# Better Security-Efficiency Trade-Offs in Permutation-Based Two-Party Computation

Yu Long Chen[1] and Stefano Tessaro[2]

[1] imec-COSIC, KU Leuven, Belgium
yulong.chen@kuleuven.be
[2] Paul G. Allen School of Computer Science & Engineering,
University of Washington, Seattle, USA
tessaro@cs.washington.edu

**Abstract.** We improve upon the security of (tweakable) correlation-robust hash functions, which are essential components of garbling schemes and oblivious-transfer extension schemes. We in particular focus on constructions from *permutations*, and improve upon the work by Guo *et al.* (IEEE S&P '20) in terms of security and efficiency.
We present a tweakable one-call construction which matches the security of the most secure two-call construction – the resulting security bound takes form $O((p+q)q/2^n)$, where $q$ is the number of construction evaluations and $p$ is the number of direct adversarial queries to the underlying $n$-bit permutation, which is modeled as random.
Moreover, we present a new two-call construction with much better security degradation – in particular, for applications of interest, where only a constant number of evaluations per tweak are made, the security degrades as $O((\sqrt{q}p + q^2)/2^n)$. Our security proof relies on on the sum-capture theorems (Babai 02; Steinberger 12, Cogliati and Seurin 18), as well as on new balls-into-bins combinatorial lemmas for limited independence ball-throws.
Of independent interest, we also provide a self-contained concrete security treatment of oblivious transfer extension.

**Keywords:** Correlation-robust hashing, two-party computation, provable security

## 1 Introduction

Secure two-party computation makes intensive use of *symmetric-key* primitives, both in *garbling* [5, 26] and *oblivious-transfer (OT) extension* [18] schemes. A common denominator of many such schemes is a special form of hash functions, known as *correlation-robust* (crHF) [18], which is pseudorandom when its input is whitened with a secret key, as well as the stronger notion of a *circular* crHF [8] (ccrHF). Recent works by Guo *et al.* [15, 16] initiated the study of the concrete security of crHFs and ccrHFs in the ideal-permutation and cipher models. They also point out that naïve constructions lead to substantial security degradation with the number of *gates* (in the case of garbling) and of *OT instances* (in the case of OT extension). In fact, the authors of [15] leverage this to attack particular instantiations of half-gate garbling [27] with 80-bit security parameters.

Main goals of this paper. This paper presents new (tweakable) crHFs and ccrHFs from *permutations* with substantially improved security-efficiency trade-offs. We give a one-call construction matching the security of the two-call construction from [16], and give a two-call construction with much better security degradation against a limited class of distinguishers sufficient for applications. We also revisit OT extension in concrete-security terms, weakening in particular the security requirements for the underlying crHF.

There are two ways in which our results can be interpreted – one is in terms of constructions from *fixed-key* block ciphers, in the spirit of [4,16]. The other, and perhaps better, interpretation is in terms of constructions from simpler objects, like block-cipher rounds, which we abstract as random permutations to model generic attacks – this is in line with the extensive research program on analyzing symmetric constructions. (We discuss this further below.)

Next, we briefly review the definiton of crHFs, as well as the achievable levels of security, before giving an overview of our results in greater detail.

Correlation-robust hashing. A *tweakable correlation-robust hash function* [16, 18] is an efficiently computable two-argument function $H : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$ with the property that the oracle

$$\mathcal{O}_R^{\mathrm{tcr}}(w,t) = H(w \oplus R, t)$$

for a random $R \overset{\$}{\leftarrow} \{0,1\}^n$ is indistinguishable from a random function $f : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$. The second argument is the *tweak* – it enables domain separation (i.e., querying the same $w$ on different tweaks should result in independent outputs), but also controls security degradation. To see what this means, note first that if $H$ is a random oracle, then the distinguishing advantage of a $q$-query distinguisher making $p$ direct queries to $H$ is $\frac{pq}{2^n}$. (The proof is folklore and follows that of the Even-Mansour construction [11].) However, a crucial point is that for many applications we can restrict the distinguisher to make *at most* $B$ *queries per tweak*, where $B$ can be *very* small (even just $B = 1$) - in this case the advantage is[3]

$$\delta(q,p,B) \leq \frac{Bp}{2^n} \ . \tag{1}$$

As we show in Section 3, for OT extension, it is enough to use $B = 1$. Similarly, $B = 1$ is enough for garbling schemes [15,16]. Moreover, [15] gives a tweakable crHF construction making one call to an ideal cipher with concrete security

$$\delta(q,p,B) \leq \frac{Bp}{2^n} + \frac{(B-1)q}{2^n} \ .$$

In fact, both constructions can be adapted to satisfy *circular* crHF security, which is amenable to half-gate garbling [27] and free-XOR [8].

[3] The basic idea of the simple proof is that a direct query $H(m,t)$ only helps if $m = w \oplus R$ for one of the $B$ oracle queries $(w,t)$.

The above constructions make however fairly strong assumptions – either a monolithic random oracle or a monolithic ideal cipher. In the following, we want to study constructions from simpler primitives.

Why is the problem hard? Before moving on, it is worth pointing out that the main technical challenge in the design of secure crHFs is that we are aiming for a secret-key object with no designated secret key input – the secret key is XORed to the actual input, and we cannot change this. This makes crHFs very challenging to build. In particular, one cannot obtain crHFs from tweakable block ciphers directly, since the latter require a designated secret-key input.

Instead, the problem is related to designing related-key secure block ciphers – indeed, if a cipher $E$ is pseudorandom against related-key attacks [6], it is not hard to see that $H(x, t) = E(x, t)$ is a good crHF – our warm-up construction below can indeed be thought as the case where $E$ is the (one-key) Even-Mansour construction with non-linear key schedule from [9]. However, we prove the stronger notion of circular crHF, here, which does not follow generically. Also, our main two-call construction below however does not match any construction from prior works [9, 12]. Tessaro [25] introduces related-key key-derivation functions which achieve similar security as (non-tweakable) crHFs, but with the goal of achieving near-optimal security (from random *functions*), and the resulting constructions are quite inefficient. Further, we actually do not know any standard-model construction for such additive (in $\mathbb{F}_{2^n}$) attacks, except under very strong multilinear-map assumptions [1].

The one-call construction. Our first warm-up result is concerned with one-call constructions from a permutation $\pi : \{0,1\}^n \to \{0,1\}^n$. Here, Guo *et al.* (GKWY) [16], proposed a construction – called MMO – which simply outputs $\pi(m) \oplus m$. MMO is not tweakable, and they prove a bound of $\frac{q(q+p)}{N}$. To additionally support a tweak, GKWY propose a two-call construction, called TMMO, while also achieving a similar security bound of $O\left(\frac{q(q+p)}{N}\right)$.

Here, we show that a very simple variant of MMO already achieves the same quantitative security with one single permutation call. Namely,

$$H(m, t) = \pi(m \otimes t) \oplus (m \otimes t) \ ,$$

where $\otimes$ stands for multiplication of bit-strings interpreted as elements of $\mathbb{F}_{2^n}$. Clearly, the tweak $t = 0^n$ needs to be excluded, but this is usually not a limitation, and all other tweaks are usable. To achieve tweakable ccrHF security, it is enough to also exclude the tweak $t = 0^{n-1}1$ (i.e., the neutral element of multiplication).

The analysis inherits ideas from tweakable block ciphers [21], however we need to take into account that no secret key can be used other than the one injected implicitly via whitening the input – the core of the security proof (which we carry out using the H-coefficient method [7, 23]) relies on the fact that for given input-tweak pairs $\{(w_i, t_i)\}_{i=1,\ldots,q}$, the probability that for some $i \neq j$ we have

$$t_i \otimes (w_i \oplus R) = t_j \otimes (w_j \oplus R)$$

is at most $2^{-n}$, over the random choice of $R$.

The two-call construction. Our more interesting result looks at two-call constructions. Ideally, we would like to obtain a construction improving upon the bound $qp/2^n$, but this is impossible *in general* [16]. However, we show that a positive result is possible if we limit the distinguisher's queries so that (1) the number of queries per tweak is bounded by $B$, and (2) the tweaks are chosen from a *nice* combinatorial subset $T \subseteq \{0,1\}^t$. We already discussed (1) as being sufficient for applications, but (2) is also not a major restriction – for our instantiation, we need to pick $T$ as a *random* subset, but we can actually *fix* this set once and for all, and re-use it across instances.[4]

Our construction is called FPTP (this stands for Feed-forward Permutation-Tweak-Permutation), and on input $m \in \{0,1\}^n$ and tweak $t \in \{0,1\}^n$, it outputs

$$\mathrm{FPTP}(m,t) = \pi(t \oplus \pi(\sigma(m))) \oplus \sigma(m) \ .$$

Here, $\sigma$ is linear, and an *orthomorphism*, i.e., $\sigma(x) \oplus x$ is *also* a permutation. Removing $\sigma$, this construction resembles TMMO from [16], but the main (and crucial) difference is that we feed the *input* forward, as opposed to $\pi(m)$.

Assuming $T$ is a good set for which all non-principal Fourier coefficients[5] are sufficiently small (and this is true for a randomly chosen $T$, as proved e.g. in [3, 24]), then any distinguisher as above achieves advantage at most of order

$$\delta(q,p,B) \leq \frac{B\sqrt{q}p}{2^n} + \frac{q^2}{2^n} \ .$$

against *circular* crHF security. The first term here is significantly better than $qp/2^n$ for small $B < \sqrt{q}$, and in particular we usually want $B = 1$.

One restriction for this result is that it only holds for distinguishers for which inputs to the construction are distinct, even across tweaks. This restriction is strictly speaking not-necessary (we could input $m \otimes t$ instead of $m$), but in most applications, it is not necessary, and thus decide to opt for presenting this more efficient construction which is only secure under this input restriction. Indeed, in Section 3 we give a modified version of OT-extension that only requires security for *distinct* inputs. Moreover, for garbling applications, it is already known that it is sufficient to achieve security for *random* inputs, which are distinct with high probability (up to the birthday bound).

We also note that if we are only concerned with (non-circular) crHF security, then we can drop the map $\sigma$. We also give an analysis of our construction in the multi-user setting. We focus on the case of random inputs, which are sufficient for multi-user garbling, as studied in [15].

OT Extension and Concrete Security. We also revisit the concrete security of oblivious-transfer extension [18]. In particular, we follow the angle of [16], and look specifically at the concrete security of transforming the $\Delta$-random-OT functionality into an OT functionality using tweakable crHFs. We focus specifically on malicious security.

[4] Heuristically, one could evaluate a hash function on a fixed subset of inputs to obtain the corresponding tweaks.

[5] I.e., of the characteristic function of the set

In addition to making the treatment concrete, we show that it is enough to consider a crHF construction which is secure for *distinct* inputs only by slightly modifying the classical transformation. Moreover, we also discuss instantiations from random tweaks (and see that the cost can be kept fairly low if these need to be generated on the fly, for example by recycling them across instances). Indeed, interestingly, we see that despite the common belief, tweaks for active security serve more as a mean of controlling concrete security than to mitigate active attackers that force inputs to be equal across OT instances.

As a result of this, we obtain OT extension making two permutation calls per OT instance, and whose security degrades as $\frac{\sqrt{m}p}{2^n}$, where $m$ is the number of OT instances (assuming $m < 2^{n/2}$). If we have $n = 102$, then we can for example have $m = 2^{32}$, and obtain 80-bit security.

Interpreting the results. We see this work as part of the general program on understanding the security of cryptographic primitives. One way to think of a random permutation is not as a heuristic property of a complex object, but instead as a black-box abstraction for a component of the scheme that can be leveraged by an attack. In that sense, the simpler the component, the better. So, for example, the permutation could abstract a few rounds of AES (instead of the full AES) – of course proofs in this model should be backed by additional cryptanalysis (as it is always the case with any ideal-model proof).

An alternative interpretation (as in [16]) is that our constructions are instantiated from a fixed-key block cipher (like AES). However, it is not clear this interpretation is the most suitable one – the number of calls need to necessarily increase to obtain better security, and it is hard to beat the one-call construction from [15] – while the latter *does* use re-keying, it has already been shown that with appropriate implementation care, the costs of re-keying can be mitigated (as e.g. in [14]).

### 1.1 Technical Overview

We give an overview of the main ingredients behind the proof of security for the FPTP construction, which is our main result. To this end, we look at the two-permutation version (i.e., $\pi_1, \pi_2$ are independent permutations), namely the crHF candidate

$$H(m, t) = \pi_2(t \oplus \pi_1(m)) \oplus m \ .$$

This variant is analyzed in the full version of the paper. Its analysis is somewhat cleaner and pedagogical than the (more relevant) one-permutation version, which however follows similar ideas. Here, we focus also on discussing the proof that the construction is correlation-robust, i.e., we do not consider the circular version.

The full analysis adopts the H-coefficient method [7,23] – we give some intuition about possible bad interaction transcripts which lead to distinguishing and why they can only occur with probability consistent with the claimed bound in the ideal world. (This is only part of the analysis – we also need to show that the probabilities of a good transcript occurring are similar in the real and ideal worlds.) Note that the discussion here does not exhaust all the bad events, we only discuss the most important ones. Every transcript contains $q$ tweak-input-output triples $(t_1, w_1, z_1), \dots, (t_q, w_q, z_q)$, where (1) $w_1, \dots, w_q$ are disjoint and (2) every tweak $t_i$ appears at most $B$ times. Further, we have two sub-transcripts $\tau_1$ and $\tau_2$ of queries to $\pi_1$ and $\pi_2$, respectively – each containing (at most) $p$ entries of the form $(u, v)$ resulting from either a forward and backward queries to $\pi_1$ and $\pi_2$, respectively. Then, the key $R$ is also included in the transcript – in the ideal world, in particular, the key $R \overset{\$}{\leftarrow} \{0,1\}^n$ is chosen *last* and independently from the interaction so far (as opposed to the real world, where it is chosen first).

Chains. One natural way of breaking the construction is to produce a so-called *chain*. One type of such a chain occurs if for a query $(t_i, w_i, z_i)$, there exists one query $(u, v) \in \tau_1$ to $\pi_1$ and one query $(u', v') \in \tau_2$ to $\pi_2$ such that

$$w_i = u \oplus R \, , v \oplus t_i = u' \, .$$

Then, in the real world, we necessarily have $v' \oplus w_i \oplus R = z_i$, whereas in the ideal world this is unlikely to be the case, as the values $z_1, \dots, z_q$ have been generated randomly and independently.

Now imagine we can bound the number of query pairs $(u, v) \in \tau_1$ and $(u', v') \in \tau_2$ for which $v \oplus u' \in T$ by some number $\phi \leq p^2$. Then, for every such pair, we have a well-defined tweak $t \in T$ such that $v \oplus u' = t$, and the probability that at least one of the queries for tweak $t$ satisfies $w \oplus R = u$ is therefore (by union bound) $2^{-n}$, assuming $R$ is chosen last. It turns out that if $T$ is well chosen, then $\phi$ can be smaller than $p^2$ – for example, for a randomly sampled set, we can show that roughly $\phi \leq \sqrt{q}p + qp^2/2^n$, using a sum-capture theorem [3, 24]. This gives us the desired bound.

Other types of double-chains. There are other types of chains that can occur. One accounts to the symmetric case to the above – namely $v' = w_i \oplus R \oplus z_i \, , v \oplus t_i = v'$. This is handled in a similar manner.

However, we also need to handle a third case, namely one where

$$u = w_i \oplus R \, , \quad v' = z_i \oplus w_i \oplus R \, . \tag{2}$$

In particular, the above means that $u \oplus v' = z_i$, where $z_i$ is the output of a random function. Because the values $z_1, \dots, z_q$ are random, we can use a slightly different sum-capture theorem [10], and by a similar discussion to the above, the number of relevant pairs is also (with high probability) at most $\sqrt{q}p + qp^2/2^n$, and this thus the probability of each pair satisfying additional (2) is at most $\sqrt{q}p/2^n + qp^2/2^{2n}$.

Merging chains. A final issue that can happen is that, even though no chains are completed, we learn that two chains are bound to *merge*. For example, this means that for two queries $(t_i, w_i, z_i)$ and $(t_j, w_j, z_j)$, for which $w_i \neq w_j$, we can find $(u_1, v_1) \in \tau_1, (u_2, v_2) \in \tau_1$, such that

$$u_1 = w_i \oplus R \, , \; u_2 = w_j \oplus R \, , \; v_1 \oplus t_i = v_2 \oplus t_j \, . \tag{3}$$

Then we know we ought to have $z_i \oplus z_j = w_i \oplus w_j$, which is unlikely to be true in the ideal world. It turns out that upper bounding the probability of chains merging is the most involved part of our proof.

To see how this is resolved, fix now a pair of queries $(t_i, w_i, z_i)$ and $(t_j, w_j, z_j)$, and assume that we have a bound $L$ on the number of pairs of permutation queries $(u_1, v_1), (u_2, v_2)$ such that $u_1 \oplus u_2 = w_i \oplus w_j$ and $v_1 \oplus v_2 = t_i \oplus t_j$, then the random choice $R$ will satisfy (3) additionally with probability at most $L/2^n$. In fact, if we can show that for any $\Delta, \Delta'$ the number of pairs $(u_1, v_1), (u_2, v_2) \in \tau_1$ such that $u_1 \oplus u_2 = \Delta$ and $v_1 \oplus v_2 = \Delta'$ is at most $L$, then we would get an upper bound of $q^2 L/2^n$ that any such merge occurs.

It turns out that proving such bound $L$ accounts to a balls-into-bins problem, where an adaptive adversary interacts with a random permutation by means of $p$ queries, and then *every pair* of queries $(u_1, v_1), (u_2, v_2)$ results into one of $\binom{p}{2}$ balls being thrown into bin $(u_1 \oplus u_2, v_1 \oplus v_2)$. We will prove that the load of the heaviest bin is, with high probability, small enough (roughly linear in $n$). This is actually surprising and non-trivial – the main reason is that the $\binom{p}{2}$ balls are not-independent, and the result of an adaptive process, yet their behavior is very similar to the assignment of $p^2$ random balls into $2^{2n}$ bins. We give an analysis (of a more general setting) in Section 5.2.

## 2 Preliminaries

For $n \in \mathbb{N}$, we denote by $\{0,1\}^n$ the set of bit strings of length $n$. For two bit strings $X, Y \in \{0,1\}^n$, we denote by $X \oplus Y$ their bitwise addition and by $X \otimes Y$ the multiplication of the bit strings interpreted as elements of $\mathbb{F}_{2^n}$. For any value $Z$, we denote by $A \leftarrow Z$ the assignment of $Z$ to the variable $A$. For any finite set $\mathcal{S}$, we define by $S \overset{\$}{\leftarrow} \mathcal{S}$ the uniformly random selection of $S$ from $\mathcal{S}$. For any integers $a, b$ such that $1 \leq b \leq a$, we denote $(a)_b = a \cdot (a-1) \dots (a-b+1)$ and $(a)_0 = 1$. We denote by $\mathrm{Perm}(n)$ the set of all permutations on $\{0,1\}^n$, and by $\mathrm{Func}(m,n)$ the set of all functions that maps $\{0,1\}^m$ to $\{0,1\}^n$. For $\pi \overset{\$}{\leftarrow} \mathrm{Perm}(n)$ and a list $\mathcal{Q}_\pi = \{(x_1, y_1), \dots\}$, we denote by $\pi \vdash \mathcal{Q}_\pi$ the event that permutation $\pi$ is consistent with the queries-response tuples in $\mathcal{Q}_\pi$, i.e. that $\pi(x) = y$ for all $(x,y) \in \mathcal{Q}_\pi$.

For any subset $A \subseteq \{0,1\}^n$ such that $|A| = q$, we denote $1_A : \{0,1\}^n \to \{0,1\}$ the characteristic functions of $A$, namely $1_A(x) = 1$ if $x \in A$ and $1_A(x) = 0$ if $x \notin A$. Given any function $f : \{0,1\}^n \to \mathbb{R}$ and $\alpha \in \{0,1\}^n$, the Fourier coefficient of $f$ corresponding to $\alpha$ is

$$\widehat{f}(\alpha) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x)(-1)^{\alpha \cdot x} \,,$$

where $\alpha \cdot x$ denotes inner product. The coefficient corresponding to $\alpha = 0^n$ is called the principal Fourier coefficient, all the other ones are called non-principal Fourier coefficients. We define $\Phi(A) = \max\left\{2^n \left|\widehat{1}_A(\alpha)\right| : \alpha \in \{0,1\}^n, \alpha \neq 0^n\right\}$.

### 2.1 Tweakable (Circular) Correlation Robustness Hash Functions

We rely on the multi-instance tweakable correlation robustness (miTCR) and the multi-instance tweakable circular correlation robustness (miTCCR) notion introduced by Guo et al. [15, 16].

For $n, t \in \mathbb{N}$, we consider a hash function that takes as input a $n$-bit message, a $t$-bit tweak, and returns a $n$-bit ciphertext. More formally, let $H\colon \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$ be a hash function that is based on $r$ $n$-bit permutations $\pi_1, \ldots, \pi_r$, let $\mathcal{R}$ be a distribution on the message space $\{0,1\}^n$ of $H$, and define

$$\mathcal{O}_R^{\mathrm{tcr}}(w,t) = H(w \oplus R, t)\,,$$
$$\mathcal{O}_R^{\mathrm{tccr}}(w,t,b) = H(w \oplus R, t) \oplus b \cdot R\,,$$

for $R \xleftarrow{\$} \mathcal{R}$ and $b \in \{0,1\}$. We will consider both the miTCR and the miTCCR security of $H$, where we assume that $\pi_1, \ldots, \pi_r \xleftarrow{\$} \mathrm{Perm}(n)$. For the case of the miTCR security, the distinguisher $\mathcal{D}$ is given access to either $(\mathcal{O}_{R_1}^{\mathrm{tcr}}, \ldots, \mathcal{O}_{R_u}^{\mathrm{tcr}}, \pi_1^{\pm}, \ldots, \pi_r^{\pm})$ for $R_1, \ldots, R_u \xleftarrow{\$} \mathcal{R}$, or $(f_1, \ldots, f_u, \pi_1^{\pm}, \ldots, \pi_r^{\pm})$ for $f_1, \ldots, f_u \xleftarrow{\$} \mathrm{Func}(n+t, n)$. Its goal is to determine which oracle it is given access to:

$$\mathbf{Adv}_{H,\mathcal{R}}^{\mathrm{miTCR}}(\mathcal{D}) = \left|\Pr\left[\mathcal{D}^{\mathcal{O}_{R_1}^{\mathrm{tcr}}, \ldots, \mathcal{O}_{R_u}^{\mathrm{tcr}}, \pi_1^{\pm}, \ldots, \pi_r^{\pm}} = 1\right] - \Pr\left[\mathcal{D}^{f_1, \ldots, f_u, \pi_1^{\pm}, \ldots, \pi_r^{\pm}} = 1\right]\right|\,.$$

For the case of the miTCCR security, the distinguisher $\mathcal{D}$ is given access to either $(\mathcal{O}_{R_1}^{\mathrm{tccr}}, \ldots, \mathcal{O}_{R_u}^{\mathrm{tccr}}, \pi_1^{\pm}, \ldots, \pi_r^{\pm})$ for $R_1, \ldots, R_u \xleftarrow{\$} \mathcal{R}$, or $(f_1, \ldots, f_u, \pi_1^{\pm}, \ldots, \pi_r^{\pm})$ for $f_1, \ldots, f_u \xleftarrow{\$} \mathrm{Func}(n+t+1, n)$. Its goal is to determine which oracle it is given access to:

$$\mathbf{Adv}_{H,\mathcal{R}}^{\mathrm{miTCCR}}(\mathcal{D}) = \left|\Pr\left[\mathcal{D}^{\mathcal{O}_{R_1}^{\mathrm{tccr}}, \ldots, \mathcal{O}_{R_u}^{\mathrm{tccr}}, \pi_1^{\pm}, \ldots, \pi_r^{\pm}} = 1\right] - \Pr\left[\mathcal{D}^{f_1, \ldots, f_u, \pi_1^{\pm}, \ldots, \pi_r^{\pm}} = 1\right]\right|\,.$$

In the both cases the superscript ± for the $\pi_i$'s indicates that the distinguisher has bi-directional access. For the miTCCR security, we require that $\mathcal{D}$ never queries both $(w,t,0)$ and $(w,t,1)$ to the same oracle (for any $(w,t)$ couple).

When $u = 1$, we consider the single instance security of $H$ with the distribution $\mathcal{R}$, and we simply denote $\mathcal{D}$'s advantage in distinguishing the real world from random by $\mathbf{Adv}_{H,\mathcal{R}}^{\mathrm{TCR}}(\mathcal{D})$ for the case of tweakable correlation robustness, and by $\mathbf{Adv}_{H,\mathcal{R}}^{\mathrm{TCCR}}(\mathcal{D})$ for the case of tweakable circular correlation robustness.

It is easy to see that the miTCCR (TCCR) notion implies the miTCR (TCR) notion (when $b$ is always zero). In the remainder of this work, we mainly focus on the miTCCR (TCCR) notion, and on hash functions with tweak space $\{0,1\}^n$.

### 2.2 Universal Hash Functions

For $n \in \mathbb{N}$, let $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ such that for $K_h \in \mathcal{K}_h$, $H_{K_h}(\cdot) = H(K_h, \cdot)$ is called an $\epsilon$-almost XOR universal ($\epsilon$-AXU) hash function [20] if for all distinct $M, M' \in \{0,1\}^*$ and all $C \in \{0,1\}^n$, we have

$$\Pr\left[K_h \xleftarrow{\$} \mathcal{K}_h \colon H_{K_h}(M) \oplus H_{K_h}(M') = C\right] \leq \epsilon\,.$$

### 2.3 Linear Orthomorphism

A function $\sigma\colon \{0,1\}^n \to \{0,1\}^n$ is a *linear orthomorphism* if $\sigma$ (1) linear: $\sigma(x \oplus y) = \sigma(x) \oplus \sigma(y)$; and (2) an orthomorphism: $\sigma$ is a permutation, and the function $\sigma'(x) = \sigma(x) \oplus x$ is also a permutation. In this work, we will need the following result of [16].

**Lemma 1.** *Let $\sigma\colon \{0,1\}^n \to \{0,1\}^n$ be a linear orthomorphism and for a distribution $\mathcal{R}$, set $\mathbf{H}_\infty(\sigma(\mathcal{R}) \oplus \mathcal{R}) = -\log\left(\max_{R^*} \Pr_{R \leftarrow \mathcal{R}}[\sigma(R) \oplus R = R^*]\right)$. Then, we have $\mathbf{H}_\infty(\sigma(\mathcal{R}) \oplus \mathcal{R}) = \mathbf{H}_\infty(\mathcal{R})$.*

### 2.4 Patarin's H-Coefficient Technique

In this work, we use H-coefficient technique by Patarin [23], but we will follow the modernization of Chen and Steinberger [7].

We consider a deterministic distinguisher $\mathcal{D}$ that is given access to either the real world oracle $\mathcal{O}$ or the ideal world oracle $\mathcal{P}$. The distinguisher's goal is to determine which oracle it is given access to and we denote by

$$\mathbf{Adv}(\mathcal{D}) = \left|\Pr\left[\mathcal{D}^{\mathcal{O}} = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{P}} = 1\right]\right|$$

its advantage. We define a transcript $\tau$ that summarizes all query-response tuples learned by $\mathcal{D}$ during its interaction with its oracle $\mathcal{O}$ or $\mathcal{P}$. We denote by $X_{\mathcal{O}}$ (resp. $X_{\mathcal{P}}$) the probability distribution of transcripts when interacting with $\mathcal{O}$ (resp. $\mathcal{P}$). We call a transcript $\tau \in \mathcal{T}$ attainable if $\Pr[X_{\mathcal{P}} = \tau] > 0$.

**Lemma 2 (H-coefficient Technique).** *Consider a deterministic distinguisher $\mathcal{D}$. Define a partition $\mathcal{T} = \mathcal{T}_{\mathrm{good}} \cup \mathcal{T}_{\mathrm{bad}}$, where $\mathcal{T}_{\mathrm{good}}$ is the subset of $\mathcal{T}$ which contains all the "good" transcripts and $\mathcal{T}_{\mathrm{bad}}$ is the subset with all the "bad" transcripts. Let $0 \le \epsilon \le 1$ be such that for all $\tau \in \mathcal{T}_{\mathrm{good}}$:*

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} \ge 1 - \epsilon\,. \tag{4}$$

*Then, we have $\mathbf{Adv}(\mathcal{D}) \le \epsilon + \Pr[X_{\mathcal{P}} \in \mathcal{T}_{\mathrm{bad}}]$.*

### 2.5 Babai's Lemma

Define the following quantity

$$\mu(A, U, V) = |\{(a, u, v) \in A \times U \times V : a = u \oplus v\}|\;.$$

We consider the following lemma of Babai [3].

**Lemma 3 (Babai [3] Theorem 4.1).** *Let $A, U, V \subseteq \{0,1\}^n$. We have*

$$\mu(A, U, V) \le \frac{|A|\,|U|\,|V|}{2^n} + \Phi(A)\sqrt{|U|\,|V|}\,,$$

As shown in [3, 24], when the set $A$ is a randomly chosen subset of $\{0,1\}^n$ of size $q$, we have $\Phi(A) \le 4\sqrt{2\ln(2^n)q}$, except for probability $4/2^n$. Cogliati and Seurin [10] also showed that when $A$ is a multiset where the elements of $A$ are chosen uniformly at random with replacement, then we have $\Phi(A) \le \sqrt{3nq}$, except for probability $2/2^n$.

**Functionality $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m, k)$:**

**Initialization:** Inputs:

- Player $\mathsf{P}_A$: $\Delta \in \{0,1\}^k$
- Player $\mathsf{P}_B$: $\perp$.
- Adversary $\mathcal{A}$: If $\mathsf{P}_B \in \mathsf{Corr}$, $P : \{0,1\}^k \to \{0,1\}$. Else set $P$ to be the constant 1 predicate.

Return $P(\Delta)$ to $\mathcal{A}$. If $P(\Delta) = 0$, then return $\mathsf{abort}$ to $\mathsf{P}_A$, and stop.

**Correlation phase.** Inputs:

- Player $\mathsf{P}_A$: $\perp$.
- Player $\mathsf{P}_B$: $(x_1, \ldots, x_m) \in \{0,1\}^m$
- Adversary $\mathcal{A}$: $\mathbf{z}_1, \ldots, \mathbf{z}_m \in \{0,1\}^k$.

If $\mathsf{P}_A \in \mathsf{Corr}$, then $\mathbf{a}_i \leftarrow \mathbf{z}_i$, $\mathbf{b}_i \leftarrow \mathbf{a}_i \oplus x_i \cdot \Delta$ for all $i \in [m]$.
If $\mathsf{P}_B \in \mathsf{Corr}$, then $\mathbf{b}_i \leftarrow \mathbf{z}_i$, $\mathbf{a}_i \leftarrow \mathbf{b}_i \oplus x_i \cdot \Delta$ for all $i \in [m]$.
If $\mathsf{Corr} = \emptyset$ then $\mathbf{b}_i \overset{\$}{\leftarrow} \{0,1\}^m$, $\mathbf{a}_i \leftarrow \mathbf{b}_i \oplus x_i \cdot \Delta$ for all $i \in [m]$.
Return $(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ to $\mathsf{P}_A$ and $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ to $\mathsf{P}_B$.

Fig. 1: **The $\Delta$-Random-OT functionality $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m, k)$.** The set $\mathsf{Corr}$ takes one of the three values $\emptyset$, $\{\mathsf{P}_A\}$, or $\{\mathsf{P}_B\}$.

**Functionality $\mathcal{F}_{\mathsf{S\text{-}OT}}(m, \ell)$:**

Inputs:

- Player $\mathsf{P}_A$: $(\mathbf{m}_1^0, \mathbf{m}_1^1), \ldots, (\mathbf{m}_m^0, \mathbf{m}_m^1)$, where $\mathbf{m}_i^b \in \{0,1\}^\ell$ for all $i \in [m]$ and $b \in \{0,1\}$.
- Player $\mathsf{P}_B$: $(x_1, \ldots, x_m) \in \{0,1\}^m$.
- Adversary $\mathcal{A}$: $\perp$

Return $\perp$ to $\mathsf{P}_A$ and $(\mathbf{m}_1^{x_1}, \ldots, \mathbf{m}_m^{x_m})$ to $\mathsf{P}_B$.

Fig. 2: **The Standard OT functionality $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m, \ell)$.**

## 3 A Concrete Security Treatment of OT Extension

Prior work [15] already gives a concrete treatment of garbling from tweakable circular crHFs. As further motivation, we revisit the concrete security of OT extension via correlation-robust hashing, and present a slightly more general protocol that only assumes the underlying function to be secure against distinct inputs. We follow the angle of Guo et al. [16], who gave an asymptotic treatment, and focus on protocols implementing the standard-OT functionality $\mathcal{F}_{\mathsf{S\text{-}OT}}$ (cf.

Figure 2) from the random-OT functionality $\mathcal{F}_{\Delta\text{-ROT}}$ (cf. Figure 1), and discuss instantiations from the constructions presented below. Protocols to implement the latter functionality are known, both in the semi-honest and malicious settings [2, 18, 19].

Modeling 2PC. We give a concrete security definition of (stand-alone) 2PC malicious security. This is a fairly straightforward adaptation of the asymptotic treatment [13], with some notational simplifications that narrow the scope.

Ideal functionalities proceed in rounds of simultaneous inputs, for which they produce (simultaneously) outputs. A functionality $\mathcal{F}$ offers three interfaces – two are to the players $\mathsf{P}_A$ and $\mathsf{P}_B$, and the third to the adversary $\mathcal{A}$. Here, we are specifically interested in running a (synchronous) two-party hybrid-model protocol $\Pi = (\Pi_A, \Pi_B)$ accessing a functionality $\mathcal{F}$ and implementing a target functionality $\mathcal{G}$. In each round, either (1) one party sends a message to the other party, or (2) they simultaneously interact with the functionality $\mathcal{G}$. We will distinguish now the *real-world* from the *ideal-world* execution. Both of them are parameterized by a set $\mathsf{Corr} \subsetneq \{\mathsf{P}_A, \mathsf{P}_B\}$ of corrupted parties controlled by the adversary $\mathcal{A}$. (The case $\mathsf{Corr} = \{\mathsf{P}_A, \mathsf{P}_B\}$ is uninteresting, but the case $\mathsf{Corr} = \emptyset$ is needed to define correctness.)

- **Real-world execution.** Initially, we fix the input(s) $x_{\overline{\mathsf{Corr}}}$ of the uncorrupted parties (remember both parties could be uncorrupted). Then, we run the protocol, and the adversary (1) can choose the messages meant to be sent by the corrupted player (if any) in the protocol $\Pi$, (2) has access to the player's interface in $\mathcal{F}$, and (3) it has access to $\mathcal{A}$'s dedicated interface in $\mathcal{F}$, as well as to all messages sent in the protocol. Finally, the adversary outputs some value $z$. We let $\mathsf{REAL}^{\Pi,\mathcal{F}}_{\mathsf{Corr},\mathcal{A}}(x_{\overline{\mathsf{Corr}}}) = (x_{\overline{\mathsf{Corr}}}, z)$.
- **Ideal-world execution.** Here, we instead supply the input(s) $x_{\overline{\mathsf{Corr}}}$ to the corresponding interfaces of $\mathcal{G}$, and the adversary $\mathcal{A}$ interacts with a simulator $\mathcal{S}$. The latter can use $\mathcal{G}$'s interface for corrupted parties (if any), as well as the adversarial interface. Again $\mathcal{A}$ will produce an output $z$, and define $\mathsf{IDEAL}^{\mathcal{G}}_{\mathsf{Corr},\mathcal{A},\mathcal{S}}(x_{\overline{\mathsf{Corr}}}) = (x_{\overline{\mathsf{Corr}}}, z)$.

We then define

$$\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})-\mathsf{mpc}}_{\Pi,\mathsf{Corr}}(\mathcal{A}, \mathcal{D}, \mathcal{S}, x_{\overline{\mathsf{Corr}}}) = \Pr\left[\mathcal{D}(\mathsf{REAL}^{\Pi,\mathcal{F}}_{\mathsf{Corr},\mathcal{A}}(x_{\overline{\mathsf{Corr}}})) = 1\right] - \Pr\left[\mathcal{D}(\mathsf{IDEAL}^{\mathcal{G}}_{\mathsf{Corr},\mathcal{A},\mathcal{S}}(x_{\overline{\mathsf{Corr}}})) = 1\right] .$$

Intuitively, we want to show that for any $\mathcal{A}$, there exists some $\mathcal{S}$, such that $\mathbf{Adv}^{\mathsf{mpc}}_{\mathcal{F},\mathcal{G},\Pi,\mathsf{Corr}}(\mathcal{A}, \mathcal{D}, \mathcal{S}, x_{\overline{\mathsf{Corr}}})$ is "negligible." (Of course, we aim for a concrete bound, which we aim to optimize.)

A protocol. We present and analyze a protocol implementing $\mathcal{F}_{\mathsf{S\text{-}OT}}(m, \ell)$ from $\mathcal{F}_{\Delta\text{-ROT}}(m, k)$ using a (tweakable) correlation-robust hash function $H : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^\ell$. The protocol differs from the "standard approach" in that $H$ is only required to be secure for *distinct* inputs – this will be instrumental for our instantiation below, as we give high-security constructions which are only secure if the inputs are distinct. The modification is in fact very simple, and relies on using a $\epsilon$-almost XOR universal hash function $\mathsf{AXU} : \mathcal{K} \times [m] \to \{0,1\}^k$, for a small $\epsilon$. Then, in the $i$-th OT instance, we invoke $H$ as $H(x \oplus \mathsf{AXU}(K, i), t_i)$ on any input $x$, where $t_i$ is a tweak associated with the $i$-th instance. The key $K$ is actually publicly generated by the sender, and revealed to the receiver – the only requirement is that it is chosen after the inputs $x$ to $H$ are determined.

The resulting protocol $\Pi_{\mathcal{OT}}^{m,k,\ell}$ is described in Figure 3. The description assumes that there exists a set of usable tweaks $T = \{t_1, \dots, t_m\} \subseteq \{0,1\}^n$ for the construction – depending on the instantiation, this set $T$ may need to be chosen carefully.

Security of the protocol. Security against a corrupt sender is trivial and holds perfectly. The next theorem characterizes the *sender security* of Protocol $\Pi_{\mathsf{OT}}^{m,k,\ell}$, i.e., the case $\mathsf{Corr} = \{\mathsf{P}_B\}$ where the receiver is corrupted. We target ideal-model security here – i.e., the function $H$ makes calls to an ideal primitive (e.g., a random permutation), and so do $\mathcal{A}$, $\mathcal{D}$ and $\mathcal{S}$. We however assume that $P$ input to $\mathcal{A}$'s interface in $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$ does not make queries to this primitive, though the *choice* of $P$ itself *may* depend adaptively on earlier queries. (This is sufficient to handle existing $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$ protocols.)

To properly handle ideal-model security, the following theorem (proved in the full version of the paper) differs from the work of Guo et al. [16], which as far as we can tell, cannot be used for ideal-model constructions.[6] Here, we instead assume indistinguishability *even if* at the end of the ideal-model interaction, the distinguisher learns the secret shift $R$ (but is otherwise prevented from making any queries, including those to the ideal primitive) – in the ideal model, this shift is simply generated independently of the interaction. We refer to this notion as TCR$^*$ security, and we note that our proofs (as most $H$-coefficient proofs) do give bounds also for TCR$^*$ security *for free*, as we include $R$ in the transcripts.

**Theorem 1 (Sender-security).** *Let* $\mathsf{AXU} : \mathcal{K} \times [m] \to \{0,1\}^k$ *be* $\epsilon$*-almost XOR universal. For every adversary* $\mathcal{A}$*, every distinguisher* $\mathcal{D}$*, there exists a simulator* $\mathcal{S}$ *and an adversary* $\mathcal{B}$ *such that for every* $x = ((\mathbf{m}_1^0, \mathbf{m}_1^1), \dots, (\mathbf{m}_m^0, \mathbf{m}_m^1))$*,*

$$\mathbf{Adv}^{(\mathcal{F}\to\mathcal{G})-\mathsf{mpc}}_{\Pi_{\mathsf{OT}}^{m,k,\ell},\{\mathsf{P}_B\}}(\mathcal{A}, \mathcal{D}, \mathcal{S}, x) \leq \mathbf{Adv}^{\mathsf{TCR}^*}_{H,\{0,1\}^k}(\mathcal{B}) + q^2\epsilon \;, \qquad (5)$$

*where* $\mathcal{F} = \mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$ *and* $\mathcal{G} = \mathcal{F}_{\mathsf{S}\text{-}\mathsf{OT}}(m,\ell)$*. Here,* $\mathcal{B}$ *makes* $m$ distinct *queries, for distinct tweaks. Further, in an ideal model, the number of ideal-primitive queries* $p_{\mathcal{B}}$ *of* $\mathcal{B}$ *satisfies* $p_{\mathcal{B}} = 2(p_{\mathcal{A}} + p_{\mathcal{D}}) + p_H$*, where* $p_{\mathcal{A}}$ *and* $p_{\mathcal{D}}$ *are the number of ideal-primitive queries of* $\mathcal{A}$ *and* $\mathcal{D}$*'s, respectively, and* $p_H$ *is the number of ideal-primitive queries in one evaluation of* $H$*.*

[6] Their proof, for a slightly simpler protocol, is in the standard model and tacitly assumes *non-uniform* tweakable crHF security. Roughly, their proof needs to build an adversary $\mathcal{B}$ for keys chosen from a set $\mathcal{R}$, but this set needs to be fixed non-uniformly – this is problematic in ideal models, because the choice of $\mathcal{R}$ itself depends on the ideal primitive.

**Protocol $\Pi_{\mathsf{OT}}^{m,k,\ell}$:**

Inputs:

- Player $\mathsf{P}_A$: $(\mathbf{m}_1^0, \mathbf{m}_1^1), \ldots, (\mathbf{m}_m^0, \mathbf{m}_m^1)$, where $\mathbf{m}_i^b \in \{0,1\}^\ell$ for all $i \in [m]$ and $b \in \{0,1\}$.
- Player $\mathsf{P}_B$: $(x_1, \ldots, x_m) \in \{0,1\}^m$.

Protocol:

**(1)** Player $\mathsf{P}_A$ chooses $\Delta \xleftarrow{\$} \{0,1\}^k$, and inputs $\Delta$ to $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$. Player $\mathsf{P}_B$ inputs $\perp$ to $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$.

**(2)** Player $\mathsf{P}_A$ inputs $\perp$ to $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$ if $\mathsf{abort}$ was not output in **(1)**. Player $\mathsf{P}_B$ inputs $(x_1, \ldots, x_m)$ to $\mathcal{F}_{\Delta\text{-}\mathsf{ROT}}(m,k)$. The players receive respectively $\{\mathbf{a}_i\}_{i\in[m]}$ and $\{\mathbf{b}_i\}_{i\in[m]}$ such that $\mathbf{a}_i \oplus \mathbf{b}_i = \Delta \cdot x_i$ for all $i \in [m]$.

**(3)** Player $\mathsf{P}_A$ chooses $K \xleftarrow{\$} \mathcal{K}$, and computes, for all $i \in [m]$,

$$\mathbf{c}_i^0 \leftarrow H(\mathbf{a}_i \oplus \mathsf{AXU}(K,i), t_i) \oplus \mathbf{m}_i^0;$$
$$\mathbf{c}_i^1 \leftarrow H(\mathbf{a}_i \oplus \Delta \oplus \mathsf{AXU}(K,i), t_i) \oplus \mathbf{m}_i^1\ .$$

It then sends $K, \mathbf{c}_1^0, \mathbf{c}_1^1, \ldots, \mathbf{c}_m^0, \mathbf{c}_m^1$ to $\mathsf{P}_B$

**(4)** Player $\mathsf{P}_B$ then computes

$$\mathbf{m}_i^{x_i} \leftarrow H(\mathbf{b}_i \oplus \mathsf{AXU}(K,i), t_i) \oplus \mathbf{c}_i^{x_i}$$

for all $i \in [m]$, and outputs $(\mathbf{m}_1^{x_1}, \ldots, \mathbf{m}_m^{x_m})$. Player $\mathsf{P}_A$ outputs $\perp$.

Fig. 3: **The OT Protocol.**

Instantiation. We give an instantiation of $\Pi_{\mathcal{OT}}^{n,m,n}$ making two permutation calls per instance, using the FPTP1 construction below and Theorem 3. To this end, we also choose a random set of tweaks $T$ of size $m$, for which $\Phi(T) = O(\sqrt{nm})$, except with probability $O(1/2^n)$ (cf. Section 2.5) – this could be fixed a-priori, generated heuristically, and/or chosen randomly in the protocol (in which case the tweaks $t_i$ would be sent along). Moreover, we have efficient constructions of $\mathsf{AXU}$ with $\epsilon = 1/2^n$, and the bound thus takes the form $O((\sqrt{m}p + m^2)n/2^n)$, where $p$ is the sum of the numbers of queries to $\pi$ by $\mathcal{A}$ and $\mathcal{D}$. The construction makes two calls to the permutation per OT instance.

This should be compared with an instantiation using directly a monolithic random oracle (as we claimed in the introduction), or the ideal-cipher construction from [15] – this would achieve security of $O(p/2^n)$, however under a stronger assumption. The term $m^2n/2^n$ in our bounds is not very relevant – we would never be able to scale to $m$'s large enough to be a concern. However, it is a great question to see whether one can improve upon the $\sqrt{m}$ degradation without increasing (or at least, without increasing by much) the number of permutation calls per OT instance.

Random tweaks extension. The usage of random tweaks can increase bandwidth (if the sender chooses them, then they need to be sent over to the receiver). But note that for our context, tweaks are used only for concrete security, and since inputs are already guaranteed to be distinct, we can actually re-use tweaks through a small number $r$ of instances (say $r = 64$), and this would lead to a factor $r$ in the bound, but only a $1/r$ increase in communication complexity.

## 4 Hash Function Using One Permutation Call

We consider the following hash function, based on one permutation call and one non-linear operation $\otimes$. Let $n \in \mathbb{N}$, and let $\pi \in \mathrm{Perm}(n)$. One can consider a generic hash function construction $H\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ as

$$H[\pi](m,t) = \pi(m \otimes t) \oplus m \otimes t\,, \tag{6}$$

The security is considered against distinguishers making arbitrary input messages to the construction oracle. For simplicity, we consider the single user security ($u = 1$).

**Theorem 2.** *Let $n \in \mathbb{N}$, and consider $H\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ based on permutation $\pi \xleftarrow{\$} \mathrm{Perm}(n)$. For any distinguisher $\mathcal{D}$ making at most $q$ construction queries, and at most $p$ primitive queries to $\pi^{\pm}$. When the input tweaks are chosen from $\{0,1\}^n \setminus \{0^n\}$ for TCR security, and chosen from $\{0,1\}^n \setminus \{0^n, 0^{n-1}1\}$ for TCCR security, then we have*

$$\mathbf{Adv}^{\mathrm{TCR}}_{H,\mathcal{R}}(\mathcal{D}),\, \mathbf{Adv}^{\mathrm{TCCR}}_{H,\mathcal{R}}(\mathcal{D}) \le \frac{2qp}{|\mathcal{R}|} + \frac{q^2}{2\,|\mathcal{R}|} + \frac{q^2}{2^{n+1}}\,. \tag{7}$$

*Proof.* We only look at the TCCR security in the proof. Let $R \xleftarrow{\$} \mathcal{R}$, $\pi \xleftarrow{\$} \mathrm{Perm}(n)$, and $f \xleftarrow{\$} \mathrm{Func}(2n+1, n)$. Consider any distinguisher $\mathcal{D}$ that has access to two oracles: $(\mathcal{O}_R, \pi^{\pm})$ in the real world with

$$\mathcal{O}_R(w,t,b) = H[\pi](w \oplus R, t) \oplus bR = \pi((w \oplus R) \otimes t) \oplus (w \oplus R) \otimes t \oplus bR\,,$$

or $(f, \pi^{\pm})$ in the ideal world. We require that $\mathcal{D}$ is computational unbounded and deterministic. The distinguisher makes $q$ construction queries to $\mathcal{O}_R$ or $f$ such that $t \neq 0^n$ and $t \oplus 0^{n-1}1 \neq 0^n$, and these are summarized in a transcript of the form $\tau_0 = \{(w^{(1)}, t^{(1)}, b^{(1)}, z^{(1)}), \ldots, (w^{(q)}, t^{(q)}, b^{(q)}, z^{(q)})\}$. It also makes $p$ primitive queries to $\pi^{\pm}$, and these are summarized in transcripts $\tau_1$. We assume that $\tau_0$ and $\tau_1$ do not contain duplicate elements. After $\mathcal{D}$'s interaction with the oracles, but before it outputs its decision, we disclose the random value $R$ to the distinguisher. In the real world, this is the randomness for the message input of construction. In the ideal world, $R$ is a dummy value that is drawn uniformly at random. The complete view is denoted by $\tau = (\tau_0, \tau_1, R)$.

**Bad Events.** We say that $\tau \in \mathcal{T}_{\mathrm{bad}}$ if and only if there exist construction queries $(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}), (w^{(j')}, t^{(j')}, b^{(j')}, z^{(j')}) \in \tau_0$ such that $j \neq j'$, and primitive queries $(u,v),(u',v')\in\tau_1$ such that one of the following conditions holds:

$\mathrm{bad}_1: (w^{(j)}\oplus R)\otimes t^{(j)} = u\,,$

$\mathrm{bad}_2: (w^{(j)}\oplus R)\otimes t^{(j)}\oplus z^{(j)}\oplus b^{(j)}R = v\,,$

$\mathrm{bad}_3: (w^{(j)}\oplus R)\otimes t^{(j)} = (w^{(j')}\oplus R)\otimes t^{(j')}\,,$

$\mathrm{bad}_4: (w^{(j)}\oplus R)\otimes t^{(j)}\oplus z^{(j)}\oplus b^{(j)}R = (w^{(j')}\oplus R)\otimes t^{(j')}\oplus z^{(j')}\oplus b^{(j')}R\,.$

Note that for any attainable transcript $\tau$, $\tau\notin T_{bad}$ implies that $\tau$ is a good transcript.

**$\mathbf{Pr}[\boldsymbol{X_{\mathcal{P}}}\in\boldsymbol{\mathcal{T}_{\mathrm{bad}}}]$.** We want to bound the probability that an ideal world transcript $\tau$ satisfies either of $\mathrm{bad}_1$-$\mathrm{bad}_4$. Therefore, the probability that $\tau\in\mathcal{T}_{\mathrm{bad}}$ is given by

$$\Pr[\tau\in\mathcal{T}_{\mathrm{bad}}]\le\sum_{i=1}^{4}\Pr[\mathrm{bad}_i]\,.$$

We first consider the bad event $\mathrm{bad}_1$, which we rewrite as

$$w^{(j)}\otimes t^{(j)}\oplus u = R\otimes t^{(j)}\,.$$

Since we have $t\neq 0^n$, and $R\leftarrow\mathcal{R}$ is a dummy value generated independently of $\tau_0$ and $\tau_1$, the probability that the above equation holds for fixed $j$ and $(u,v)$ is $1/|\mathcal{R}|$. Summed over all $q$ possible $j$'s and all $p$ possible $(u,v)$'s, we have

$$\Pr[\mathrm{bad}_1]\le\frac{qp}{|\mathcal{R}|}\,.$$

The same reasoning applies for $\mathrm{bad}_2$, which we rewrite as

$$w^{(j)}\otimes t^{(j)}\oplus z^{(j)}\oplus v = (t^{(j)}\oplus 0^{n-1}b^{(j)})\otimes R\,.$$

Since we have $t\neq 0^n$ and $t\oplus 0^{n-1}1\neq 0^n$, the probability that the above equation holds for fixed $j$ and $(u,v)$ is $1/|\mathcal{R}|$ as before. Summed over all $q$ possible $j$'s and all $p$ possible $(u,v)$'s, we have

$$\Pr[\mathrm{bad}_2]\le\frac{qp}{|\mathcal{R}|}\,.$$

Now, we consider the bad event $\mathrm{bad}_3$, which we rewrite as

$$w^{(j)}\otimes t^{(j)}\oplus w^{(j')}\otimes t^{(j')} = (t^{(j)}\oplus t^{(j')})R\,.$$

Since we have $t\neq 0^n$, if $t^{(j)}=t^{(j')}$, then we must have $w^{(j)}\neq w^{(j')}$, in that case the above equation never holds. If $t^{(j)}\neq t^{(j')}$, then since $R\leftarrow\mathcal{R}$ is a dummy value generated independently of $\tau_0$ and $\tau_1$, the probability that the above equation holds for fixed $j \neq j'$ is $1/|\mathcal{R}|$. Summing over all possible choices of $j \neq j'$, we have

$$\Pr[\mathrm{bad}_3] \leq \binom{q}{2} \frac{1}{|\mathcal{R}|} \,.$$

The same reasoning applies for $\mathrm{bad}_4$, which we rewrite as

$$w^{(j)} \otimes t^{(j)} \oplus w^{(j')} \otimes t^{(j')} \oplus (t^{(j)} \oplus t^{(j')} \oplus 0^{n-1}b^{(j')} \oplus 0^{n-1}b^{(j)})R = z^{(j)} \oplus z^{(j')} \,.$$

Since the values $z^{(j)}$ and $z^{(j')}$ are generated uniform and independent in the ideal world, the probability that the above equation holds for fixed $j \neq j'$ is $1/2^n$. Summing over all possible choices of $j \neq j'$, we have

$$\Pr[\mathrm{bad}_4] \leq \binom{q}{2} \frac{1}{2^n} \,.$$

Summing the these probabilities, we get

$$\Pr[\tau \in \mathcal{T}_{\mathrm{bad}}] \leq \frac{2qp}{|\mathcal{R}|} + \frac{q^2}{2\,|\mathcal{R}|} + \frac{q^2}{2^{n+1}} \,. \tag{8}$$

**$\Pr[X_{\mathcal{O}} = \tau]/\Pr[X_{\mathcal{P}} = \tau]$.** Consider an attainable transcript $\tau \in \mathcal{T}_{\mathrm{good}}$. To compute $\Pr[X_{\mathcal{O}} = \tau]$ and $\Pr[X_{\mathcal{P}} = \tau]$, it suffices to compute the probability of oracles that could result in view $\tau$. We first consider the ideal world $\mathcal{P}$, and obtain

$$\Pr[X_{\mathcal{P}} = \tau] = \frac{1}{|\mathcal{R}|} \cdot \frac{(2^n - p)!}{2^n!} \cdot \frac{2^{n(2^{2n+1} - q)}}{2^{n2^{2n+1}}} = \frac{1}{|\mathcal{R}|} \cdot \frac{1}{(2^n)_p} \cdot \frac{1}{2^{nq}} \,.$$

The first term corresponds to the number of randomly drawn $R$ values; the second term is the ratio of public random permutations $\pi$ compliant with $\tau_1$; and the last term is the ratio of random functions $f \in \mathrm{Func}(2n+1, n)$ compliant with $\tau_0$.

Similarly we say that a real world oracle $\mathcal{O}$ is compatible with $\tau$ if it is compatible with $\tau_0$ and $\tau_1$. We have

$$\Pr[X_{\mathcal{O}} = \tau] = \frac{1}{|\mathcal{R}|} \cdot \frac{1}{(2^n)_p} \cdot \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n) \colon \mathcal{O}_R[\pi] \vdash \tau_0 \mid \pi \vdash \tau_1] \,.$$

As before, the first term corresponds to the number of randomly drawn $R$ values; the second term is the ratio of public random permutations $\pi$ compliant with $\tau_1$; and the last term is the ratio of $\mathcal{O}_R[\pi]$ compliant with $\tau_0$, given that $\pi$ compliant with $\tau_1$.

Define $\rho(\tau) = \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n) \colon \mathcal{O}_R[\pi] \vdash \tau_0 \mid \pi \vdash \tau_1]$, we obtain

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} = 2^{nq} \rho(\tau) \,. \tag{9}$$

Since $\tau$ is good, all values $\sigma(w^{(j)} \oplus R) \otimes t^{(j)}$ for $(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in \tau_0$ are distinct by $\neg\text{bad}_3$, and are also distinct from all values $u$ for $(u, v) \in \tau_1$ by $\neg\text{bad}_1$. Similarly, all values $\sigma(w^{(j)} \oplus R) \otimes t^{(j)} \oplus z^{(j)} \oplus b^{(j)}R$ for $(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in \tau_0$ are distinct by $\neg\text{bad}_4$, and are also distinct from all values $v$ for $(u, v) \in \tau_1$ by $\neg\text{bad}_2$. This clearly implies that

$$\rho(\tau) = \frac{1}{(2^n - p)_q} \, ,$$

Processing further from (9), we have

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} = \frac{2^{nq}}{(2^n - p)_q} \geq \frac{2^{nq}}{2^{nq}} = 1 \, . \; \square$$

## 5 Hash Function Using Two Permutation Calls

We consider the FPTP construction (Feed-forward Permutation- Tweak-Permutation), based on two permutations. Let $n \in \mathbb{N}$, let $\pi_1, \pi_2 \in \text{Perm}(n)$, and let $\sigma\colon \{0,1\}^n \to \{0,1\}^n$ be a linear orthomorphism. One can consider a generic hash function construction $\text{FPTP}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ as

$$\text{FPTP}[\pi_1, \pi_2](m, t) = \pi_2(\pi_1(\sigma(m)) \oplus t) \oplus \sigma(m) \, . \tag{10}$$

We will consider the construction for two variants: FPTP2 for the case where $\pi_1, \pi_2$ are independent in the full version of the paper, and FPTP1 for the case where $\pi_1, \pi_2$ are identical in Section 5.1. For the both cases, security is considered against distinguishers making distinct or uniform independent input messages to the construction oracle for the case of single user, and against distinguishers making uniform independent input messages to the construction oracles for the case of multi-user. The single user security proof of FPTP1 is given in Section 5.3.

### 5.1 FPTP based on Two Same Permutations

We prove the security of FPTP1 where $\pi_1 = \pi_2$. Let $n \in \mathbb{N}$, and consider the given set $T$ of the tweaks such that the size of $T$ is $\ell$ and $\ell \leq q$ (since there are $q$ different tweaks when $B = 1$). We present the following result against distinguishers making distinct input messages to the construction oracle for $u = 1$ (single user security). Recall that $\Phi(A) = \max\left\{2^n \left|\widehat{1}_A(\alpha)\right| : \alpha \in \{0,1\}^n, \alpha \neq 0^n\right\}$ (see Section 2.0).

**Theorem 3.** *Let* $n \in \mathbb{N}$*, and consider* $\text{FPTP1}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *based on permutation* $\pi \xleftarrow{\$} \text{Perm}(n)$*, where the input tweaks are chosen from the set* $T$*. For any distinguisher* $\mathcal{D}$ *making at most* $q$ *construction queries, at most* $B$ *construction queries per tweak, and at most* $p$ *primitive queries to* $\pi^{\pm}$*.*

*(a) When $\mathcal{D}$ makes $q$ construction queries with distinct input messages, we have*

$$\mathbf{Adv}^{\mathrm{TCCR}}_{\mathrm{FPTP1},\mathcal{R}}(\mathcal{D}) \leq \frac{7}{2^n} + \frac{(2B+1)qp^2}{2^n\,|\mathcal{R}|} + \frac{p\sqrt{3nq}}{|\mathcal{R}|} + \frac{2B\Phi(T)p}{|\mathcal{R}|} + \frac{6nq^2}{|\mathcal{R}|} + \frac{9q^2}{2^{n+1}} + \frac{4q(p+q)(p+2q)}{2^{2n}}\,. \quad (11)$$

*(b) When $\mathcal{D}$ makes $q$ construction queries with uniform independent input messages, $\mathbf{Adv}^{\mathrm{TCCR}}_{\mathrm{FPTP1},\mathcal{R}}(\mathcal{D})$ is the same as the case of distinct input messages, except that there is an additional $q^2/2^{n+1}$ term.*

Note that (11) is dominated by the terms $2B\Phi(T)p/\,|\mathcal{R}|+9q^2/2^{n+1}$. For $|\mathcal{R}| = 2^n$, and a carefully chosen set $T$ such that $\Phi(T) \leq \sqrt{q}$ (like the one mentioned in the introduction), the security bound in (11) matches with the asymptotic bound given in the abstract and introduction.

*Proof.* The proof of (a) is given in Section 5.3. The proof of (b) follows straightforwardly from Theorem 3 (a), and the fact that two uniform independent values collide with probability at most $q^2/2^{n+1}$ by the birthday bound. □

Let $n \in \mathbb{N}$, and consider the given set $T = T_1 \cup \cdots \cup T_u \subseteq \{0,1\}^n$ of the tweaks such that the size of $T = \ell$ and $\ell \leq q$. We present the following result against distinguishers making uniform independent input messages to the construction oracles for $u > 1$ (multi-user security).

**Theorem 4.** *Let $n \in \mathbb{N}$, and consider* $\mathrm{FPTP1}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *based on permutation $\pi \xleftarrow{\$} \mathrm{Perm}(n)$, where the input tweaks of $i$-th oracle are chosen from the set $T_i$. For any distinguisher $\mathcal{D}$ making at most $q/u$ construction queries with uniform independent input messages to each of its $u$ construction oracles, at most $B$ construction queries per tweak across all oracles, and at most $p$ primitive queries to $\pi^{\pm}$, we have*

$$\mathbf{Adv}^{\mathrm{miTCCR}}_{\mathrm{FPTP1},\mathcal{R}}(\mathcal{D}) \leq \frac{7}{2^n} + \frac{(2B+1)qp^2}{2^n\,|\mathcal{R}|} + \frac{p\sqrt{3nq}}{|\mathcal{R}|} + \frac{2B\Phi(T_1 \cup \cdots \cup T_u)p}{|\mathcal{R}|} + \frac{6nq^2}{|\mathcal{R}|} + \frac{10q^2}{2^{n+1}} + \frac{q^2p}{|\mathcal{R}|^2} + \frac{4q(p+q)(p+2q)}{2^{2n}}\,. \quad (12)$$

The proof is given in the full version of the paper.

We can extend the FPTP construction to process the input $w \otimes t$ instead of $w$. For plain (non-circular) TCR security, this would give us security under arbitrary inputs. Let call FPTP1* the FPTP1 construction using the input $w \otimes t$, then the TCR security of FPTP1* is given in Theorem 5.

**Theorem 5.** *Let $n \in \mathbb{N}$, and consider* $\mathrm{FPTP1}^*\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *based on permutation $\pi \xleftarrow{\$} \mathrm{Perm}(n)$, where the input tweaks are chosen from the set $T$. For any distinguisher $\mathcal{D}$ making at most $q$ construction queries, at most*

*$B$ construction queries per tweak, and at most $p$ primitive queries to $\pi^{\pm}$. We have*

$$\mathbf{Adv}^{\mathrm{TCR}}_{\mathrm{FPTP1}^*,\mathcal{R}}(\mathcal{D}) \leq \frac{7}{2^n} + \frac{(2B+1)qp^2}{2^n\,|\mathcal{R}|} + \frac{p\sqrt{3nq}}{|\mathcal{R}|} + \frac{2B\Phi(T)p}{|\mathcal{R}|} + \frac{q^2(12n+1)}{2\,|\mathcal{R}|} + \frac{9q^2}{2^{n+1}} + \frac{4q(p+q)(p+2q)}{2^{2n}}\,. \quad (13)$$

*Proof (Sketch).* The proof of Theorem 5 is very similar to the proof of Theorem 3, but with a few minor differences. First of all, the bad transcripts analysis remains basically the same, except that $w \otimes t$ needs to be considered instead of $w$, and this can be modified in a straightforward way. However, there is an additional bad event, namely

$$\exists (w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \neq (w^{(j')}, t^{(j')}, b^{(j')}, z^{(j')}) \in \tau_0 \colon (w^{(j)} \oplus R) \otimes t^{(j)} = (w^{(j')} \oplus R) \otimes t^{(j')}\,.$$

This is the same event as $\mathrm{bad}_3$ of the one permutation call construction in (6), hence this event will lead to an extra term $\binom{q}{2}/\mathcal{R}$ in the final bound. Finally, the ratio analysis remains roughly the same. □

### 5.2 Balls-into-Bins Lemmas

Before we turn to our proofs, we state and prove some generic balls-into-bins lemmas for the setting where an adversary queries a random permutation. These may be of independent interest. We rely below on the following generalized version of the Chernoff bound [17,22], which does not need to assume independence, and instead only requires a weaker direct-product condition.

**Theorem 6 (Generalized Chernoff Bound).** *Let $X_1, \ldots, X_n \in \{0,1\}$ be random variables such that, for some $\delta \in [0,1]$, $\Pr\left[\bigwedge_{i \in S} X_i = 1\right] \leq \delta^{|S|}$ for every $S \subseteq [n]$. Then, for any $\gamma \in [\delta, 1]$, $\Pr\left[\sum_{i=1}^{n} X_i \geq \gamma n\right] \leq e^{-nD(\gamma \,\|\, \delta)}$, where $D(\gamma \,\|\, \delta) = \gamma \ln\left(\frac{\gamma}{\delta}\right) + (1-\gamma)\ln\left(\frac{1-\gamma}{1-\delta}\right)$ is the relative binary entropy function.*

THE INPUT-OUTPUT BALLS-INTO-BINS LEMMA. We assume that an adversary $\mathcal{A}$ makes $p$ adaptive queries to a random permutation $\pi \overset{\$}{\leftarrow} \mathrm{Perm}(n)$, which then defines a transcript $\tau = ((u_1, v_1), \ldots, (u_p, v_p))$ of input-output pairs, i.e., a pair $(u_i, v_i)$ indicates that either $\pi(u_i)$ was queried, returning $v_i$ or $\pi^{-1}(v_i)$ was queried, returning $u_i$. (Without loss of generality, we assume that these queries are non-redundant, i.e., $u_1, \ldots, u_p$ are distinct.) Further, let $\sigma, \rho \in \mathrm{Perm}(n)$ be *fixed* permutations. We then assign each query $(u_i, v_i)$ to a bin labeled by $\sigma(u_i) \oplus \rho(v_i)$. (I.e., there are $2^n$ possible bins.) We also define $L^{\mathsf{io}}$ as the max load of the bins, and show it is small with high probability. The proof is similar to that of classical balls-into-bins lemmas, but we use Theorem 6 to deal with the adversary's adaptivity and the permutation structure of outputs.

**Lemma 4 (Input-output Balls-into-Bins).** *For every $p \leq 2^{n-1}$, let $\mathcal{A}$ be any $p$-query adversary $\mathcal{A}$ querying an $n$-bit random permutation, and let $L^{\mathsf{io}}$ be as above. Then, for any $\epsilon > 0$, we have $\Pr\left[L^{\mathsf{io}} \geq n\ln(2) + \ln(1/\epsilon) + 2\right] \leq \epsilon$.*

The proof is given in the full version of the paper.

The XOR Balls-into-bins Lemma. We also consider a more complex setting where each (ordered) query *pair* $i, j$ is assigned to one of $(2^n-1)^2$ bins, each denoted as $B_{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}}$, where $\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}} \in \{0,1\}^n \setminus \{0^n\}$. In particular, we fix *four* permutations $\sigma, \sigma', \rho, \rho' \in \mathrm{Perm}(n)$, and the query pair $(i,j)$ is added to the bin with $\Delta_{\mathsf{in}} = \sigma(u_i) \oplus \sigma'(u'_i)$ and $\Delta_{\mathsf{out}} = \rho(v_i) \oplus \rho'(v'_i)$. We define now $L^{\mathsf{xor}}$ as the max load of one of the bins.

We want to show a bound on the load, similar to Lemma 4. The challenge here is that the $p(p-1)$ ball assignments are (1) highly dependent, and (2) defined by an adaptive process, where $\mathcal{A}$ chooses some of the $u_i$'s and of the $v_i$'s. The following lemma shows that, however, their behavior is similar to $p(p-1)$ independent balls thrown into $(2^n-1)^2$ bins.

**Lemma 5 (XOR Balls-into-Bins).** *For every $p \leq 2^{n-1}$, let $\mathcal{A}$ be any $p$-query adversary $\mathcal{A}$ querying an $n$-bit random permutation, and let $L^{\mathsf{xor}}$ be defined as above. Then, for any $\epsilon > 0$, we have* $\Pr\left[L^{\mathsf{xor}} \geq 4n\ln(2) + 2\ln(1/\epsilon) + 4\right] \leq 2\epsilon$.

Before we turn to the proof, we note that in the symmetric case where $\sigma = \sigma'$ and $\rho = \rho'$, it is often enough to count unordered pairs $\{i,j\}$ as ball throws, and one can then replace $2\epsilon$ by $\epsilon$, and $4n\ln(2)$ by $2n\ln(2)$.

*Proof.* Let us fix any $\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}} \in \{0,1\}^n \setminus \{0^n\}$, and one assume $\mathcal{A}$ generates the transcript $\tau = ((u_1,v_1),\ldots,(u_p,v_p))$ of non-redundant queries to the random permutation $\pi$. We are interested in the random variable

$$Z^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} = \left|\{(i,j) \mid j < i,\ \sigma(u_i) \oplus \sigma'(u_j) = \Delta_{\mathsf{in}},\ \rho(v_i) \oplus \rho'(v_j) = \Delta_{\mathsf{out}}\}\right| \ .$$

Also, define $Z_i^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}}$ as the indicator random variable, which is 1 if there exists $j < i$ such that $\sigma(u_i) \oplus \sigma'(u_j) = \Delta_{\mathsf{in}}$ and $\rho(v_i) \oplus \rho'(v_j) = \Delta_{\mathsf{out}}$. (It is 0 otherwise.) Then, note that $Z^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} = \sum_{i=1}^{p} Z_i^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}}$, because for each query $(u_i, v_i)$, there is at most one earlier query $(u_j, v_j)$ such that $\sigma(u_i) \oplus \sigma'(u_j) = \Delta_{\mathsf{in}}$ and $\rho(v_i) \oplus \rho'(v_j) = \Delta_{\mathsf{out}}$. Because $p < 2^{n-1}$, and the queries are guaranteed not to be redundant, we have

$$\Pr\left[Z_i^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} = 1 \mid Z_1^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} = b_1, \ldots, Z_{i-1}^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} = b_{i-1}\right] \leq \frac{2}{2^n} \ , \tag{14}$$

for any $b_1, \ldots, b_{i-1} \in \{0,1\}$. To see this, assume the $i$-th query is in the forward direction, for some $u_i$. Then $Z_i^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} = 1$ if and only if there exists $j < i$ with $\sigma'(u_j) \oplus \sigma(u_i) = \Delta_{\mathsf{in}}$, and (assuming this is the case) we also have $\rho'(v_j) \oplus \rho(v_i) = \Delta_{\mathsf{out}}$. The latter happens with probability at most $1/(2^n - (i-1)) \leq 2/2^n$. For a query in the backward direction, the argument is entirely symmetric. Then, in turn, (14) implies that for any set $S \subseteq [p]$, we have

$$\Pr\left[\bigwedge_{i \in S} Z_i^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} = 1\right] \leq \left(\frac{2}{2^n}\right)^{|S|} \ .$$

Theorem 6 yields, for any $k \geq 1$, $\Pr\left[Z^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} \geq k\right] \leq e^{-p\cdot D(k/p \,\|\, 2/2^n)}$ . One can actually show that $D(\gamma \,\|\, \delta) \geq (\gamma-\delta)^2/(2\gamma)$,[7] and this yields

$$p \cdot D(k/p \,\|\, 2/2^n) \geq \frac{p^2(k/p - 2/2^n)^2}{k} \geq \frac{(k-1)^2}{k} > k-2 \,,$$

because $2/2^n \leq 1/p$. Thus, with $k = 2n\ln(2) + \ln(1/\epsilon) + 2$, we get

$$\Pr\left[\exists \Delta_{\mathsf{in}}, \Delta_{\mathsf{out}} : Z^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} \geq k\right] \leq 2^{2n} \cdot 2^{-2n} \cdot \epsilon = \epsilon \,.$$

Similarly, we can define a random variable $W^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}}$ which counts pairs $i < j$ such that $\sigma(u_i) \oplus \sigma'(u_j) = \Delta_{\mathsf{in}}$ and $\rho(v_i) \oplus \rho'(v_j) = \Delta_{\mathsf{out}}$, and conclude that $\Pr\left[W^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} \geq k\right] \leq 2^{-2n} \cdot \epsilon$. By the union bound,

$$\begin{aligned}\Pr\left[L^{\mathsf{xor}} \geq 2k\right] &\leq \Pr\left[\exists \Delta_{\mathsf{in}}, \Delta_{\mathsf{out}} : Z^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} \geq k \ \vee\ W^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} \geq k\right] \\ &\leq \Pr\left[\exists \Delta_{\mathsf{in}}, \Delta_{\mathsf{out}} : Z^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} \geq k\right] + \Pr\left[\exists \Delta_{\mathsf{in}}, \Delta_{\mathsf{out}} : W^{\Delta_{\mathsf{in}},\Delta_{\mathsf{out}}} \geq k\right] \\ &\leq 2 \cdot 2^{2n} \cdot 2^{-2n}\epsilon = 2\epsilon \,. \ \square\end{aligned}$$

### 5.3 Proof of Theorem 3 on FPTP1

Let $R \xleftarrow{\$} \mathcal{R}$, $\pi \xleftarrow{\$} \mathrm{Perm}(n)$, and $f \xleftarrow{\$} \mathrm{Func}(2n+1, n)$. Consider any distinguisher $\mathcal{D}$ that has access to two oracles: $(\mathcal{O}1_R, \pi^{\pm})$ in the real world with

$$\mathcal{O}1_R(w,t,b) = \mathrm{FPTP1}[\pi](w \oplus R, t) \oplus bR = \pi(\pi(\sigma(w \oplus R)) \oplus t) \oplus \sigma(w \oplus R) \oplus bR \,,$$

or $(f, \pi^{\pm})$ in the ideal world. We require that $\mathcal{D}$ is computational unbounded and deterministic. The distinguisher makes $q$ construction queries to $\mathcal{O}1_R$ or $f$, and $B$ construction queries per tweak. These are summarized in a transcript of the form $\tau_0 = \{(w^{(1)}, t^{(1)}, b^{(1)}, z^{(1)}), \ldots, (w^{(q)}, t^{(q)}, b^{(q)}, z^{(q)})\}$. It also makes $p$ primitive queries to $\pi^{\pm}$, and these are summarized in transcripts $\tau_1$. We assume that $\tau_0$, and $\tau_1$ do not contain duplicate elements. After $\mathcal{D}$'s interaction with the oracles, but before it outputs its decision, we disclose the random value $R$ to the distinguisher. In the real world, this is the randomness for the message input of the construction. In the ideal world, $R$ is a dummy value that is drawn uniformly at random. The complete view is denoted $\tau = (\tau_0, \tau_1, R)$.

**Bad Events.** We say that $\tau \in \mathcal{T}_{\text{bad}}$ if there exist construction queries $(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}), (w^{(j')}, t^{(j')}, b^{(j')}, z^{(j')}) \in \tau_0$ such that $j \neq j'$, and primitive queries

[7] For $\gamma \geq \delta$, by looking at the Taylor series, one can show that $f_\delta(\epsilon) = D((1+\epsilon)\delta \| \delta) \geq \epsilon^2\delta/2(1+\epsilon)$. This yields the inequality with $\epsilon\delta = (\gamma - \delta)$ and $1 + \epsilon = \gamma/\delta$.

$(u,v),(u',v') \in \tau_1$ such that one of the following conditions holds:

$$\begin{aligned}
&\mathrm{bad}_1\colon \sigma(w^{(j)} \oplus R) = u \,\wedge\, \sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R = v' \,,\\
&\mathrm{bad}_2\colon \sigma(w^{(j)} \oplus R) = u \,\wedge\, t^{(j)} \oplus v \oplus u' = 0 \,,\\
&\mathrm{bad}_3\colon t^{(j)} \oplus v \oplus u' = 0 \,\wedge\, \sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R = v' \,,\\
&\mathrm{bad}_4\colon \sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(i)}R = \sigma(w^{(j')} \oplus R) \oplus z^{(j')} \oplus b^{(i')}R \,,\\
&\mathrm{bad}_5\colon \sigma(w^{(j)} \oplus R) = u \,\wedge\, \sigma(w^{(j')} \oplus R) = u' \,\wedge\, v \oplus t^{(j)} = v' \oplus t^{(j')} \,,\\
&\mathrm{bad}_6\colon \sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R = v \,\wedge\, \sigma(w^{(j')} \oplus R) \oplus z^{(j')} \oplus b^{(j')}R = v'\\
&\qquad \wedge\, u \oplus t^{(j)} = u' \oplus t^{(j')} \,,\\
&\mathrm{bad}_7\colon \sigma(w^{(j)} \oplus R) = u \,\wedge\, v \oplus t^{(j)} = \sigma(w^{(j')} \oplus R) \,,\\
&\mathrm{bad}_8\colon \sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R = v \,\wedge\, u \oplus t^{(j)} = \sigma(w^{(j')} \oplus R) \oplus z^{(j')} \oplus b^{(j')}R \,.
\end{aligned}$$

Note that for any attainable transcript $\tau$, $\tau \notin T_{bad}$ implies that $\tau$ is a good transcript.

**$\mathbf{Pr}[\boldsymbol{X_{\mathcal{P}}} \in \boldsymbol{\mathcal{T}_{\mathrm{bad}}}]$.** We want to bound the probability that an ideal world transcript $\tau$ satisfies either of $\mathrm{bad}_1$-$\mathrm{bad}_8$. Therefore, the probability that $\tau \in \mathcal{T}_{\mathrm{bad}}$ is given by

$$\Pr[\tau \in \mathcal{T}_{\mathrm{bad}}] \le \sum_{i=1}^{8} \Pr[\mathrm{bad}_i] \,.$$

We denote

$$U = \{u \in \{0,1\}^n \colon (u,v) \in \tau_1\} \,, \quad V = \{v \in \{0,1\}^n \colon (u,v) \in \tau_1\} \,.$$

We first consider the bad event $\mathrm{bad}_1$. Using the fact that $\sigma$ is a linear orthomorphism, we can rewrite $\mathrm{bad}_1$ as

$$\sigma(w^{(j)}) \oplus u = \sigma \circ \sigma'^{-1}\left(\sigma(w^{(j)}) \oplus z^{(j)} \oplus v'\right) = \sigma(R) \,.$$

Here we have $\sigma'(x) = \sigma(x)$ when $b^{(j)} = 0$, and $\sigma'(x) = \sigma(x) \oplus x$ when $b^{(j)} = 1$. We define the sets

$$\begin{aligned}
&A^* = \{(\sigma(w^{(1)}) \oplus \sigma \circ \sigma'^{-1}(\sigma(w^{(1)}) \oplus z^{(1)}), \ldots, \sigma(w^{(q)}) \oplus \sigma \circ \sigma'^{-1}(\sigma(w^{(q)}) \oplus z^{(q)})\} \,,\\
&V' = \{\sigma \circ \sigma'^{-1}(v') : v' \in V\} \,,
\end{aligned}$$

Then, combining Lemma 3 and the result of Cogliati and Seurin [10], there are $\mu(A^*, U, V')$ possible combinations of $\sigma(w^{(j)}) \oplus \sigma \circ \sigma'^{-1}(\sigma(w^{(j)}) \oplus z^{(j)})$, $u$ and $\sigma \circ \sigma'^{-1}(v')$ that satisfy $\mathrm{bad}_1$. We denote

$$\varOmega_1 = \left| \left\{ \left(j, (u,v), (u',v')\right) \;\middle|\; \sigma(w^{(j)}) \oplus u = \sigma \circ \sigma'^{-1}\left(\sigma(w^{(j)}) \oplus z^{(j)} \oplus v'\right) \right\} \right| \,.$$

It is easy to see that $\Omega_1 = \mu(A^*, U, V')$. Note that in the ideal world, $\Omega_1$ only depends on $f$ and $\pi$. $\Omega_1$ does not depend on the randomness $R$, which is drawn uniformly at random at the end of the interaction. Hence, for any $C_1 > 0$, we have

$$\Pr[\mathrm{bad}_1] \leq \Pr[\mu(A^*, U, V') \geq C_1] + \frac{C_1}{|\mathcal{R}|}\,.$$

We thus set $C_1 = \frac{qp^2}{2^n} + p\sqrt{3nq}$ and obtain

$$\Pr[\mathrm{bad}_1] \leq \frac{2}{2^n} + \frac{qp^2}{2^n\,|\mathcal{R}|} + \frac{p\sqrt{3nq}}{|\mathcal{R}|}\,.$$

For the second bad event $\mathrm{bad}_2$, we first consider the right hand side of the bad event. Consider the given set $T \subseteq \{0,1\}^n$ of the tweaks. Then, combining Lemma 3, there are $\mu(T, U, V)$ possible combinations of $t^{(j)}$, $(u, v)$ and $(u', v')$ that satisfy the second equation of $\mathrm{bad}_2$, with

$$\mu(T, U, V) \leq \frac{qp^2}{2^n} + \Phi(T)p\,.$$

We denote

$$\Omega_2 = \left|\left\{\big(j, (u, v), (u', v')\big) \;\middle|\; t^{(j)} \oplus u' \oplus v = 0\right\}\right|\,.$$

Since there are $B$ construction queries per tweak, we have that $\Omega_2 = B\mu(T, U, V)$. We rewrite the first equation of $\mathrm{bad}_2$ as

$$\sigma(w^{(j)}) \oplus u = \sigma(R)\,.$$

By the fact that $R \leftarrow \mathcal{R}$ is a dummy value generated independently of $\tau_0$ and $\tau_1$, the probability that the first equation of $\mathrm{bad}_2$ holds for fixed $j$ and $(u, v)$ is $1/\,|\mathcal{R}|$. We have

$$\Pr[\mathrm{bad}_2] \leq \frac{Bqp^2}{2^n\,|\mathcal{R}|} + \frac{B\Phi(T)p}{|\mathcal{R}|}\,.$$

The same reasoning applies for the left hand side of $\mathrm{bad}_3$, and we rewrite the second equation of $\mathrm{bad}_3$ as

$$\sigma(w^{(j)}) \oplus z^{(j)} \oplus v' = \sigma(R) \oplus b^{(j)}R\,.$$

If $b^{(j)} = 0$, the probability that the second equation of $\mathrm{bad}_3$ holds for fixed $j$ and $(u', v')$ is $1/\,|\mathcal{R}|$ as before. If $b^{(j)} = 1$, this probability is at most $1/\,|\mathcal{R}|$ (see Lemma 1). Together, we have

$$\Pr[\mathrm{bad}_3] \leq \frac{Bqp^2}{2^n\,|\mathcal{R}|} + \frac{B\Phi(T)p}{|\mathcal{R}|}\,.$$

Now, we consider the bad event $\mathrm{bad}_4$, which we rewrite as

$$\sigma(w^{(j)} \oplus w^{(j')}) \oplus (b^{(j')} \oplus b^{(j)})R = z^{(j)} \oplus z^{(j')} \,.$$

Since the values $z^{(j)}$ and $z^{(j')}$ are generated uniformly and independent in the ideal world, the probability that the above equation holds for fixed $j \neq j'$ is $1/2^n$. Summing over all possible choices of $j \neq j'$, we have

$$\Pr[\mathrm{bad}_4] \leq \binom{q}{2} \frac{1}{2^n} \,.$$

Next, we consider the bad events $\mathrm{bad}_5$ and $\mathrm{bad}_6$. The bad event $\mathrm{bad}_5$ implies

$$u \oplus u' = \sigma(w^{(j)}) \oplus \sigma(w^{(j')}) \,\wedge\, v \oplus v' = t^{(j)} \oplus t^{(j')} \,.$$

Now we take $\mathit{\Delta}_{\mathsf{in}} = \sigma(w^{(j)}) \oplus \sigma(w^{(j')})$ and $\mathit{\Delta}_{\mathsf{out}} = t^{(j)} \oplus t^{(j')}$, and by applying Lemma 5, we define $L^{\mathsf{xor}}$ as the max load of the bin $B_{\mathit{\Delta}_{\mathsf{in}},\mathit{\Delta}_{\mathsf{out}}}$. Hence, for any $C_5 > 0$, and by the fact that $R \leftarrow \mathcal{R}$ is a dummy value generated independently of $\tau_0$ and $\tau_1$, the probability that the first two equations of $\mathrm{bad}_5$ hold for a fixed $(j, j')$ couple is $1/|\mathcal{R}|$. By a union bound over all possible choices of $j \neq j'$, we have

$$\Pr[\mathrm{bad}_5] \leq \Pr\left[L^{\mathsf{xor}} \geq C_5\right] + \binom{q}{2} \frac{C_5}{|\mathcal{R}|} \,,$$

Thus, with $C_5 = 2n\ln(2) + \ln(1/\epsilon) \leq 3n$ and with $\epsilon = 1/2^n$, we have

$$\Pr[\mathrm{bad}_5] \leq \frac{1}{2^n} + \binom{q}{2} \frac{3n}{|\mathcal{R}|} \,.$$

For $\mathrm{bad}_6$, when $b^{(j)} \oplus b^{(j')} = 0$, the analysis is identical as the one of $\mathrm{bad}_5$. We now consider the case when $b^{(j)} = 0 \wedge b^{(j')} = 1$ (the case $b^{(j)} = 1 \wedge b^{(j')} = 0$ is entirely symmetric). We first rewrite the first two equations of $\mathrm{bad}_6$ as

$$\sigma(w^{(j)}) \oplus z^{(j)} \oplus v = \sigma \circ \sigma'^{-1}\left(\sigma(w^{(j')}) \oplus z^{(j')} \oplus v'\right) = \sigma(R) \,,$$

with $\sigma'(x) = \sigma(x) \oplus x$. Then $\mathrm{bad}_6$ implies

$$\begin{aligned} v \oplus \sigma \circ \sigma'^{-1}(v') = \sigma(w^{(j)}) \oplus z^{(j)} \oplus \sigma \circ \sigma'^{-1}\left(\sigma(w^{(j')}) \oplus z^{(j')}\right) \wedge \\ u \oplus u' = t^{(j)} \oplus t^{(j')} \,. \end{aligned}$$

Now we take $\mathit{\Delta}_{\mathsf{in}} = t^{(j)} \oplus t^{(j')}$ and $\mathit{\Delta}_{\mathsf{out}} = \sigma(w^{(j)}) \oplus z^{(j)} \oplus \sigma \circ \sigma'^{-1}\left(\sigma(w^{(j')}) \oplus z^{(j')}\right)$, and by applying Lemma 5 (here we should use the case of $4n\ln(2)$), we get

$$\Pr[\mathrm{bad}_6] \leq \frac{2}{2^n} + \binom{q}{2} \frac{5n}{|\mathcal{R}|} \,.$$

Finally, we consider the bad events $\mathrm{bad}_7$ and $\mathrm{bad}_8$. The bad event $\mathrm{bad}_7$ implies

$$u \oplus v = \sigma(w^{(j)}) \oplus \sigma(w^{(j')}) \oplus t^{(j)} \,.$$

Now we take $\varDelta = \sigma(w^{(j)}) \oplus \sigma(w^{(j')}) \oplus t^{(j)}$, and by applying Lemma 4, we define $L^{\mathsf{io}}$ as the max load of the bin $B_{\varDelta}$. Hence, for any $C_7 > 0$, and by the fact that $R \leftarrow \mathcal{R}$ is a dummy value generated independently of $\tau_0$ and $\tau_1$, the probability that $\mathrm{bad}_7$ holds for a fixed $(j, j')$ couple is $1/\left|\mathcal{R}\right|$. By a union bound over all possible choices of $j \neq j'$, we have

$$\Pr[\mathrm{bad}_7] \leq \Pr\left[L^{\mathsf{io}} \geq C_7\right] + \binom{q}{2}\frac{C_7}{|\mathcal{R}|} \,,$$

Thus, with $C_7 = n\ln(2) + \ln(1/\epsilon) \leq 2n$ and with $\epsilon = 1/2^n$, we have

$$\Pr[\mathrm{bad}_7] \leq \frac{1}{2^n} + \binom{q}{2}\frac{2n}{|\mathcal{R}|} \,.$$

For $\mathrm{bad}_8$, when $b^{(j)} \oplus b^{(j')} = 0$, the analysis is identical as the one of $\mathrm{bad}_7$. We now consider the case when $b^{(j)} = 0 \wedge b^{(j')} = 1$ (the case $b^{(j)} = 1 \wedge b^{(j')} = 0$ is entirely symmetric). We first rewrite $\mathrm{bad}_8$ as

$$\sigma(w^{(j)}) \oplus z^{(j)} \oplus v = \sigma \circ \sigma'^{-1}\left(\sigma(w^{(j')}) \oplus z^{(j')} \oplus u \oplus t^{(j')}\right) = \sigma(R) \,,$$

with $\sigma'(x) = \sigma(x) \oplus x$. Then $\mathrm{bad}_8$ implies

$$\sigma \circ \sigma'^{-1}(u) \oplus v = \sigma(w^{(j)}) \oplus z^{(j)} \oplus \sigma \circ \sigma'^{-1}\left(\sigma(w^{(j')}) \oplus z^{(j')} \oplus t^{(j')}\right) \,.$$

Now we take $\varDelta = \sigma(w^{(j)}) \oplus z^{(j)} \oplus \sigma \circ \sigma'^{-1}\left(\sigma(w^{(j')}) \oplus z^{(j')} \oplus t^{(j')}\right)$, and by applying Lemma 4, we get

$$\Pr[\mathrm{bad}_8] \leq \frac{1}{2^n} + \binom{q}{2}\frac{2n}{|\mathcal{R}|} \,.$$

Summing the these probabilities, we get

$$\Pr[\tau \in \mathcal{T}_{\mathrm{bad}}] \leq \frac{7}{2^n} + \frac{(2B+1)qp^2}{2^n\left|\mathcal{R}\right|} + \frac{p\sqrt{3nq}}{|\mathcal{R}|} + \frac{2B\varPhi(T)p}{|\mathcal{R}|} + \frac{6nq^2}{|\mathcal{R}|} + \frac{q^2}{2^{n+1}} \,.$$

**$\Pr[X_{\mathcal{O}} = \tau]/\Pr[X_{\mathcal{P}} = \tau]$.** Consider an attainable transcript $\tau \in \mathcal{T}_{\mathrm{good}}$. To compute $\Pr[X_{\mathcal{O}} = \tau]$ and $\Pr[X_{\mathcal{P}} = \tau]$, it suffices to compute the probability of oracles that could result in view $\tau$. As explained in the proof of Theorem 2, we have

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} = 2^{nq}\rho(\tau) \,. \tag{15}$$

with $\rho(\tau) = \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n) \colon \mathcal{O}1_R[\pi] \vdash \tau_0 \mid \pi \vdash \tau_1]$.

In order to bound $\rho(\tau)$, we re-group the construction queries in $\tau_0$ according to their collisions with the primitive queries.

$$\begin{aligned}
Q_U &= \{(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in \tau_0 \colon \sigma(w^{(j)} \oplus R) \in U\}\,,\\
Q_V &= \{(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in \tau_0 \colon \sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R \in V\}\,,\\
Q_0 &= \{(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in \tau_0 \colon \sigma(w^{(j)} \oplus R) \notin U \wedge \sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R \notin V\}\,.
\end{aligned}$$

We define $|Q_U| = \alpha_1$ and $|Q_V| = \alpha_2$. Note that we have $Q_U \cap Q_V = \emptyset$ by $\neg\mathrm{bad}_1$, $Q_U \cap Q_0 = \emptyset$ and $Q_V \cap Q_0 = \emptyset$ by the definition of $Q_U$, $Q_V$, and $Q_0$.

We denote respectively $E_1$, $E_2$, and $E_0$ the event that $\mathcal{O}1_R[\pi] \vdash Q_U$, $Q_V$, and $Q_0$ such that $\rho(\tau) = \rho'(\tau)\rho''(\tau)$, with $\rho'(\tau) = \Pr[E_1 \wedge E_2 \mid \pi \vdash \tau_1]$ and $\rho''(\tau) = \Pr[E_0 \mid E_1 \wedge E_2 \wedge \pi \vdash \tau_1]$.

**Lower Bounding $\boldsymbol{\rho'(\tau)}$.** At this moment, $\pi \vdash \tau_1$ defines *exactly* $p$ distinct input-output tuples for $\pi$. We know that for each $(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in Q_U$, there is a unique $(u, v) \in \tau_1$ such that $\sigma(w^{(j)} \oplus R) = u$, and $\pi(\sigma(w^{(j)} \oplus R)) = v$. We define

$$\begin{aligned}
\tilde{U}_2 &= \{\pi(\sigma(w^{(j)} \oplus R)) \oplus t^{(j)} \colon (w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in Q_U\}\,,\\
\tilde{V}_2 &= \{\sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R \colon (w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in Q_U\}\,.
\end{aligned}$$

Similarly, for each $(w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in Q_V$, there is a unique $(u, v) \in \tau_1$ such that $\sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R = v$, and $\pi^{-1}(\sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R) = u$. Again, define

$$\begin{aligned}
\tilde{V}_1 &= \{\pi^{-1}(\sigma(w^{(j)} \oplus R) \oplus z^{(j)} \oplus b^{(j)}R) \oplus t^{(j)} \colon (w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in Q_V\}\,,\\
\tilde{U}_1 &= \{\sigma(w^{(j)} \oplus R) \colon (w^{(j)}, t^{(j)}, b^{(j)}, z^{(j)}) \in Q_V\}\,.
\end{aligned}$$

Note that all values in $\tilde{U}_1$ are distinct since $w^{(j)}$'s are distinct, all values in $\tilde{U}_2$ are distinct by $\neg\mathrm{bad}_5$, $U \cap \tilde{U}_1 = \emptyset$ by $\neg\mathrm{bad}_1$, $U \cap \tilde{U}_2 = \emptyset$ by $\neg\mathrm{bad}_2$, and $\tilde{U}_1 \cap \tilde{U}_2 = \emptyset$ by $\neg\mathrm{bad}_7$; and that all values in $\tilde{V}_1$ are distinct by $\neg\mathrm{bad}_6$, all values in $\tilde{V}_2$ are distinct by $\neg\mathrm{bad}_4$, $V \cap \tilde{V}_1 = \emptyset$ by $\neg\mathrm{bad}_3$, $V \cap \tilde{V}_2 = \emptyset$ by $\neg\mathrm{bad}_1$, and $\tilde{V}_1 \cap \tilde{V}_2 = \emptyset$ by $\neg\mathrm{bad}_8$.

Hence, the event $E_1$ and $E_2$ define *exactly* $\alpha_1 + \alpha_2$ new and distinct input-output tuples for $\pi$, we have

$$\rho'(\tau) = \frac{1}{(2^n - p)_{\alpha_1 + \alpha_2}}\,. \tag{16}$$

**Lower Bounding $\boldsymbol{\rho''(\tau)}$.** At this moment, $\pi \vdash \tau_1$, $E_1$ and $E_2$ define *exactly* $p + \alpha_1 + \alpha_2$ distinct input-output tuples for $\pi$. Our goal now is to count the number of new and distinct evaluations on $\pi$, introduced by the event $E_0$. Let

$$\begin{aligned}
q' &= |Q_0| = q - \alpha_1 - \alpha_2\,,\\
p' &= \left|U \cup \tilde{U}_1 \cup \tilde{U}_2\right| = \left|V \cup \tilde{V}_1 \cup \tilde{V}_2\right| = p + \alpha_2 + \alpha_1\,.
\end{aligned}$$

To ease the subsequent counting, we rewrite the queries in $Q_0$ as

$$Q_0 = \{(w_1, t_1, b_1, z_1), \ldots, (w_{q'}, t_{q'}, b_{q'}, z_{q'})\}\,.$$

For $i = 1, \ldots, q'$, let

$$\begin{aligned} \bar{U}_1 &= \{\bar{u}_{1,1}, \ldots, \bar{u}_{1,q'}\} \quad \text{with} \quad \bar{u}_{1,i} = \sigma(w_i \oplus R)\,, \\ \bar{V}_2 &= \{\bar{v}_{2,1}, \ldots, \bar{v}_{2,q'}\} \quad \text{with} \quad \bar{v}_{2,i} = \sigma(w_i \oplus R) \oplus z_i \oplus b_i R\,, \end{aligned}$$

Note that by definition of $Q_0$, the $\bar{u}_{1,i}$'s are distinct and outside $U \cup \tilde{U}_1$, and the $\bar{v}_{2,i}$'s are distinct and outside $V \cup \tilde{V}_2$. Besides that, we also know that $\bar{u}_{1,i}$'s are outside $\tilde{U}_2$ by $\neg\text{bad}_7$, and that $\bar{v}_{2,i}$'s are outside $\tilde{V}_1$ by $\neg\text{bad}_8$.

We define by FRESH the event that the underlying permutation calls to $\pi$ introduced by the construction queries in $Q_0$ evaluate on distinct inputs, and we also define $\rho''^{*}(\tau) = \Pr[E_0 \wedge \text{FRESH} \mid E_1 \wedge E_2 \wedge \pi \vdash \tau_1]$. Note that we have $\rho''(\tau) \geq \rho''^{*}(\tau)$. Hence it is sufficient to focus on $\rho''^{*}(\tau)$ instead of $\rho''(\tau)$. Let $N_0$ be the number of solutions

$$\{\bar{v}_{1,1}, \ldots, \bar{v}_{1,q'}, \bar{u}_{2,1}, \ldots, \bar{u}_{2,q'}\}$$

where $\bar{u}_{2,1}, \ldots, \bar{u}_{2,q'} \notin \bar{U}_1$ and $\bar{v}_{1,1}, \ldots, \bar{v}_{1,q'} \notin \bar{V}_2$ because of the event FRESH.

$N_0$ satisfies the following conditions.

1. $\forall i\colon \bar{v}_{1,i} \oplus t_i = \bar{u}_{2,i}$. There are in total $2^n$ different choices for each $(\bar{v}_{1,i}, \bar{u}_{2,i})$ couple.
2. Conditions for $\bar{v}_{1,i}$:
   (a) $\forall i\colon \bar{v}_{1,i} \notin (V \cup \tilde{V}_1 \cup \tilde{V}_2 \cup \bar{V}_2)$. This excludes at most $p' + q'$ choices for each $(\bar{v}_{1,i}, \bar{u}_{2,i})$ couple,
   (b) $\forall (i, i')$ and $i' < i\colon \bar{v}_{1,i} \neq \bar{v}_{1,i'}$. This excludes at most $i - 1$ choices for each $(\bar{v}_{1,i}, \bar{u}_{2,i})$ couple.
3. Conditions for $\bar{u}_{2,i}$:
   (a) $\forall i\colon \bar{u}_{2,i} \notin (U \cup \tilde{U}_1 \cup \tilde{U}_2 \cup \bar{U}_1)$. This excludes at most $p' + q'$ choices for each $(\bar{v}_{1,i}, \bar{u}_{2,i})$ couple,
   (b) $\forall (i, i')$ and $i' < i\colon \bar{u}_{2,i} \neq \bar{u}_{2,i'}$. This excludes at most $i - 1$ choices for each $(\bar{v}_{1,i}, \bar{u}_{2,i})$ couple.

Taking into account the conditions (1)-(3), we can bound the number $N_0$ as

$$N_0 \geq \prod_{i=1}^{q'} \big(2^n - 2p' - 2q' - 2(i-1)\big)\,.$$

All in all, we have that for any of the $N_0$ possible choices for the solutions $\{\bar{v}_{1,1}, \ldots, \bar{v}_{1,q'}, \bar{u}_{2,1}, \ldots, \bar{u}_{2,q'}\}$ satisfying all conditions, the event $E_0$ is equivalent to exactly $2q'$ new equations on $\pi$. Hence, it follows that

$$\rho''^{*}(\tau) \geq \frac{N_0}{(2^n - p - \alpha_1 - \alpha_2)_{2q'}}\,. \tag{17}$$

Combining (15), (16) and (17) and using that $q - q' = \alpha_1 + \alpha_2$., we obtain

$$\begin{aligned}\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} &\geq \frac{N_0 \cdot 2^{nq}}{(2^n - p)_{\alpha_1+\alpha_2+2q'}} \\ &= \frac{N_0 2^{nq'}}{(2^n - p')_{2q'}} \cdot \frac{2^{nq}}{2^{nq'}(2^n - p)_{\alpha_1+\alpha_2}} \\ &\geq \frac{N_0 2^{nq'}}{(2^n - p')_{2q'}} \cdot \frac{2^{n(q-q')}}{2^{n(\alpha_1+\alpha_2)}} = \frac{N_0 2^{nq'}}{(2^n - p')_{2q'}} \,. \end{aligned} \tag{18}$$

Processing further from (18), we have

$$\begin{aligned}(18) &\geq \frac{\prod_{i=1}^{q'} 2^n \big(2^n - 2p' - 2q' - 2(i-1)\big)}{(2^n - p')_{2q'}} \\ &= \prod_{i=1}^{q'} \frac{2^n \big(2^n - 2p' - 2q' - 2(i-1)\big)}{(2^n - p' - (i-1))(2^n - p' - q' - (i-1))}\end{aligned} \tag{19}$$

We denote $B = p' + (i-1)$ and $C = p' + q' + (i-1)$. The equation (19) can be written as

$$\begin{aligned}(19) &= \prod_{i=1}^{q'} \frac{2^{2n} - 2 \cdot 2^n C}{(2^n - B)(2^n - C)} \\ &= \prod_{i=1}^{q'} \frac{2^{2n} - 2 \cdot 2^n C}{2^{2n} - 2^n B - 2^n C + BC} \\ &= \prod_{i=1}^{q'} \Big(1 - \frac{2^n (C - B) + BC}{2^{2n} - 2^n B - 2^n C + BC}\Big) \geq \prod_{i=1}^{q'} \Big(1 - \frac{4(C-B)}{2^n} - \frac{4BC}{2^{2n}}\Big)\end{aligned} \tag{20}$$

where for the last inequality we used $B \leq C = p' + q' + (i-1) \leq 2^n/2$.

Fill in the values of $B$, $C$, and $C - B = q'$, and using union bound, we obtain

$$\begin{aligned}(20) &= \prod_{i=1}^{q'} \left(1 - \frac{4q'}{2^n} - \frac{4(p' + (i-1))(p' + q' + (i-1))}{2^{2n}}\right) \\ &\geq 1 - \frac{4q'^2}{2^n} - \frac{4q'(p' + (i-1))(p' + q' + (i-1))}{2^{2n}} \,.\end{aligned} \tag{21}$$

By definition of $p'$, and $q'$, we have

$$\begin{aligned} q' &\leq q \,, \\ p' + (i-1) &\leq p' + q' = p + q \,, \\ p' + q' + (i-1) &\leq p' + 2q' \leq p + 2q \,. \end{aligned}$$

Then, we conclude from (21) that

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} \geq 1 - \Big(\frac{8q^2}{2^{n+1}} + \frac{4q(p+q)(p+2q)}{2^{2n}}\Big) =: 1 - \epsilon \,.$$

Acknowledgments. This work was done at the University of Washington, Seattle, USA, when the first author was visiting there. Yu Long Chen is supported by a Ph.D. Fellowship and and a long term travel grant from the Research Foundation - Flanders (FWO). Stefano Tessaro was supported in part by NSF grants CNS-1930117 (CAREER), CNS-1926324, CNS-2026774, a Sloan Research Fellowship, and a JP Morgan Faculty Award. The authors would like to thank the anonymous reviewers for their comments and suggestions.

## References

1. Michel Abdalla, Fabrice Benhamouda, and Alain Passelègue. Algebraic XOR-RKA-secure pseudorandom functions from post-zeroizing multilinear maps. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part II*, volume 11922 of *LNCS*, pages 386–412. Springer, Heidelberg, December 2019.
2. Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner. More efficient oblivious transfer and extensions for faster secure computation. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM CCS 2013*, pages 535–548. ACM Press, November 2013.
3. László Babai. The fourier transform and equations over finite abelian groups: An introduction to the method of trigonometric sums (lecture notes).
4. Mihir Bellare, Viet Tung Hoang, Sriram Keelveedhi, and Phillip Rogaway. Efficient garbling from a fixed-key blockcipher. In *2013 IEEE Symposium on Security and Privacy*, pages 478–492. IEEE Computer Society Press, May 2013.
5. Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In Ting Yu, George Danezis, and Virgil D. Gligor, editors, *ACM CCS 2012*, pages 784–796. ACM Press, October 2012.
6. Mihir Bellare and Tadayoshi Kohno. Hash function balance and its impact on birthday attacks. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 401–418. Springer, Heidelberg, May 2004.
7. Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, Heidelberg, May 2014.
8. Seung Geol Choi, Jonathan Katz, Ranjit Kumaresan, and Hong-Sheng Zhou. On the security of the “free-XOR” technique. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 39–53. Springer, Heidelberg, March 2012.
9. Benoit Cogliati and Yannick Seurin. On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 584–613. Springer, Heidelberg, April 2015.
10. Benoît Cogliati and Yannick Seurin. Analysis of the single-permutation encrypted davies-meyer construction. *Des. Codes Cryptogr.*, 86(12):2703–2723, 2018.
11. Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. *Journal of Cryptology*, 10(3):151–162, June 1997.
12. Pooya Farshim and Gordon Procter. The related-key security of iterated Even-Mansour ciphers. In Gregor Leander, editor, *FSE 2015*, volume 9054 of *LNCS*, pages 342–363. Springer, Heidelberg, March 2015.
13. Oded Goldreich. *Foundations of Cryptography: Basic Applications*, volume 2. Cambridge University Press, Cambridge, UK, 2004.

14. Shay Gueron, Yehuda Lindell, Ariel Nof, and Benny Pinkas. Fast garbling of circuits under standard assumptions. *Journal of Cryptology*, 31(3):798–844, July 2018.
15. Chun Guo, Jonathan Katz, Xiao Wang, Chenkai Weng, and Yu Yu. Better concrete security for half-gates garbling (in the multi-instance setting). In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 793–822. Springer, Heidelberg, August 2020.
16. Chun Guo, Jonathan Katz, Xiao Wang, and Yu Yu. Efficient and secure multiparty computation from fixed-key block ciphers. In *2020 IEEE Symposium on Security and Privacy*, pages 825–841. IEEE Computer Society Press, May 2020.
17. Russell Impagliazzo and Valentine Kabanets. Constructive proofs of concentration bounds. In Maria J. Serna, Ronen Shaltiel, Klaus Jansen, and José D. P. Rolim, editors, *APPROX-RANDOM 2010*, volume 6302 of *Lecture Notes in Computer Science*, pages 617–631. Springer, 2010.
18. Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 145–161. Springer, Heidelberg, August 2003.
19. Marcel Keller, Emmanuela Orsini, and Peter Scholl. Actively secure OT extension with optimal overhead. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 724–741. Springer, Heidelberg, August 2015.
20. Hugo Krawczyk. LFSR-based hashing and authentication. In Yvo Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 129–139. Springer, Heidelberg, August 1994.
21. Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. *Journal of Cryptology*, 24(3):588–613, July 2011.
22. Alessandro Panconesi and Aravind Srinivasan. Randomized distributed edge coloring via an extension of the chernoff-hoeffding bounds. *SIAM J. Comput.*, 26(2):350–368, 1997.
23. Jacques Patarin. The "coefficients H" technique (invited talk). In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, Heidelberg, August 2009.
24. John P Steinberger. The sum-capture problem for abelian groups. *arXiv preprint arXiv:1309.5582*, 2013.
25. Stefano Tessaro. Optimally secure block ciphers from ideal primitives. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 437–462. Springer, Heidelberg, November / December 2015.
26. Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *27th FOCS*, pages 162–167. IEEE Computer Society Press, October 1986.
27. Samee Zahur, Mike Rosulek, and David Evans. Two halves make a whole - reducing data transfer in garbled circuits using half gates. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 220–250. Springer, Heidelberg, April 2015.