, amplifying the hardness of *computing* boolean functions (rather than inverting functions) using direct product constructions is at the heart of rich lines of work on worst-case to average-case reductions, constructions of non-cryptographic pseudorandom generators, circuit lower bounds, and many more – see e.g. [2,3,11,15,18,21,25,31,33–35,37] and references therein.

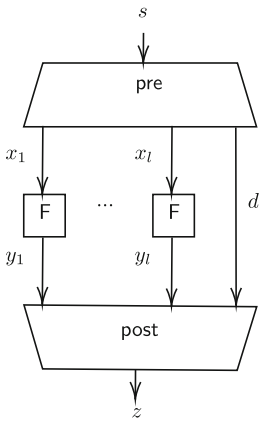
1.5 Technical Overview

To prove our black-box separations, we exhibit an oracle relative to which there is a weak one-way function, yet all strong one-way functions with an appropriate structure can be inverted efficiently with constant probability. The standard method to do so is to design oracles relative to which the starting primitive (here, the weak one-way function) clearly exists and is the *only possible source of hardness*. For example, in the seminal work by Impagliazzo and Rudich (IR) on the separation of key exchange from OWFs [20], IR introduce a random oracle, which is a strong OWF with high probability, as well as assuming $\mathsf{P} = \mathsf{NP}$, thereby ruling out most other (stronger) cryptographic primitives. In our setting, we instantiate this intuition by choosing three oracles:

(1) A PSPACE oracle, which *destroys* all possible sources of hardness,

(2) a random oracle F, which instantiates the weak OWF, and
(3) an inverter INV, which inverts F on a (roughly) $1-1/p$ fraction of its inputs, effectively turning it into a weak OWF. Note that a random oracle F alone would already be a strong OWF, if we did not weaken it by adding INV.

In this oracle world, we consider *non-adaptive* constructions of strong OWFs g from the weak OWF F. Since we wish to rule out (relativizing) *fully black-box* reductions (as defined by Reingold, Trevisan and Vadhan [29]), we do not give g access to INV. In fact, this is inherent in our setting: observe that given access to INV, it is not too hard to build a strong OWF (e.g. the strong OWF can perform a random walk starting from the input x, until it lands on a hard input y – which can be tested using INV – and outputs $\mathsf{F}(y)$). In general, whenever one can efficiently test which inputs are hard, constructing a security-preserving OWF becomes feasible – and it is precisely the lack of any such tester that makes it highly nontrivial to improve over Yao's seminal construction. Since we rule out fully black-box reductions, we do not let g access INV and thus, g does not know where the easy inputs are.



$g(\mathrm{s})$

$x_1, ..., x_l, d \leftarrow \mathsf{pre}(s)$
for $i = 1..l$
  $y_i \leftarrow \mathsf{F}(x_i)$
$z \leftarrow \mathsf{post}(y_1, ..., y_l, d)$
return z

Fig. 1. (n, m)-non-adaptive construction. F is the weak OWF. Length of d can be arbitrary, $|x_i| = |y_i| = m$ and $|s| = n$.

Modeling Non-adaptive Constructions. Non-adaptive construction can be thought of as a circuit which first has a pre-processing layer, followed by a layer of parallel calls to a weak OWFs and then some post-processing, see Fig. 1. When the construction omits the post-processing layer, as in Yao's construction, this corresponds to a *direct product* construction. The input size n of the construction might be different from the input size m of the weak OWF. As a starting point, we consider what happens when the construction does not use any post-processing, as is the case in Yao's construction. When there is no post-processing, the additional data d in Fig. 1 only reduces the input domain and does not add any security. Thus, w.l.o.g., we assume that there is no d.

Inverting Direct Product Constructions. Considering the simple case with no post-processing and no d, the first observation is that g must make more than $p(m)$ calls to the weak OWF, since otherwise *all* the calls will be easy to invert with constant probability. In that case the adversary could simply invert all the weak OWF calls and then use PSPACE to invert the pre-processing layer, thus inverting g with constant probability.

Now that g makes at least $p(m)$ calls to the weak OWF, we can make the main observation of the paper: if we can invert a $1-1/p(m)$ fraction of the weak

OWF calls and n is slightly smaller than $p(m)$, then the remaining entropy of the input s cannot be very high, on the average. This is formalized in Lemma 21. This is because the number of calls to the weak OWF is at least the same order of magnitude as the length of the input to the strong OWF. Hence, there is not enough entropy in the strong OWF input to distribute among all the weak OWF calls, so most of the calls will end up having very little entropy of their own, i.e. entropy that is not shared with other calls.

Now the probability that an adversary can indeed invert a $1-1/p(m)$ fraction of the weak OWF calls is high, since that is the expected fraction of easy calls. Since the entropy of the input s is low, given the easy calls, and the adversary has the PSPACE oracle, the adversary can guess s with high probability. Note that low entropy alone is not enough to guess s, since inverting pre-processing might be inefficient, hence we also need PSPACE.

To summarize, we know that there must be many calls to the underlying weak one-way function—and since we can also show that each of them must have a non-trivial amount of entropy (i.e., information about the input)—we can show that we can invert all non-adaptive constructions without post-processing, unless n is larger than a small constant times $p(m)$, establishing the first lower bound on the randomness efficiency of non-adaptive constructions. Note that Yao's construction consumes $n = m^2 p(m)$ many bits.

On Strong OWFs with Injectiveish Post-processing. We sketched above why constructions without post-processing (direct product constructions) cannot be strongly one-way. It is relatively easy to extend the above argument to constructions with *not too lossy* post-processing, i.e., constructions where any output of the post-processing has at most polynomially many preimages: the inverter chooses a uniformly random value amongst the (polynomial size) list of all possible preimages of the post-processing, and applies the previous inversion attack on the candidate. It then succeeds with probability $\frac{1}{\mathsf{poly}}$ times the success probability of the previous attack.

1.6 Relation to Threshold Secret Sharing

The pre-processing pre in Fig. 1 is conceptually similar to a threshold secret sharing scheme, where the participants' shares correspond to the values x_i and the secret together with the dealer's randomness corresponds to the strong OWF input s. On average, we learn the 'shares' of all but a $\frac{1}{p(m)}$ fraction of the 'participants'. So effectively, we are interested in how long the secret and the dealer's randomness together must be in a $(1-\frac{1}{p(m)}+\epsilon)$-threshold secret sharing scheme. The difference is that we allow a negligible failing probability for the secret sharing scheme and we do not distinguish which part of the input is the secret and which part of the input is the randomness of dealer in the secret sharing scheme.

To make the intuition concrete, our result can be formulated as a result on the threshold achievable by any *deterministic* threshold secret sharing schemes with short secret.

Definition 2 (Deterministic Threshold Secret Sharing Scheme). *We say that function* $S : \{0,1\}^n \to (\{0,1\}^m)^l$ *(i.e. S outputs l bitstrings of length m) is* (l,t)-deterministic threshold secret sharing scheme *if for all adversaries* $\mathcal{A}$*:*

$$\Pr_{\pi \leftarrow\$ \text{ permutations of } (1,\ldots,l), x \leftarrow\$ \{0,1\}^n}\left[x \leftarrow\$ \mathcal{A}(S(x)_{\pi(1)}, ..., S(x)_{\pi(t)})\right] \leq negl(n),$$

where $S(x)_i$ *denotes the* i*th share, i.e., the* i*th length* n *bitstring of the output of* S*. The secret length* n *should be polynomial in the share length* m *(hence, negligible in* n *is also negligible in* m*).*

Note that any threshold secret sharing scheme can be made deterministic by considering the randomness as part of the secret – but then the randomness must be counted towards the secret length. The fact that Definition 2 uses probability over permutations of the shares only makes the definition cover a larger class of schemes, in particular, a scheme that is secure for all permutations is also secure by Definition 2.

Also, notice that Definition 2 relies on a very weak hiding notion: no subset of size less than t should be able to *fully recover* the secret (except with negligible probability). This sets our result apart from most known bounds on secret sharing, which apply to the indistinguishability setting.

In this language, our result states the following: let m be the share length and p be any polynomial. Consider any candidate (l,t)-threshold deterministic secret sharing scheme with $t \geq (1 - 1/p(m)) \cdot l$, now the scheme must have secret size $n > p(m)/c$, for a certain constant. For traditional (l,t)-threshold secret sharing schemes, this means that the combined length of the secret and the randomness used by the scheme must be $> p(m)/c$, if $t \geq (1 - 1/p(m)) \cdot l$. Naturally, in order to this result being meaningful, the number of shares l should be bigger than the polynomial $p(m)$.

The result follows from our main conceptual Lemma 21, which effectively states that the expected entropy of the remaining shares, when you know $(1 - 1/p(m))$ fraction of the shares, is small. Hence, the remaining shares can be guessed with non-negligible probability.

Our result stays the same even if we change Definition 2 to cover only *efficient*, i.e. probabilistic polynomial time, adversaries $\mathcal{A}$, provided that the scheme S is such that you can compute the secret in polynomial time, when you know *all* the shares. That is, we even rule out computational security if $t \geq (1 - 1/p(m)) \cdot l$ and $n < p(m)/c$.

More precisely, let us change the Definition 2 to a definition that covers an even larger class of schemes (the difference to Definition 2 is high-lighted in pink) and subsequently state our result in the secret-sharing terminology.

Definition 3 (Computational Deterministic Threshold Secret Sharing Scheme). *A function* $S : \{0,1\}^n \to (\{0,1\}^m)^l$ *(i.e. S outputs l bitstrings of length m) is* (l,t)-computational deterministic threshold secret sharing scheme *if for all probabilistic polynomial time adversaries* $\mathcal{A}$*:*

$$\Pr_{\pi \leftarrow\$ \text{ permutations of } (1,\ldots,l), x \leftarrow\$ \{0,1\}^n}\left[x \leftarrow\$ \mathcal{A}(S(x)_{\pi(1)}, ..., S(x)_{\pi(t)})\right] \leq negl(n),$$

where $S(x)_i$ denotes the ith share, i.e., the ith length n bitstring of the output of S. The secret length n should be polynomial in the share length m. The function S^{-1} should be computable in polynomial time.

Theorem 4 (Threshold Secret Sharing View). *Fix a large enough m and a polynomial p. Consider a computational deterministic threshold secret sharing scheme where*

- *the dealer has an n bits secret;*
- *there are l participants, each getting a share of length m;*
- *the threshold t satisfies $t \geq (1 - \frac{1}{p(m)})l$.*

Then the secret must be long: $n > \frac{1}{c}p(m)$, where c is some constant.

Blundo, Santis, Vaccaro [5] discuss the minimum amount of randomness needed by an information theoretically secure secret sharing scheme. They prove that if the secret length is m and there are l participants, then the dealer needs to use $l \cdot m$ bits of randomness (to choose both the secret and the participants' shares). This is the same as the analogous number in Yao's weak to strong OWF construction (when number of weak OWF calls is $l > mp(m)$, we use lm input length) and it is close to the analogous number that we get in this paper (input length to strong OWF needs to be $\mathcal{O}(p(m))$, i.e. there is m^2 gap between our result and Yao's).

It is intuitive that some gap should exist between the information theoretically secure secret sharing scheme and our more relaxed "mostly secure secret sharing scheme", where the adversary is allowed to learn part of the secret as long as they cannot learn the whole input and additionally, the adversary is only allowed to run in polynomial time. However, the two secret sharing schemes are not really comparable (because we do not distinguish between randomness and secret) and a better lower bound, than what we present, might be possible.

2 Preliminaries

Definition 5 (One-Way Functions). *Let $f : \{0,1\}^* \to \{0,1\}^*$ be a polynomial-time computable function. f is called a* (strong) *one-way function (OWF), if for every probabilistic polynomial-time algorithm $\mathcal{A}$ there exists a negligible function $\epsilon : \mathbb{N} \to [0,1]$ such that for every n,*

$$\Pr_{\mathcal{A},x\leftarrow\{0,1\}^n}\left[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))\right] \leq \epsilon(n).$$

Further, f is called a weak *one-way function, if there exists a polynomial $p(n)$ such that for every probabilistic polynomial-time algorithm $\mathcal{A}$ there exists a $N_0 \in \mathbb{N}$ such that for all $n \geq N_0$:*

$$\Pr_{\mathcal{A},x\leftarrow\{0,1\}^n}\left[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))\right] \leq 1 - \frac{1}{p(n)}.$$

*In this case we sometimes say that f is a p-*weak *OWF.*

Definition 6 (Oracle Algorithms). *The complexity of an oracle algorithm (e.g., Turing Machine) is the number of steps it makes, where an oracle query is counted as one step.*

In particular, a probabilistic polynomial-time (PPT) oracle algorithm makes at most polynomial queries. Since our oracle algorithms have access to a PSPACE oracles, we usually limit the discussion to the number of oracle calls the algorithm makes.

We use the following Borel-Cantelli style theorem from [28, Lemma 2.9].

Theorem 7 *Let $(E_1, E_2, ...)$ be a sequence of events such that $\exists c \forall m \in \mathbb{N} : \Pr[E_m] \geq c$, where c is a constant strictly between 0 and 1. Then,*

$$\Pr\left[\bigwedge_{k=1}^{\infty} \bigvee_{m>k} E_m\right] \geq c \tag{1}$$

2.1 Entropy Toolbox

Throughout this paper, the term *entropy* refers to *Shannon entropy* which satisfies a *chain rule*.

Definition 8 (Shannon Entropy). *Let X be a random variable and let $\mathsf{dom}(X)$ be its domain, then*

$$H(X) := -\sum_{z \in \mathsf{dom}(X)} \Pr[X = z] \cdot \log_2(\Pr[X = z]),$$

is the Shannon entropy *of X.*

Lemma 9 (Chain Rule for Entropy). *Let $X_1, \ldots, X_n$ be random variables. Then the following holds*

$$H(X_1, \ldots, X_n) = H(X_1) + H(X_2|X_1) + \cdots + H(X_n|X_1, \ldots, X_{n-1}).$$

We use also other simple but useful properties of entropy. In particular, Definition 8 implies that entropy is non-negative. Also, the entropy $H(X)$ of a random variable X is always more or equal to the entropy $H(f(X))$ of the random variable $f(X)$ for any deterministic function f—if f is injective, the entropy is preserved, if f is not injective, it decreases. Finally, for any three random variables X, Y, Z, we have that $H(X|Y) \geq H(X|Y, Z)$, i.e., conditioning on additional information maintains or decreases the entropy of a random variable.

3 Main Results

In this section, we introduce different types of constructions of strong OWF from weak OWF which we study in this paper (Sect. 3.1) and state our main theorems (Sect. 3.2). In particular, we introduce non-adaptive constructions, non-adaptive constructions without post-processing and non-adaptive constructions with injective*ish* post-processing.

3.1 Black-Box Constructions and Reductions

Definition 10 (Non-adaptive). *A construction* $g = (\mathsf{pre}, \mathsf{post})$ *from a weak one-way function* F *is non-adaptive, if it computes its output as* $\mathsf{post}(\mathsf{F}(\mathsf{pre}(s)))$ *(see Fig. 1). The number of queries* l *is induced by* pre*.* (n, m)*-NA denotes a non-adaptive construction with input length* n *based on a weak OWF* F *whose input length is* m*.*

Definition 11 (Non-adaptive, no post-processing construction). *We say that a construction* $g = (\mathsf{pre}, \mathsf{post})$ *is a* (n, m)*-NANPP, if it is* (n, m)*-NA and the post-processing function is the identity function, i.e.,* $\mathsf{post}(y_1, ..., y_l, d) := y_1||..||y_l||d$*.*

Definition 12 (Non-adaptive, injective*ish* post-processing constr). *We say that a construction* $g = (\mathsf{pre}, \mathsf{post})$ *is a* (n, m)*-NAIPP, if it is* (n, m)*-NA and the post-processing function is almost injective, that is, every image of* post *has at most a polynomial (in* n*) number of preimages.*

Note that the identity function is injective and thus, in particular, is injective*ish*. Therefore, every NANPP is also a NAIPP, but the converse does not hold. Likewise, both NANPP and NAIPP are NA constructions, but the converse does not hold. Since we are interested in ruling out negative results, whenever we rule out NAIPP, we also rule out NANPP.

We formalized the kind of constructions our negative results capture, and now specify which type of reduction proofs our theorems rule out. Namely, our results concern BBB-style proofs following the notation of [4] or fully black-box proofs following the notation of [29]. Since we consider parametrized definitions, we here state a customized version of fully black-box security which precisely captures the quantifiers our negative results capture.

Definition 13 (Fully Black-Box Proof). *We say that a proof that weak OWF implies strong OWF is* fully black-box *if it establishes a* relativizing *statement of the following type:*

$$\forall \textit{poly } p, \exists \textit{ poly-time computable } g, \forall \textit{poly } q, \exists PPT\, \mathcal{R}\, \forall p\textit{-weak OWF } \mathsf{F}, \mathcal{A}:$$
$$\textit{if } \Pr_{x \leftarrow\$ \{0,1\}^n}\left[g^{\mathsf{F}}(\mathcal{A}(1^n, g^{\mathsf{F}}(x))) = g^{\mathsf{F}}(x)\right] > \tfrac{1}{q(n)} \textit{ for inf. many } n \in \mathbb{N}$$
$$\textit{then } \Pr_{x \leftarrow\$ \{0,1\}^n}\left[\mathsf{F}(\mathcal{R}^{\mathcal{A},\mathsf{F}}(1^n, \mathsf{F}(x))) = \mathsf{F}(x)\right] > 1 - \tfrac{1}{p}(n) \textit{ for inf. many } n \in \mathbb{N}.$$

In this case, we also refer to the construction g *as fully black-box.*

Note that typically, in the definition of fully black-box, the pink parts are omitted. That is, the polynomial p is considered as part of the definition of F and the polynomial q is considered as part of the definition of $\mathcal{A}$ (i.e. the adversary's success probability). We allow the construction g to depend on the polynomial p and the reduction $\mathcal{R}$ to depend on q, since we seek to cover a larger and meaningful class of proofs. In particular, Yao's original proof building strong OWFs from weak OWFs is fully black-box in the sense of Definition 13, but would not be covered if the construction were now allowed to depend on p or if the reduction were not allowed to depend on q.

3.2 Theorems

We now state our main theorems, all of which rely on the two-oracle technique. Namely, we construct a distribution over oracles $(\mathcal{O}_1, \mathcal{O}_2)$ such that $\mathcal{O}_1$ will be a weak one-way function and $\mathcal{O}_2$ will help to invert the strong one-way function. Since we rule out black-box reductions rather than provide an oracle separation, only the reduction has access to the oracle $\mathcal{O}_2$ while the construction does not (cf. Section 1.5). Note that in Corollary 16, we extract a single oracle from the oracle distribution, using the Borel-Cantelli style argument Theorem 7. However, we prefer to state our theorem in terms of oracle distributions since this more closely matches the technical core arguments of our separation results.

Theorem 14 (NANPP Impossibility). *$\exists$ constant $\mathbf{c}$ such that $\forall$poly p, $\forall(n,m)$-NANPP g with input length $n \leq \frac{1}{\mathbf{c}}p(m)$, $\exists$ poly-query $\mathcal{A}$, $\exists$poly $q(n) = n^c, c \in \mathbb{N}_+$, $\forall$PPT $\mathcal{R}$, $\exists$ distribution $\mathcal{D}$ over pairs of oracles $(\mathcal{O}_1, \mathcal{O}_2)$:*

$$\Pr_{(\mathcal{O}_1,\mathcal{O}_2) \leftarrow\$ \mathcal{D}}\left[\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}\right] = \text{constant} < 1$$

where $\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}$ is an indicator variable that is 1 iff at least one of the following is true:

1. *Weak OWF breaks:*
   $\Pr_{x \leftarrow\$ \{0,1\}^m, \mathcal{R}}\left[\mathcal{R}^{\mathcal{A}^{\mathcal{O}_1,\mathcal{O}_2},\mathcal{O}_1,\mathcal{O}_2}(1^m, \mathcal{O}_1(x)) \in \mathcal{O}_1^{-1}(\mathcal{O}_1(x))\right] \geq 1 - \frac{1}{p(m)}$.
2. *Strong OWF is secure-ish:*
   $\Pr_{s \leftarrow\$ \{0,1\}^n, \mathcal{A}}\left[\mathcal{A}^{\mathcal{O}_1,\mathcal{O}_2}(1^n, g^{\mathcal{O}_1}(s)) \in (g^{\mathcal{O}_1})^{-1}(g^{\mathcal{O}_1}(s))\right] \leq \frac{1}{q(n)}$.

We emphasize that in the definition of the bad event, the oracles are *fixed* and the randomness is taken only over the sampling of x as well as the internal randomness of $\mathcal{A}$ and $\mathcal{R}$, respectively.

Theorem 15 (NAIPP Impossibility). *$\exists$ constant $\mathbf{c}$ $\forall$poly p, $\forall(n,m)$-NAIPP g with input length $n \leq \frac{1}{\mathbf{c}}p(m)$, $\exists$ poly-query $\mathcal{A}$, $\exists$poly $q(n) = n^c, c \in \mathbb{N}_+$, $\forall$PPT $\mathcal{R}$, $\exists$ distribution $\mathcal{D}$ over pairs of oracles $(\mathcal{O}_1, \mathcal{O}_2)$:*

$$\Pr_{(\mathcal{O}_1,\mathcal{O}_2) \leftarrow\$ \mathcal{D}}\left[\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}\right] = \text{constant} < 1$$

where $\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}$ is the same indicator variable as in Theorem 14.

We use the same oracle distribution for Theorem 15 and Theorem 14, see Sect. 4. Theorem 15 implies Theorem 14, so it would suffice to prove Theorem 15. However, we found the presentation to be easier to follow when presenting the proof of the weaker Theorem 14 first (Sect. 5.2) and then discussing the generalization to the proof of Theorem 15 (Sect. 6). For both theorems, we prove that relative to $\mathcal{O}_1, \mathcal{O}_2$, oracle $\mathcal{O}_1$ is a weak OWF. Before proving the theorems for oracle distributions, we now use the strengthened Borel-Cantelli lemma by Mahmoody, Mohammed, Nematihaji, Pass and Shelat [28] to extract a single oracle from the distribution where the bad event happens with *constant* probability, as opposed to less than $1/m^2$ required by standard Borel-Cantelli.

Corollary 16 (Main). *There is no fully black-box (n, m)-NAIPP construction of a OWF from a $p(m)$-weak OWF with $n \leq \frac{1}{\mathbf{c}} p(m)$, where $\mathbf{c}$ is some constant.*

Proof. Recall that a black-box proof means the following:

$$\begin{aligned}
&\forall \text{poly } p, \exists \text{ poly-time computable } g, \forall \text{poly } q, \exists \text{PPT } \mathcal{R}\, \forall p\text{-weak OWF } \mathsf{F}, \mathcal{A}: \\
&(\mathcal{A} \text{ inverts } g) \Rightarrow (\mathcal{R}^{\mathcal{A}} \text{ inverts } \mathsf{F}) \text{ Formally:} \\
&\quad \left(\Pr_{x \leftarrow\!\$ \{0,1\}^n}\left[g^{\mathsf{F}}(\mathcal{A}(1^n, g^{\mathsf{F}}(x))) = g^{\mathsf{F}}(x)\right] > \tfrac{1}{q(n)} \text{ for inf. many } n \in \mathbb{N}\right) \\
&\Rightarrow \left(\Pr_{x \leftarrow\!\$ \{0,1\}^n}\left[\mathsf{F}(\mathcal{R}^{\mathcal{A},\mathsf{F}}(1^n, \mathsf{F}(x))) = \mathsf{F}(x)\right] > 1 - \tfrac{1}{p}(n) \text{ for inf. many } n \in \mathbb{N}\right)
\end{aligned}$$

In order to rule out a black-box proof, we thus define an oracle $\mathcal{O}_1$ (and an oracle $\mathcal{O}_2$ helping the adversary) such that the following holds:

$$\begin{aligned}
&\forall \text{poly } p, \forall \text{ poly-time } g^{\mathcal{O}_1}, \exists \text{poly } q, \forall \text{PPT } \mathcal{R}^{\mathcal{O}_1,\mathcal{O}_2}\, \exists \mathcal{A}^{\mathcal{O}_1,\mathcal{O}_2}, \exists \mathcal{O}_1, \mathcal{O}_2: \\
&\mathcal{A} \text{ breaks } g_1^{\mathcal{O}}, \text{ but } \mathcal{R} \text{ does not } p\text{-invert } \mathcal{O}_1. \text{ Formally:} \\
&\Pr_{x \leftarrow\!\$ \{0,1\}^n}\left[g^{\mathcal{O}_1}(\mathcal{A}^{\mathcal{O}_1,\mathcal{O}_2}(1^n, g^{\mathcal{O}_1}(x))) = g^{\mathcal{O}_1}(x)\right] > \tfrac{1}{q(n)} \text{ for inf. many } n \in \mathbb{N}. \\
&\Pr_{x \leftarrow\!\$ \{0,1\}^n}\left[\mathcal{O}_1(\mathcal{R}^{\mathcal{A},\mathcal{O}_1,\mathcal{O}_2}(1^n, \mathcal{O}_1(x))) = \mathcal{O}_1(x)\right] < 1 - \tfrac{1}{p}(n) \\
&\qquad\qquad \text{for all but finitely many } n \in \mathbb{N}.
\end{aligned}$$

In order to rule out a fully black-box reduction, we would only need to show that statement with the pink universal quantifier being replaced by existential quantifier. However, proving the statement for all polynomials p is stronger without making the proof more complicated. Now, let us fix a polynomial p, a candidate NAIPP g, a polynomial q (s.t. it satisfies Theorem 15) and a candidate reduction $\mathcal{R}$ and show the existence of an adversary and a p-weak OWF F.

By Theorem 15, there is an oracle distribution over pairs $(\mathcal{O}_1, \mathcal{O}_2)$, and an adversary $\mathcal{A}$ such that the probability of the bad event $\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}$ is constant in m. We show that there exists a *fixed* oracle pair $(\mathcal{O}_1, \mathcal{O}_2)$ for which the bad event $\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}$ in Theorem 15 happens only for finitely many m. From that it follows that there is a fixed oracle pair for which $\mathcal{A}^{\mathcal{O}_1,\mathcal{O}_2}$ breaks the candidate strong OWF $g^{\mathcal{O}_1}$ infinitely many often, but the reduction $\mathcal{R}^{\mathcal{A}^{\mathcal{O}_1,\mathcal{O}_2}}$ inverts the weak OWF $\mathcal{O}_1$ well enough at most on finitely many m. Thus, it suffices to show via Theorem 7, that Theorem 15 implies that there is an oracle relative to which $\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}$ happens only for finitely many m.

By Theorem 15, we have

$$\Pr_{(\mathcal{O}_1,\mathcal{O}_2) \leftarrow\!\$ \mathcal{D}}\left[\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}\right] = \mathsf{constant} < 1.$$

Hence, the constant probability version of Borel-Cantelli (Theorem 7) yields

$$\Pr_{(\mathcal{O}_1,\mathcal{O}_2) \leftarrow\!\$ \mathcal{D}}\left[\bigwedge_{m=1}^{\infty} \bigvee_{m>k} \mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}\right] = \mathsf{constant} < 1,$$

which means that, with constant probability, there is a k for which no $m > k$ satisfies $\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}$. Taking such an oracle pair $(\mathcal{O}_1, \mathcal{O}_2)$ concludes the proof of Corollary 16. □

4 Oracle Distributions

In this section, we define the oracle (distribution)s we rely on. Firstly, a PSPACE creates a world where no one-way functions exist. Then, we add an oracle (distribution) F in order to create a world where weak one-way functions exist, and finally, we add an oracle (distribution) $\mathcal{O}_2$ which breaks NANPP and NAIPP constructions. The adversary will have access to $\mathcal{O}_2$, PSPACE and F while the candidate strong OWF construction only has access to PSPACE and F, but not to $\mathcal{O}_2$. We recall from Sect. 1.5 that it is *necessary* to not give the construction access to the information which parts of F are easy and which parts are hard, and not giving the construction access to $\mathcal{O}_2$ is related to this necessary restriction, since the adversary (modeled by $\mathcal{O}_2$) uses the information of which parts are easy. On a technical-conceptual level, it is meaningful to not give the construction access to the adversary (modeled by $\mathcal{O}_2$), since the adversary is *inefficient*, while the construction is efficient (in this (oracle) world where all algorithms have access to PSPACE and F). We consider an inefficient adversary since we rule out black-box reduction which work for *any* black-box adversary that breaks the strong OWF, including inefficient ones.

As mentioned before, we denote our adversary by $\mathcal{O}_2$. We encode the pair of oracles PSPACE and F into a single oracle $\mathcal{O}_1$ so that we are aligned with the terminology of a two-oracle separation result (and this is also convenient notation in the proof).

Definition 17 (Oracle Distributions). *Let* $\mathbf{p}$ *be any fixed polynomial. The oracle distribution* $D_{\mathbf{p}}$ *over oracles* $\mathcal{O}_1$ *and* $\mathcal{O}_2$ *samples permutations* Π_m *of the elements in* $\{0,1\}^m$ *for every* $m \in \mathbb{N}$ *and a random subset* $\mathsf{EASY}^m_{\mathsf{in}}$ *of* $\{0,1\}^m$ *s.t.* $|\mathsf{EASY}^m_{\mathsf{in}}| = \lceil (1-1/\mathbf{p}(m))2^m \rceil$. *We define*

$$\mathcal{O}_1 := (\mathsf{PSPACE}, \mathsf{F}) \text{ and } \mathcal{O}_2 := \mathsf{INV},$$

where F *and* INV *behave as follows:*

$\mathsf{F}(x)$	$\mathsf{INV}(y)$
$m \leftarrow \lvert x \rvert$	$m \leftarrow \lvert y \rvert$
$y \leftarrow \Pi_m(x)$	**if** $y \in \mathsf{EASY}^m_{\mathsf{out}}$
return y	**return** $\mathsf{F}^{-1}(y)$
	else return $\perp$

Here, we use $\mathsf{EASY}^m_{\mathsf{out}} := \Pi_m(\mathsf{EASY}^m_{\mathsf{in}})$.

Remark. Throughout this paper we treat $(1-1/\mathbf{p}(m))2^m$ as an integer, omitting the ceil function since the difference is negligible and does not affect our proofs.

5 Proof of Theorem 14

We split the proof of Theorem 14 into two parts. We first show that the probability of Case 1 (weak OWF breaks) of the bad event introduced in Theorem 14 is smaller than any constant (Sect. 5.1), and then we show that the probability of Case 2 (strong OWF is secure-ish) of the bad event introduced in Theorem 14 is a small constant (Sect. 5.2). Recall that both probabilities are (only) over the sampling of the oracles $\mathcal{O}_1$ and $\mathcal{O}_2$.

5.1 $\mathcal{R}^{\mathcal{A}}$ is Not a Successful Weak OWF Inverter

In this section, we show that the probability (over the oracle distributions) that F is not a $2\mathbf{cp}(m)$-weak OWF is small.

Theorem 18 (F is Weak OWF). *For all constants* $\mathbf{c}$*, for all polynomials* $\mathbf{p}$*, for all poly-query* $\mathcal{A}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}$*, for all adversaries* $\mathcal{R}$ *making polynomially many (in* m*) queries to the oracles* $\mathsf{F}, \mathsf{PSPACE}, \mathsf{INV}, \mathcal{A}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}$*,*

$$\Pr_{\mathsf{F},\mathsf{PSPACE},\mathsf{INV} \leftarrow\$ D_{\mathbf{p}}}\left[\mathsf{SuccInv}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}_{\mathcal{A},\mathcal{R}} \geq 1 - \frac{1}{2\mathbf{cp}(m)}\right] \leq 1/\mathbf{c}$$

where $\mathsf{SuccInv}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}_{\mathcal{A},\mathcal{R}}$ *is defined as*

$$\Pr_{x \leftarrow\$ \{0,1\}^m,\mathcal{R}}\left[\mathcal{R}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV},\mathcal{A}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}}(1^m, \mathsf{F}(x)) \in \mathsf{F}^{-1}(\mathsf{F}(x))\right].$$

When we define $\mathbf{p}(m) := \frac{1}{2\mathbf{c}}p(m)$*, the above is equivalent to*

$$\Pr_{(\mathcal{O}_1,\mathcal{O}_2) \leftarrow\$ \mathcal{D}}\left[\textit{Case 1 of } \mathsf{Bad}^{\mathcal{R},\mathcal{A},g}_m\right] \leq 1/\mathbf{c},$$

where $\mathcal{D} := D_{\mathbf{p}}$*,* $\mathcal{O}_1 := \mathsf{F}, \mathsf{PSPACE}$*,* $\mathcal{O}_2 := \mathsf{INV}$ *and* $\mathsf{Bad}^{\mathcal{R},\mathcal{A},g}_m$ *is defined as in Theorem 14.*

We prove Theorem 18 in Appendix B.

5.2 $\mathcal{A}$ is a Successful Strong OWF Inverter

We prove that an adversary with access to the oracles F, INV and PSPACE (cf. Sect. 4), can break all short input NANPP constructions which have access to F and PSPACE only.

Theorem 19 (Inverting OWF Candidate). *$\forall$ poly* $\mathbf{p}$*, $\forall(n,m)$-NANPP* g *with input length* $n \leq \frac{1}{4}\mathbf{p}(m)$*, $\exists$ poly-query* $\mathcal{A}^{\mathsf{F},\mathsf{INV},\mathsf{PSPACE}}$*, $\exists$constant* $c > 0$ *s. t.*

$$\Pr_{(\mathsf{F},\mathsf{INV}) \leftarrow\$ D_{\mathbf{p}}}\left[\Pr_{s,\ \textit{coins of } \mathcal{A}}\left[\mathcal{A}^{\mathsf{F},\mathsf{INV},\mathsf{PSPACE}} \textit{ inverts } g(s)\right] \leq c\right] = \mathsf{constant} < 1$$

This implies that

$$\Pr_{(\mathcal{O}_1,\mathcal{O}_2) \leftarrow\$ \mathcal{D}}\left[\textit{Case 2 of } \mathsf{Bad}^{\mathcal{R},\mathcal{A},g}_m\right] = \mathsf{constant} < 1$$

where $\mathcal{D} := D_{\mathbf{p}}$*,* $\mathcal{O}_1 := \mathsf{F}, \mathsf{PSPACE}$*,* $\mathcal{O}_2 := \mathsf{INV}$ *and* $\mathsf{Bad}^{\mathcal{R},\mathcal{A},g}_m$ *is defined as in Theorem 14.*

For the proof of Theorem 19, let $\mathbf{p}(m)$ be a fixed polynomial. We start by showing that Theorem 19 holds for constructions which make few queries. More precisely, we show that no matter what the input length to g is, g must make at least $l > c\mathbf{p}(m)$ calls to F, otherwise all the F calls are easy with constant probability, which makes inverting g trivial.

Proposition 20 (Easy inversion if few F-Calls). *Consider a NANPP* $g = (\mathsf{pre}, \mathsf{post})$ *(where we recall that* $\mathsf{post}(y_1, .., y_l, d) = y_1||..||y_l||d$*). For all constants* c*, if* $\mathsf{pre}(s) = (x_1, .., x_l, d)$ *induces at most* $l \leq c\mathbf{p}(m)$ *(parallel) calls to* F*, then all* $y_i := \mathsf{F}(x_i)$ *are in* $\mathsf{EASY}^m_{\mathsf{out}}$ *with constant probability, more precisely*

$$\Pr_{\mathsf{F} \leftarrow\$ D_{\mathbf{p}}}[\Pr_s[\forall y_i \in g(s) : y_i \in \mathsf{EASY}^m_{\mathsf{out}}] > constant > 0] > constant > 0 \quad (2)$$

In particular, with constant probability over the choice of the oracle F*,* g *can be inverted with non-negligible (constant) probability by a poly-query adversary.*

Proof. Suppose there are $l \leq c\mathbf{p}(m)$ parallel calls to F. Denote by $y_1, ..., y_l$ the outputs of the parallel calls to F. Now, when considering the randomness of choosing $\mathsf{EASY}^m_{\mathsf{in}}$, we have

$$\begin{aligned}
&\Pr_{\mathsf{F} \leftarrow\$ D_{\mathbf{p}}, s}[y_1, ..., y_l \in \mathsf{EASY}^m_{\mathsf{out}}] \\
&\geq \underbrace{\sum_s 2^{-|s|}}_{=1} \Pr_{\mathsf{F} \leftarrow\$ D_{\mathbf{p}}}[y_1 \in \mathsf{EASY}^m_{\mathsf{out}} \mid s] \cdot ... \cdot \Pr_{\mathsf{F} \leftarrow\$ D_{\mathbf{p}}}[y_l \in \mathsf{EASY}^m_{\mathsf{out}} \mid s] \\
&= \left(1 - \frac{1}{\mathbf{p}(m)}\right)^l \geq \left(1 - \frac{1}{\mathbf{p}(m)}\right)^{c\mathbf{p}(m)} \geq \left(\frac{1}{4}\right)^c \quad \forall\, \mathbf{p}(m) > 2.
\end{aligned}$$

where the first inequality is an equality iff $y_i \neq y_j \forall i \neq j$ and the second inequality follows since $(1 - \frac{1}{x})^x$ converges monotonously to $\frac{1}{e}$ and is greater than $\frac{1}{4}$ whenever $x \geq 2$. Now since $\left(\frac{1}{4}\right)^c$ is constant, we can use a simple averaging argument (see Appendix A, Lemma 23) to prove (2).

In the case where all $y_1, ..., y_l$ are all easy, $\mathcal{A}$ can invert $y_1, ..., y_l$ using INV oracle. Note that there is only a single pre-image x_i per y_i and thus, given the list $x_1, ..., x_l$, $\mathcal{A}$ can use the PSPACE oracle to find an s such that $\mathsf{pre}(s) = x_1, ..., x_l$. □

Due to Proposition 20, for the remainder of this section, we can focus on constructions where pre makes more than $c \cdot \mathbf{p}(m)$ calls. Also in the case where g makes many queries, we can always invert the easy fraction of $(y_1, .., y_l)$. However, if many queries are made, then (with high probability) some y_i will also be hard. Of course, if pre-processing $\mathsf{pre}(s) = (x_1, .., x_l)$ distributes the entropy well, then knowing some of the x_i might suffice to restrict the set of suitable candidate values s to a polynomial-sized set, and once a polynomial-sized set of candidates is obtained, a random candidate s is a suitable pre-image with high enough probability. How well does this strategy work when considering *arbitrary* pre-processing pre?

To analyze this strategy, we study the entropy of the hard values x_i given $(1 - \frac{1}{\mathbf{p}(m)})l$ many easy values x_i (note that in expectation, $(1 - \frac{1}{\mathbf{p}(m)})l$ many values are easy) and seek to prove that their entropy is low. Towards that goal, we fix a permutation π and look at the entropy of the $\frac{1}{\mathbf{p}(m)}l$ many first x_i under that permutation:

$$h(\pi) := H(X_{\pi(1)}, \ldots, X_{\pi(\frac{l}{\mathbf{p}(m)})} | X_{\pi(\frac{l}{\mathbf{p}(m)}+1)}, \ldots, X_{\pi(l)}),$$

where X_i is the random variable defined as follows: sample a uniformly random s from $\{0,1\}^n$, compute $\mathsf{pre}(s)$ and take the ith output (i.e. the input to the ith F-call in g).

First, in Lemma 21 (Small Entropy Expectation), we show that the expectation of entropy $h(\pi)$ is small in our case. This is our main conceptual lemma.

Lemma 21 (Small Entropy Expectation). *Suppose* $\mathbf{p}(m)$ *divides* l*. Then,*

$$\mathbb{E}_{\pi \in \Pi(l)}[h(\pi)] \leq \frac{n}{\mathbf{p}(m)},$$

which is equivalent to

$$\mathbb{E}_{\pi \in \Pi(l)}\left[H(X_{\pi(1)}, \ldots, X_{\pi(\frac{l}{\mathbf{p}(m)})} | X_{\pi(\frac{l}{\mathbf{p}(m)}+1)}, \ldots, X_{\pi(l)})\right] \leq \frac{n}{\mathbf{p}(m)}. \quad (3)$$

Proof. Let's consider a permutation π of the weak OWF inputs $x_{\pi(1)}, ..., x_{\pi(l)}$. Let's divide the inputs x_i into $\mathbf{p}(m)$ equal-sized blocks as follows:

$$\left(x_{\pi(1)}, ..., x_{\pi(l/\mathbf{p}(m))}, \underbrace{x_{\pi(l/\mathbf{p}(m)+1)}, ..., x_{\pi(2l/\mathbf{p}(m))}}_{\text{one block}}, x_{\pi(2l/\mathbf{p}(m)+1)}, ..., x_{\pi(l)}\right).$$

Each pink index starts a new block. Let's denote the set of the pink indices by $J := \{1, l/\mathbf{p}(m) + 1, 2l/\mathbf{p}(m) + 1, ..., (\mathbf{p}(m) - 1)l/\mathbf{p}(m) + 1\}$. Now consider the following sum

$$\sum_{j \in J} \mathbb{E}_{\pi \in \Pi(l)}\left[H\left(\underbrace{X_{\pi(j)}, \ldots, X_{\pi(j+\frac{l}{\mathbf{p}(m)}-1)}}_{\text{one block}} | \underbrace{X_{\pi(j+\frac{l}{\mathbf{p}(m)})}, \ldots, X_{\pi(l)}}_{\text{all } X_i \text{ after the block}}\right)\right] \quad (4)$$

$$= \mathbb{E}_{\pi \in \Pi(l)}\left[\sum_{j \in J} H\left(X_{\pi(j)}, \ldots, X_{\pi(j+\frac{l}{\mathbf{p}(m)}-1)} | X_{\pi(j+\frac{l}{\mathbf{p}(m)})}, \ldots, X_{\pi(l)}\right)\right] \quad (5)$$

$$= \mathbb{E}_{\pi \in \Pi(l)}\left[H\left(X_{\pi(1)}, \ldots, X_{\pi(l)}\right)\right] \quad (6)$$

$$\leq \mathbb{E}_{\pi \in \Pi(l)}\left[H\left(S\right)\right] \quad (7)$$

$$= n \quad (8)$$

where (5) holds by linearity of expectation and (6) holds by Lemma 9 (Chain Rule for Entropy). The inequality (7) is equality iff the pre-processing is injective (entropy of a random variable cannot increase when it is passed through a deterministic function). The equality (8) follows from the fact that $H(S) = |s| = n$.

Now, from (4), we have that n is greater or equal to

$$\sum_{j\in J} \mathbb{E}_{\pi\in\Pi(l)} \left[H\left(X_{\pi(j)}, .., X_{\pi\left(j+\frac{l}{\mathbf{p}(m)}-1\right)} | X_{\pi\left(j+\frac{l}{\mathbf{p}(m)}\right)}, .., X_l \right) \right] \tag{9}$$

$$\geq \sum_{j\in J} \mathbb{E}_{\pi\in\Pi(l)} \left[H\left(X_{\pi(j)}, .., X_{\pi\left(j+\frac{l}{\mathbf{p}(m)}-1\right)} | X_{\pi(i)}, i = 1, .., j-1, j+\frac{l}{\mathbf{p}(m)}, .., l \right) \right] \tag{10}$$

$$= \sum_{j\in J} \mathbb{E}_{\pi'\in\Pi(l)} \left[H\left(X_{\pi'(1)}, .., X_{\pi'\left(\frac{l}{\mathbf{p}(m)}\right)} | X_{\pi'\left(\frac{l}{\mathbf{p}(m)}+1\right)}, .., X_{\pi'(l)} \right) \right] \tag{11}$$

$$= \mathbf{p}(m)\, \mathbb{E}_{\pi'\in\Pi(l)} \left[H\left(X_{\pi'(1)}, .., X_{\pi'\left(\frac{l}{\mathbf{p}(m)}\right)} | X_{\pi'\left(\frac{l}{\mathbf{p}(m)}+1\right)}, .., X_{\pi'(l)} \right) \right] \tag{12}$$

where (10) follows from the general property of entropy: $\forall A, B, C : H(A|B) \geq H(A|B, C)$, i.e. conditioning the entropy on more random variables can only decrease the entropy. In this case, we condition additionally on all X_i for $i < \pi(j)$ and not only on those for $i \geq \pi(j + \frac{l}{\mathbf{p}(m)})$. At (11) we change to a more convenient indexing where we choose permutation $\pi'(1) = \pi(j)$,...,$\pi'(\frac{l}{\mathbf{p}(m)}) = \pi(j + \frac{l}{\mathbf{p}(m)} - 1)$. Now, consider any of the summands, i.e. the expectation for some fixed j. Now for that j, π' still goes through all possible permutations (like π did in (10)). At (12) we notice that the summands do not depend on j and recall that $|J| = \mathbf{p}(m)$. Dividing by $\mathbf{p}(m)$ proves the Lemma 21. □

With Lemma 21 as a tool, we can now prove Theorem 19. Note that, interestingly, the result of Theorem 19, does not depend on the number of calls to F in the strong OWF construction g. That is, if the input length of the construction g is too short, then no number of calls to F can make it a strong OWF.

$\mathcal{A}(y_1||...||y_l||d)$

for $i \in 1, ..., l$

  $x_i \leftarrow \mathsf{INV}(y_i)$

$s \leftarrow\!\!\$\ \mathsf{pre}^{-1}(x_1, ..., x_l, d)$

return s

Proof of Theorem 19. Let g be a (n, m)-NANPP g with input length $n \leq \frac{1}{4}\mathbf{p}(m)$ and let l be the number of queries to F which g makes. The adversary $\mathcal{A}$ (described on the right) now tries to invert all y_1,..,y_l using INV and put $\perp$ when inversion fails. $\mathcal{A}$ then computes a random pre-image of the pre-processing that matches the known x_is and d which is possible in polynomial-time when using the PSPACE oracle. We now argue that a random pre-image of the pre-processing,

that matches the known x_is and d, is an actual preimage of $y_1||...||y_l||d$ under g with constant probability.

W.l.o.g., we assume that $|d| = 0$. This is because the data d is known to the adversary, so it cannot add entropy. From now on, we assume that there is no d. Further and also w.l.o.g., we assume that $\mathbf{p}(m)$ divides l for all m, n (if there was some remainder, we could add constant dummy F-calls until there is no remainder. Such F-calls would not make g weaker nor stronger, so our result would still hold.) Note that if $l \leq \mathbf{p}(m)$, then with constant probability all x_i are easy and INV inverts all of them (cf. Theorem 20). In that case $\mathcal{A}$ can use PSPACE oracle to find a correct preimage s with probability 1. Hence, we can assume that $l > \mathbf{p}(m)$.

First, in Lemma 21 (Small Entropy Expectation) establishes that the expectation of entropy $h(\pi)$ is small. Namely, since Theorem 19 assumes that $\mathbf{p}(m) > 4n$, we have

$$\mathbb{E}_{\pi \leftarrow\$ \Pi(l)}[h(\pi)] \leq \frac{n}{\mathbf{p}(m)} < \frac{1}{4}.$$

Since the expectation of the entropy over π is small, an averaging argument (cf. Lemma 24 (Small Entropy w.h.p.) in Appendix A) yields that for at least half of the permutations, the entropy is small, i.e.,

$$\Pr_{\pi \in \Pi(l)}\left[h(\pi) < \frac{2n}{\mathbf{p}(m)}\right] \geq \frac{1}{2}. \tag{13}$$

We call a π such that $h(\pi) < \frac{2n}{\mathbf{p}(m)}$ *good*. If π is good, then the remaining entropy of the input is small and thus, some inputs are very likely (cf. Lemma 25 (Predictable Inputs) in Appendix A) and thus likely chosen by adversary $\mathcal{A}$ which chooses a random pre-image amongst the possible candidates.

With this high level intuition of the proof in mind, we can now lower-bound the probability of $\mathcal{A}$'s success.

$$\begin{aligned}
&\Pr_{\mathsf{F},s}[\mathcal{A} \text{ inverts } g(s)] \\
&\geq \Pr_{\mathsf{F}}\left[\exists \pi : x_{\pi(1)}, ..., x_{\pi\left(\left(1-\frac{1}{\mathbf{p}(m)}\right)l\right)} \in \mathsf{EASY}^m_{\mathsf{in}}\right] \\
&\quad \cdot \Pr_s\left[\mathcal{A} \text{ inverts } g(s) \;\middle|\; \exists \pi : x_{\pi(1)}, ..., x_{\pi\left(\left(1-\frac{1}{\mathbf{p}(m)}\right)l\right)} \in \mathsf{EASY}^m_{\mathsf{in}}\right] \\
&\geq \frac{1}{2} \Pr_s\left[\mathcal{A} \text{ inverts } g(s) \;\middle|\; \exists \pi : x_{\pi(1)}, ..., x_{\pi\left(\left(1-\frac{1}{\mathbf{p}(m)}\right)l\right)} \in \mathsf{EASY}^m_{\mathsf{in}}\right]
\end{aligned} \tag{14}$$

$$\geq \frac{1}{2}\Pr_s\left[\underbrace{\mathrm{H}\left(X_{\pi(1)},\ldots,X_{\pi\left(\frac{l}{\mathbf{p}(m)}\right)}\;\middle|\;X_{\pi\left(\frac{l}{\mathbf{p}(m)}+1\right)},\ldots,X_{\pi(l)}\right)<\frac{2n}{\mathbf{p}(m)}}_{=:C}\right]\cdot \tag{15}$$

$$\Pr_s\left[\Pr_{s'}\left[\begin{matrix}\forall k & \in\\ \pi(1),\ldots,\pi(l/\mathbf{p}(m)),\\ X_k=\mathsf{pre}(s')_k\end{matrix}\;\middle|\;\begin{matrix}\forall j & \in\\ \pi(l/\mathbf{p}(m)+1),\ldots,\pi(l),\\ X_j=\mathsf{pre}(s)_j\end{matrix}\right]>\frac{1}{4}\mid C\right]\cdot \tag{16}$$

$$\Pr_s\left[\mathcal{A}\text{ inverts }g(s)\;\middle|\;\Pr_{s'}\left[\begin{matrix}\forall k & \in\\ \pi(1),\ldots,\pi(l/\mathbf{p}(m)),\\ X_k=\mathsf{pre}(s')_k\end{matrix}\;\middle|\;\begin{matrix}\forall j & \in\\ \pi(l/\mathbf{p}(m)+1),\ldots,\pi(l),\\ X_j=\mathsf{pre}(s)_j\end{matrix}\right]>\frac{1}{4}\;\wedge\;C\right] \tag{17}$$

$$\geq \frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{1}{4}=\text{constant} \tag{18}$$

where (14) follows from the fact that whether x_i is easy or not follows binomial distribution with $(1-\frac{1}{\mathbf{p}(m)})l$ many easy values in expectation. Inequality (15) uses chain rule of probability. The fractions at (18) follow from the lemmas, namely, the probability on line (15) is less than 1/2 by Lemma 21 (Small Entropy Expectation) and probability on line (16) is less than 3/4 by Lemma 25 (Predictable Inputs). The last fraction follows from the definition of adversary $\mathcal{A}$ and the probability statement at (17). Namely, if adversary guesses a random s which is consistent with the known x_i, and we condition the probability on such s being correct 1/4 of the time, adversary must be right 1/4 of the time.

Now that we know that

$$\Pr_{\mathsf{F},s}[\mathcal{A}\text{ inverts }g(s)]\geq\text{const}>0,$$

we can use a simple averaging argument (see Appendix A, Lemma 23) to show that $\Pr_{\mathsf{F}}[\Pr_s[\mathcal{A}\text{ inverts }g(s)]>\text{const}>0]\geq\text{const}>0$ which proves Theorem 19. □

Theorem 14 follows from the Theorems 19 and 18 by union bound, namely

$$\begin{aligned}\Pr_{(\mathcal{O}_1,\mathcal{O}_2)\leftarrow\$\,\mathcal{D}}\left[\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}\right]&=\Pr\left[\text{Case 1 of }\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}\text{ or Case 2 of }\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}\right]\\&\leq 1/\mathbf{c}+\text{constant from Theorem 19}<1\end{aligned}$$

Note that since the constant $\mathbf{c}$ in Theorem 18 can be made arbitrarily large, in particular, it can be chosen s.t. $1/\mathbf{c}+\text{constant from Theorem 19}$ is <1.

6 Constructions with Post-processing

In this section, we prove Theorem 15. Towards this goal, we use the oracles F,INV and PSPACE (cf. Sect. 4), and show that there are no short input NAIPP constructions under the oracles.

Theorem 22 (No Strong OWFs with Injectiveish Post-Processing). $\forall$ *poly* $\mathbf{p}$, $\forall(n,m)$*-NAIPP* g *with input length* $n \leq \frac{1}{4}\mathbf{p}(m)$, $\exists$*poly* $q(n) = n^c, c \in \mathbb{N}_+$, $\exists$ *poly-query* $\mathcal{A}^{\mathsf{F},\mathsf{INV},\mathsf{PSPACE}}$ *such that*

$$\Pr_{(\mathsf{F},\mathsf{INV}) \leftarrow\!\$\, D_{\mathbf{p}}}\left[\Pr_{s,\ coins\ of\ \mathcal{A}}\left[\mathcal{A}^{\mathsf{F},\mathsf{INV},\mathsf{PSPACE}}\ inverts\ g(s)\right] \leq q(n)\right] = \mathsf{constant} < 1$$

$$and\ thus\ \Pr_{(\mathcal{O}_1,\mathcal{O}_2) \leftarrow\!\$\, \mathcal{D}}\left[Case\ 2\ of\ \mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}\right] = \mathsf{constant} < 1$$

where $\mathsf{Bad}_m^{\mathcal{R},\mathcal{A},g}$ *is defined as in Theorem 15.*

Theorems 18 and 22 together imply Theorem 15 by union bound analogously to the NANPP case. It thus remains to prove Theorem 22.

$\mathcal{A}(z)$

$y_1, ..., y_l, d \leftarrow \mathsf{post}^{-1}(z)$

for $i \in 1, ..., l$

  $x_i \leftarrow \mathsf{INV}(y_i)$

$s \leftarrow\!\$\, \mathsf{pre}^{-1}(x_1, ..., x_l, d)$

return s

Proof. Let g be (n,m)-NAIPP which makes l queries to F and let $\mathcal{A}$ be the adversary on the right which samples a uniformly random pre-image of z under post, then inverts the easy queries and returns a seed s which is consistent with the pre-image of the easy values. Firstly observe that $\mathcal{A}$ runs in polynomial-time since it can use the PSPACE oracle for inverting post. Moreover, it makes only a polynomial number of queries since l is a polynomial.

As the post-processing of g is almost injective, $y_1, ..., y_l, d \leftarrow\!\$\, \mathsf{post}^{-1}(z)$ returns the values $y_1, ..., y_l, d$ which the one-wayness experiment used to compute z with probability $\frac{1}{\mathsf{poly}(n)}$. This probability is independent of F. If $y_1, ..., y_l, d$ are indeed the correct values, then adversary $\mathcal{A}$ also finds a pre-image s with constant probability by the same arguments as in Theorem 19. Thus, the overall success of $\mathcal{A}$ is $\frac{1}{\mathsf{poly}(n)} \cdot \mathsf{constant}$ which is inverse polynomial as required by Theorem 22. □

Acknowledgments. We thank the anonymous reviewers for valuable comments. Parts of this work have been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) - SFB 1119 - 236615297 and by the Academy of Finland.

A Additional Lemmas and Proofs

Lemma 23 (Averaging Argument). *Let* A_n *and* B_n *be probability distributions that depend on natural number* n *(e.g. uniform distribution over* $\{0,1\}^n$*). For convenience, we write* $A := A_n, B := B_n$*. Let* $E(\cdot,\cdot)$ *be any event.*

If $\Pr_{a \leftarrow\!\$\, A, b \leftarrow\!\$\, B}[E(a,b)] \geq c$*, where* $c > 0$ *constant, then there exist constants* $d, d' > 0$ *s.t.* $\Pr_{a \leftarrow\!\$\, A}[\Pr_{b \leftarrow\!\$\, B}[E(a,b)] \geq d] \geq d'$.

The proof is standard, we defer it to the full version.

Lemma 24 (Small Entropy w.h.p.). *If* $\mathbb{E}_{\pi\in\Pi(l)}[h(\pi)] \le \frac{n}{\mathbf{p}(m)}$ *then*

$$\Pr_{\pi\in\Pi(l)}\left[h(\pi) < \frac{2n}{\mathbf{p}}\right] \ge 1/2,$$

where $h(\pi) = \mathrm{H}\left(X_{\pi(1)},\ldots,X_{\pi\left(\frac{l}{\mathbf{p}(m)}\right)} \;\middle|\; X_{\pi\left(\frac{l}{\mathbf{p}(m)}+1\right)},\ldots,X_{\pi(l)}\right)$.

The proof is a direct application of Markov bound, we defer it to the full version.

Lemma 25 (Predictable Inputs). *If*

$$\mathrm{H}\left(X_{\pi(1)},\ldots,X_{\pi\left(\frac{l}{\mathbf{p}(m)}\right)} \;\middle|\; X_{\pi\left(\frac{l}{\mathbf{p}(m)}+1\right)},\ldots,X_{\pi(l)}\right) < \frac{2n}{\mathbf{p}(m)}$$

then

$$\Pr_{s'}\left[\Pr_s\left[X_k=\mathsf{pre}(s)_k\,\forall k\in\pi(1),\ldots,\pi\left(\tfrac{l}{\mathbf{p}(m)}\right) \mid X_j=\mathsf{pre}(s')_j\,\forall j\in\pi\left(\tfrac{l}{\mathbf{p}(m)}+1\right),\ldots,\pi(l)\right]>\tfrac{1}{4}\right] \ge \frac{3}{4}$$

Proof. Since $4n < \mathbf{p}(m)$, we get that

$$\mathrm{H}\left(X_{\pi(1)},\ldots,X_{\pi\left(\frac{l}{\mathbf{p}(m)}\right)} \;\middle|\; X_{\pi\left(\frac{l}{\mathbf{p}(m)}+1\right)},\ldots,X_{\pi(l)}\right) < \frac{2n}{\mathbf{p}(m)} < \frac{1}{2} \tag{19}$$

Let $S_{h,e} \subseteq \{0,1\}^m$ be defined as

$$S_{h,e} = \{s' : \Pr_s[P_h = p_h(s') \mid P_e = p_e(s')] < \frac{1}{4}\},$$

where we define $\Pr_s[P_h = p_h(s') \mid P_e = p_e(s')]$ below. Using (19) and the definition of conditional Shannon entropy, we get that

$$\begin{aligned}
\frac{1}{2} &> \mathrm{H}\left(\underbrace{X_{\pi(1)},\ldots,X_{\pi\left(\frac{l}{\mathbf{p}(m)}\right)}}_{=:P_h} \;\middle|\; \underbrace{X_{\pi\left(\frac{l}{\mathbf{p}(m)}+1\right)},\ldots,X_{\pi(l)}}_{=:P_e}\right) \\
&= \sum_{s'\in\{0,1\}^m} \Pr_s\left[P_h = p_h(s') \textbf{ and } P_e = p_e(s')\right] \cdot \left|\log \Pr_s\left[P_h = p_h(s') \mid P_e = p_e(s')\right]\right| \\
&= \sum_{s'\in S_{h,e}} \Pr_s\left[P_h = p_h(s') \textbf{ and } P_e = p_e(s')\right] \cdot \left|\log \Pr_s\left[P_h = p_h(s') \mid P_e = p_e(s')\right]\right| \\
&\quad + \sum_{s'\notin S_{h,e}} \Pr_s\left[P_h = p_h(s') \textbf{ and } P_e = p_e(s')\right] \cdot \left|\log \Pr_s\left[P_h = p_h(s') \mid P_e = p_e(s')\right]\right| \\
&\ge \left(\sum_{s'\in S_{h,e}} \Pr_s\left[P_h = p_h(s') \textbf{ and } P_e = p_e(s')\right]\right) \cdot \left|\log \frac{1}{4}\right| \\
&\quad + \left(\sum_{s'\notin S_{h,e}} \Pr_s\left[P_h = p_h(s') \textbf{ and } P_e = p_e(s')\right]\right) \cdot |\log 1| \\
&\ge \Pr_{s'}\left[\Pr_s\left[P_h = p_h(s') \mid P_e = p_e(s')\right] < \frac{1}{4}\right] \cdot 2 + 0
\end{aligned}$$

where log is the base-2 logarithm and

$$p_e(s') := \mathsf{pre}(s')_{\pi\left(\frac{l}{\mathbf{p}(m)}+1\right)}, ..., \mathsf{pre}(s')_{\pi(l)}$$

and

$$p_h(s') := \mathsf{pre}(s')_{\pi(1)}, \ldots, \mathsf{pre}(s')_{\pi\left(\frac{l}{\mathbf{p}(m)}\right)}.$$

Now

$$\begin{aligned}
& \frac{1}{2} \geq \Pr_{s'}\left[\Pr_s[P_h = p_h(s') \mid P_e = p_e(s')] < \frac{1}{4}\right] \cdot 2 \\
\Leftrightarrow \quad & \frac{1}{4} \geq \Pr_{s'}\left[\Pr_s[P_h = p_h(s') \mid P_e = p_e(s')] < \frac{1}{4}\right] \\
\Rightarrow & \Pr_{s'}\left[\Pr_s[P_h = p_h(s') \mid P_e = p_e(s')] \geq \frac{1}{4}\right] \\
& = 1 - \Pr_{s'}\left[\Pr_s[P_h = p_h(s') \mid P_e = p_e(s')] < \frac{1}{4}\right] \\
& > 1 - \frac{1}{4} = \frac{3}{4}
\end{aligned}$$

which proves the statement. □

B Proof of Theorem 18 (F is a weak OWF)

In order to prove Theorem 18, we need to show that F is weak OWF with inversion probability $1 - 1/2\mathbf{cp}(m)$ with all but small constant probability. Namely, we need to show that for all polynomials $\mathbf{p}$, for all poly-query $\mathcal{A}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}$, for all adversaries $\mathcal{R}$ making polynomially many (in m) queries to the oracles $\mathsf{F}, \mathsf{PSPACE}, \mathsf{INV}, \mathcal{A}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}$,

$$\Pr_{\mathsf{F},\mathsf{PSPACE},\mathsf{INV} \leftarrow\$ D_{\mathbf{p}}}\left[\mathsf{SuccInv}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}_{\mathcal{A},\mathcal{R}} \geq 1 - \frac{1}{2\mathbf{cp}(m)}\right] \leq 1/\mathbf{c}, \qquad (20)$$

where $\mathsf{SuccInv}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}_{\mathcal{A},\mathcal{R}}$ is defined as

$$\Pr_{x \leftarrow\$ \{0,1\}^m,\mathcal{R}}\left[\mathcal{R}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV},\mathcal{A}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}}(1^m, \mathsf{F}(x)) \in \mathsf{F}^{-1}(\mathsf{F}(x))\right].$$

Proof. Fix $\mathbf{p}$, $\mathcal{R}$ and $\mathcal{A}$. Since $\mathcal{A}$ and $\mathcal{R}$ both make polynomially many queries to the same oracles, $\mathcal{R}$ can simply simulate $\mathcal{A}$. Thus, w.l.o.g., we can assume that $\mathcal{R}$ only makes queries to F, PSPACE and INV. Additionally, we consider $\mathcal{R}$ to be a computationally unbounded algorithm so that w.l.o.g., we can assume that it does not make queries to the PSPACE oracle.

Let q be a polynomial such that adversary $\mathcal{R}$ makes exactly $q(m)$ queries to the oracle F and an arbitrary number of queries to INV. Since we let the

adversary $\mathcal{R}$ make an arbitrary number of queries to INV, that is, the adversary can be assumed to know the $\mathsf{EASY}^m_{\mathsf{in}}$ and $\mathsf{EASY}^m_{\mathsf{out}}$ and how F maps $\mathsf{EASY}^m_{\mathsf{in}}$ to $\mathsf{EASY}^m_{\mathsf{out}}$ completely. This only makes the adversary stronger. Importantly, using INV does not give the adversary any information on F on the *hard* values (only the fact that the values are hard).

Denote the preimages to F queries by $x_1, ..., x_{q(m)}$ and the adversary's guess for the pre-image of its input y by $x_{q(m)+1}$.

$$
\begin{aligned}
&\Pr_{\mathsf{F},\mathsf{INV} \leftarrow\!\$\, D_{\mathbf{p}}, x \leftarrow\!\$\, \{0,1\}^m, \mathcal{R}} \left[\mathcal{R}(\mathsf{F}(x)) \in \mathsf{F}^{-1}(\mathsf{F}(x))\right] \\
&= \Pr\left[\mathcal{R}(\mathsf{F}(x)) \in \mathsf{F}^{-1}(\mathsf{F}(x)) \;\middle|\; x \in \mathsf{EASY}^m_{\mathsf{in}}\right] \cdot \Pr[x \in \mathsf{EASY}^m_{\mathsf{in}}] \\
&\quad + \Pr\left[\mathcal{R}(\mathsf{F}(x)) \in \mathsf{F}^{-1}(\mathsf{F}(x)) \;\middle|\; x \notin \mathsf{EASY}^m_{\mathsf{in}}\right] \cdot \Pr[x \notin \mathsf{EASY}^m_{\mathsf{in}}] \\
&\leq 1 \cdot \left(1 - \frac{1}{\mathbf{p}(m)}\right) + \Pr\left[\mathcal{R}(\mathsf{F}(x)) \in \mathsf{F}^{-1}(\mathsf{F}(x)) \;\middle|\; x \notin \mathsf{EASY}^m_{\mathsf{in}}\right] \cdot \frac{1}{\mathbf{p}(m)} \\
&\leq 1 - \frac{1}{\mathbf{p}(m)} + \frac{1}{\mathbf{p}(m)} \sum_{i=1}^{q(m)+1} \Pr\left[\mathsf{F}(x_i) = \mathsf{F}(x) \;\middle|\; \begin{array}{l} \mathsf{F}(x_1), ..., \mathsf{F}(x_{i-1}) \neq \mathsf{F}(x), \\ x \notin \mathsf{EASY}^m_{\mathsf{in}} \end{array}\right] \\
&\leq 1 - \frac{1}{\mathbf{p}(m)} + \frac{1}{\mathbf{p}(m)} \sum_{i=1}^{q(m)+1} \frac{1}{\frac{1}{\mathbf{p}(m)} 2^m - i} \leq 1 - \frac{1}{2\mathbf{p}(m)} \text{ when } m \text{ is large enough.}
\end{aligned}
$$

Next, we apply an averaging argument. Consider the random variable

$$\mathsf{SuccInv}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}_{\mathcal{A},\mathcal{R}}$$

which maps $\mathsf{F}, \mathsf{PSPACE}, \mathsf{INV} \leftarrow\!\$\, D_{\mathbf{p}}$ to the probability that

$$\mathcal{R}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV},\mathcal{A}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}}$$

inverts F over the randomness of $\mathcal{R}$, $\mathcal{A}$ and sampling x. Then, by the previous analysis, the expected value μ of $\mathsf{SuccInv}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}_{\mathcal{A},\mathcal{R}}$ is at most $1-\epsilon$ for $\epsilon := \frac{1}{2\mathbf{p}(m)}$. Using Markov inequality on $1 - \mathsf{SuccInv}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}_{\mathcal{A},\mathcal{R}}$, we obtain that

$$\Pr_{\mathsf{F},\mathsf{PSPACE},\mathsf{INV} \leftarrow\!\$\, D_{\mathbf{p}}}\left[\mathsf{SuccInv}^{\mathsf{F},\mathsf{PSPACE},\mathsf{INV}}_{\mathcal{A},\mathcal{R}} \geq 1 - c\epsilon\right] \leq \frac{1}{c}.$$

for any c. □

References

1. Attrapadung, N., Matsuda, T., Nishimaki, R., Yamada, S., Yamakawa, T.: Constrained PRFs for NC^1 in traditional groups. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part II. LNCS, vol. 10992, pp. 543–574. Springer, Heidelberg (2018)

2. Babai, L., Fortnow, L., Lund, C.: Non-deterministic exponential time has two-prover interactive protocols. Comput. Complex. **1**(1), 3–40 (1991)
3. Babai, L., Fortnow, L., Nisan, N., Wigderson, A.: BPP has subexponential time simulations unlessexptime has publishable proofs. Comput. Complex. **3**(4), 307–318 (1993)
4. Baecher, P., Brzuska, C., Fischlin, M.: Notions of black-box reductions, revisited. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 296–315. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42033-7_16
5. Blundo, C., Santis, A.D., Vaccaro, U.: Randomness in distribution protocols. Inf. Comput. **131**(2), 111–139 (1996)
6. Canetti, R., Rivest, R., Sudan, M., Trevisan, L., Vadhan, S., Wee, H.: Amplifying collision resistance: a complexity-theoretic treatment. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 264–283. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_15
7. Döttling, N., Garg, S., Ishai, Y., Malavolta, G., Mour, T., Ostrovsky, R.: Trapdoor hash functions and their applications. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part III. LNCS, vol. 11694, pp. 3–32. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26954-8_1
8. Gennaro, R., Gertner, Y., Katz, J.: Lower bounds on the efficiency of encryption and digital signature schemes. In: 35th ACM STOC, pp. 417–425. ACM Press, June 2003
9. Gennaro, R., Trevisan, L.: Lower bounds on the efficiency of generic cryptographic constructions. In: 41st FOCS, pp. 305–313. IEEE Computer Society Press, November 2000
10. Goldreich, O., Impagliazzo, R., Levin, L.A., Venkatesan, R., Zuckerman, D.: Security preserving amplification of hardness. In: 31st FOCS, pp. 318–326. IEEE Computer Society Press, October 1990
11. Goldreich, O., Nisan, N., Wigderson, A.: On yao's xor lemma. Technical report TR95-050, Electronic Colloquium on Computational Complexity (1995)
12. Goyal, V., O'Neill, A., Rao, V.: Correlated-input secure hash functions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 182–200. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_12
13. Haitner, I., Reingold, O., Vadhan, S.P.: Efficiency improvements in constructing pseudorandom generators from one-way functions. In: Schulman, L.J. (ed.) 42nd ACM STOC, pp. 437–446. ACM Press, June 2010
14. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM J. Comput. **28**(4), 1364–1396 (1999)
15. Healy, A., Vadhan, S.P., Viola, E.: Using nondeterminism to amplify hardness. In: Babai, L. (ed.) 36th ACM STOC, pp. 192–201. ACM Press, June 2004
16. Hemenway, B., Lu, S., Ostrovsky, R.: Correlated product security from any one-way function. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 558–575. Springer, Heidelberg (May (2012)
17. Hsiao, C.-Y., Reyzin, L.: Finding collisions on a public road, or do secure hash functions need secret coins? In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 92–105. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_6
18. Impagliazzo, R.: Hard-core distributions for somewhat hard problems. In: 36th FOCS, pp. 538–545. IEEE Computer Society Press, October 1995
19. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: 21st ACM STOC, pp. 44–61. ACM Press, May 1989

20. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 8–26. Springer, New York (1990). https://doi.org/10.1007/0-387-34799-2_2
21. Impagliazzo, R., Wigderson, A.: P = BPP if E requires exponential circuits: derandomizing the XOR lemma. In: 29th ACM STOC, pp. 220–229. ACM Press, May 1997
22. Ishai, Y., Kilian, J., Nissim, K., Petrank, E.: Extending oblivious transfers efficiently. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 145–161. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_9
23. Kim, J.H., Simon, D.R., Tetali, P.: Limits on the efficiency of one-way permutation-based hash functions. In: 40th FOCS, pp. 535–542. IEEE Computer Society Press, October 1999
24. Lin, H., Trevisan, L., Wee, H.: On hardness amplification of one-way functions. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 34–49. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30576-7_3
25. Lipton, R.: New directions in testing. Distrib. Comput. Cryptogr. **2**, 191–202 (1991)
26. Lu, C.-J.: On the complexity of parallel hardness amplification for one-way functions. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 462–481. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_24
27. Lu, C.-J.: On the security loss in cryptographic reductions. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 72–87. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01001-9_4
28. Mahmoody, M., Mohammed, A., Nematihaji, S., Pass, R., Shelat, A.: A note on black-box separations for indistinguishability obfuscation. Cryptology ePrint Archive, Report 2016/316 (2016). https://eprint.iacr.org/2016/316
29. Reingold, O., Trevisan, L., Vadhan, S.: Notions of reducibility between cryptographic primitives. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 1–20. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24638-1_1
30. Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 419–436. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00457-5_25
31. Shaltiel, R., Viola, E.: Hardness amplification proofs require majority. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC, pp. 589–598. ACM Press, May 2008
32. Simon, D.R.: Finding collisions on a one-way street: can secure hash functions be based on general assumptions? In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 334–345. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054137
33. Sudan, M., Trevisan, L., Vadhan, S.: Pseudorandom generators without the XOR lemma. J. Comput. Syst. Sci. **62**(2), 236–266 (2001)
34. Trevisan, L.: List-decoding using the XOR lemma. In: 44th FOCS, pp. 126–135. IEEE Computer Society Press, October 2003
35. Trevisan, L.: On uniform amplification of hardness in NP. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC, pp. 31–38. ACM Press, May 2005
36. Vadhan, S.P., Zheng, C.J.: Characterizing pseudoentropy and simplifying pseudorandom generator constructions. In: Karloff, H.J., Pitassi, T. (eds.) 44th ACM STOC, pp. 817–836. ACM Press, May 2012
37. Viola, E.: The complexity of constructing pseudorandom generators from hard functions. Comput. Complex. **13**(3–4), 147–188 (2005)
38. Wee, H.: One-way permutations, interactive hashing and statistically hiding commitments. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 419–433. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-70936-7_23

39. Wichs, D.: Barriers in cryptography with weak, correlated and leaky sources. In: Kleinberg, R.D. (ed.) ITCS 2013, pp. 111–126. ACM, January 2013
40. Yao, A.C.C.: Theory and applications of trapdoor functions (extended abstract). In: 23rd FOCS, pp. 80–91. IEEE Computer Society Press, November 1982