Tweakable Permutation-based Luby-Rackoff Constructions ***

Bishwajit Chakraborty[1] and Abishanka Saha[2]

[1] Nanyang Technological University, Singapore
bishu.math.ynwa@gmail.com
[2] Eindhoven University of Technology, The Netherlands
sahaa.1993@gmail.com

Abstract Liskov, Rivest, and Wagner, in their seminal work, formulated tweakable blockciphers and proposed two blockcipher-based design paradigms, LRW1 and LRW2, where the basic design strategy is to xor the masked tweak to the input and output of a blockcipher. The 2-round cascaded LRW2 and 4-round cascaded LRW1 have been proven to be secure up to $\mathcal{O}(2^{3n/4})$ queries, but n-bit optimal security still remains elusive for these designs. In their paper, Liskov also posed an open challenge of embedding the tweak directly in the blockcipher, and to address this, Goldenberg et al. introduced the tweakable Luby-Rackoff (LR) constructions. They showed that if the internal primitives are random functions, then for tweaks with t blocks, the construction needs $t+6$ rounds to be optimally n-bit CPA secure and $2t+8$ rounds to be optimally n-bit CCA secure, where respectively t and $2t$ rounds were required to process the tweaks. Since blockciphers can be designed much more efficiently than pseudorandom functions, in many practical applications the internal primitives of LR ciphers are instantiated as blockciphers, which however would lead to a birthday-bound factor, which is not ideal for say lightweight cryptography.

This paper addresses the following two key questions affirmatively: (1) Can Goldenberg et al.'s results be extended to LR constructions with random permutations as internal primitives without compromising the optimal n-bit security? (2) Can the number of rounds required for handling long tweaks be reduced?

We formally define TLR-compatible functions, for processing the tweak, which when composed with 4-rounds and 5-rounds of LR construction with random permutations as internal primitives gives us respectively n-bit CPA and CCA secure tweakable permutations. For the security analysis, we proved general Mirror Theory result for three permutations. We also propose instantiating TLR-compatible functions with one round LR where a permutation (resp, two AXU hash functions) is used to mask

* This is the extended version of the paper accepted at CRYPTO 2025.
** Addendum: We have noticed another implication of our analysis, which is that we get optimally secure MAC constructions from permutation-based LR, and these results are presented in the newly added Section 8 : The DbHtF MAC Family. This will not appear in the CRYPTO 2025 version either.

single-block tweaks (resp., variable-length tweaks), thus proposing the n-bit CPA (resp., CCA) secure tweakable permutation candidates, TLRP5 and TLRP5+ (resp., TLRP7 and TLRP7+), using 5 (resp., 7) LR rounds, which is a significant reduction from the tweak-length-dependent results of Goldenberg et al.
We further extend the implications of our analysis of permutation-based LR as follows:

- We show n-bit CPA (resp., CCA) security of 5-rounds (resp. 7-rounds) permutation-based LR construction, which is quite an improvement over the existing $2n/3$-bit security proved by Guo et al.
- We propose a new design paradigm, DbHtF, for n-bit secure MACs, that involves hashing the message, then passing the diblock tag through four rounds of permutation-based LR and then truncating the left block.

Keywords: Variable-length Tweak · Tweakable block cipher · Permutation-based Feistel Construction · Optimal security.

1 Introduction

A block cipher (BC), also referred to as a keyed pseudo-random permutation (PRP), is a function defined over a key-space $\mathcal{K}$ and a message-space $\mathcal{M}$, denoted as $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$, such that for every $k \in \mathcal{K}$, the function $E_k : \mathcal{M} \to \mathcal{M}$, defined by $E_k(M) := E(k, M)$, acts as a permutation. One of the most influential block cipher design paradigms is the Feistel structure, also known as LR ciphers, introduced by Luby and Rackoff in 1986 [35]. They demonstrated that a three-round LR cipher with randomized round functions is indistinguishable from a random permutation up to $\mathcal{O}(2^{n/2})$ queries. Patarin later extended this result, showing that a four-round LR cipher remains secure against chosen-ciphertext attacks up to $\mathcal{O}(2^{n/2})$ queries [43]. Since then, LR ciphers have been extensively studied in the symmetric-key cryptography community [41].

Most of the available literature on LR construction deals with non-bijective functions as the underlying primitive. However, in most practical applications [30,19,1,49] the inner round functions are instantiated with blockciphers, which leads to the bane of birthday-bound due to PRP-PRF switching lemma [6]. The obvious alternative is to analyze the security of LR with inner permutation rounds. Piret [48] introduced provable security for permutation-based LR ciphers but only achieved birthday bound. Beyond birthday-bound security for permutation-based LR is achieved by Guo et al. [21]. They showed that 3-round, 5-round, and 7-round LR constructions with random permutations as inner round functions achieve respectively known-plaintext attack (KPA), chosen-plaintext attack (CPA) and chosen-ciphertext attack (CCA) security up to $\mathcal{O}(2^{2n/3})$ queries. Since there are no matching attacks to these security bounds, the natural question arises *whether permutation-based LR can achieve optimal security*?

Tweakable Block ciphers. Despite the prevalence of BC designs, in many practical scenarios, BCs are not enough and we require multiple independent PRPs under

the same key. For example, in authenticated encryption (AE) schemes tweaks are very effective in handling nonces or associated data without rekeying. This requirement leads to the conceptualization of the tweakable block cipher (TBC), which is a function $\tilde{E} : \mathcal{T} \times \mathcal{K} \times \mathcal{M} \to \mathcal{M}$, such that for each tweak T in the tweak space $\mathcal{T}$, $\tilde{E}_T$ behaves as a blockcipher. One of the earliest AE schemes OCB3 [31], the CEASER-finalist Deoxys-II [24] or their lightweight alternatives SKINNY [3], GIFT-COFB [2] and the CEASER-finalist Romulus [22], are all based on tweakable block ciphers, where the tweaks are typically derived from the IV, nonce, or associated data. As noticed above, since TBCs are employed in lightweight cryptography too, we want a good TBC candidate to be beyond-birthday-bound (BBB) secure, since the birthday bound, $q^2/2^n$, corresponding to q adversarial queries, leads to a poor security guarantee in case of a small block size n, which is typically the case in lightweight cryptography. Of course, an ideal TBC candidate can be expected to have optimal n-bit security.

There is a multitude of BC candidates in practice, and a very efficient choice for building a TBC will be to build one based on BCs. Liskov, Rivest and Wagner, in their seminal paper [34], formulated the tweakable blockciphers and proposed two provably secure constructions, the LRW1 and LRW2, in which the basic design principle was to use an almost-xor-universal (AXU) hash function to mask the tweak and xor the masked tweak to the input and output of a blockcipher. The cascaded versions of these designs achieve BBB security: the 2-round cascaded LRW2 construction is shown by [27] to be $3n/4$-bit secure, with a matching attack provided by [38]; while the minimal number of rounds needed for the cascaded LRW1 construction to achieve BBB security is 4, as shown by [25], who provided a $3n/4$-bit security proof for the 4-round LRW1, which is however not tight.

Liskov et al. [34] also posed an open challenge: embedding the tweak directly within the block cipher. Goldenberg et al. [20] addressed this by constructing tweakable LR structures with direct tweak injection, producing TBCs that are CPA-secure under plaintext attacks and strongly tweakable pseudorandom permutation (CCA) secure under chosen-ciphertext attacks. Their main results for single-tweak block injection can be summarized as follows:

- No such construction is CPA-secure for $r \leq 3$ rounds.
- No such construction is CCA-secure for $r \leq 5$ rounds.
- Constructions secure against CPA adversaries making $\ll 2^{n/2}$ queries exist when $r \geq 4$ rounds.
- Constructions secure against CCA adversaries making $\ll 2^{n/2}$ queries exist when $r \geq 6$ rounds.
- Constructions secure against CPA adversaries making $\ll 2^n$ queries exist when $r \geq 7$ rounds.
- Constructions secure against CCA adversaries making $\ll 2^n$ queries exist when $r \geq 10$ rounds.

Further for longer tweaks, the constructions by Goldenberg et al. [20] require $t+6$-round (resp. $2t+8$-round) LR constructions with tweak injection to achieve

$\ll 2^n$ CPA (resp. CCA) security, where t is the number of tweak blocks. Building on this we can raise two questions:

- *Can the results of Goldenberg et al. [20] be extended to LR constructions with random permutations as inner rounds?*
- *Can the number of rounds required to process those tweaks be reduced?*

Message Authentication Codes. Another important cryptographic primitive is the message authentication codes (MAC). Many BC-based MAC constructions, like CBC-MAC [4], PMAC [9], OMAC [23], LightMAC [36] follows the UHF-then-PRF paradigm, where the message is first hashed with an UHF and then passed through a block-cipher to generate the authentication tag. This paradigm is inherently at most birthday-bound secure since a collision on the UHF output will lead to a tag collision. To go beyond birthday-bound the obvious step is to replace the blockcipher with a BC-based PRF candidate, as the name of the paradigm already suggests. One of the simplest such PRF candidates is the sum of two blockciphers, and this is utilized in the Diblock-Hash-then-Sum (DbHtS) paradigm proposed by Datta et al. [17], where the message is hashed by a diblock hash, and the two output blocks are then passed through a blockcipher each and summed to get the final tag. Several popular MAC candidates fall under this paradigm, for example, PolyMAC [7,11,28], SUM-ECBC [51], PMAC+ [52], LightMAC+ [42], 3kf9 [53]. As proved by Kim et al. [29], the DbHtS scheme achieves BBB $3n/4$-bit security, and this is tight due to matching attacks by Leurent et al. [32]. This state of affairs leads to the final question we will tackle, is whether there exists *optimally secure MAC constructions?*

1.1 Our Contributions

In this paper, we answer all the questions raised in the previous section affirmatively. The crux of our approach lies in revisiting the security of the permutation-based LR construction and then formulate our TPRP/MAC constructions based on permutation-based LR. Below we discuss our contributions:

Optimal Mirror Theory bound involving three permutations: The security analysis of 3/5/7-round LR by Guo et al. [21] via H-coefficient technique [44,46] involved lower bounding the real-world probability of a transcript, which reduces to lower bounding the number of solutions to a system of equations in the internal variables of the respective construction, such that the solutions are compatible with the inner permutations. This combinatorial method is termed Mirror Theory [47], which informally says that a system of equations should have at least as many as the expected number of solutions satisfying the compatibility conditions. Guo et al. [21] proved a *sub-optimal version* of Mirror Theory involving variables derived from the i/o pairs of the three independent internal permutations of 3-round LR which resulted in the $\mathcal{O}(2^{2n/3})$ security bound.

Recently, Choi et al. [13] proved optimal Mirror Theory bound for general systems of equations and non-equations involving the i/o variables of *two* permutations. We adopt their proof strategy to prove optimal Mirror Theory bound for general systems of equations involving the i/o variables of *three* permutations. Informally, our Mirror Theory result (Theorem 4) states that, for a 'general' system of e equations over some variables, and a tripartition of the variable set, such that the partitions are of size p_1, p_2, p_3, the number of solutions to these system of equations such that variables within the same partition are assigned distinct values, is at least

$$\frac{(2^n-2)_{p_1}(2^n-2)_{p_2}(2^n-2)_{p_3}}{2^{ne}}.$$

This result plays a crucial role in real-world transcript analysis of the constructions in this paper, yielding n-bit security for such.

In fact, in Section 10, we extend this result to more general partitions of the variable set, into p disjoint sets, of size $c_1, \ldots, c_p$, and we show that (Theorem 6) the number of solutions to a system of e equations such that variables within the same partition are assigned distinct values is at least,

$$\frac{\prod_{i=1}^{p}(2^n-2)_{c_i}}{2^{ne}}$$

Tweakable permutation-based LR: In this paper we revisit Goldenberg et al.'s [20] LR-based tweakable permutation constructions in the setting where the internal primitives of LR are random permutations instead of being random functions, as assumed in [20]. Our contributions can be outlined as follows:

1. We formally define *TLR-compatible family* of $2n$-bit tweakable permutations with b-bit tweaks (Defn. 4), such that a function sampled uniformly from the family has a negligible probability of collision in the right half of outputs as well as negligible probability of full collision of outputs.
2. Using such TLR-compatible function family for processing tweaks and composing them with permutation-based LR constructions we construct n-bit secure tweakable pseudorandom permutations:
   (a) We prove (Theorem 2) that for F being uniformly sampled from a TLR-compatible family of functions and E being the 4-round LR with independent uniformly random permutations as internal primitives, $E \circ F$ is a n-bit CPA secure tweakable pseudorandom permutation.
   (b) We prove (Theorem 3) that for F, F' being uniformly sampled from a TLR-compatible family of functions and E being the 5-round LR with independent uniformly random permutations as internal primitives, $F^{-1} \circ E \circ F'$ is a n-bit CCA secure tweakable pseudorandom permutation.

   The security analysis is done via the H-coefficient technique where our Mirror Theory result for three permutations is crucial for real-world good transcript analysis.
3. We instantiate TLR-compatible families as follows:

   (a) For n-bit single-block tweaks we process the tweak by a n-bit random permutation and xor it to both the left and right half of the input to 1-round LR construction. This family is formally defined in (1) and its TLR compatibility is proved in Proposition 4.
   (b) For variable-length tweaks we process the tweak by 2 AXU hash functions and xor one to the left and the other to the right half of the input to 1-round LR construction. This family is formally defined in (2) and its TLR compatibility is proved in Proposition 5.
4. We combine the aforementioned instantiations of TLR-compatible families with 4-round (respectively 5-round) permutation-based LR as suggested in the second point, and propose the following constructions:
   (a) TLRP5 (Fig. 1.1): An n-bit secure tweakable pseudorandom permutation (Corollary 3) with single-block tweaks that involves 5 LR-rounds and 6 n-bit permutation calls, thus using 2 less rounds and 1 less primitive calls than required by [20].
   (b) TLRP7 (Fig. 1.1): An n-bit secure tweakable strong pseudorandom permutation (Corollary 3) with single-block tweaks that involves 7 LR-rounds and 8 n-bit permutation calls, thus using 3 less round and 2 less primitive calls than required by [20].
   (c) TLRP5+ (Fig. 1.1): An n-bit secure tweakable pseudorandom permutation (Corollary 4) with variable-length tweaks that involves 5 LR-rounds with 5 n-bit permutation calls and 2 AXU hash function calls.
   (d) TLRP7+ (Fig. 1.1): An n-bit secure tweakable strong pseudorandom permutation (Corollary 4) with variable-length tweaks that involves 7 LR-rounds with 7 n-bit permutation calls and 2 AXU hash function calls.

   For the last two constructions, TLRP5+ and TLRP7+, it might seem that using two AXU hash functions is overkill. However, we would like to point out that each distinct tweak is processed only once. This is a significant reduction in complexity as compared to the LR constructions proposed by [20] as there for each query, even with the same tweak, one has to process $t + 6$ round (resp. $2t + 8$ round) of LR.

Optimal security of permutation-based LR PRP: As a simpler consequence of Theorem 2 and 3, we get that permutation-based 5-round LR is n-bit secure pseudorandom permutation and permutation-based 7-round LR is n-bit secure strong pseudorandom permutation (Corollary 2). As noted earlier, the latest security analyses of these constructions by Guo et al. [21] achieved only $2n/3$-bit security bound.

Design and Analysis of LR-based MAC constructions: Recalling our discussion on MACs, we note that for the diblock hash-then-PRF paradigm, one could also use the n-bit truncation of a $2n$-bit blockcipher as the PRF candidates. This motivates our design paradigm, which we dub as Double-block Hash-then-Fiestel (DbHtF) construction (see Figure 2), where the $2n$-bit hash output

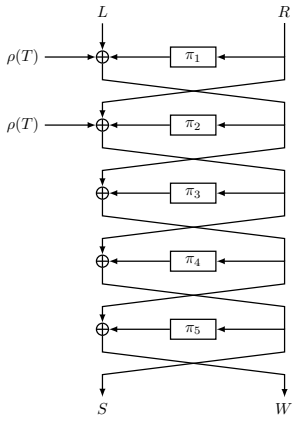
(double n-bit blocks) are passed through the $2n$-bit blockcipher, 4-round LR, and then only the left n-bits of the output gives the authentication tag. In other words, given any diblock hash function, we modify the DbHtS design corresponding to it, by replacing the "sum-of-two n-bit independent random permutations" operation on the $2n$-bit hash output with a "4-LR permutation", defined using four independent random n-bit permutations as it's round functions. The n-bit MAC output is then defined as the left half of the $2n$-bit output of the 4-LR. We show that the DbHtF-versions of some popular DbHtS constructions such as, PolyMAC, SUM-ECBC, PMAC+, LightMAC+ achieve PRF security up to $q \ll 2^n$ queries ignoring the maximum message length. We note that [16] proposed the variable input-length PRF construction, 2HtmB-p2, that also uses 4 blockcipher calls, and is optimally secure [14]. But here, we propose a different paradigm using permutation-based LR, leaving open the security of constructions based on less than 4-rounds of LR.

Table 1. Comparative study of beyond birthday bound results for LR-based constructions. RP:= Random Permutation, RF:= Random Function, AXU:= almost XOR universal hash function of output size n where (T)LR is the (tweakable) balanced construction from $2n$ bit to $2n$-bit.

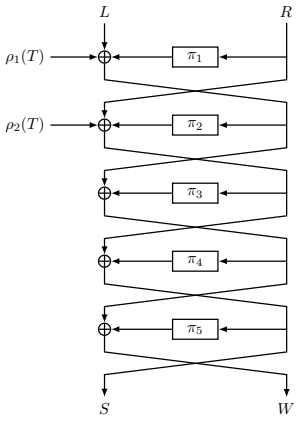
Design	Primitive Count	Security(bits) CPA(CCA)
5(6)-round LR[45,14]	5(6) RF	$n-\epsilon$
7(10)-round TLR with n-bit tweak[20]	7 (10) RF	$n-\epsilon$
$t+6(2t+8)$-round TLR with tn-bit tweak[20]	$t+6$ $(2t+8)$ RF	$n-\epsilon$
5(7)-round LR[21]	5 (7) RP	$2n/3$
5(7)-round TLR with n-bit tweak [**this paper**]	6 (8) RP	$n-\epsilon$
5(7)-round TLR with tn-bit tweak [**this paper**]	5 (7) RP+ 2 AXU	$n-\epsilon$

Table 2. Comparing the PRF security of existing MAC constructions with the security achieved for their respective DbHtF-variants as defined and analyzed in this paper.

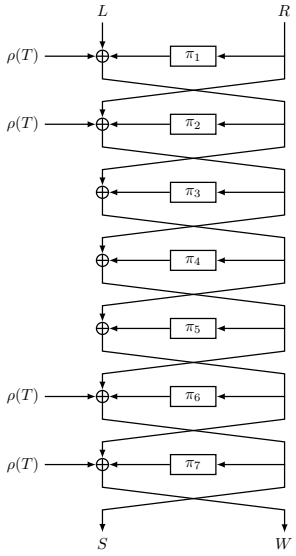
MAC construction	Security[29,33]	DbHtF-variant	Security
PolyMac	$\Theta(2^{\frac{3n}{4}})$	4F-PolyHash-DbHtF	$\mathcal{O}(2^n)$
SUM-ECBC	$\Theta(2^{\frac{3n}{4}})$	4F-ECBC-DbHtF	$\mathcal{O}(2^n)$
$\mathsf{PMAC}_{\mathsf{plus}}$	$\Theta(2^{\frac{3n}{4}})$	4F-PHash-DbHtF	$\mathcal{O}(2^n)$
$\mathsf{LightMac}_{\mathsf{plus}}$	$\Theta(2^{\frac{3n}{4}})$	4F-LightHash-DbHtF	$\mathcal{O}(2^n)$



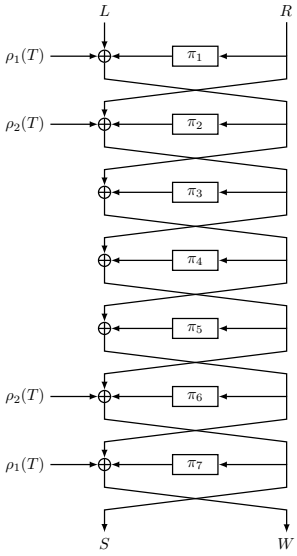
(a) The TLRP5 construction



(b) The TLRP5+ construction



(c) The TLRP7 construction



(d) The TLRP7+ construction

Figure 1. In this figure, $\rho, \pi_1, \ldots, \pi_7 \xleftarrow{\$} \mathsf{Perm}(n)$ and $\rho_1, \rho_2 \xleftarrow{\$} \mathcal{H}$ are sampled independently, where $\mathcal{H}$ is an AXU hash function family.

2 Preliminaries

2.1 Notations

For any non-zero integer n, $[n]$ denotes the set of integers $\{1, \ldots, n\}$, $\{0,1\}^n$ denotes the set of all n-bit strings, $\{0,1\}^* := \cup_{n \in \mathbb{Z}_{\geq 0}} \{0,1\}^n$. Given any two integers q, n, we denote the falling factorial as, $(q)_n := q(q-1)\cdots(q-n+1)$, which can be interpreted as the number of without replacement samples of size n chosen from a set of size q.

Given any two-bit strings x, y, $x\|y$ denotes the concatenation of x and y. For a $2n$-bit string x, we will denote by x_L, the n most significant bits of x and by x_R the n least significant bits of x, i.e., $x = x_L\|x_R$.

Given two functions $F : \{0,1\}^n \to \{0,1\}^m$ and $G : \{0,1\}^m \to \{0,1\}^k$, $G \circ F : \{0,1\}^n \to \{0,1\}^k$ denotes the composition function defined by $x \mapsto G(F(x))$. For any sets $\mathcal{X}$ and $\mathcal{Y}$, we denote by $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ the set of all functions $f : \mathcal{X} \to \mathcal{Y}$ and by $\mathsf{Perm}(\mathcal{X})$ the set of all permutations $\pi : \mathcal{X} \to \mathcal{X}$. For $\mathcal{X} = \{0,1\}^n, \mathcal{Y} = \{0,1\}^m$, we alternatively denote $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ as $\mathsf{Func}(n, m)$ and $\mathsf{Perm}(\mathcal{X})$ as $\mathsf{Perm}(n)$. Also the set of all tweakable permutations $\tilde{\pi} : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ with tweak space $\mathcal{T}$ is denoted as $\mathsf{TPerm}(\mathcal{T}, \mathcal{X})$. For $\mathcal{X} = \{0,1\}^n$ and $\mathcal{T} = \{0,1\}^b$, we denote $\mathsf{TPerm}(\mathcal{T}, \mathcal{X})$ as $\mathsf{TPerm}(b, n)$. Given any function $F \in \mathsf{TPerm}(b, n)$, we define it's inverse $F^{-1} \in \mathsf{TPerm}(b, n)$ as follows,

$$F^{-1}(T, X) = Y \iff F(T, Y) = X.$$

If $F, F' \in \mathsf{TPerm}(b, n)$ and $\pi \in \mathsf{Perm}(n)$, then $F^{-1} \circ \pi \circ F \in \mathsf{TPerm}(b, n)$ is defined as

$$F^{-1} \circ \pi \circ F'(T, X) := F^{-1}(T, \pi(F'(T, X))).$$

Definition 1 (LR permutation function). *Given any function $f : \{0,1\}^n \to \{0,1\}^n$, $\Psi_1^f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ denotes the 1-round LR permutation function defined by*

$$\Psi_1^f(L\|R) := (R\|L \oplus f(R)).$$

Similarly, for r functions $f_1, \ldots, f_r \in \mathsf{Func}(n, n)$, $\Psi_r^{(f_1,\ldots,f_r)} \in \mathsf{Perm}(2n)$ denotes the r-round LR construction defined by the functional composition

$$\Psi_r^{(f_1,\ldots,f_r)} := \Psi_1^{f_r} \circ \cdots \circ \Psi_1^{f_1}.$$

For any set $\mathcal{S}$, we denote by $X \xleftarrow{\mathcal{D}} \mathcal{S}$ that X is a random variable following distribution $\mathcal{D}$ over $\mathcal{S}$. We also write $X \sim \mathcal{D}$. Alternatively, the distribution of the random variable X is denoted as $\mathcal{D}_X$. In particular, we use $X \leftarrow\!\!\$\, \mathcal{S}$ to denote that X is a random variable distributed uniformly over $\mathcal{S}$.

Definition 2 (Random function, permutation and tweakable permutation). *Any random variable F over $\mathsf{Func}(n)/\mathsf{Perm}(n)/\mathsf{TPerm}(b, n)$ is called a* random n-bit function/ n-bit permutation/ n-bit tweakable permutation with b-bit tweak. *The distribution of F is denoted as $\mathcal{D}_F$.*

Moreover if $F \leftarrow\!\!\$\, \mathsf{Func}(n)/\mathsf{Perm}(n)/\mathsf{TPerm}(b, n)$ then it is respectively called a uniform *a random n-bit function/ n-bit permutation/ n-bit tweakable permutation with b-bit tweak.*

A very common choice of such random functions involves specifying a family of functions, a subset $\mathcal{F} \subseteq \mathsf{Func}(n)/\mathsf{Perm}(n)/\mathsf{TPerm}(b,n)$, and let the random function be uniformly distributed over $\mathcal{F}$.

Definition 3 (AXU hash function). *A hash function family $\mathcal{H} = \{H : \{0,1\}^* \to \{0,1\}^n\}$ is called a ϵ-*almost-xor-universal*, if for any $x \neq x' \in \{0,1\}^*, a \in \{0,1\}^n$,*

$$\Pr_{H \leftarrow\$ \mathcal{H}}[H(x) \oplus H(x') = a] \leq \epsilon.$$

Below we observe a very straightforward fact about random permutations:

Proposition 1. *Let $\pi \leftarrow\$ \mathit{Perm}(n)$ be a uniform random permutation. Then given any $x \neq y, \delta \in \{0,1\}^n \setminus \{0^n\}$*

$$\frac{1}{2^n} \leq \Pr\left[\pi(x) \oplus \pi(y) = \delta\right] = \frac{1}{2^n - 1} \leq \frac{2}{2^n}.$$

2.2 H-coefficient Technique

Consider a deterministic and computationally unbounded adversary $\mathcal{A}$ trying to distinguish the real oracle (say $\mathcal{O}_1$) from the ideal oracle (say $\mathcal{O}_0$). Let the transcript ω denote the query-response tuple of $\mathcal{A}$'s interaction with its oracle. Sometimes, at the end of the query-response phase of the game, if the oracle chooses to reveal any additional information to the distinguisher then that information may also be included in the extended definition of the transcript. Let Θ_1 (resp. Θ_0) denote the random transcript variable when $\mathcal{A}$ interacts with $\mathcal{O}_1$ (resp. $\mathcal{O}_0$). The probability of realizing a given transcript ω in the security game with an oracle $\mathcal{O}$ is known as the *interpolation probability* of ω with respect to $\mathcal{O}$. Since $\mathcal{A}$ is deterministic, this probability depends only on the oracle $\mathcal{O}$ and the transcript ω. A transcript ω is said to be *attainable* if $\Pr\left[\Theta_0 = \omega\right] > 0$.

Theorem 1 (H-coefficient technique [44,46]). *Let Ω be the set of all realizable transcripts. For some $\epsilon_{\text{bad}}, \epsilon_{\text{ratio}} > 0$, suppose there is a set $\Omega_{\mathsf{bad}} \subseteq \Omega$ satisfying the following:*

- $\Pr\left[\omega \in \Omega_{\mathsf{bad}}\right] \leq \epsilon_{\text{bad}}$;
- *For any $\omega \notin \Omega_{\mathsf{bad}}$,*

$$\frac{\Pr\left[\Theta_1 = \omega\right]}{\Pr\left[\Theta_0 = \omega\right]} \geq 1 - \epsilon_{\text{ratio}}.$$

Then for any adversary $\mathcal{A}$, we have the following bound on its distinguishing advantage:

$$\mathbf{Adv}^{\text{dist}}_{\mathcal{O}_1}(\mathcal{A}) \leq \epsilon_{\text{bad}} + \epsilon_{\text{ratio}}.$$

A proof of theorem 1 can be found in multiple papers including [46,12,39].

2.3 CPA and CCA security of Tweakable Pseudo-random permutations

Let $\mathcal{E} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ be an b-bit tweakable permutation construction with tweak space $\mathcal{T}$. The CPA/TPRP advantage [34] of $\mathcal{E}$ against an adversary $\mathcal{A}$ with oracle access to $\mathcal{E}$ is defined as follows:

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(\mathcal{A}) = \left|\Pr\left[\mathcal{A}^{\mathcal{E}} = 1\right] - \Pr\left[\mathcal{A}^{\tilde{\Pi}} = 1\right]\right|,$$

where $\tilde{\Pi} \leftarrow\!\!\$\ \mathsf{TPerm}(\mathcal{T}, \{0,1\}^n)$. We write

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(q) = \max_{\mathcal{A}} \mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(\mathcal{A})$$

where maximum is taken over all adversaries $\mathcal{A}$ making at most q queries.

For a tweakable permutation construction $\mathcal{E}$, the CCA/TSPRP advantage of $\mathcal{E}$ against an adversary $\mathcal{A}$ with oracle access to both $\mathcal{E}$ and $\mathcal{E}^{-1}$, is defined as follows:

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{E}}(\mathcal{A}) = \left|\Pr\left[\mathcal{A}^{\mathcal{E},\mathcal{E}^{-1}} = 1\right] - \Pr\left[\mathcal{A}^{\tilde{\Pi},\tilde{\Pi}^{-1}} = 1\right]\right|.$$

where $\tilde{\Pi} \leftarrow\!\!\$\ \mathsf{TPerm}(\mathcal{T}, \{0,1\}^n)$ and $\tilde{\Pi}^{-1}$ is the inverse of $\tilde{\Pi}$ as defined in the preliminary.

We write

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{E}}(q) = \max_{\mathcal{A}} \mathbf{Adv}^{\mathrm{cca}}_{\mathcal{E}}(\mathcal{A})$$

where maximum is taken over all adversaries $\mathcal{A}$ making at most q queries.

2.4 PRF Security of Message Authentication Codes

Let $\mathcal{C} : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^n$ be an MAC construction with key space $\mathcal{K}$ that produces n-bit authentication tags for messages of arbitrary length. The PRF advantage of $\mathcal{C}$ against an adversary $\mathcal{A}$ with oracle access to $\mathcal{C}$ is defined as follows:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathcal{C}}(\mathcal{A}) = \left|\Pr\left[\mathcal{A}^{\mathcal{C}} = 1\right] - \Pr\left[\mathcal{A}^{\varphi} = 1\right]\right|,$$

where $\varphi \leftarrow\!\!\$\ \mathsf{Func}(\mathcal{K} \times \{0,1\}^*, \{0,1\}^n)$. We write

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathcal{C}}(q) = \max_{\mathcal{A}} \mathbf{Adv}^{\mathrm{prf}}_{\mathcal{C}}(\mathcal{A})$$

where maximum is taken over all adversaries $\mathcal{A}$ making at most q queries.

2.5 Revisiting Tweakable LR Constructions

Consider an r round LR construction. As shown by Goldenberg et al. [20] for $1 \leq i \leq r-1$, adding a tweak at any position in the i-th round is equivalent to a construction, where the tweaks are added to the left-hand side of the $i-1, i$, and $i+1$-th round.

More formally, for $i \geq 1$, consider the i-th round of a LR construction defined as $(L_{i-1}, R_{i-1}) \xrightarrow{\Psi_1^{f_i}} (L_i, R_i)$. The possible places where a tweak can be added are

- tweak addition to L_{i-1},
- tweak addition to R_{i-1},
- tweak addition to the part of R_{i-1} which goes into the round function f_i
- tweak addition to L_i,
- tweak addition to R_i

Lemma 1. *[20]*

- *If $i \geq 1$, then tweak addition to R_i is equivalent to tweak addition to L_{i-1}.*
- *If $i \geq 1$, Then tweak addition to the part of R_{i-1} which goes into the round function f_i is equivalent to tweak addition to both R_{i-1} and L_i.*

Corollary 1. *Any r-round tweakable LR construction with arbitrary tweak additions can be reduced to an r-round LR construction where some composition of the tweaks are added to, a subset of $\{R_0\} \cup \{L_i\}_{i=0}^{r}$.*

Consider any subset I of $\{R_0\} \cup \{L_i\}_{i=0}^{r}$. Define

$$a_0(I) := \begin{cases} 0 \text{ if } R_0 \neq I \\ 1 \text{ otherwise.} \end{cases} \quad ; \quad b_i(I) := \begin{cases} 0 \text{ if } L_i \neq I \\ 1 \text{ otherwise.} \end{cases}$$

Then any r-round tweakable LR constructions can be represented by a tuple of bits $(a_0, b_0, \ldots, b_r) \in \{0,1\}^{r+2}$, where

$$\begin{aligned} L_1 \| R_1 &= R_0 + a_0 \cdot T + b_1 \cdot T \parallel L_0 + b_0 \cdot T + f_1(R_0 + a_0 \cdot T) \\ L_i \| R_i &= R_{i-1} + b_i \cdot T \parallel L_{i-1} + f_i(R_{i-1}) \qquad \forall\ i \in \{2, \ldots, r\} \end{aligned}$$

In this paper, we will only consider adversaries that make $\ll 2^n$ queries and try to inspect the minimum round required for obtaining securities against such adversaries. We also consider a more general case of tweak addition, i.e. we consider a tweak modification function ρ (possibly a key-ed function) such that given any tweak T, $\rho(T)$ is added to the LR construction. Note that if ρ is identity then our construction reduces to the construction of [20].

3 Definition and construction of TLR-compatible functions

We define the TLR-compatible family of tweak modification functions as follows:

Definition 4 (TLR-compatible). *A family of tweakable permutations* $\mathcal{F} \subseteq \mathsf{TPerm}(b, 2n)$ *is called* TLR-compatible *if it has the following properties: For* $(T_1, X_1) \neq (T_2, X_2) \in \{0,1\}^b \times \{0,1\}^{2n}$,

- *probability of full collision is negligible, specifically*

$$\Pr_{F \leftarrow\$ \mathcal{F}}[F(T_1, X_1) = F(T_2, X_2)] \leq 2^{-2n+2}.$$

- *probability of collision in the right half of the output is negligible, specifically*

$$\Pr_{F \leftarrow\$ \mathcal{F}}[F(T_1, X_1)_R = F(T_2, X_2)_R] \leq 2^{-n+1}.$$

We observe in the following proposition, the property of TLR-compatible families, that if a function is drawn uniformly from the family then the probability that it will have n multicollisions in the right half of its outputs, is negligible. This fact is useful for our security analyses.

Proposition 2. *Let* $\mathcal{F}$*-be a TLR-compatible function family. Consider any adversary which makes* q *queries to* $F \leftarrow\$ \mathcal{F}$ *to generate outputs* $\{(L_i \| R_i) \mid i \in [q]\}$. *Then if* `mcoll` *denote that event that there exists* $\{i_1, \ldots, i_n\} \subseteq [1, q]$ *such that* $\{R_{i_1} = \cdots = R_{i_n}\}$,

$$\Pr[\texttt{mcoll}] \leq \frac{1}{2} \cdot \left(\frac{4q}{2^n}\right)^n.$$

Proof. It is easy to see that the probability is bounded by $\binom{q}{n} \cdot \left(\frac{2}{2^n}\right)^{n-1} \leq \frac{1}{2} \cdot \left(\frac{4q}{2^n}\right)^n$. □

In what follows we now demonstrate some examples of how to construct TLR-compatible function families for different sizes of the tweak space $\mathcal{T}$. Since our final objective is to use these TLR-compatible functions to construct LR-based constructions, to maintain consistency, we only consider TLR-compatible functions which are constructed using LR rounds. We remark here, that our constructions are examples and not a classification of all possible TLR-compatible function families. Classification of all TLR-compatible functions is a good research direction and is out of the scope of this paper.

3.1 Example of a TLR-compatible function family with $\mathcal{T} = \phi$

Proposition 3. $\mathcal{F} = \{\Psi_1^\pi \mid \pi \in \mathsf{Perm}(n)\}$ *is a TLR-compatible function family.*

Proof. The proposition follows from the observation that Ψ_1^π is a permutation over $\mathsf{Perm}(2n) = \mathsf{TPerm}(0, 2n)$. Hence for any $X_1 \neq X_2$, $\Psi_1^\pi(X_1) \neq \Psi_1^\pi(X_2)$. Further $(\Psi_1^\pi(X_i))_R = \pi((X_i)_R) \oplus (X_i)_L$. Hence by proposition 1;

$$\Pr_{F \leftarrow\$ \mathcal{F}}[(F(X_1))_R = (F(X_2))_R] = \Pr_{\pi \leftarrow\$ \mathsf{Perm}(n)}[(\Psi_1^\pi(X_1))_R = (\Psi_1^\pi(X_2))_R] \leq \frac{2}{2^n}.$$

□

3.2 Example of a TLR-compatible function family $\mathcal{T} = \{0,1\}^n$

Proposition 4. *Given any tweak modification function $\rho \in \mathsf{Perm}(n)$, and a permutation $\pi \in \mathsf{Perm}(n)$, define,*

$$\begin{aligned} F^{\rho,\pi} &: \{0,1\}^{3n} \to \{0,1\}^{2n} \\ &(T, L, R) \mapsto (R \oplus \rho(T), L \oplus \rho(T) \oplus \pi(R)) \end{aligned} \tag{1}$$

Then $\mathcal{F} = \{F^{\rho,\pi} \mid \rho, \pi \in \mathsf{Perm}(n)\}$ is TLR-compatible.

Proof. Let us consider any two tuples $(T_1, L_1 \| R_1) \neq (T_2, L_2 \| R_2)$ and let

$$S_1 \| W_1 := F^{\rho,\pi}((T_1, L_1 \| R_1)); \quad S_2 \| W_2 := F^{\rho,\pi}((T_2, L_2 \| R_2)).$$

In the following calculations, for all symbols corresponding to the tweak, left/right pairs of inputs and outputs, $X \in \{T, L, R, S, W\}$, we write δX to mean $X_1 \oplus X_2$ and for any function f we write $\delta f(X)$ to mean $f(X_1) \oplus f(X_2)$. Note that, $F \leftarrow\$ \mathcal{F}$ has the same distribution as $F^{\rho,\pi}$ where $\rho, \pi \leftarrow\$ \mathsf{Perm}(n)$ are independent uniform random permutations, since the mapping $(\rho, \pi) \mapsto F^{\rho,\pi}$ is bijective.

- If $\delta R \neq 0$

$$\begin{aligned} &\Pr_{F \leftarrow\$ \mathcal{F}}[\delta W = 0] \leq \Pr_{\substack{\pi,\rho \leftarrow\$ \\ \mathsf{Perm}(n)}}[\delta\pi(R) = \delta L \oplus \delta\rho(T)] \\ &= \sum_{C \in \{0,1\}^n} \Pr_{\substack{\pi,\rho \leftarrow\$ \\ \mathsf{Perm}(n)}}[\delta\pi(R) = \delta L \oplus C \mid \delta\rho(T) = C] \times \Pr_{\rho \leftarrow\$ \mathsf{Perm}(n)}[\delta\rho(T) = C] \\ &= \sum_{C \in \{0,1\}^n} \Pr_{\pi \leftarrow\$ \mathsf{Perm}(n)}[\delta\pi(R) = \delta L \oplus C] \times \Pr_{\rho \leftarrow\$ \mathsf{Perm}(n)}[\delta\rho(T) = C] \\ &\overset{(1)}{\leq} \frac{2^n}{(2^n - 1)^2} \leq \frac{2}{2^n}, \qquad [\text{for } n \geq 2] \end{aligned}$$

$$\begin{aligned} &\Pr_{F \leftarrow\$ \mathcal{F}}[\delta S = 0 \wedge \delta W = 0] \\ &\leq \Pr_{\substack{\pi,\rho \leftarrow\$ \\ \mathsf{Perm}(n)}}[\delta R = \delta\rho(T) \wedge \delta\pi(R) = \delta L \oplus \delta\rho(T)] \\ &= \Pr_{\rho \leftarrow\$ \mathsf{Perm}(n)}[\delta R = \delta\rho(T)] \times \Pr_{\pi \leftarrow\$ \mathsf{Perm}(n)}[\delta\pi(R) = \delta L \oplus \delta R] \overset{(2)}{\leq} \frac{4}{2^{2n}} \end{aligned}$$

– If $\delta R = 0$ but $\delta L \neq 0$

$$\begin{aligned}\Pr_{F \leftarrow\$ \mathcal{F}}[\delta W = 0] &= \Pr_{\rho \leftarrow\$ \mathsf{Perm}(n)}[\delta\rho(T) = \delta L] \overset{(3)}{\leq} \frac{2}{2^n}.\\ \Pr_{F \leftarrow\$ \mathcal{F}}[\delta S = 0 \wedge \delta W = 0] &= \Pr_{\rho \leftarrow\$ \mathsf{Perm}(n)}[\delta\rho(T) = 0] \times \Pr_{\rho \leftarrow\$ \mathsf{Perm}(n)}[\delta L = 0 \mid \delta\rho(T) = 0]\\ &= 0.\end{aligned}$$

– If $\delta R = 0, \delta L = 0$ but $\delta T \neq 0$

$$\begin{aligned}\Pr_{F \leftarrow\$ \mathcal{F}}[\delta W = 0] &= \Pr_{\rho \leftarrow\$ \mathsf{Perm}(n)}[\delta\rho(T) = 0] = 0.\\ \Pr_{F \leftarrow\$ \mathcal{F}}[\delta S = 0 \wedge \delta W = 0] &= \Pr_{\rho \leftarrow\$ \mathsf{Perm}(n)}[\delta\rho(T) = 0] = 0.\end{aligned}$$

where inequalities (1), (2), (3) follow from proposition 1. □

3.3 Example of a TLR-compatible function family $\mathcal{T} \in \{0,1\}^*$

As before we start by considering the function defined by Goldenberg et al. [20]. For b blocks of tweak their construction of an *TLR-compatible* function F involves $b + 2$ round LR construction. In what follows we try to minimize this heavy processing with two tweak processing functions and a 1-round LR construction with suitable processed-tweak injections.

Proposition 5. *Given $\rho_1, \rho_2 \in \mathcal{H}$ where $\mathcal{H}$ is any $2^{-(n+1)}$-AXU hash family, and a permutation $\pi \in \mathsf{Perm}(n)$, define,*

$$\begin{aligned}F^{\rho_1,\rho_2,\pi} : \{0,1\}^{3n} &\to \{0,1\}^{2n}\\ (T, L, R) &\mapsto (R \oplus \rho_1(T), L \oplus \rho_2(T) \oplus \pi(R))\end{aligned} \tag{2}$$

Then $\mathcal{F} = \{F^{\rho_1,\rho_2,\pi} \mid \rho_1, \rho_2 \in \mathcal{H}; \pi \in \mathsf{Perm}(n)\}$ is TLR-compatible.

Proof. Again let us consider any two tuples $(T_1, L_1 \| R_1) \neq (T_2, L_2 \| R_2)$ and let

$$S_1 \| W_1 := F^{\rho_1,\rho_2,\pi}((T_1, L_1 \| R_1)); \quad S_2 \| W_2 := F^{\rho_1,\rho_2,\pi}((T_2, L_2 \| R_2)).$$

As before for all symbols corresponding to the tweak, left/right pairs of inputs and outputs, $X \in \{T, L, R, S, W\}$, we write δX to mean $X_1 \oplus X_2$ and for any function f we write $\delta f(X)$ to mean $f(X_1) \oplus f(X_2)$. Note that, $F \leftarrow\$ \mathcal{F}$ has the same distribution as $F^{\rho_1,\rho_2,\pi}$ where $\rho_1, \rho_2 \leftarrow\$ \mathcal{H}; \pi \leftarrow\$ \mathsf{Perm}(n)$ since the mapping $(\rho_1, \rho_2, \pi) \mapsto F^{\rho_1,\rho_2,\pi}$ is bijective.

– If $\delta R \neq 0$

$$\begin{aligned}
&\Pr_{F \leftarrow\$ \mathcal{F}}[\delta W = 0] \\
&\leq \Pr_{\substack{\pi \leftarrow\$ \mathsf{Perm}(n) \\ \rho_2 \leftarrow\$ \mathcal{H}}}[\delta\pi(R) = \delta L \oplus \delta\rho_2(T)] \overset{(1)}{\leq} \frac{2}{2^n} \\
&\Pr_{F \leftarrow\$ \mathcal{F}}[\delta S = 0 \wedge \delta W = 0] \\
&\leq \Pr_{\rho_1 \leftarrow\$ \mathcal{H}}[\delta R = \delta\rho_1(T)] \times \Pr_{\substack{\pi \leftarrow\$ \mathsf{Perm}(n) \\ \rho_2 \leftarrow\$ \mathcal{H}}}[\delta\pi(R) = \delta L \oplus \delta\rho_2(T)] \overset{(2)}{\leq} \frac{4}{2^{2n}}
\end{aligned}$$

– If $\delta R = 0$ but $\delta L \neq 0$

$$\begin{aligned}
\Pr_{F \leftarrow\$ \mathcal{F}}[\delta W = 0] &= \Pr_{\rho_2 \leftarrow\$ \mathcal{H}}[\delta\rho_2(T) = \delta L] \overset{(3)}{\leq} \frac{2}{2^n}. \\
\Pr_{F \leftarrow\$ \mathcal{F}}[\delta S = 0 \wedge \delta W = 0] &= \Pr_{\rho_1 \leftarrow\$ \mathcal{H}}[\delta\rho_1(T) = 0] \times \Pr_{\substack{\rho_1, \rho_2 \\ \leftarrow\$ \mathcal{H}}}[\delta\rho_2(T) = \delta L \mid \rho_1(T) = 0] \\
&\leq \Pr_{\rho_1 \leftarrow\$ \mathcal{H}}[\delta\rho_1(T) = 0] \times \Pr_{\rho_2 \leftarrow\$ \mathcal{H}}[\delta\rho_2(T) = \delta L] \\
&\overset{(4)}{\leq} \frac{4}{2^{2n}}.
\end{aligned}$$

– If $\delta R = 0, \delta L = 0$ but $\delta T \neq 0$

$$\begin{aligned}
\Pr_{F \leftarrow\$ \mathcal{F}}[\delta W = 0] &= \Pr_{\rho_2 \leftarrow\$ \mathcal{H}}[\delta\rho_2(T) = 0] \overset{(5)}{\leq} \frac{2}{2^n}. \\
\Pr_{F \leftarrow\$ \mathcal{F}}[\delta S = 0 \wedge \delta W = 0] &= \Pr_{\rho_1 \leftarrow\$ \mathcal{H}}[\delta\rho_1(T) = 0] \times \Pr_{\rho_2 \leftarrow\$ \mathcal{H}}[\delta\rho_2(T) = 0] \overset{(6)}{\leq} \frac{4}{2^{2n}}.
\end{aligned}$$

where inequalities (1), (2), (3), (4), (5), (6) depend on proposition 1 and AXU-property. □

4 Constructing CPA/CCA secure LR constructions using random permutations

In this section, we describe how to use TLR-compatible function families to process tweaks and inject them into permutation-based LR to achieve n-bit secure TPRP and TSPRP. We also instantiate TLR-compatible function families to deal with single-block tweaks and variable-length tweaks. Combining these, we propose TPRP and TSPRP constructions for fixed-length and variable-length tweaks.

Theorem 2. *Let $\mathcal{F} \subseteq \mathsf{TPerm}(b, 2n)$ be a TLR-compatible function family. Given independent uniform random permutations $\pi_1, \ldots, \pi_4 \leftarrow\!\$\ \mathsf{Perm}(n)$ and $F \leftarrow\!\$\ \mathcal{F}$, consider the construction*

$$\Psi_4^{(\pi_1,\pi_2,\pi_3,\pi_4)} \circ F : \{0,1\}^b \times \{0,1\}^{2n} \to \{0,1\}^{2n}.$$

If $n \geq 30$ and $q \leq \frac{2^n}{48n^2}$, then

$$\mathbf{Adv}^{\mathrm{cpa}}_{\Psi_4^{(\pi_1,\pi_2,\pi_3,\pi_4)} \circ F}(q) \leq \frac{45q}{2^n} + \frac{(36n+79)q^2}{2^{2n}} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Theorem 3. *Let $\mathcal{F} \subseteq \mathsf{TPerm}(b, 2n)$ be a TLR-compatible function family. Given independent uniform random permutations $\pi_1, \ldots, \pi_5 \leftarrow\!\$\ \mathsf{Perm}(n)$ and random functions $F_1, F_2 \leftarrow\!\$\ \mathcal{F}$, consider the construction $F_2^{-1} \circ \Psi_5^{(\pi_1,\pi_2,\pi_3,\pi_4,\pi_5)} \circ F_1$. If $n \geq 30$ and $q \leq \frac{2^n}{48n^2}$, then*

$$\mathbf{Adv}^{\mathrm{cca}}_{F_2^{-1} \circ \Psi_5^{(\pi_1,\pi_2,\pi_3,\pi_4,\pi_5)} \circ F_1}(q) \leq \frac{45q}{2^n} + \frac{(36n+81)q^2}{2^{2n}} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Remark 1. The proof of theorem 2 and 3 are given in sections 6 and 7 respectively.

Corollary 2. *Let $\pi_1, \ldots, \pi_7 \leftarrow\!\$\ \mathsf{Perm}(n)$ be independent uniform random permutations. If $n \geq 30$ and $q \leq \frac{2^n}{48n^2}$, then*

$$\mathbf{Adv}^{\mathrm{cpa}}_{\Psi_5^{(\pi_1,\ldots,\pi_5)}} \leq \frac{(36n+79)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

$$\mathbf{Adv}^{\mathrm{cca}}_{\Psi_7^{(\pi_1,\ldots,\pi_7)}} \leq \frac{(36n+81)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Proof. The corollary follows from theorems 2,3 and proposition 3.

Corollary 3. *Let $\rho, \pi_1, \ldots, \pi_7 \leftarrow\!\$\ \mathsf{Perm}(n)$ be independent uniform permutations. Let F^{ρ,π_1} and F^{ρ,π_7} be defined as in (1). Then if $n \geq 30$ and $q \leq \frac{2^n}{48n^2}$, the* TLRP5 *construction (see Fig. 1.1) and* TLRP7 *construction (see Fig. 1.1), defined as*

$$\begin{aligned}\mathsf{TLRP5} : \{0,1\}^n \times \{0,1\}^{2n} &\to \{0,1\}^{2n} \\ (T, L, R) &\mapsto \Psi_4^{(\pi_2,\ldots,\pi_5)} \circ F^{\rho,\pi_1}(T, L, R)\end{aligned}$$

$$\begin{aligned}\mathsf{TLRP7} : \{0,1\}^n \times \{0,1\}^{2n} &\to \{0,1\}^{2n} \\ (T, L, R) &\mapsto (F^{\rho,\pi_7})^{-1} \circ \Psi_5^{(\pi_2,\ldots,\pi_6)} \circ F^{\rho,\pi_1}(T, L, R)\end{aligned}$$

satisfies

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{TLRP5}}(q) \leq \frac{(36n+79)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n;$$

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TLRP7}} \leq (q)\frac{(36n+81)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Proof. The corollary follows from theorems 2,3 and proposition 4.

Corollary 4. *Let $\pi_1, \ldots, \pi_7 \leftarrow\!\$\ \mathsf{Perm}(n)$ be independent uniform permutations, and let $\rho_1, \rho_2 \leftarrow\!\$\ \mathcal{H}$, where $\mathcal{H}$ is a 2^{-n+1}-AXU hash function family. Let F^{ρ_1,ρ_2,π_1} and F^{ρ_1,ρ_2,π_7} be defined as in (2). Then if $n \geq 30$ and $q \leq \frac{2^n}{48n^2}$, the* TLRP5+ *construction (see Fig. 1.1) and* TLRP7+ *construction (see Fig. 1.1), defined as*

$$\begin{aligned}\mathsf{TLRP5}+ : \{0,1\}^* \times \{0,1\}^{2n} &\to \{0,1\}^{2n}\\ (T,L,R) &\mapsto \Psi_4^{(\pi_2,\ldots,\pi_5)} \circ F^{\rho_1,\rho_2,\pi_1}(T,L,R)\end{aligned}$$

$$\begin{aligned}\mathsf{TLRP7}+ : \{0,1\}^* \times \{0,1\}^{2n} &\to \{0,1\}^{2n}\\ (T,L,R) &\mapsto (F^{\rho_1,\rho_2,\pi_7})^{-1} \circ \Psi_5^{(\pi_2,\ldots,\pi_6)} \circ F^{\rho_1,\rho_2,\pi_1}(T,L,R)\end{aligned}$$

satisfies

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{TLRP5}+}(q) \leq \frac{(36n+79)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n;$$

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TLRP7}+} \leq (q)\frac{(36n+81)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Proof. The corollary follows from theorems 2,3 and proposition 5.

5 Mirror Theory for three independent permutations

At a high level, Mirror Theory [47] results state that the number of "constrained" solutions[3] to a system of equations is at least as much as the expected number of such constrained solutions to the system of equations where the constants are chosen uniformly randomly. Typically, such lower bounds hold under some assumption on the block-maximality of the system of equations, denoted $\xi_{\max}$, which is defined as the maximum number of variables whose values get determined if you assign value to one variable. Patarin [47] studied this problem with the constraint on the solution being that every variable should be distinct from each other, and conjectured lower bounds, with an incomplete proof for the case

[3] By constrained solutions we mean solutions that satisfy particular constraints, often manifested as a system of non-equations

$\xi_{\max} = 2$. Mennink et al. [40] conjectured a more generalized version of this result, termed "relaxed mirror theory" [40, Theorem 3], where they partitioned the variable set into some p disjoint sets and the solutions are required to satisfy the constraint that variables belonging to the same partition must be distinct from each other. Note that if there are v variables and $[v] = I_1 \sqcup \cdots \sqcup I_p$ is a partition of the variable indices into p disjoint sets, then the expected number of such constrained solutions for a random system of equations containing e equations (i.e., the constants of these equations are chosen uniformly randomly) in these variables will be

$$\frac{(2^n)_{|I_1|} \times \cdots \times (2^n)_{|I_p|}}{2^{ne}}$$

Guo et al. [21] proved a suboptimal version of this result for $p = 3$ with an $O(e^3/2^{2n})$ error term. Later, Cogliati et al. [14] came up with a verifiable proof for Patarin's conjecture [47] for general $\xi_{\max}$, and following their proof approach, Choi et al. [13] proved Mennink's conjecture [40, Theorem 3] for $p = 2$. In this paper, we have adopted Choi et al.'s proof strategy to prove Mennink's relaxed Mirror theory conjecture for $p = 3$. As we will see later in the security analyses of our constructions, the i/o variables of the 3 inner permutations must satisfy a system of equations to be compatible with the LR design, and the i/o variables corresponding to the same permutation must be distinct from each other, result in the 3-way partition of the variable set.

General system of equations and properties. Consider a system of $2q \geq 1$ equations,

$$\mathcal{E} = \begin{Bmatrix} P_{\omega(a_1)} \oplus P_{\omega(b_1)} = \lambda_1, & P_{\omega(b_1)} \oplus P_{\omega(c_1)} = \gamma_1, \\ & \vdots \\ P_{\omega(a_q)} \oplus P_{\omega(b_q)} = \lambda_q, & P_{\omega(b_q)} \oplus P_{\omega(c_q)} = \gamma_q. \end{Bmatrix} \tag{3}$$

over $k \geq 1$ unknowns $\mathcal{P} = \{P_1, \ldots, P_k\}$ where ω is some onto index mapping

$$\omega : \{a_1, b_1, c_1, \ldots, a_q, b_q, c_q\} \to \{1, \ldots, k\}.$$

such that $I_1 := \{\omega(a_i) : i \in [q]\}, I_2 := \{\omega(b_i) : i \in [q]\}, I_3 := \{\omega(c_i) : i \in [q]\}$ forms a disjoint partition of $[k]$.

Definition 5 ((I_1, I_2, I_3)-respecting). *We call a tuple, $(x_1, \ldots, x_k)$, (I_1, I_2, I_3)-respecting if $x_i \neq x_j$ for any $i, j \in I_s, s \in \{1, 2, 3\}$.*

For such a system of bivariate equations $\mathcal{E}$, we say two unknowns P_j and P'_j are in the same block if the system of equation $\mathcal{E}$ implies $P_i \oplus P_j = c$ for some known constant c. With this definition we define

- **Cycles:** We say $\mathcal{E}$ has a cycle if there exists $I \subseteq [q]$ such that $\{P_i \mid i \in I\}$ are in the same block and for all $i \in I$, P_i has even multiplicity.

- **Block-maximality**: Let $[k] = R_1 \cup R_2 \cdots \cup R_m$ be a partition of $[k]$ in m minimal blocks such that for each $i \in [q]$ there exists a unique $l \in [m]$ with $\{\omega(a_i), \omega(b_i), \omega(c_i)\} \subseteq R_l$. then we say $\mathcal{E}$ is ξ- block maximal for $\xi \geq 3$ if $|R_l| < \xi$ for all $l \in [m]$.
- **Degeneracy:** There exists two distinct indices $j, j' \in I_s, s \in \{1,2,3\}$ such that $\mathcal{E}$ implies $P_j = P'_j$.

With this definition, we now state our Mirror Theory result for 3 independent permutations.

Theorem 4. *Let $\mathcal{E}$ be a system of $2q$ equations over the unknowns $\mathcal{P}$ and each unknown takes value in $\{0,1\}^n, n \geq 1$. Then if $\mathcal{E}$ is (i) circle-free, (ii) ξ-block-maximal for some ξ such that $q \leq \frac{2^n}{48\xi^2}$ and $2^{n/2} > n\xi^2 + n$, and (iii) non-degenerate with respect to some partition I_1, I_2, I_3 of $[k]$, then we have number of (I_1, I_2, I_3)-respecting solutions to the system of equations $\mathcal{E}$ is lower bounded by*

$$\frac{(2^n - 2)_{|I_1|}(2^n - 2)_{|I_2|}(2^n - 2)_{|I_3|}}{2^{2nq}}.$$

Graphical representation of a system of equations. Any system of bivariate equations, $\mathcal{E}'$, can be represented by an undirected edge-labeled graph, denoted $\mathcal{G}(\mathcal{E}')$, by letting the vertices represent the variables and corresponding to each equation in the system, say $P_i \oplus P_j = \lambda$, there is an edge between the vertices P_i and P_j labeled λ. Equivalently, any undirected edge-labeled graph $\mathcal{G}$ corresponds to a unique system of bivariate equations, denoted as $\mathcal{E}(\mathcal{G})$. In particular, for the type of systems of equations considered in this paper, $\mathcal{E}$ described in (3), the corresponding graph, $\mathcal{G}(\mathcal{E})$, with vertex set $\mathcal{V}(\mathcal{E}) := \{P_1, \ldots P_k\}$ and $2q$ edges, also turns out to be tripartite: the partition $[k] = I_1 \sqcup I_2 \sqcup I_3$ induces the partition of the vertex set $\mathcal{V}(\mathcal{E}) = \mathcal{V}_1 \sqcup \mathcal{V}_2 \sqcup \mathcal{V}_3$ where $\mathcal{V}_i := \{P_j : j \in I_i\}, i \in \{1,2,3\}$. Note that there are edges between vertices of I_1 and I_2 or between vertices of I_2 and I_3, and the graph is indeed tripartite. The partition $\mathcal{V} = \mathcal{V}_1 \sqcup \mathcal{V}_2 \sqcup \mathcal{V}_3$ induces the equivalence relation $P \sim P'$ if both $P, P' \in \mathcal{V}_i$ for some $i \in \{1,2,3\}$.

Now recall the definition of blocks: $i, j \in [k]$ are said to be in the same block if the system of equations implies $P_i \oplus P_j = \lambda$. This definition translates in graph-theoretic terminology to have a path from vertex P_i to P_j with edge-label-sum λ. Thus the partition $[k] = R_1 \sqcup \cdots \sqcup R_m$ of the index set $[k]$ into m minimal blocks corresponds to the partition of the vertex set $\mathcal{V}(\mathcal{E})$ into the connected components of the graph, $\mathcal{V}(\mathcal{E}) = \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_m$, with $\mathcal{C}_i = \{P_j : j \in R_i\}$, $i \in [m]$. Note that for every $i \in [q]$, there exists a unique $\ell \in [m]$, such that $P_{\omega(a_i)}, P_{\omega(b_i)}, P_{\omega(c_i)} \in \mathcal{C}_\ell$. We abuse notation when we also denote by $\mathcal{G}$ the collection $\{\mathcal{C}_1, \ldots, \mathcal{C}_m\}$ of components of the graph $\mathcal{G}$. For a vertex $v \in \mathcal{G}$, we denote by $\mathcal{C}_v(\mathcal{G})$, the component containing of $\mathcal{G}$ containing v.

Thus, we can express the cycle-free, ξ-block-maximality and degeneracy conditions on a system of equations, $\mathcal{E}$, in equivalent graph-theoretic terms as:

- **Cycle-free:** $\mathcal{G}(\mathcal{E})$ is acyclic.

- ξ**-block-maximality:** Size of the largest component of $\mathcal{G}(\mathcal{E})$ is upper bounded by ξ, i.e., $|\mathcal{C}_i| < \epsilon$.
- **Degeneracy:** For some $P_r \sim P_s$, there exists a path between P_r and P_s that have edge-label-sum 0.

Note that the cycle-free condition implies that there is at most one path between any two vertices. The non-degeneracy condition is necessary for $\mathcal{E}$ to have a (I_1, I_2, I_3)-respecting solution. We are concerned with the number of (I_1, I_2, I_3)-respecting solutions satisfying a cycle-free, ξ-block-maximal and non-degenerate system of equations, with the corresponding graph $\mathcal{G}$, which we will denote by $N(\mathcal{G})$.

Label Function. For any undirected edge-labeled graph $\mathcal{G}$ with vertex set $\mathcal{V}$ we can define a label function $\Lambda : \mathcal{V} \times \mathcal{V} \to \{0,1\}^n \cup \{\perp\}$ which maps (P_i, P_j) to λ if there is a path between P_i and P_j with edge-label-sum λ, or maps (P_i, P_j) to $\perp$ if there exists no path between P_i and P_j. We assume the convention that $\Lambda(P_i, P_i) = 0$. Note that the label function captures all possible bivariate equations implied by $\mathcal{E}(\mathcal{G})$, that is if $\mathcal{E}$ implies the equation $P_i \oplus P_j = \lambda$, then we have $\Lambda(P_i, P_j) = \lambda$, and if $\mathcal{E}$ does not imply such a relation between P_i and P_j, then $\Lambda(P_i, P_j) = \perp$. All graphs, $\mathcal{G}$, sharing a common vertex set, that induces the same label function are equivalent, in the sense that they have the exact same set of (I_1, I_2, I_3)-respecting solutions.

Graph Transformations. We will start with the system of equations $\mathcal{E}$ described in (3) and then prove Theorem 4 via induction. For that purpose, we will make several modifications to the underlying graph $\mathcal{G}(\mathcal{E})$. For a general undirected edge-labeled graph $\mathcal{G}$ with components $\mathcal{A}_1, \ldots, \mathcal{A}_a$, or abusing notation, $\mathcal{G} = \{\mathcal{A}_1, \ldots, \mathcal{A}_a\}$, we will consider the following transformations:

- *Removing a component.* Consider a component $S \in \mathcal{G}$, then the graph obtained by removing the entire component S is denoted as $\mathcal{G}_{-S}$.
- *Removing a vertex.* Consider a vertex $v \in S \in \mathcal{G}$. Suppose we remove the vertex v from $\mathcal{G}$, choose a vertex u in the neighborhood of v, and for any other vertex u' in the neighborhood of v add an edge between u and u' with label $\Lambda(u, u')$. If $\mathcal{G}$ was cycle-free, ξ-block-maximal, and non-degenerate, then this reduced graph will also have these properties. This transformation would result in a different graph for every choice of u in the neighborhood of v, however, all of them will be equivalent, in the sense that they will have the exact same set of (I_1, I_2, I_3)-respecting solutions. We denote any such graph as $\mathcal{G}_{-v}$. When vertices $v_1, \ldots, v_r$ are removed from $\mathcal{G}$ one by one in the aforementioned way, we denote the resulting graph as $\mathcal{G}_{-v_1-\cdots-v_r}$.

Any graph $\mathcal{G}$ obtained as a result of applying the above transformations, multiple times in some arbitrary order, to $\mathcal{G}(\mathcal{E})$, is called a reduced graph of $\mathcal{G}(\mathcal{E})$, and the corresponding system of equations, $\mathcal{E}(\mathcal{G})$, is called a reduced system of $\mathcal{E}$.

We start with a system of equations $\mathcal{E}$ with its collection of variables, that is the vertex set $\mathcal{V}(\mathcal{E}) = \mathcal{V}_1 \sqcup \mathcal{V}_2 \sqcup \mathcal{V}_3$ of $\mathcal{G}(\mathcal{E})$, and compare its number of (I_1, I_2, I_3)-respecting solutions with that of the reduced graphs with reduced number of vertices. For such a reduced graph $\mathcal{G} = \{\mathcal{A}_1, \ldots, \mathcal{A}_a\}$, we denote the number of vertices belonging to each of the partitions $\mathcal{V}_1, \mathcal{V}_2$ and $\mathcal{V}_3$ as

$$\eta_1(\mathcal{G}) := \sum_{i=1}^{a} |\mathcal{A}_i \cap \mathcal{V}_1|, \qquad \eta_2(\mathcal{G}) := \sum_{i=1}^{a} |\mathcal{A}_i \cap \mathcal{V}_2|, \qquad \eta_3(\mathcal{G}) := \sum_{i=1}^{a} |\mathcal{A}_i \cap \mathcal{V}_3|.$$

Moreover, for $i \in \{1, 2, 3\}$, $v \in \mathcal{V}_i$, we write $\eta_v(\mathcal{G}) := \eta_i(\mathcal{G})$. Note that $\sum_{i=1}^{3} \eta_i(\mathcal{G}(\mathcal{E})) = k$, the number of variables in $\mathcal{E}$. Since we are dealing with bivariate equations the number of variables must be at most twice the number of equations. Thus $k \leq 2 \cdot 2q \leq 2^n/12\xi_{\max}^2$. We will use this bound on the number of variables/vertices in the following proof.

Finally, for such a reduced graph we will denote the size of the largest component of $\mathcal{G}$ as $\xi_{\mathcal{G}} = \max_{i \in [a]} |\mathcal{A}_i|$.

Multiplicity of paths. Given two vertices u and v and a component $S \in \mathcal{G}$, the number of paths between vertices $a, b \in S$, with $a \sim u$ and $b \sim v$, that has edge-label-sum same as the edge-label-sum of the path between u and v, is denoted as

$$\delta_S(u, v) := \#\{\{a, b\} \mid a, b \in S, a \sim u, b \sim v, \Lambda(a, b) = \Lambda(u, v)\}$$

Moreover, we denote

$$\delta_{\mathcal{G}}(u, v) := \sum_{S \in \mathcal{G}} \delta_S(u, v), \quad \Delta_{\mathcal{G}} := \max_{S \in \mathcal{G}} \max_{(u,v) \in S^{*2}} \delta_{\mathcal{G}}(u, v)$$

With the above notations we are equipped to present the proof of Theorem 4.

Proof of Theorem 4. Let $\mathcal{G}$ be a reduced graph of $\mathcal{G}(\mathcal{E})$. For any component $S \in \mathcal{G}$ we claim that

$$N(\mathcal{G}) \geq 2^n \cdot N(\mathcal{G}_{-S}) \cdot \prod_{i=1}^{3} \prod_{\substack{j= \\ \eta_i(\mathcal{G}_{-S})+1}}^{\eta_i(\mathcal{G})} \left(1 - \frac{i+1}{2^n}\right)$$

If the above claim holds then we have our result, since then we will start with $\mathcal{G}(\mathcal{E}) = \{\mathcal{C}_1, \ldots, \mathcal{C}_m\}$ and remove the components one after one and multiply the resulting inequality implied by the claim for $\mathcal{G}(\mathcal{E}), \mathcal{G}(\mathcal{E}) \setminus \{\mathcal{C}_1\}, \ldots, \mathcal{G} \setminus \{\mathcal{C}_1, \ldots, \mathcal{C}_{m-1}\}$ and noting the following:

- the number of components $m = k - 2q$, k being the number of variables/vertices and $2q$ being the number of equations/edges,
- $\eta_i(\mathcal{G}(\mathcal{E})) = |\mathcal{V}_i|$ for $i \in \{1, 2, 3\}$,

we have the statement of the theorem.

Now we prove the above claim by dividing it into the following cases:

- $|S| = 1$. That is $S = \{v\}$. Corresponding to each (I_1, I_2, I_3)-respecting solution to $\mathcal{E}(\mathcal{G}_{-S})$, there are at least $2^n - \eta_v(\mathcal{G}_{-S}) = 2^n - \eta_v(\mathcal{G}) + 1$ possible n-bit values which if assigned to v will yield that many solutions for $\mathcal{E}(\mathcal{G})$. This directly yields our claim since

$$N(\mathcal{G}) = N(\mathcal{G}_{-S}) \cdot (2^n - \eta_v(G) + 1)$$

- $|S| \geq 2$. We consider two subcases:
  - $k \leq 2^{n/2}$. Now if some vertex $u \in S$ is assigned a n-bit value $x_u \in \{0,1\}^n$ the values of all the other variables $v \in S$ are determined as $x_u \oplus \Lambda(u, v)$. Given a solution to $\mathcal{E}(\mathcal{G}_{-S})$, the values thus assigned to the $\eta_i(S)$ vertices in $S \cap \mathcal{V}_i$ should not coincide with any of the values assigned to $\eta_i(\mathcal{G}_{-S})$ vertices in $\mathcal{V}(\mathcal{G}_{-S}) \cap \mathcal{V}_i$. Hence we have

$$N(\mathcal{G}) \geq N(\mathcal{G}_{-S}) \cdot \left(2^n - \sum_{i=1}^{3} \eta_i(S) \cdot \eta_i(\mathcal{G}_{-S})\right) \tag{4}$$

    Thus if we can show

$$1 - \sum_{i=1}^{3} \frac{\eta_i(S) \cdot \eta_i(\mathcal{G}_{-S})}{2^n} \geq \prod_{i=1}^{3} \prod_{\substack{j= \\ \eta_i(\mathcal{G}_{-S})+1}}^{\eta_i(\mathcal{G})} \left(1 - \frac{i+1}{2^n}\right)$$

    then we have our claim.
    Substituting $a = \eta_1(S), r = \eta_1(\mathcal{G}_{-S}), b = \eta_2(S), s = \eta_2(\mathcal{G}_{-S}), c = \eta_3(S), t = \eta_3(\mathcal{G}_{-S})$, we have to show

$$1 - \frac{ar + bs + ct}{2^n} \geq \prod_{i=2}^{r+1} \left(1 - \frac{a+i}{2^n}\right) \cdot \prod_{i=2}^{s+1} \left(1 - \frac{b+i}{2^n}\right) \cdot \prod_{i=2}^{t+1} \left(1 - \frac{c+i}{2^n}\right) \tag{5}$$

    This can be shown by induction on r, s, and t. For $r = s = t = 1$, the inequality holds since

$$\begin{aligned}\left(1 - \frac{a+2}{2^n}\right)\left(1 - \frac{b+2}{2^n}\right)\left(1 - \frac{c+2}{2^n}\right) &= 1 - \frac{a+b+c}{2^n} - C \\ &\leq 1 - \frac{a+b+c}{2^n}\end{aligned}$$

    where

$$C = \frac{8}{2^n}\left(1 - \frac{(a+2)(b+2)}{2^{n+3}} - \frac{(b+2)(c+2)}{2^{n+3}} - \frac{(c+2)(a+2)}{2^{n+3}} + \frac{(a+2)(b+2)(c+2)}{2^{2n+3}}\right) \geq 0$$

since $a, b, c \le a+b+c \le k \le 2^{n/2} \implies (a+2)(b+2)+(b+2)(c+2)+(c+2)(a+2) \le 2^{n+2}$. W.l.o.g. assume $r \ge s = t$. A similar argument will also hold for any other ordering of r, s and t too. In this case, the inequality holds because

$$\begin{aligned}
&\left(1-\frac{a(r-1)+bs+ct}{2^n}\right)\left(1-\frac{a+r+1}{2^n}\right)\\
&\le 1-\frac{ar+bs+ct}{2^n}-\frac{r+1}{2^n}+\frac{(a(r-1)+bs+ct)(a+r+1)}{2^{2n}}\\
&\le 1-\frac{ar+bs+ct}{2^n}-\frac{r+1}{2^n}\left(1-\frac{(a+b+c)(a+r+1)}{2^n}\right)\\
&\le 1-\frac{ar+bs+ct}{2^n}
\end{aligned}$$

since $a+b+c \le 2^{n/2}$ and $a+r+1 \le 2^{n/2}$.

- $2^{n/2} \le k \le 2^n/12\xi_{\max}^2$. For this case, we state the following lemma, the proof of which can be found in section 9.

  Lemma 2 (Core Lemma). *Suppose for $u, v \in S \in \mathcal{G}$, the edge-label-sum of the path between u, v attains the maximum multiplicity $\Delta_{\mathcal{G}}$. If $2^{n/2} \le k \le 2^n/12\xi_{\max}^2$, we have*

  $$N(\mathcal{G}) \ge N(\mathcal{G}_{-v})\left(1-\frac{\eta_v(\mathcal{G})+1}{2^n}\right)$$

  Now we remove the vertices one by one from $\mathcal{G}$ in an order, $v_1, v_2, \ldots, v_\ell$, until the number of vertices left, $k-\ell$, falls below $2^{n/2}$. Here v_{i+1} is chosen in such a way that there are exactly $\Delta_{\mathcal{G}_{-v_1-\cdots-v_i}}$ paths starting from v_{i+1} having the same edge-label-sum, in which case we can apply Lemma 2 iteratively ℓ times. Finally, when the number of vertices falls below $2^{n/2}$, we can apply the first subcase and multiply all the inequalities to yield our desired result.

This proves Theorem 4 modulo the proof of Lemma 2. □

6 Proof of theorem 2

We employ the coefficient H-technique and assume that the adversary doesn't make any redundant queries. The proof approach is an adaptation of the CPA security proof of 5-round LR construction by Guo et al. [21] with the new mirror theory result in Theorem 4.

Consider the CPA challenger which proceeds as follows.

– In the ideal world, the oracle chooses a random tweakable permutation, $\tilde{\Pi} : \{0,1\}^b \times \{0,1\}^{2n} \to \{0,1\}^{2n}$. For each query $(T_i, X_i) \in \{0,1\}^b \times \{0,1\}^{2n}$, the oracle outputs $S_i \| W_i := \Pi(T_i, X_i)$ as it's response.

– In the real world, for each query $(T_i, X_i) \in \{0,1\}^b \times \{0,1\}^{2n}$, the oracle makes all the necessary computations honestly and outputs the honest response $S_i \| W_i$.

After the query-response phase is done with the adversary the oracle release some additional states as follows,

– In the real world for each query $((T_i, X_i) \in \{0,1\}^b \times \{0,1\}^{2n})_{i\in[q]}$, the oracle computes, $L_i \| |R_i := \Psi_1^{\pi_1} \circ F(T_i, X_i)$. Finally it sends $(T_i, X_i, L_i \| R_i, S_i \| W_i)_{i\in[q]}$ as the query transcript for the adversary.
– in the ideal world the oracle selects a random permutations $\pi_1' : \{0,1\}^n \to \{0,1\}^n$ and a $F' \leftarrow\!\$\ \mathcal{F}$. It computes $L_i \| R_i := \Psi_1^{\pi_1'} \circ F'(T_i, X_i)$. Finally it sends $(T_i, X_i, L_i \| R_i, S_i \| W_i)_{i\in[q]}$ as the query transcript for the adversary.

let $\tau := \{(T_i, X_i, L_i \| R_i, S_i \| W_i) \mid i \in [q]\}$ be the final query transcript of the adversary.

6.1 Bad transcripts in the ideal world

Note that in the ideal world the function $F \leftarrow\!\$\ \mathcal{F}$ is simulated with another function $F' \leftarrow\!\$\ \mathcal{F}_b$. And the random permutation π_1 is simulated with a random permutation pi_1'. So no adversary can distinguish between the ideal world or real world by only observing $(T_i, X_i, L_i \| R_i)_{i\in[q]}$.

Note that in the real world $\Psi_3^{(\pi_2,\pi_3,\pi_4)}(L_i \| R_i) = S_i \| W_i$. Hence the transcript is permutation compatible. On the other hand in the ideal world $S_i \| W_i$ are chosen using a variable-tweak length-ed tweakable random permutation. Further $L_i \| R_i$ are chosen using $\Psi_1^{\pi_1'} \circ F'$. Hence if $(L_i \| R_i, S_i \| W_i)_{i\in[q]}$ is not permutation compatible in the ideal world then the adversary can distinguish them trivially. To avoid this we define the following bad event in the ideal world.

$\texttt{BAD}_{\texttt{id}}$: for two queries $i \neq j \in [q]$, $L_i \| R_i = L_j \| R_j$ or $S_i \| W_i = S_j \| W_j$.

Lemma 3.

$$\Pr\left[\texttt{BAD}_{\texttt{id}}\right] \leq \frac{6q^2}{2^{2n}}.$$

Proof. Note that since $F' \leftarrow\!\$\ \mathcal{F}$, for any two distinct $(T_i, X_i) \neq (T_j, X_j)$,

$$\begin{aligned}\Pr\left[L_i \| R_i = L_j \| R_j\right] &= \Pr\left[\Psi^{\pi_1'} \circ F'(T_i, X_i) = \Psi^{\pi_1'} \circ F'(T_j, X_j)\right] \\ &= \Pr\left[F'(T_i, X_i) = F'(T_j, X_j)\right] \\ &= \frac{4}{2^{2n}}.\end{aligned}$$

Further since $S_i \| W_i$ are generated using Π we have

$$\Pr\left[S_i \| W_i = S_j \| W_j\right] \leq \frac{2}{2^{2n}}.$$

Varying over all i, j, and using union bound we have

$$\Pr\left[\texttt{BAD}_{\texttt{id}}\right] \leq \frac{6q^2}{2^{2n}}.$$

6.2 Real World bad transcript analysis

Given a transcript τ suppose $\texttt{BAD}_{\texttt{id}}$ doesn't occur in the real world i.e. $(L_i \| R_i, S_i \| W_i)_{i \in [q]}$ is permutation compatible. Then to interpolate the real world we can approach in the similar way as Guo et al. [21].

So let us define $x_i := R_i \oplus S_i$ for all $i \in [q]$. Let $\vec{R} := (R_1, \ldots, R_q), \vec{x} = (x_1, \ldots, x_q)$ and $\vec{S_i} := (S_1, \ldots, S_q)$. Further let α, β, γ denotes the number of distinct values in $\vec{R}, \vec{x}$ and $\vec{S}$.

Let $\omega^\tau : \{a_1, b_1, c_1, ..., a_q, b_q, c_q\} \to 1, ..., \alpha + \beta + \gamma$ be the unique index mapping corresponding to the system of equations. Let $P_{\omega^\tau(a_i)} := \pi_2(R_i); P_{\omega^\tau(b_i)} := L_i \oplus \pi_2(R_i); P_{\omega^\tau(c_i)} = \pi_4(S_i)$. then the transcript τ defines q pairs of equations:

$$\begin{aligned} P_{\omega^\tau(a_1)} \oplus P_{\omega^\tau(b_1)} = L_1; \quad & P_{\omega^\tau(b_1)} \oplus P_{\omega^\tau(c_1)} = W_1 \\ \ldots \quad & \ldots \\ P_{\omega^\tau(a_q)} \oplus P_{\omega^\tau(b_q)} = L_q; \quad & P_{\omega^\tau(b_q)} \oplus P_{\omega^\tau(c_q)} = W_q. \end{aligned}$$

Denote this system of equation as $\mathcal{P}$. Then following the work of Guo et. al. [21], the real world bad transcripts can be defined as follows:

BAD3: **(Circles).** there exists some integer $k \geq 3$ and k indices $i_1, \ldots, i_k$ such that:

- $i_1, \ldots, i_{k-1}$ are pairwise distinct and $i_k = i_1$
- for all $l \in [1, k-1]$

$$R_{i_l} = R_{i_{l+1}} \bigvee S_{i_l} = S_{i_{l+1}} \bigvee R_{i_l} \oplus S_{i_l} = R_{i_{l+1}} \oplus S_{i_{l+1}}.$$

BAD4: **(large blocks).** there exists some integer $k > n$ and k indices $i_1, \ldots, i_k$ such that:

- for all $l \in [1, k-1]$

$$R_{i_l} = R_{i_{l+1}} \bigvee S_{i_l} = S_{i_{l+1}} \bigvee R_{i_l} \oplus S_{i_l} = R_{i_{l+1}} \oplus S_{i_{l+1}}.$$

BAD5: **(degeneracy).** the equation system induced by τ is degenerate. Formally, there exists two distinct indices $j, j' \in 1, ..., \alpha + \beta + \gamma$ such that $\mathcal{P}$ implies one of the following:

BAD5.1: $P_j = P_{j'}$ where $j, j' \in \{\omega^\tau(a_i) \mid i \in [q]\}$

BAD5.2: $P_j = P_{j'}$ where $j, j' \in \{\omega^\tau(b_i) \mid i \in [q]\}$

BAD5.3: $P_j = P_{j'}$ where $j, j' \in \{\omega^\tau(c_i) \mid i \in [q]\}$

BAD6: **(contradiction).** there exists two distinct indices i, j such that

$$R_i \oplus S_i = R_j \oplus S_j \bigwedge \left(L_i = L_j \bigvee W_i = W_j \right).$$

Define $\mathtt{BAD_{re}} := \bigvee_{i=3}^{6} \mathtt{BADi}$.

Lemma 4.

$$\Pr\left[\mathtt{BAD_{re}}\right] \leq \frac{36q}{2^n} + \frac{36(n+2)q^2}{2^{2n}} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Proof of lemma 4 is postponed to section 6.4.

6.3 Good transcript ratio and Proof of Theorem 2

We say a transcript τ good if $\mathtt{BAD_{id}}$ or $\mathtt{BAD_{re}}$ doesn't occur.

Now consider a good transcript τ.

Note that in the ideal world, Since $\mathtt{BAD_{id}}$ doesn't occur hence $L_i\|R_i$ are all distinct and $S_i\|R_i$ are all distict

$$\Pr\left[\forall i, \tilde{\Pi}(X_i) = S_i\|W_i\right] \leq \frac{1}{(2^{2n})_q \times (2^{2n})_q}$$

In the real world $S_i\|W_i$ are generated using $L_i\|R_i$, and $L_i\|R_i$ are all distinct.

Let $N_{\vec{r},\vec{X},\vec{s}}$ denote the number of consistent distinct solutions such that for all $i \in [q]$, $\{\pi_2(R_i) = r_i, \pi_2(X_i) = R_i \oplus S_i, \pi_3(S_i) = s_i\}$. Then since $\mathtt{BAD_{re}}$ doesn't occur we have, by theorem 4, We have

$$N_{\vec{r},\vec{X},\vec{s}} \geq \frac{(2^n-2)_\alpha (2^n-2)_\beta (2^n-2)_\gamma}{2^{2qn}}.$$

where α, β, γ respectively defines the distinct numbers of $R_i, S_i, R_i \oplus S_i$.

Hence the probability that

$$\begin{aligned}
\Pr\left[\forall i, \Psi_3^{(\pi_2,\pi_3,\pi_4)}(L_i\|R_i) = S_i\|W_i\right] &\geq \frac{N_{\vec{r},\vec{X},\vec{s}}}{(2^{2n})_q} \times \Pr\left[\pi_2(R_i) = r_i \forall i\right] \times \Pr\left[\pi_3 = (X_i)R_i \oplus S_i \forall i\right] \\
&\quad \times \Pr\left[\pi_4(S_i) = s_i \forall i\right] \\
&\geq \frac{1}{(2^{2n})_q} \times \frac{\frac{(2^n-2)_\alpha (2^n-2)_\beta (2^n-2)_\gamma}{2^{2qn}}}{(2^n)_\alpha (2^n)_\beta (2^n)_\gamma} \\
&\quad \frac{1}{(2^{2n})_q \times 2^{2nq}} \times \left(1 - \frac{3(\alpha+\beta+\gamma)}{2^n}\right) [\text{Since } \alpha, \beta, \gamma \geq 1] \\
&\geq \frac{1}{(2^{2n})_q \times 2^{2nq}} \times \left(1 - \frac{9q}{2^n}\right) [\text{Since } \alpha, \beta, \gamma \leq q]
\end{aligned}$$

Hence

$$\frac{\Pr[\Theta_1=\tau]}{\Pr[\Theta_0=\tau]} \geq \frac{\Pr[\forall i, \Psi_1^{\pi_1} \circ F(X_i) = (L_i \| R_i)] \times \Pr\left[\forall i, \Psi_3^{(\pi_2,\pi_3,\pi_4)}(L_i\|R_i) = S_i\|W_i\right]}{\Pr\left[\forall i, \Psi_1^{\pi_1'} \circ F'(X_i) = (L_i\|R_i)\right] \times \Pr\left[\forall i, \tilde{\Pi}(X_i) = S_i\|W_i\right]}$$
$$\geq \frac{\Pr\left[\forall i, \Psi_3^{(\pi_2,\pi_3,\pi_4)}(L_i\|R_i) = S_i\|W_i\right]}{\Pr\left[\forall i, \tilde{\Pi}(X_i) = S_i\|W_i\right]}$$
$$\geq \frac{(2^{2n})_q}{2^{2qn}} \times \left(1 - \frac{9q}{2^n}\right) \geq \frac{(2^{2n}-q)^q}{2^{2nq}} \times \left(1 - \frac{9q}{2^n}\right) \geq 1 - \frac{q^2}{2^{2n}} - \frac{9q}{2^n}. \tag{6}$$

Hence the theorem follows from equation (6),lemma 3,and lemma 4.

6.4 Proof of Lemma 4

To prove lemma 4, we start by denoting $L_{i,0}\|R_{i,0} := F(T_i, X_i)$.

Bounding BAD3:

Given any two $i \neq j$, Note that if $R_{i,0} = R_{j,0}$ or $L_{i,0} = L_{j,0}$ then $\Pr[R_i = R_j] = 0$. Now given $R_{i,0} \neq R_{j,0}, L_{i,0} \neq L_{j,0}$

$$\Pr[R_i = R_j] = \Pr[\pi_1(R_{i,0}) \oplus \pi_1(R_{j,0}) = L_{0,i} \oplus L_{j,0}] \leq \frac{2}{2^n}.$$

Since we are in the CPA settings, $S_i\|W_i$ are still distributed uniformly randomly. Hence $\Pr[S_i = S_j] \leq \frac{2}{2^n}$.

Finally,

$$\begin{aligned}\Pr[R_i \oplus S_i = R_j \oplus S_j] &= \Pr[R_i \oplus S_i = R_j \oplus S_j \mid L_i = L_j] \cdot \Pr[L_i = L_j] \\ &\oplus \Pr[R_i \oplus S_i = R_j \oplus S_j \mid L_i \neq L_j] \cdot \Pr[L_i \neq L_j] \\ &= \Pr[S_i \oplus S_j = L_{i,0} \oplus L_{j,0}] \cdot \Pr[L_i = L_j] \\ &\oplus \Pr[S_i \oplus \pi_1(R_{i,0}) \oplus L_{i,0} = S_i \oplus \pi_1(R_{i,0}) \oplus L_{i,0}] \cdot \Pr[L_i = L_j] \\ &\leq \frac{2}{2^n}.\end{aligned}$$

Hence for any $i \neq j$,

$$\Pr\left[R_i = R_j \bigvee S_i = S_j \bigvee R_i \oplus S_i = R_j \oplus S_j\right] \leq \frac{6}{2^n}.$$

Hence

$$\Pr[BAD3] \leq \sum_{k\geq 3} \left(\frac{6q}{2^n}\right)^{k-1} \leq \frac{72q^2}{2^{2n}}.$$

Bounding BAD4:

A similar analysis as in BAD3 shows that,

$$\Pr\left[\texttt{BAD4}\right] \leq q^n \left(\frac{6}{2^n}\right)^{n-1} \leq \frac{1}{6} \cdot \left(\frac{12q}{2^n}\right)^n$$

Bounding BAD5:

We only Bound BAD5.1, A similar analysis follows for BAD5.2 and BAD5.3

Note that if BAD3 doesn't occur, then the event BAD5.1 means $\pi_2(R_i) = \pi_2(R_{i'})$. As shown by Guo et al. [21] (see Lemma 4) there exists a sequence of query indices $i_1, \ldots, i_k$ which are in the same block, where $i_1 = 1, i_k = i'$, and two subsets of indices $I_1, I_2 \subseteq \{i_1, \ldots, i_k\}$, $i_1, i_k \in I_1$ such that, $R_i = R_{i'}$ and

$$\left(\bigoplus_{l \in I_1} L_l\right) \oplus \left(\bigoplus_{l \in I_2} W_l\right) = \left(\bigoplus_{l \in I_1} R_{l,0}\right) \oplus \left(\bigoplus_{l \in I_2} W_l\right) = 0$$

Note that the $R_{l,0}$ are not random as they are the right-half outputs of F. So to bound event BAD5.1 we consider two separate events.

Bounding BAD5.1.1 : $\forall l \in \{i_1, \ldots, i_k\}$ $R_{l,0}$ has even multiplicity

Note that if this case happens, then we have BAD5.1 occurs with $I_1 = \{i_1, \ldots, i_k\}$ and $I_2 = \phi$.

Now note that the set $\{i_1, \ldots, i_{k-1}\}$ can be chosen in at most q^{k-1} ways. Then the event implies that there exists an unique element $l \in \{i_1, \ldots, i_{k-1}\}$ such that it has odd multiplicity and $R_{l,0} = R_{i_k,0}$. Further note that since $R_{i_k} = R_{i_1}$, we have $L_{k,0} = L_{k_1} \oplus \pi_1(R_{i_1,0}) \oplus \pi(R_{i_k,0})$. Hence $L_{i_k,0} \| R_{i_k,0}$ is uniquely determined and since $\texttt{BAD}_{\texttt{id}}$ doesn't occur, there exists at most a unique choice for i_k. Hence the set $\{i_1, \ldots, i_k\}$ can be chosen in at most q^{k-1} ways.

Now given any such choice as in the analysis of BAD3, probability that, $\{i_1, \ldots, i_k\}$ is at most $\left(\frac{6}{2^n}\right)^{k-1}$. Hence,

$$\Pr\left[\texttt{BAD5.1.1} \mid \texttt{BAD3}\right] \leq \sum_{k \geq 2} \left(\frac{6q}{2^n}\right)^{k-1} \leq \frac{12q}{2^n}.$$

Bounding BAD5.1.2 : $\exists t \in \{i_1, \ldots, i_k\}$, $R_{t,0}$ has odd multiplicity

Then Clearly

$$R_{t,0} = \left(\bigoplus_{\substack{l \in I_1 \\ l \neq t}} R_{l,0}\right) \oplus \left(\bigoplus_{l \in I_2} W_l\right).$$

Since, $R_{t,0}$ is generated using $F \leftarrow\!\!\$\ \mathcal{F}$, given the event mcoll as in proposition 2 doesn't occur probability that

$$\Pr\left[R_{t,0} = \left(\bigoplus_{\substack{l \in I_1 \\ l \neq t}} R_{l,0}\right) \oplus \left(\bigoplus_{l \in I_2} W_l\right)\right] \leq \frac{n}{2^n}.$$

Now note that number of choices of $\{i_1, \ldots, i_k\}$ is bounded by at most q^k. Hence,

$$\Pr\left[\texttt{BAD5.1.2}|\neg\texttt{BAD3}\right] \leq \frac{n}{6}\sum_{k\geq 2}\left(\frac{6q}{2^n}\right)^k + \Pr\left[\texttt{mcoll}\right] \leq \frac{12nq^2}{2^{2n}} + \frac{1}{2}\left(\frac{4q}{2^n}\right)^n.$$

Hence by union bound we have,

$$\Pr\left[\texttt{BAD5.1}|\neg\texttt{BAD3}\right] \leq \frac{12q}{2^n} + \frac{12nq^2}{2^{2n}} + \frac{1}{2}\left(\frac{4q}{2^n}\right)^n.$$

A similar analysis shows that

$$\Pr\left[\texttt{BAD5.2}|\neg\texttt{BAD3}\right] \leq \frac{12q}{2^n} + \frac{12nq^2}{2^{2n}} + +\frac{1}{2}\left(\frac{4q}{2^n}\right)^n.$$

$$\Pr\left[\texttt{BAD5.3}|\neg\texttt{BAD3}\right] \leq \frac{12q}{2^n} + \frac{12nq^2}{2^{2n}} + \frac{1}{2}\left(\frac{4q}{2^n}\right)^n.$$

$$\Pr\left[\texttt{BAD5}|\neg\texttt{BAD3}\right] \leq \frac{36q}{2^n} + \frac{36nq^2}{2^{2n}} + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Bounding BAD6:

Note that $R_i \oplus S_i = R_j \oplus S_j => \pi_2(R_i) \oplus \pi_2(R_j) = L_i \oplus L_j$. Hence if $L_i = L_j$, Then $\pi_2(R_i) = \pi_2(R_j)$.

Similarly $R_i \oplus S_i = R_j \oplus S_j \implies x_i = x_j \implies L_i \oplus \pi_1(R_i) = L_j \oplus \pi_1(R_j)$. But then $\pi_4(S_i) \oplus \pi_4(S_j) = T_i \oplus T_j \oplus L_i \oplus \pi_1(R_i) \oplus L_j \oplus \pi_1(R_j) = T_i \oplus T_j$. Hence if $T_i = T_j$ then $\pi_4(S_i) = \pi_4(S_j)$.

Hence

$$\Pr\left[\texttt{BAD6}|\neg\texttt{BAD5}\right] = 0.$$

By union bound we have lemma 4.

7 Proof of Theorem 3

We employ the coefficient H-technique and assume that the adversary doesn't make any redundant queries. The proof approach is an adaptation of the CCA security proof of 7-round LR construction by Guo et al. [21] with our mirror theory result Theorem 4.

Consider the CCA challenger which proceeds as follows.

- In the ideal world, the oracle chooses a random tweakable permutation, $\tilde{\Pi} \leftarrow\!\!\$\ \mathsf{TPerm}(b, 2n)$. For each encryption query $(T_i, X_i) \in \{0,1\}^b \times \{0,1\}^{2n}$, the oracle outputs $Y_i := \tilde{\Pi}(T_i, X_i)$ as it's response. Similarly for each decryption query the oracle outputs $X_i := \tilde{\Pi}^{-1}(T_i, Y_i)$ as it's response

– In the real world, the oracle samples $F_1, F_2 \leftarrow\!\$\ \mathcal{F}$ and $\pi_1, \ldots, \pi_5 \leftarrow\!\$\ \mathsf{Perm}(n)$ independently, and for each encryption query $(T_i, X_i) \in \{0,1\}^b \times \{0,1\}^{2n}$ the oracle makes all the necessary computations honestly and outputs the honest response $Y_i = F_2^{-1} \circ \Psi_5^{(\pi_1,\ldots,\pi_5)} \circ F_1(T_i, X_i)$. Similarly, for each decryption query $(T_i, Y_i) \in \{0,1\}^b \times \{0,1\}^{2n}$ the oracle makes all the necessary computations honestly and outputs the honest response $X_i = F_1^{-1} \circ \Psi_5^{(\pi_5,\ldots,\pi_1)} \circ F_2(T_i, Y_i)$.

After the query-response phase is done with the adversary the oracle releases some additional states as follows,

– In the ideal world, for each query-response pair (T_i, X_i, Y_i), the oracle selects a random permutations $\pi_1', \pi_5' \leftarrow\!\$\ \mathsf{Perm}(n)$ and $F_1', F_2' \leftarrow\!\$\ \mathcal{F}$ independently. It computes $L_i \| R_i := \Psi_1^{\pi_1'} \circ F'(T_i, X_i)$ and $S_i \| W_i := (\Psi_1^{\pi_5'})^{-1} \circ F_2'(T_i, Y_i)$. Finally it sends $(T_i, X_i, Y_i, L_i \| R_i, S_i \| W_i)_{i \in [q]}$ as the query transcript for the adversary.

– In the real world for each query-response pair (T_i, X_i, Y_i), the oracle computes, $L_i \| R_i := \Psi_1^{\pi_1} \circ F_1(T_i, X_i)$ and $S_i \| W_i := (\Psi_1^{\pi_5})^{-1} \circ F_2(T_i, Y_i)$. Finally it sends $(T_i, X_i, Y_i, L_i \| R_i, S_i \| W_i)_{i \in [q]}$ as the query transcript for the adversary.

let $\tau := \{(T_i, X_i, Y_i, L_i \| R_i, S_i \| W_i) \mid i \in [q]\}$ be the final query transcript of the adversary.

7.1 Bad transcripts in the ideal world

Note that in the ideal world the $F_1, F_2 \leftarrow\!\$\ \mathcal{F}$ are simulated with $F_1', F_2' \leftarrow\!\$\ \mathcal{F}$, and the random permutations π_1, π_5 are simulated with independent random permutations π_1', π_5', for generating the extended part of the transcript. So no adversary can distinguish between the ideal world and the real world by only observing the τ.

Note that in the real world $\Psi_3^{(\pi_2,\pi_3,\pi_4)}(L_i \| R_i) = S_i \| W_i$. Hence the transcript is permutation-compatible. On the other hand in the ideal world $S_i \| W_i$ are calculated using $\Psi_1^{\pi_5'^{-1}} \circ F_2'$ on the outputs of a tweakable random permutation. Further $L_i \| R_i$ are chosen using $\Psi_1^{\pi_1'} \circ F_1'$. Hence if $(L_i \| R_i, S_i \| W_i)_{i \in [q]}$ is not permutation compatible in the ideal world then the adversary can distinguish them trivially. To avoid this we define the following bad event in the ideal world.

$\mathtt{BAD_{id}}$: for two queries $i \neq j \in [q]$, $L_i \| R_i = L_j \| R_j$ or $S_i \| W_i = S_j \| W_j$.

Lemma 5.

$$\Pr\left[\mathtt{BAD_{id}}\right] \leq \frac{8q^2}{2^{2n}}.$$

Proof. Note that since $F_1' \leftarrow\!\$\ \mathcal{F}$, for any two distinct $(T_i, X_i) \neq (T_j, X_j)$,

$$\begin{aligned}\Pr\left[L_i \| R_i = L_j \| R_j\right] &= \Pr\left[\Psi^{\pi_1'} \circ F_1'(T_i, X_i) = \Psi^{\pi_1'} \circ F_1'(T_j, X_j)\right] \\ &= \Pr\left[F_1'(T_i, X_i) = F_1'(T_j, X_j)\right] \\ &= \frac{4}{2^{2n}}.\end{aligned}$$

similarly since $F_2' \leftarrow\!\$\ \mathcal{F}$, for any two distinct $(T_i, Y_i) \neq (T_j, Y_j)$,

$$\begin{aligned}\Pr\left[S_i \| W_i = S_j \| W_j\right] &= \Pr\left[(\Psi_1^{\pi_5'})^{-1} \circ F_2'(T_i, Y_i) = (\Psi_1^{\pi_5'})^{-1} \circ F_2'(T_j, Y_j)\right] \\ &= \Pr\left[F_2'(T_i, Y_i) = F_2'(T_j, Y_j)\right] \\ &= \frac{4}{2^{2n}}.\end{aligned}$$

Varying over all i, j, and using union bound we have

$$\Pr\left[\mathtt{BAD}_{\mathtt{id}}\right] \leq \frac{8q^2}{2^{2n}}.$$

7.2 Real World bad transcript analysis

Given a transcript τ suppose $\mathtt{BAD}_{\mathtt{id}}$ doesn't occur in the real world i.e. $(L_i \| R_i, S_i \| W_i)_{i \in [q]}$ is permutation compatible. Then to interpolate the real world we again approach in a similar way as Guo et al. [21].

So let us define $x_i := R_i \oplus S_i$ for all $i \in [q]$. Let $\vec{R} := (R_1, \ldots, R_q), \vec{x} = (x_1, \ldots, x_q)$ and $\vec{S_i} := (S_1, \ldots, S_q)$. Further let α, β, γ denotes the number of distinct values in $\vec{R}, \vec{x}$ and $\vec{S}$.

Let $\omega^\tau : \{a_1, b_1, c_1, ..., a_q, b_q, c_q\} \to 1, ..., \alpha + \beta + \gamma$ be the unique index mapping corresponding to the system of equations. Let $P_{\omega^\tau(a_i)} := \pi_2(R_i); P_{\omega^\tau(b_i)} := L_i \oplus \pi_2(R_i); P_{\omega^\tau(c_i)} = \pi_4(S_i)$. Then the transcript τ defines q pairs of equations:

$$\begin{aligned} P_{\omega^\tau(a_1)} \oplus P_{\omega^\tau(b_1)} = L_1; \quad & P_{\omega^\tau(b_1)} \oplus P_{\omega^\tau(c_1)} = W_1 \\ \cdots \quad & \cdots \\ P_{\omega^\tau(a_q)} \oplus P_{\omega^\tau(b_q)} = L_q; \quad & P_{\omega^\tau(b_q)} \oplus P_{\omega^\tau(c_q)} = W_q. \end{aligned}$$

Denote this system of equation as $\mathcal{P}$. Then following the work of Guo et. al. [21], the real world bad transcripts can be defined as follows:

BAD3: **(Circles).** there exists some integer $k \geq 3$ and k indices $i_1, \ldots, i_k$ such that:

- $i_1, \ldots, i_{k-1}$ are pairwise distinct and $i_k = i_1$
- for all $l \in [1, k-1]$

$$R_{i_l} = R_{i_{l+1}} \bigvee S_{i_l} = S_{i_{l+1}} \bigvee R_{i_l} \oplus S_{i_l} = R_{i_{l+1}} \oplus S_{i_{l+1}}.$$

BAD4: **(large blocks).** there exists some integer $k > n$ and k indices $i_1, \ldots, i_k$ such that:

- for all $l \in [1, k-1]$

$$R_{i_l} = R_{i_{l+1}} \bigvee S_{i_l} = S_{i_{l+1}} \bigvee R_{i_l} \oplus S_{i_l} = R_{i_{l+1}} \oplus S_{i_{l+1}}.$$

BAD5: **(degeneracy).** the equation system induced by τ is degenerate. Formally, there exists two distinct indices $j, j' \in 1, ..., \alpha + \beta + \gamma$ such that $\mathcal{P}$ implies one of the following:

BAD5.1: $P_j = P_{j'}$ where $j, j' \in \{\omega^\tau(a_i) \mid i \in [q]\}$

BAD5.2: $P_j = P_{j'}$ where $j, j' \in \{\omega^\tau(b_i) \mid i \in [q]\}$

BAD5.3: $P_j = P_{j'}$ where $j, j' \in \{\omega^\tau(c_i) \mid i \in [q]\}$

BAD6: **(contradiction).** there exists two distinct indices i, j such that

$$R_i \oplus S_i = R_j \oplus S_j \bigwedge \left(L_i = L_j \bigvee W_i = W_j\right).$$

Define $\mathtt{BAD_{re}} := \bigvee_{i=3}^{6} \mathtt{BADi}$.

Lemma 6.

$$\Pr\left[\mathtt{BAD_{re}}\right] \leq \frac{36q}{2^n} + \frac{(36n+72)q^2}{2^{2n}} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

We postpone the proof of lemma 6 to section 7.4.

7.3 Good transcript ratio and Proof of Theorem 2

We say a transcript τ good if $\mathtt{BAD_{id}}$ or $\mathtt{BAD_{re}}$ doesn't occur.

Now consider a good transcript τ.

Note that in the ideal world, the encryption and decryption queries are responded to using a tweakable random permutation $\tilde{\Pi}$.

Let $u_t := |\{T_i = t \mid i \in [q]\}|$. Clearly, $\sum_{t \in \{0,1\}^b} u_t = q$.

$$\Pr\left[\forall i, \tilde{\Pi}(T_i, X_i) = Y_i\right] \leq \frac{1}{\prod_{t \in \{0,1\}^b} (2^{2n})_{u_t}} \leq \frac{1}{(2^{2n} - q)^q}.$$

In the real world in the encryption query $S_i \| W_i$ are generated using $L_i \| R_i$, which are generated using (T_i, X_i). Similarly in the decryption query $L_i \| R_i$ are generated using $S_i \| W_i$, which are generated using (T_i, Y_i). Hence given each query, $L_i \| R_i$ and $S_i \| W_i$ are fixed.

Let $N_{\vec{r},\vec{X},\vec{s}}$ denote the number of consistent distinct solutions such that for all $i \in [q]$, $\{\pi_2(R_i) = r_i, \pi_3(X_i) = R_i \oplus S_i, \pi_4(S_i) = s_i\}$. Then since $\mathtt{BAD_{re}}$ doesn't occur we have, by theorem 4, We have

$$N_{\vec{r},\vec{X},\vec{s}} \geq \frac{(2^n-2)_\alpha (2^n-2)_\beta (2^n-2)_\gamma}{2^{2qn}}.$$

where α, β, γ respectively denote the distinct numbers of $R_i, S_i, R_i \oplus S_i$.

Hence the probability that

$$\begin{aligned}
\Pr\left[\forall i, \Psi_3^{(\pi_2,\pi_3,\pi_4)}(L_i\|R_i) = S_i\|W_i\right] &\geq N_{\vec{r},\vec{X},\vec{s}} \times \Pr\left[\pi_2(R_i) = r_i \forall i\right] \times \Pr\left[\pi_3(X_i) = R_i \oplus S_i \forall i\right] \\
&\quad \times \Pr\left[\pi_4(S_i) = s_i \forall i\right] \\
&\geq \frac{\frac{(2^n-2)_\alpha (2^n-2)_\beta (2^n-2)_\gamma}{2^{2qn}}}{(2^n)_\alpha (2^n)_\beta (2^n)_\gamma} \\
&\geq \frac{1}{2^{2nq}} \times \left(1 - \frac{3(\alpha+\beta+\gamma)}{2^n}\right) [\text{Since } \alpha, \beta, \gamma \geq 1] \\
&\geq \frac{1}{2^{2nq}} \times \left(1 - \frac{9q}{2^n}\right) [\text{Since } \alpha, \beta, \gamma \leq q]
\end{aligned}$$

$$\begin{aligned}
\frac{\Pr\left[\Theta_1 = \tau\right]}{\Pr\left[\Theta_0 = \tau\right]} &\geq \frac{\Pr\left[\forall i, \Psi_1^{\pi_1} \circ F_1(T_i, X_i) = (L_i\|R_i)\right] \times \Pr\left[\forall i, (\Psi_1^{\pi_5})^{-1} \circ F_2(T_i, Y_i) = (S_i\|W_i)\right]}{\Pr\left[\forall i, \Psi_1^{\pi_1'} \circ F_1'(T_i, X_i) = (L_i\|R_i)\right] \times \Pr\left[\forall i, (\Psi_1^{\pi_5})^{-1} \circ F_2'(T_i, Y_i) = (S_i\|W_i)\right]} \\
&\quad \times \frac{\Pr\left[\forall i, \Psi_3^{(\pi_2,\pi_3,\pi_4)}(L_i\|R_i) = S_i\|W_i\right]}{\Pr\left[\forall i, \Pi(T_i, X_i) = Y_i\right]} \\
&\geq \frac{\Pr\left[\forall i, \Psi_3^{(\pi_2,\pi_3,\pi_4)}(L_i\|R_i) = S_i\|W_i\right]}{\Pr\left[\forall i, \tilde{\Pi}(T_i, X_i) = Y_i\right]} \\
&\geq \frac{(2^{2n}-q)^q}{2^{2nq}} \times \left(1 - \frac{9q}{2^n}\right) \qquad (7) \\
&\geq 1 - \frac{q^2}{2^{2n}} - \frac{9q}{2^n}. \qquad (8)
\end{aligned}$$

Hence the theorem follows from equation (8), lemma 5, and lemma 6.

7.4 Proof of Lemma 6

To prove lemma 6, we start by denoting $L_{i,0}\|R_{i,0} := F_1(T_i, X_i), S_{i,0}\|W_{i,0} := F_2(T_i, X_i)$.

Bounding $\mathtt{BAD3}$:

Given any two $i \neq j$, Note that if $R_{i,0} = R_{j,0}$ or $L_{i,0} = L_{j,0}$ then $\Pr\left[R_i = R_j\right] = 0$. Now given $R_{i,0} \neq R_{j,0}, L_{i,0} \neq L_{j,0}$

$$\Pr\left[R_i = R_j\right] = \Pr\left[\pi_1(R_{i,0}) \oplus \pi_1(R_{j,0}) = L_{0,i} \oplus L_{j,0}\right] \leq \frac{2}{2^n}.$$

Similarly given any two $i \neq j$, Note that if $S_{i,0} = S_{j,0}$ or $W_{i,0} = W_{j,0}$ then $\Pr[S_i = S_j] = 0$. Now given $S_{i,0} \neq S_{j,0}, W_{i,0} \neq W_{j,0}$

$$\Pr[S_i = S_j] = \Pr[\pi_1(S_{i,0}) \oplus \pi_1(S_{j,0}) = W_{0,i} \oplus W_{j,0}] \leq \frac{2}{2^n}.$$

Finally,

$$\begin{aligned}
\Pr[R_i \oplus S_i = R_j \oplus S_j] &= \Pr[R_i \oplus S_i = R_j \oplus S_j \mid L_i = L_j] \cdot \Pr[L_i = L_j] \\
&\oplus \Pr[R_i \oplus S_i = R_j \oplus S_j \mid L_i \neq L_j] \cdot \Pr[L_i \neq L_j] \\
&= \Pr[\pi_5(S_{i,0}) \oplus \pi_5(S_{j,0}) = W_{i,0} \oplus W_{j,0} \oplus L_{i,0} \oplus L_{j,0}] \cdot \Pr[L_i = L_j] \\
&\oplus \Pr[S_i \oplus \pi_1(R_{i,0}) \oplus L_{i,0} = S_j \oplus \pi_1(R_{j,0}) \oplus L_{j,0}] \cdot \Pr[L_i \neq L_j] \\
&\leq \frac{2}{2^n}.
\end{aligned}$$

Hence for any $i \neq j$,

$$\Pr\left[R_i = R_j \bigvee S_i = S_j \bigvee R_i \oplus S_i = R_j \oplus S_j\right] \leq \frac{6}{2^n}.$$

Hence

$$\Pr[BAD3] \leq \sum_{k \geq 3} \left(\frac{6q}{2^n}\right)^{k-1} \leq \frac{72q^2}{2^{2n}}.$$

Bounding BAD4:
A similar analysis as in BAD3 shows that,

$$\Pr[\texttt{BAD4}] \leq q^n \left(\frac{6}{2^n}\right)^{n-1} \leq \frac{1}{6} \cdot \left(\frac{12q}{2^n}\right)^n.$$

Bounding BAD5: Note that if BAD3 doesn't occur, then the event BAD5.1 means $\pi_2(R_i) = \pi_2(R_{i'})$. As shown by Guo et al. [21] (see Lemma 4) there exists a sequence of query indices $i_1, \ldots, i_k$ which are in the same block, where $i_1 = 1, i_k = i'$, and two subsets of indices $I_1, I_2 \subseteq \{i_1, \ldots, i_k\}$, $i_1, i_k \in I_1$ such that, $R_i = R_{i'}$ and

$$\left(\bigoplus_{l \in I_1} L_l\right) \oplus \left(\bigoplus_{l \in I_2} W_l\right) = \left(\bigoplus_{l \in I_1} R_{l,0}\right) \oplus \left(\bigoplus_{l \in I_2} S_{l,0}\right) = 0$$

Note that the $R_{l,0}$ are not random as they are the right-half outputs of F. So to bound event BAD5.1 we consider two separate events.

Bounding BAD5.1.1 : $\forall l \in \{i_1, \ldots, i_k\}$ $R_{l,0}$ has even multiplicity
Note that if this case happens, then we have BAD5.1 occurs with $I_1 = \{i_1, \ldots, i_k\}$ and $I_2 = \phi$.

Now note that the set $\{i_1, \ldots, i_{k-1}\}$ can be chosen in at most q^{k-1} ways. Then the event implies that there exists an unique element $l \in \{i_1, \ldots, i_{k-1}\}$ such that it has odd multiplicity and $R_{l,0} = R_{i_k,0}$. Further note that since $R_{i_k} = R_{i_1}$, we have $L_{k,0} = L_{k_1} \oplus \pi_1(R_{i_1,0}) \oplus \pi(R_{i_k,0})$. Hence $L_{i_k,0} \| R_{i_k,0}$ is uniquely determined and since $\mathtt{BAD}_{\mathtt{id}}$ doesn't occur, there exists at most a unique choice for i_k. Hence the set $\{i_1, \ldots, i_k\}$ can be chosen in at most q^{k-1} ways.

Now given any such choice as in the analysis of BAD3, probability that, $\{i_1, \ldots, i_k\}$ is at most $\left(\frac{6}{2^n}\right)^{k-1}$. Hence,

$$\Pr\left[\mathtt{BAD5.1.1} \mid \mathtt{BAD3}\right] \leq \sum_{k \geq 2} \left(\frac{6q}{2^n}\right)^{k-1} \leq \frac{12q}{2^n}.$$

Bounding $\mathtt{BAD5.1.2} : \exists t \in \{i_1, \ldots, i_k\}$, $R_{t,0}$ has odd multiplicity
Then Clearly

$$R_{t,0} = \left(\bigoplus_{\substack{l \in I_1 \\ l \neq t}} R_{l,0}\right) \oplus \left(\bigoplus_{l \in I_2} S_{l,0}\right).$$

Since, $R_{t,0}$ is generated using $F \leftarrow\!\$\, \mathcal{F}$, given the event mcoll as in proposition 2 doesn't occur probability that

$$\Pr\left[R_{t,0} = \left(\bigoplus_{\substack{l \in I_1 \\ l \neq t}} R_{l,0}\right) \oplus \left(\bigoplus_{l \in I_2} S_{l,0}\right)\right] \leq \frac{n}{2^n}.$$

Now note that number of choices of $\{i_1, \ldots, i_k\}$ is bounded by at most q^k. Hence,

$$\Pr\left[\mathtt{BAD5.1.2} | \neg \mathtt{BAD3}\right] \leq \frac{n}{6} \sum_{k \geq 2} \left(\frac{6q}{2^n}\right)^k + \Pr\left[\mathtt{mcoll}\right] \leq \frac{12nq^2}{2^{2n}} + \frac{1}{2}\left(\frac{4q}{2^n}\right)^n.$$

Hence by union bound we have,

$$\Pr\left[\mathtt{BAD5.1} | \neg \mathtt{BAD3}\right] \leq \frac{12q}{2^n} + \frac{12nq^2}{2^{2n}} + \frac{1}{2}\left(\frac{4q}{2^n}\right)^n.$$

A similar analysis shows that

$$\Pr\left[\mathtt{BAD5.2} | \neg \mathtt{BAD3}\right] \leq \frac{12q}{2^n} + \frac{12nq^2}{2^{2n}} + \frac{1}{2}\left(\frac{4q}{2^n}\right)^n.$$

$$\Pr\left[\mathtt{BAD5.3} | \neg \mathtt{BAD3}\right] \leq \frac{12q}{2^n} + \frac{12nq^2}{2^{2n}} + \frac{1}{2}\left(\frac{4q}{2^n}\right)^n.$$

$$\Pr\left[\texttt{BAD5}|\neg\texttt{BAD3}\right] \leq \frac{36q}{2^n} + \frac{36nq^2}{2^{2n}} + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Bounding BAD6:

Note that $R_i \oplus S_i = R_j \oplus S_j \Rightarrow \pi_2(R_i) \oplus \pi_2(R_j) = L_i \oplus L_j$. Hence if $L_i = L_j$, Then $\pi_2(R_i) = \pi_2(R_j)$.

Similarly $R_i \oplus S_i = R_j \oplus S_j \implies L_i \oplus \pi_1(R_i) = L_j \oplus \pi_1(R_j)$. But then $\pi_4(S_i) \oplus \pi_4(S_j) = T_i \oplus T_j \oplus L_i \oplus \pi_1(R_i) \oplus L_j \oplus \pi_1(R_j) = T_i \oplus T_j$. Hence if $T_i = T_j$ then $\pi_4(S_i) = \pi_4(S_j)$.

Hence

$$\Pr\left[\texttt{BAD6}|\neg\texttt{BAD5}\right] = 0.$$

By union bound we have lemma 6.

8 The DbHtF MAC family

In this section, we define a general construction paradigm which we call the Double-block Hash-then-Fiestel (DbHtF) construction. The design paradigm can be seen as a modification of the well known Double-block Hash-then-Sum construction (DbHtS) [18]. Later we will show that some of the popular DbHtS based variable-input length constructions can be tweaked to generate DbHtF based MAC constructions which are secure up to $q \ll 2^n$ queries.

Definition 6. *Let $H : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^{2n}$ be any double block keyed-hash function. Then given any integer k and k independent random permutations $\pi_1, \ldots, \pi_k \in \mathsf{Perm}(n)$ we define the Double-block Hash-then-Fiestel construction $\mathsf{kF\text{-}H\text{-}DbHtF}[\pi_1, \ldots, \pi_k]$ as follows,*

$$\begin{aligned}\mathsf{kF\text{-}H\text{-}DbHtF}[\pi_1, \ldots, \pi_k] : \mathcal{K} \times \{0,1\}^* &\to \{0,1\}^n \\ (K, M) &\mapsto R_K(M)\end{aligned}$$

where $L_K(M) \| R_K(M) := \Psi_k^{(\pi_1,\ldots,\pi_k)}(H_K(M))\ \forall M \in \{0,1\}^*$.

Theorem 5. *Let $H : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^{2n}$ be any δ-AU hash function family. Let $\pi_1, \pi_2, \pi_3, \pi_4, \pi_5 \leftarrow\!\$\ \mathsf{Perm}(n)$ be any independent random permutations. Then for any PRF adversary making at most q queries, if $n \geq 30$ and $q \leq \frac{2^n}{48n^2}$, then*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{4F\text{-}H\text{-}DbHtF}[\pi_1,\pi_2,\pi_3,\pi_4]}(q) \leq q^2\delta + \mathbf{Adv}^{\mathrm{prp}}_{\Psi_5^{(\pi_1,\ldots,\pi_5)}}(q) + \frac{q^2}{2^{2n}}.$$

Proof. Consider the construction

$$\begin{aligned}\mathcal{C} : \mathcal{K} \times \{0,1\}^* &\to \{0,1\}^{2n} \\ (K, M) &\mapsto \Psi_5^{(\pi_1,\ldots,\pi_5)} \circ H_K(M)\end{aligned}$$

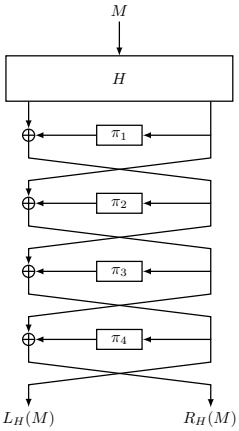


Figure 2. 4F-H-DbHtF$[\pi_1, \pi_2, \pi_3, \pi_4]$ hash function which outputs $R_K(M)$ for all $M \in \{0,1\}^*$.

Then if $\mathsf{Tr} : \{0,1\}^{2n} \to \{0,1\}^n$ be the truncation function defined as $\mathsf{Tr}(L\|R) := L$ for all $L, R \in \{0,1\}^n$, then for all $(K, M) \in \mathcal{K} \times \{0,1\}^*$

$$\mathsf{4F\text{-}H\text{-}DbHtF}[\pi_1, \pi_2, \pi_3, \pi_4](K, M) = \mathsf{Tr} \circ \mathcal{C}(K, M)$$

Hence it is easy to see that for any PRF adversary $\mathcal{A}$ of $\mathsf{Tr} \circ \Psi_5^{(\pi_1,\ldots,\pi_5)}$ making at most q queries, there exists a PRP adversary $\mathcal{B}$ of $\Psi_5^{(\pi_1,\ldots,\pi_5)}$ making at most q queries such that,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{Tr}\circ\Psi_5^{(\pi_1,\ldots,\pi_5)}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\Psi_5^{(\pi_1,\ldots,\pi_5)}}(\mathcal{B}) + \frac{q^2}{2^{2n}} \tag{9}$$

.

Further, it is also easy to follow that,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{Tr}\circ\mathcal{C}}(q) \leq \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{Tr}\circ\Psi_5^{(\pi_1,\ldots,\pi_5)}}(q) + \mathbf{Adv}^{\mathrm{coll}}_{H}(q) \tag{10}$$

.

Hence the theorem follows from (9) and (10).

In the remaining of this section we will see some applications of Theorem 5.

8.1 4F-Poly-DbHtF

Given any n-bit PolyHash[8,50] with key space $\{0,1\}^{2n}$ and $\pi_1, \ldots, \pi_4 \leftarrow\!\$\ \mathsf{Perm}(n)$ sampled independently and uniformly at random define the MAC construction 4F-Poly-DbHtF as, the construction $\mathsf{DbHtF}[(\mathsf{PolyHash}_{K_1}, \mathsf{PolyHash}_{K_2}), \pi_1, \pi_2, \pi_3, \pi_4]$.

Corollary 5. *If $n \geq 30$, then for any PRF adversary which is allowed to make $q \leq \frac{2^n}{48n^2}$ queries of message length at most nl,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{4F\text{-}Poly\text{-}DbHtF}}(q,l) \leq \frac{l^2q^2}{2^{2n}} + \frac{(36n+80)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Proof. The corollary follows from Theorem 5 and the observation that the double blocked keyed hash function family $\{H_K \mid K \in \{0,1\}^n \times \{0,1\}^n\}$ where,

$$\begin{aligned} H_{K_1,K_2} : \{0,1\}^* &\to \{0,1\}^{2n} \\ M &\mapsto \mathsf{PolyHash}_{K_1}(M) \| \mathsf{PolyHash}_{K_2}(M), \end{aligned}$$

is an $\frac{l^2}{2^{2n}}$-AU hash function family, with respect to any adversary which is restricted to making q queries of block length at most l.

8.2 4F-ECBC-DbHtF

Given any n-bit random permutation $\pi, \pi', \pi_1, \ldots, \pi_4 \xleftarrow{\$} \mathsf{Perm}(n)$ sampled independently and uniformly at random, Consider the n-bit CBC hash function [5] and define the MAC construction $\mathsf{4F\text{-}ECBC\text{-}DbHtF}$ as, the construction $\mathsf{DbHtF}[(\mathsf{CBC}_\pi, \mathsf{CBC}_{\pi'}), \pi_1, \pi_2, \pi_3, \pi_4]$.

For $m \leq l$ let $d(m)$ be the number of divisors of m and let $d'(l) = \max_{m \leq l} d(m)$. Jha et. al [26], showed that [Corollary 2], CBC hash function is δ-AU where,

$$\delta \leq \frac{d'(l)}{2^n - 2l} + \frac{l^4}{2^{2n}} \leq \frac{(2d'(l) + \frac{l^4}{2^n})}{2^n}. \text{ [assuming } l < 2^{n-1}]$$

Corollary 6. *If $n \geq 30$, then for any PRF adversary which is allowed to make $q \leq \frac{2^n}{48n^2}$ queries of block length at most l,*

$$\begin{aligned} \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{4F\text{-}ECBC\text{-}DbHtF}}(q,l) \leq &\left(\frac{q(2d'(l) + \frac{l^4}{2^n})}{2^n}\right)^2 + \frac{(36n+80)q^2}{2^{2n}} + \frac{45q}{2^n} \\ &+ \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n. \end{aligned}$$

Proof. The corollary follows from Theorem 5 and the observation that the double blocked keyed hash function family $\{H_{\pi,\pi'} \mid (\pi,\pi') \in \mathsf{Perm}(n) \times \mathsf{Perm}(n)\}$ where,

$$\begin{aligned} H_{\pi,\pi'} : \{0,1\}^* &\to \{0,1\}^{2n} \\ M &\mapsto \mathsf{CBC}_\pi(M) \| \mathsf{CBC}_{\pi'}(M), \end{aligned}$$

is an $\left(\frac{q(d'(l)+\frac{l^4}{n})}{2^n}\right)^2$-AU hash function family, with respect to any adversary which is restricted to making q queries of block length at most l.

8.3 4F-PHash-DbHtF

Given any n-bit random permutation $\pi, \pi_1, \ldots, \pi_4 \leftarrow\!\!\$\ \mathsf{Perm}(n)$ sampled independently and uniformly at random, Consider the $2n$-bit PHash hash function [10] and define the MAC construction 4F-PHash-DbHtF as, the construction $\mathsf{DbHtF}[\mathsf{PHash}_\pi, \pi_1, \pi_2, \pi_3, \pi_4]$.

Cogliati et. al [15, Lemma 15] [Lemma 15], showed that for a truncated version of PHash which they call TPHash, for any adversary making at most q queries of block length at most l,

$$\mathbf{Adv}^{\mathrm{coll}}_{\mathsf{TPHash}}(q,l) \leq \frac{16q^2l}{2^{2n}}.$$

Corollary 7. *If $n \geq 30$, then for any PRF adversary which is allowed to make $q \leq \frac{2^n}{48n^2}$ queries of block length at most l,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{4F\text{-}PHash\text{-}DbHtF}}(q,l) \leq \frac{16q^2l}{2^{2n}} + \frac{(36n+80)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

8.4 4F-LightHash-DbHtF

Given any n-bit random permutation $\pi, \pi_1, \ldots, \pi_4 \leftarrow\!\!\$\ \mathsf{Perm}(n)$ sampled independently and uniformly at random, Consider the $2n$-bit LightHash hash function [37] and define the MAC construction 4F-LightHash-DbHtF as, the construction $\mathsf{DbHtF}[\mathsf{LightHash}_\pi, \pi_1, \pi_2, \pi_3, \pi_4]$.

Cogliati et. al [15, Lemma 19] [Lemma 19], showed that for a truncated version of LightHash which they call TLightHash, for any adversary making at most q queries of block length at most l,

$$\mathbf{Adv}^{\mathrm{coll}}_{\mathsf{TLightHash}}(q,l) \leq \frac{8q^2l}{2^{2n}}.$$

Corollary 8. *If $n \geq 30$, then for any PRF adversary which is allowed to make $q \leq \frac{2^n}{48n^2}$ queries of block length at most l,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{4F\text{-}LightHash\text{-}DbHtF}}(q,l) \leq \frac{8q^2l}{2^{2n}} + \frac{(36n+80)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

8.5 PolyMAC$_{\mathsf{plus}}$: A length independent MAC construction

Given any $2n$-bit PolyHash with key space $\{0,1\}^{2n}$ and $\pi_1, \ldots, \pi_4 \leftarrow\!\!\$\ \mathsf{Perm}(n)$ sampled independently and uniformly at random define the MAC construction $\mathsf{PolyMAC}_{\mathsf{plus}}$ as the construction $\mathsf{4F\text{-}PolyHash\text{-}DbHtF}[\pi_1, \pi_2, \pi_3, \pi_4]$.

Corollary 9. *If $n \geq 30$, then for any PRF adversary which is allowed to make $q \leq \frac{2^n}{48n^2}$ queries of maximum total block length σ,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{PolyMAC}_{\mathsf{plus}}}(q,\sigma) \leq \frac{q\sigma}{2^{2n}} + \frac{(36n+80)q^2}{2^{2n}} + \frac{45q}{2^n} + \frac{1}{6}\left(\frac{12q}{2^n}\right)^n + \frac{3}{2}\left(\frac{4q}{2^n}\right)^n.$$

Proof. Note that given any two queries M_i, M_j of block lengths l_i, l_j,

$$\Pr\left[\mathsf{PolyHash}_K(M_i) = \mathsf{PolyHash}_K(M_j)\right] \leq \frac{\max\{l_i, l_j\}}{2^{2n}}.$$

Now given any q queries by an adversary to $\mathsf{PolyHash}$, by rearrangement one can index the queries as $M_1, \ldots, M_q$ such that $l_1 \leq l_2 \leq \cdots \leq l_q$. Let $\sum_{i=1}^{q} l_i \leq \sigma$.

Then

$$\mathbf{Adv}^{\mathrm{coll}}_{\mathsf{PolyHash}}(q,\sigma) \leq \sum_{j=2}^{q}\sum_{i=1}^{j}\frac{l_j}{2^{2n}} \leq \sum_{j=1}^{q}\sum_{i=1}^{q}\frac{l_j}{2^{2n}} \leq q\sum_{j=1}^{q}\frac{l_j}{2^{2n}} \leq \frac{q\sigma}{2^{2n}}.$$

9 Proof of Core Lemma for Mirror Theory, Lemma 2

For the proof of core lemma we recall the previously defined component removal and vertex deletion transformations and define some more graph transformations:

Graph Transformations. We will start with the system of equations $\mathcal{E}$ described in (3) and then prove Theorem 4 via induction. For that purpose, we will make several modifications to the underlying graph $\mathcal{G}(\mathcal{E})$. For a general undirected edge-labeled graph $\mathcal{G}$ with components $\mathcal{A}_1, \ldots, \mathcal{A}_a$, or abusing notation, $\mathcal{G} = \{\mathcal{A}_1, \ldots, \mathcal{A}_a\}$, we will consider the following transformations:

- *Removing a component.* Consider a component $S \in \mathcal{G}$, then the graph obtained by removing the entire component S is denoted as $\mathcal{G}_{-S}$.
- *Adding a component.* Consider a graph $\mathcal{G}$ and another connected graph T on disjoint set of vertices. Then we denote the union of these two graphs $\mathcal{G}_{+T}$. If $\mathcal{G}$ and T are both cycle-free and non-degenerate then $\mathcal{G}_{+T}$ also has these properties. Moroever, for $\xi = \max\{\xi_{\mathcal{G}}, |T|\}$, $\mathcal{G}_{+T}$ is ξ-block-maximal.
- *Removing a vertex.* Consider a vertex $v \in S \in \mathcal{G}$. Suppose we remove the vertex v from $\mathcal{G}$, choose a vertex u in the neighborhood of v, and for any other vertex u' in the neighborhood of v add an edge between u and u' with label $\Lambda(u, u')$. If $\mathcal{G}$ was cycle-free, ξ-block-maximal and non-degenerate, then this reduced graph will also have these properties. This transformation would result in a different graph for every choice of u in the neighborhood of v, however, all of them will be equivalent, in the sense that they will have

the exact same set of (I_1, I_2, I_3)-respecting solutions. We denote any such graph as $\mathcal{G}_{-v}$. When vertices $v_1, \ldots, v_r$ are removed from $\mathcal{G}$ one by one in the aforementioned way, we denote the resulting graph as $\mathcal{G}_{-v_1-\cdots-v_r}$.

– *Merging two components.* Suppose two vertices v and w belonging to distinct components with $v \sim w$. Then the graph obtained by merging the two vertices v and w is denoted by $\mathcal{G}_{v=w}$. Let the component in $\mathcal{G}_{w=v}$ obtained by merging the components $\mathcal{C}_v(\mathcal{G})$ and $\mathcal{C}_w(\mathcal{G})$, be denoted as $\mathcal{C}_{v=w}(\mathcal{G})$. Note that if $\mathcal{G}$ results in the label function Λ, then $\mathcal{G}_{v=w}$ has the label function $\Lambda_{v=w}$ defined as

$$\Lambda_{v=w}(P_i, P_j) = \begin{cases} \Lambda(v, P_i) \oplus \Lambda(w, P_j), & \text{when } \Lambda(v, P_i), \Lambda(w, P_j) \neq \perp. \\ \Lambda(P_i, P_j), & \text{otherwise.} \end{cases}$$

– *Breaking a component.* Suppose $\mathcal{G}$ induces the label function Λ and let $U \subseteq S \in \mathcal{G}$. We define the graph $\mathcal{G}^{S\|U}$ as the graph containing component structure $\mathcal{G}_{-S} \cup \{S \setminus U, U\}$, such that for $T \in \{S \setminus U, U\}$ there exists $u \in T$ with an edge between u and any other vertex $u' \in T$ labeled $\Lambda(u, u')$. Of course, this transformation leads to a different graph for each choice of the central vertex $u \in T$, however, all these graphs are equivalent in the above sense, and hence any of those graphs can be denoted as $\mathcal{G}^{S\|U}$. Note that, if $v, w \in \mathcal{G}$ are vertices in different components, with $v \sim w$, and if $T = \mathcal{C}_{v=w}(\mathcal{G})$ is the component in $\mathcal{G}_{w=v}$ obtained by merging the components of v and w, then $\mathcal{G}_{v=w}^{T\|\mathcal{C}_w(\mathcal{G})}$ is equivalent to $\mathcal{G}_{-v}$.

Extending from the definition fo reduced graphs in the main body, any graph $\mathcal{G}$ obtained as a result of applying all the above transformations (including the newly defined ones), multiple number of times in some arbitrary order, to $\mathcal{G}(\mathcal{E})$, is called a reduced graph of $\mathcal{G}(\mathcal{E})$, and the corresponding system of equations, $\mathcal{E}(\mathcal{G})$, is called a reduced system of $\mathcal{E}$. Note that merging two vertices may not yield a system of equations that admits a (I_1, I_2, I_3)-respecting solution. Given a vertex $v \in \mathcal{V}(\mathcal{G})$ we will be interested in all the vertices $w \notin \mathcal{C}_v(\mathcal{G})$ with $w \sim v$, such that $\mathcal{E}(\mathcal{G}_{v=w})$ has at least one (I_1, I_2, I_3)-respecting solution. Thus we define

$$I_v(\mathcal{G}) := \{w \mid w \in \mathcal{V}(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}), w \sim v, N(\mathcal{G}_{v=w}) > 0\}$$

We start with a system of equations $\mathcal{E}$ with its collection of variables, that is the vertex set $\mathcal{V}(\mathcal{E}) = \mathcal{V}_1 \sqcup \mathcal{V}_2 \sqcup \mathcal{V}_3$ of $\mathcal{G}(\mathcal{E})$, and compare its number of (I_1, I_2, I_3)-respecting solutions with that of the reduced graphs with reduced number of vertices. For such a reduced graph $\mathcal{G} = \{\mathcal{A}_1, \ldots, \mathcal{A}_a\}$, we recall the notations $\xi_{\mathcal{G}}$, denoting size of the largest component in $\mathcal{G}$, and $\eta_1(\mathcal{G}), \eta_2(\mathcal{G}), \eta_3(\mathcal{G})$ denoting the number of vertices in $\mathcal{G}$ belonging to each of the partitions $\mathcal{V}_1, \mathcal{V}_2$ and $\mathcal{V}_3$, respectively. Also for $u, v \in \mathcal{V}(\mathcal{G}), S \in \mathcal{G}$, we recall the definitions of $\delta_S(u, v), \delta_{\mathcal{G}}(u, v)$, denoting the multiplicity of paths in the subgraph induced by S, and in $\mathcal{G}$, respectively, having label sum $\Lambda(u, v)$, and $\Delta_{\mathcal{G}}$ denoting maximum among all these multiplicities for different choices of $u, v \in \mathcal{G}$.

9.1 Vertex deletion equation

We want to compare $N(\mathcal{G})$ and $N(\mathcal{G}_{-v})$. We assume $\mathcal{G}$ is cycle-free and non-degenerate. Consider any particular (I_1, I_2, I_3)-respecting solution $(x_u \mid u \in \mathcal{G}_{-v})$ of $\mathcal{E}(\mathcal{G}_{-v})$. Suppose $v \in \mathcal{V}(\mathcal{G})$. For any $u \in S$, $u \neq v$, the value assigned to v will be $x_v = x_u \oplus \Lambda(u, v)$. If there exists no other such vertex, that is $\mathcal{C}_v(\mathcal{G}) = \{v\}$, then v can be assigned any value $x_v \in \{0,1\}^n$. One of the following cases might occur:

- Either $x_v \notin \{x_u \mid u \in \mathcal{G}_{-v}, u \sim v\}$. Then $(x_u \mid u \in \mathcal{G})$ is a (I_1, I_2, I_3)-respecting solution to $\mathcal{E}(\mathcal{G})$.
- Or $x_v = x_w$ for some $w \in \mathcal{G}_{-v}$ with $w \sim v$. Of course, it follows from the non-degeneracy of $\mathcal{G}$, that for any $u \in \mathcal{C}_v(\mathcal{G})$ with $u \sim v$, since $\Lambda(u, v) \neq 0$ we must have $x_u \neq x_v$. Thus $w \in \mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}$. In this case $(x_u \mid u \in \mathcal{G}_{-v})$ is a solution to $\mathcal{G}_{v=w}$. Recall that the set of all such $w \in \mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}$ is denoted as

$$I_v(\mathcal{G}) = \{w \mid w \in \mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}, w \sim v, N(\mathcal{G}_{v=w}) > 0\}$$

Thus we arrive at the following vertex-deletion equation

$$N(\mathcal{G}) = N(\mathcal{G}_{-v}) - \sum_{w \in I_v(\mathcal{G})} N(\mathcal{G}_{v=w}) \tag{11}$$

To go from (11) to Lemma 2, we need to establish the following things:

- Upper bound the size of the set $I_v(\mathcal{G})$.
- Upper bound $N(\mathcal{G}_{v=w})$ in terms of $N(\mathcal{G}_{-v})$.

9.2 Upper bounding $|I_v(\mathcal{G})|$

For $w \in \mathcal{V}(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})$ with $w \sim v$, we will have $w \notin I_v(\mathcal{G})$, if there exists $u \in \mathcal{C}_v(\mathcal{G})$ and $x \in \mathcal{C}_w(\mathcal{G})$ with $x \sim u$ such that $\Lambda_{v=w}(u, x) = 0$, which can be equivalently written as $\Lambda(v, u) = \Lambda(w, x)$. Thus recalling the definition of $\delta_S(u, v)$ and $\delta_{\mathcal{G}}(u, v)$ we have

$$\begin{aligned}
|I_v| &= \sum_{S \in \mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}} \left(\eta_v(S) - \sum_{u \in \mathcal{C}_v(\mathcal{G})} \delta_S(u, v) \right) \\
&= \eta_v(\mathcal{G}) - \eta_v(\mathcal{C}_v(\mathcal{G})) - \sum_{u \in \mathcal{C}_v(\mathcal{G})} \delta_{\mathcal{G}}(u, v) + \sum_{u \in \mathcal{C}_v(\mathcal{G})} \delta_{\mathcal{C}_v(\mathcal{G})}(u, v) \\
&\leq \eta_v(\mathcal{G}) - \sum_{u \in \mathcal{C}_v(\mathcal{G})} \delta_{\mathcal{G}}(u, v)
\end{aligned}$$

since $\eta_v(\mathcal{C}_v(\mathcal{G})) \geq \sum_{u \in \mathcal{C}_v(\mathcal{G})} \delta_{\mathcal{C}_v(\mathcal{G})}(u, v)$.

If, in fact, for some $u \in \mathcal{C}_v(\mathcal{G})$, u, v achieves the maximum $\Delta_{\mathcal{G}}$, as assumed in Lemma 2, then we have

$$|I_v(\mathcal{G})| \leq \eta_v(\mathcal{G}) - \Delta_{\mathcal{G}}. \tag{12}$$

9.3 Relation between $\mathcal{G}_{v=w}$ and $\mathcal{G}_{-v}$

Let $\mathcal{G} = \{\mathcal{A}_1, \ldots, \mathcal{A}_a\}$. Suppose $v \in \mathcal{V}(\mathcal{G})$. Then, for $\alpha \in [a]$, $\ell \geq 0$ we define

$$D(\alpha, \ell) = \max_{\mathcal{H},T,U} \left| N(\mathcal{H}_{+T}) - \frac{1}{2^n} \cdot N\left((\mathcal{H}_{+T})^{T \| U} \right) \right|$$

where the maximum is taken over all subgraphs $\mathcal{H} \subseteq \mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}$ containing $\alpha - 1$ components, all non-degenerate trees T with number of vertices bounded by $\ell + 1 \leq \mathcal{V}(T) \leq \xi_{\mathcal{G}} + \ell + 1$ and all subsets $U \subseteq T$ containing $\ell + 1$ vertices.

Note that, letting $\alpha = a$, $T = \mathcal{C}_{w=v}(\mathcal{G})$ obtained by merging the components of w and v in $\mathcal{G}$, $\mathcal{H} = \mathcal{G}_{-T}$, and $U = \mathcal{C}_w(\mathcal{G})$, we have

$$\left| N(\mathcal{G}_{v=w}) - 2^{-n} \cdot N(\mathcal{G}_{-v}) \right| \leq D(a, \ell)$$

where $|\mathcal{C}_w(\mathcal{G})| = \ell + 1$. Thus it is enough to upper bound $D(a, \ell)$, for which we will first state a crude bound and a recursive inequality for the double sequence $D(\alpha, \ell)$ and give an upper bound for terms of any double sequence satisfying the crude bound and the recursive inequality.

Lemma 7. *We can crudely upper bound the terms $D(\alpha, \ell)$ as follows:*

$$D(\alpha, \ell) \leq \frac{2^{n+1} N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{(2^n - (a-1)\xi_{\mathcal{G}}^2)^{a-\alpha}}$$

Proof. There are $a - \alpha$ components in $\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})} \setminus \mathcal{H}$. Thus by iterating (4) and observing that $\sum_{i=1}^{3} \eta_i(S) \cdot \eta_i(\mathcal{G}'_{-S}) \leq |S| \cdot |\mathcal{V}(\mathcal{G}'_{-S})| \leq (a-1)\xi_{\mathcal{G}}^2$, for any $\mathcal{H} \subseteq \mathcal{G}' \subseteq \mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}$ and $S \in \mathcal{G}' \setminus \mathcal{H}$, we have

$$N(\mathcal{H}) \leq \frac{N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{(2^n - (a-1)\xi_{\mathcal{G}}^2)^{a-\alpha}}$$

Moreover $N(\mathcal{H}_{+T}) \leq 2^n \cdot N(\mathcal{H})$. Hence we have

$$N(\mathcal{H}_{+T}) \leq \frac{2^n \cdot N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{(2^n - (a-1)\xi_{\mathcal{G}}^2)^{a-\alpha}} \tag{13}$$

Similarly, we have

$$N((\mathcal{H}_{+T})^{T \| U}) \leq \frac{2^{2n} \cdot N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{(2^n - (a-1)\xi_{\mathcal{G}}^2)^{a-\alpha}} \tag{14}$$

Doing (13) $-2^{-n} \cdot$(14) and taking maximum over $\mathcal{H}, T, U$ gives the statement of the lemma. □

Lemma 8. *Let $\mathcal{B}_1, \ldots, \mathcal{B}_{a-1}$ be any enumeration of the components of $\mathcal{G}_{-S}$ and let $|\xi_i| = |\mathcal{B}_i|$ for $i \in [a-1]$. Then the following recursive inequality holds:*

$$D(\alpha, \ell) \leq D(\alpha, \ell - 1) + \xi_{\mathcal{G}} \sum_{i=1}^{a-1} D(\alpha - 1, \ell + \xi_i - 1) + \frac{\xi_{\mathcal{G}}(\Delta_{\mathcal{G}} + 1) \cdot N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{(2^n - (a-1)\xi_{\mathcal{G}}^2)^{a-\alpha}}$$

Proof. We fix $\mathcal{H} \subseteq \mathcal{G}_{-S}$ containing $\alpha - 1$ components, a non-degenerate tree T with number of vertices bounded by $\ell + 1 \leq \mathcal{V}(T) \leq \ell + \xi_{\mathcal{G}} + 1$ and a subset $U \subseteq \mathcal{V}(T)$ with $|U| = \ell+1$, such that this choice of $\mathcal{H}, T, U$ achieves the maximum $D(\alpha, \ell)$, that is, $|N(\mathcal{H}_{+T}) - 2^{-n} \cdot N\left((\mathcal{H}_{+T})^{T\|U}\right)| = D(\alpha, \ell)$. We prove the lemma by dividing it into two subcases.

– $|U| = 1$. That is $U = \{v\}$ for some $v \in T$. Then $\mathcal{H}_{+T\setminus U} = (\mathcal{H}_{+T})_{-v}$. Thus by the vertex deletion equation, (11), we have

$$N(\mathcal{H}_{+T}) = N(\mathcal{H}_{+T\setminus U}) - \sum_{(w,S')\in I_v} N((\mathcal{H}_{+T})_{v=w}) \tag{15}$$

Here,

$$I_v(\mathcal{H}_{+T}) = \{w \in \mathcal{V}\left((\mathcal{H}_{+T})_{-\mathcal{C}_v(\mathcal{H}_{+T})}\right) \mid w \sim v, N((\mathcal{H}_{+T})_{v=w}) > 0\}$$

For $w \in \mathcal{V}(\mathcal{H})$, $w \notin I_v(\mathcal{H}_{+T})$ if and only if there exists $v' \in T$ and $w' \in \mathcal{C}_w(\mathcal{H})$ such that $\Lambda(v, v') = \Lambda(w, w')$. Thus we have

$$\begin{aligned} |I_v(\mathcal{H}_{+T})| &= \sum_{S\in\mathcal{H}} \left(\eta_v(S) - \sum_{u\in T\setminus U} \delta_S(u, v) \right) \\ &= \eta_v(\mathcal{H}_{+T\setminus U}) - \eta_v(T \setminus U) - \sum_{u\in T} \delta_{\mathcal{H}}(u, v) \\ &\geq \eta_v(\mathcal{H}_{+T\setminus U}) - \xi_{\mathcal{G}}(\Delta_{\mathcal{G}} + 1) \end{aligned} \tag{16}$$

Also, $(\mathcal{H}_{+T})^{T\|U} = (\mathcal{H}_{+T})_{-v} \sqcup \{U\}$, which implies that given a solution of $(\mathcal{H}_{+T})_{-v}$, there exist $2^n - \eta_v(\mathcal{H}_{+T\setminus U})$ possible n-bit values which when assigned to v, extends the given solution to a (I_1, I_2, I_3)-respecting tuple satisfying the larger system of equations $(\mathcal{H}_{+T})^{T\|U}$. Hence,

$$N\left((\mathcal{H}_{+T})^{T\|U}\right) = (2^n - \eta_v(\mathcal{H}_{+T\setminus U})) \cdot N((\mathcal{H}_{+T})_{-v}). \tag{17}$$

Now doing (15) $-2^{-n}\cdot$(17), and using (16) we have

$$\begin{aligned} D(\alpha, 0) &\leq \sum_{w\in I_v(\mathcal{H}_{+T})} \left|N((\mathcal{H}_{+T})_{v=w}) - 2^{-n} \cdot N(\mathcal{H}_{+T\setminus U})\right| + \frac{\xi_{\mathcal{G}}(\Delta_{\mathcal{G}} + 1) \cdot N(\mathcal{H}_{+T\setminus U})}{2^n} \\ &\leq \xi_{\mathcal{G}} \sum_{S'\in\mathcal{H}} D(\alpha - 1, |S'| - 1) + \frac{\xi_{\mathcal{G}}(\Delta_{\mathcal{G}} + 1) \cdot N(\mathcal{H}_{+T\setminus U})}{2^n} \\ &\leq \xi_{\mathcal{G}} \sum_{S'\in\mathcal{H}} D(\alpha - 1, |S'| - 1) + \frac{\xi_{\mathcal{G}}(\Delta_{\mathcal{G}} + 1) \cdot N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{(2^n - (a-1)\xi_{\mathcal{G}}^2)^{a-\alpha}} \end{aligned}$$

where in the second inequality is obtained by taking $S' = \mathcal{C}_w(\mathcal{H})$ for $w \in I_v(\mathcal{H}_{+T})$, observing that each such set S' can contribute to at most $|S'| \leq \xi_{\mathcal{G}}$ terms to the summation, and noting that $((\mathcal{H}_{+T})_{v=w})^{\mathcal{C}_{v=w}(\mathcal{H}_{+T})\|U} = \mathcal{H}_{+T\setminus U}$. The third inequality follows from (13).

– $|U| \geq 2$. For $v \in U$ we can use the vertex deletion equation (11) we have

$$N(\mathcal{H}_{+T}) = N((\mathcal{H}_{+T})_{-v}) - \sum_{w \in I_v(\mathcal{H}_{+T})} N((\mathcal{H}_{+T})_{v=w}) \tag{18}$$

and

$$N((\mathcal{H}_{+T})^{T\|U}) = N(((\mathcal{H}_{+T})^{T\|U})_{-v}) - \sum_{w \in I_v((\mathcal{H}_{+T})^{T\|U})} N(((\mathcal{H}_{+T})^{T\|U})_{v=w})$$

which can be written as

$$N\left((\mathcal{H}_{+T})^{T\|U}\right) = N\left(((\mathcal{H}_{+T})_{-v})^{T'\|U'}\right) - \sum_{w \in I_v((\mathcal{H}_{+T})^{T\|U})} N\left(((\mathcal{H}_{+T})_{v=w})^{T''\|U''}\right) \tag{19}$$

where $T' = T \backslash \{v\}$, $U' = U \backslash \{v\}$, $T'' = \mathcal{C}_{v=w}(\mathcal{H}_{+T})$ and $U'' = \mathcal{C}_{v=w}\left(\mathcal{H}_{+T}^{T\|U}\right)$. Of course, we have $T'' \setminus U'' = T \setminus U$.

Note that

$$I_v(\mathcal{H}_{+T}) = \{w \in \mathcal{H} \mid w \sim v, N((\mathcal{H}_{+T})_{v=w}) > 0\}$$
$$I_v((\mathcal{H}_{+T})^{T\|U}) = \{w \in \mathcal{H}_{+T\setminus U} \mid w \sim v, N\left(((\mathcal{H}_{+T})^{T\|U})_{v=w}\right) > 0\}$$

Now if $w \in I_v(\mathcal{H}_{+T})$, then $w \in \mathcal{H}$, $w \sim v$ and $N((\mathcal{H}_{+T})_{v=w}) > 0$, which implies $N((\mathcal{H}_{+T})^{T\|U})_{v=w}) > 0$, and hence we have $w \in I_v((\mathcal{H}_{+T})^{T\|U})$. If $w \in I_v((\mathcal{H}_{+T})^{T\|U}) \setminus I_v(\mathcal{H}_{+T})$, then one of the following two cases can happen:

- $w \in T \setminus U$, satisfying $w \sim v$ and $N((\mathcal{H}_{+T})^{T\|U})_{v=w}) > 0$. We can simply bound the number of such w's by $|T \setminus U|$.
- $w \in \mathcal{H}$ satisfying $w \sim v$ such that $N((\mathcal{H}_{+T})^{T\|U})_{v=w}) > 0$ and $N((\mathcal{H}_{+T})_{v=w}) = 0$. This happens if there exists $v' \in T \setminus U$ and $w' \in \mathcal{C}_w(\mathcal{H})$ such that $\Lambda(v, v') = \Lambda(w, w')$.

Thus we have

$$\left|I_v((\mathcal{H}_{+T})^{T\|U}) \setminus I_v(\mathcal{H}_{+T})\right| \leq |T \setminus U| + \sum_{v' \in T\setminus U} \delta_{\mathcal{H}}(v, v') \leq \xi_{\mathcal{G}}(\Delta_{\mathcal{G}} + 1) \tag{20}$$

By doing (18) $-2^{-n}\cdot$(19), and using (20) we get

$$\begin{aligned}
D(\alpha,\ell) &\le \left|N((\mathcal{H}_{+T})_{-v}) - 2^{-n}\cdot N\left(((\mathcal{H}_{+T})_{-v})^{T'\|U'}\right)\right| \\
&\quad + \left|\sum_{w\in I_v(\mathcal{H}_{+T})} N((\mathcal{H}_{+T})_{v=w}) - 2^{-n}\cdot \sum_{w\in I_v((\mathcal{H}_{+T})^{T\|U})} N\left(((\mathcal{H}_{+T})_{v=w})^{T''\|U''}\right)\right| \\
&\le D(\alpha,\ell-1) \\
&\quad + \sum_{w\in I_v(\mathcal{H}_{+T})} \left|N((\mathcal{H}_{+T})_{v=w}) - 2^{-n}\cdot N\left(((\mathcal{H}_{+T})_{v=w})^{T''\|U''}\right)\right| \\
&\quad + 2^{-n}\cdot \sum_{w\in I_v((\mathcal{H}_{+T})^{T\|U})\setminus I_v(\mathcal{H}_{+T})} N\left(((\mathcal{H}_{+T})_{v=w})^{T''\|U''}\right) \\
&\le D(\alpha,\ell-1) + \xi_{\mathcal{G}}\sum_{S\in\mathcal{H}} D(\alpha-1,\ell+|S|-1) + \frac{\xi_{\mathcal{G}}(\Delta_{\mathcal{G}}+1)\cdot N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{(2^n-(a-1)\xi_{\mathcal{G}}^2)^{a-\alpha}}
\end{aligned}$$

Thus we have our result. □

If we define the double sequence

$$s_{d,\ell} := \frac{\xi_{\mathcal{G}}^d}{4N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})} D(a-d,\ell), \tag{21}$$

then, from Lemmas 7 and 8, we have that $s_{d,\ell}$ satisfies the conditions of the following lemma from [14], with $c = a-1$, $\xi = \xi_{\mathcal{G}}$ and $A = \xi_{\mathcal{G}}(\Delta_{\mathcal{G}}+1)/2^n$, by noting the following

- The number of components in $\mathcal{H}$ is at most the number of edges in $\mathcal{H}$, which implies $a-1 \le 2q \le 2^n/12\xi_{\max}^2 \le 2^n/12\xi_{\mathcal{G}}^2 \implies \frac{2^{n+1}}{4(2^n-(a-1)\xi_{\mathcal{G}}^2)} \le 12/22 \le 1$, and hence it follows from Lemma 7 that
$$s_{d,\ell} \le \left(\frac{\xi_{\mathcal{G}}}{2^n-(a-1)\xi_{\mathcal{G}}^2}\right)^d.$$
- Moreover, the taking $x = (a-1)\xi_{\mathcal{G}}^2/2^n$, we have $x \le 1/12$, which implies $\frac{x}{1-x} \le 1/4e$, hence we have
$$\frac{\xi_{\mathcal{G}}}{2^n-(a-1)\xi_{\mathcal{G}}^2} \le \frac{1}{4e\xi_{\mathcal{G}}(a-1)}.$$

Lemma 9 ([14]). *Suppose $s_{d,\ell} \ge 0$ be such that:*

1. *$s_{d,k} := 0$ for any $k < 0$, and*
2. *for all $0 \le d \le \xi n$ and $0 \le \ell_i \le \xi - 1$ for $i \in [c]$, we have*

$$s_{d,\ell} \le (4\xi ec)^{-d}, \qquad s_{d,\ell} \le s_{d,\ell-1} + \sum_{i=1}^{c} s_{d+1,\ell+\ell_i} + A\cdot(4\xi ec)^{-d}$$

for some $A > 0$. Then for every $\ell \in [\xi-1]$,

$$s_{0,\ell} \le \frac{4}{2^n} + 4A\xi$$

9.4 Proof of Lemma 2

Since the double sequence $s_{d,\ell}$ defined in (21) follows the conditions of Lemma 9 we have that, for every $w \in I_v(\mathcal{G})$,

$$\begin{aligned}\left|N(\mathcal{G}_{v=w}) - 2^{-n} \cdot N(\mathcal{G}_{-v})\right| \leq D(a, |\mathcal{C}_w(\mathcal{G})| - 1) &= 4N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}) \cdot s_{0,|\mathcal{C}_w(\mathcal{G})|-1} \\ &\leq \frac{8N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{2^n}(2 + \xi_{\mathcal{G}}^2(\Delta_{\mathcal{G}} + 1))\end{aligned}$$

We also have

$$N(\mathcal{G}_{-v}) \geq (2^n - \eta_v(\mathcal{G})\xi_{\mathcal{G}})N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}) \geq 2^n \left(1 - \frac{1}{12\xi_{\mathcal{G}}}\right) N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})}) \geq \frac{23 \cdot 2^n}{24} N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})$$

Combining, we have

$$\begin{aligned}N(\mathcal{G}_{v=w}) &\leq \frac{1}{2^n} N(\mathcal{G}_{-v}) + \frac{8N(\mathcal{G}_{-\mathcal{C}_v(\mathcal{G})})}{2^n}(2 + \xi_{\mathcal{G}}^2(\Delta_{\mathcal{G}} + 1)) \\ &\leq \frac{1}{2^n}\left(1 + \frac{9(2 + \xi_{\mathcal{G}}^2(\Delta_{\mathcal{G}} + 1))}{2^n}\right) N(\mathcal{G}_{-v}) \\ &\leq \frac{1}{2^n}\left(1 + \frac{C(\Delta_{\mathcal{G}} + 1)}{2^n}\right) N(\mathcal{G}_{-v})\end{aligned}$$

where $C = 9(\xi_{\mathcal{G}}^2 + 2)$. Finally, from the vertex deletion equation, (11), and the upper bound, (12), on the size of $|I_v(\mathcal{G})|$, we have

$$\begin{aligned}N(\mathcal{G}) &= N(\mathcal{G}_{-v}) - \sum_{w \in I_v(\mathcal{G})} N(\mathcal{G}_{v=w}) \\ &\geq N(\mathcal{G}_{-v}) - \sum_{w \in I_v(\mathcal{G})} \frac{1}{2^n}\left(1 + \frac{C(\Delta_{\mathcal{G}} + 1)}{2^n}\right) N(\mathcal{G}_{-v}) \\ &\geq N(\mathcal{G}_{-v})\left(1 - \frac{\eta_v(\mathcal{G}) - \Delta_{\mathcal{G}}}{2^n}\left(1 + \frac{C(\Delta_{\mathcal{G}} + 1)}{2^n}\right)\right) \\ &\geq N(\mathcal{G}_{-v})\left(1 - \frac{\eta_v(\mathcal{G}) + 1}{2^n} + \frac{\Delta_{\mathcal{G}} + 1}{2^n}\left(1 - \frac{C(\eta_v(\mathcal{G}) - \Delta_{\mathcal{G}})}{2^n}\right)\right) \\ &\geq N(\mathcal{G}_{-v})\left(1 - \frac{\eta_v(\mathcal{G}) + 1}{2^n}\right)\end{aligned}$$

since $C \cdot \eta_v(\mathcal{G}) \leq 2^n$.

10 Mirror Theory for general p partitions

Here, we formally state our version of the "relaxed mirror theory" conjecture of [40, Theorem 3] and prove it. Note that [40] claimed that this conjecture follows from [47, Theorem 7], and we think the claim is not well-founded. Moreover, the proofs in [47] had unverifiable gaps. Finally, our proof solves this open problem. This result is of theoretical interest mostly, we do not currently have applications for the $p > 3$ partitions case.

Theorem 6. *Let $\mathcal{E}$ be a system of $2q$ equations over $k \geq 10$ unknowns $\mathcal{P}$ and each unknown takes value in $\{0,1\}^n, n \geq 1$. Then if $\mathcal{E}$ is (i) circle-free, (ii) ξ-block-maximal for some ξ such that $q \leq \frac{2^n}{48\xi^2}$ and $2^{n/2} > n\xi^2 + n$, and (iii) non-degenerate with respect to some partition $I_1, \ldots, I_p$ of $[k]$[4], then we have number of $(I_1, \ldots, I_p)$-respecting solutions to the system of equations $\mathcal{E}$ is lower bounded by*

$$\frac{(2^n-2)_{|I_1|} \cdot \cdots \cdot (2^n-2)_{|I_p|}}{2^{2nq}}.$$

Proof. The proof of Theorem 6 almost follows the same arguments that justified the specific $p = 3$ case (Theorem 4) The main artifact that is different in this case is that instead of Eq. (5) we need to prove

$$1 - \frac{\sum_{i\in[p]} a_i r_i}{2^n} \geq \prod_{i=1}^{p} \prod_{j=2}^{r_i+1} \left(1 - \frac{a_i + j}{2^n}\right)$$

where $a_i = \eta_i(S), r_i = \eta_i(\mathcal{G}_{-S}), i \in [p]$, are the number of vertices in S and $\mathcal{G}_{-S}$ respectively, that belong to the i-th partition.

This inequality can be shown by induction on $r_i, i \in [p]$. We just need to show the base case, that for $r_i = 1$ for all $i \in [p]$, the inequality holds. This can be shown as follows:

$$\begin{aligned}\prod_{i=1}^{p} \left(1 - \frac{a_i + 2}{2^n}\right) &= 1 - \frac{\sum_{i\in[p]} a_i}{2^n} - C \\ &\leq 1 - \frac{\sum_{i\in[p]} a_i}{2^n}\end{aligned}$$

where

$$C = \frac{2^k}{2^n}\left(1 - \sum_{i\neq j\in[p]} \frac{(a_i+2)(a_j+2)}{2^{n+k}} + \underbrace{\text{higher order terms}}_{\geq 0}\right) \geq 0$$

since $a_i \leq \sum_{i\in[p]} a_i \leq k \leq 2^{n/2} \implies \sum_{i\neq j\in[p]} (a_i+2)(a_j+2) \leq 2^{n+2}p^2 \leq 2^{n+k-1}$ ($p \leq k \leq 2^{(k-3)/2}$ for $k \geq 10$).

The induction step and the rest follow exactly as the proof of Theorem 4. □

11 Conclusion and Future Directions

This paper revisits the security of permutation-based LR ciphers and their application in constructing tweakable block ciphers, addressing gaps in the current literature and proposing more efficient constructions. We formally define TLR-compatible functions, for processing the tweak, which when composed with 4-rounds and 5-rounds of LR construction with random permutations as internal

[4] We assume that all the partitions, I_i, are non-empty.

primitives gives us respectively n-bit CPA and CCA secure tweakable permutations. We also propose instantiating TLR-compatible functions with one round LR where a permutation (resp, an AXU hash) is used to mask single-block tweaks (resp., variable-length tweaks), thus proposing the n-bit CPA (resp., CCA) secure tweakable permutation candidates, TLRP5 and TLRP5+ (resp., TLRP7 and TLRP7+), using 5 (resp., 7) LR rounds, which is a significant reduction from the tweak-length-dependent results of Goldenberg et al. As a corollary, we also show n-bit CPA (resp., CCA) security of 5-rounds (resp. 7-rounds) permutation-based LR construction, which is quite an improvement over the existing $2n/3$-bit security proved by Guo et al. For the security analysis, we proved the general Mirror Theory result for three permutations. In fact we extend our proof to the case when there are more than 3 partitions of the variable set, leading to the proof of Mennink's conjecture [40, Theorem 3].

A possible future direction will be to reduce the number of LR rounds even further without compromising n-bit security. A more general challenge will be to specify the minimal number of blockcipher calls needed to obtain optimal, even BBB, secure tweakable blockciphers. Moreover, we have crucially used the independence of underlying permutations in our security analysis, which in practice will be instantiated with a blockcipher with independent keys, thus leaving open the security analysis of the single-keyed versions of our constructions. Of course, the single-keyed version of our CCA constructions has symmetric encryption and decryption and hence is trivially insecure. So the single-keyed version of such needs careful modification of our construction. Another possible future direction is to extend the security results for key-alternating ciphers using public permutation. Finally, in this paper we have restricted ourselves to showing the existence of TLR-compatible function families by constructing examples, hence a comprehensive study of TLR-compatible function families is also of future interest.

Acknowledgments

We would like to thank Wonseok Choi and Avijit Dutta for their valuable suggestions on mirror theory and overall presentation of this paper. We are grateful to the anonymous CRYPTO 2025 reviewers for their constructive and encouraging comments.

Bishwajit Chakraborty was supported by the NRF-ANR project SELECT ("NRF2020-NRF-ANR072"). Abishanka Saha was funded in part by the European Commission through the Horizon Europe program under project number 101135475 (TALER) and in part by the Swiss State Secretariat for Education, Research and Innovation (SERI).

References

1. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: Camellia: A 128-bit block cipher suitable for multiple platforms - design and

analysis. In: Stinson, D.R., Tavares, S.E. (eds.) Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 14-15, 2000, Proceedings. Lecture Notes in Computer Science, vol. 2012, pp. 39–56. Springer (2000). https://doi.org/10.1007/3-540-44983-3_4, https://doi.org/10.1007/3-540-44983-3_4

2. Banik, S., Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT-COFB. Cryptology ePrint Archive, Report 2020/738 (2020), https://eprint.iacr.org/2020/738
3. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9815, pp. 123–153. Springer (2016). https://doi.org/10.1007/978-3-662-53008-5_5, https://doi.org/10.1007/978-3-662-53008-5_5
4. Bellare, M., Kilian, J., Rogaway, P.: The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences **61**(3), 362–399 (2000). https://doi.org/https://doi.org/10.1006/jcss.1999.1694, https://www.sciencedirect.com/science/article/pii/S002200009991694X
5. Bellare, M., Kilian, J., Rogaway, P.: The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences **61**(3), 362–399 (2000)
6. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4004, pp. 409–426. Springer (2006). https://doi.org/10.1007/11761679_25, https://doi.org/10.1007/11761679_25
7. Bierbrauer, J., Johansson, T., Kabatianskii, G., Smeets, B.: On families of hash functions via geometric codes and concatenation. In: Stinson, D.R. (ed.) Advances in Cryptology — CRYPTO' 93. pp. 331–342. Springer Berlin Heidelberg, Berlin, Heidelberg (1994)
8. Bierbrauer, J., Johansson, T., Kabatianskii, G., Smeets, B.: On families of hash functions via geometric codes and concatenation. In: Stinson, D.R. (ed.) Advances in Cryptology – CRYPTO'93. Lecture Notes in Computer Science, vol. 773, pp. 331–342. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 22–26, 1994). https://doi.org/10.1007/3-540-48329-2_28
9. Black, J., Rogaway, P.: A block-cipher mode of operation for parallelizable message authentication. In: Knudsen, L.R. (ed.) Advances in Cryptology — EUROCRYPT 2002. pp. 384–397. Springer Berlin Heidelberg, Berlin, Heidelberg (2002)
10. Black, J., Rogaway, P.: A block-cipher mode of operation for parallelizable message authentication. In: Knudsen, L.R. (ed.) Advances in Cryptology – EUROCRYPT 2002. Lecture Notes in Computer Science, vol. 2332, pp. 384–397. Springer, Heidelberg, Germany, Amsterdam, The Netherlands (Apr 28 – May 2, 2002). https://doi.org/10.1007/3-540-46035-7_25
11. den Boer, B.: A simple and key-economical unconditional authentication scheme. J. Comput. Secur. **2**, 65–72 (1993)
12. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Advances in Cryptology - EUROCRYPT 2014. Proceedings. pp. 327–350 (2014)

13. Choi, W., Lee, J., Lee, Y.: Toward full n-bit security and nonce misuse resistance of block cipher-based macs. In: Chung, K., Sasaki, Y. (eds.) Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part IX. Lecture Notes in Computer Science, vol. 15492, pp. 251–279. Springer (2024). https://doi.org/10.1007/978-981-96-0947-5_9, https://doi.org/10.1007/978-981-96-0947-5_9
14. Cogliati, B., Dutta, A., Nandi, M., Patarin, J., Saha, A.: Proof of mirror theory for a wide range of $\xi_{\max}$. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part IV. Lecture Notes in Computer Science, vol. 14007, pp. 470–501. Springer, Heidelberg, Germany, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30634-1_16
15. Cogliati, B., Ethan, J., Jha, A., Nandi, M., Saha, A.: On the number of restricted solutions to constrained systems and their applications. Cryptology ePrint Archive (2024)
16. Cogliati, B., Jha, A., Nandi, M.: How to build optimally secure PRFs using block ciphers. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12491, pp. 754–784. Springer, Heidelberg, Germany, Daejeon, South Korea (Dec 7–11, 2020). https://doi.org/10.1007/978-3-030-64837-4_25
17. Datta, N., Dutta, A., Nandi, M., Paul, G.: Double-block hash-then-sum: A paradigm for constructing bbb secure prf. IACR Transactions on Symmetric Cryptology **2018**(3), 36–92 (Sep 2018). https://doi.org/10.13154/tosc.v2018.i3.36-92, https://tosc.iacr.org/index.php/ToSC/article/view/7297
18. Datta, N., Dutta, A., Nandi, M., Paul, G.: Double-block hash-then-sum: A paradigm for constructing BBB secure PRF. IACR Transactions on Symmetric Cryptology **2018**(3), 36–92 (2018). https://doi.org/10.13154/tosc.v2018.i3.36-92
19. Dolmatov, V.: GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms. RFC 5830 (Mar 2010). https://doi.org/10.17487/RFC5830, https://www.rfc-editor.org/info/rfc5830
20. Goldenberg, D., Hohenberger, S., Liskov, M., Schwartz, E.C., Seyalioglu, H.: On tweaking Luby-Rackoff blockciphers. In: Kurosawa, K. (ed.) Advances in Cryptology – ASIACRYPT 2007. Lecture Notes in Computer Science, vol. 4833, pp. 342–356. Springer, Heidelberg, Germany, Kuching, Malaysia (Dec 2–6, 2007). https://doi.org/10.1007/978-3-540-76900-2_21
21. Guo, C., Zhang, G.: Beyond-birthday security for permutation-based feistel networks. Designs, Codes and Cryptography **89**, 407–440 (2021)
22. Iwata, T., Khairallah, M., Minematsu, K., Peyrin, T.: Duel of the titans: The Romulus and Remus families of lightweight AEAD algorithms. IACR Transactions on Symmetric Cryptology **2020**(1), 43–120 (2020). https://doi.org/10.13154/tosc.v2020.i1.43-120
23. Iwata, T., Kurosawa, K.: Omac: One-key cbc mac. In: Johansson, T. (ed.) Fast Software Encryption. pp. 129–153. Springer Berlin Heidelberg, Berlin, Heidelberg (2003)
24. Jean, J., Nikolic, I., Peyrin, T.: Tweaks and keys for block ciphers: The TWEAKEY framework. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II. Lecture Notes in Computer Science, vol. 8874, pp. 274–

288. Springer (2014). https://doi.org/10.1007/978-3-662-45608-8_15, https://doi.org/10.1007/978-3-662-45608-8_15
25. Jha, A., Khairallah, M., Nandi, M., Saha, A.: Tight security of TNT and beyond - attacks, proofs and possibilities for the cascaded LRW paradigm. In: Joye, M., Leander, G. (eds.) Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 249–279. Springer (2024). https://doi.org/10.1007/978-3-031-58716-0_9, https://doi.org/10.1007/978-3-031-58716-0_9
26. Jha, A., Nandi, M.: Revisiting structure graphs: Applications to cbc-mac and emac. Journal of Mathematical Cryptology **10**(3-4), 157–180 (2016)
27. Jha, A., Nandi, M.: Tight security of cascaded LRW2. J. Cryptol. **33**(3), 1272–1317 (2020). https://doi.org/10.1007/S00145-020-09347-Y, https://doi.org/10.1007/s00145-020-09347-y
28. Kim, S., Lee, B., Lee, J.: Tight security bounds for double-block hash-then-sum macs. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020. pp. 435–465. Springer International Publishing, Cham (2020)
29. Kim, S., Lee, B., Lee, J.: Tight security bounds for double-block hash-then-sum MACs. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12105, pp. 435–465. Springer, Heidelberg, Germany, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45721-1_16
30. Knudsen, L.: Deal-a 128-bit block cipher. complexity **258**(2), 216 (1998)
31. Krovetz, T., Rogaway, P.: The software performance of authenticated-encryption modes. In: Joux, A. (ed.) Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers. Lecture Notes in Computer Science, vol. 6733, pp. 306–327. Springer (2011). https://doi.org/10.1007/978-3-642-21702-9_18, https://doi.org/10.1007/978-3-642-21702-9_18
32. Leurent, G., Nandi, M., Sibleyras, F.: Generic attacks against beyond-birthday-bound macs. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology – CRYPTO 2018. pp. 306–336. Springer International Publishing, Cham (2018)
33. Leurent, G., Nandi, M., Sibleyras, F.: Generic attacks against beyond-birthday-bound MACs. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology – CRYPTO 2018, Part I. Lecture Notes in Computer Science, vol. 10991, pp. 306–336. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2018). https://doi.org/10.1007/978-3-319-96884-1_11
34. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) Advances in Cryptology – CRYPTO 2002. Lecture Notes in Computer Science, vol. 2442, pp. 31–46. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2002). https://doi.org/10.1007/3-540-45708-9_3
35. Luby, M., Rackoff, C.: Pseudo-random permutation generators and cryptographic composition. In: 18th Annual ACM Symposium on Theory of Computing. pp. 356–363. ACM Press, Berkeley, CA, USA (May 28–30, 1986). https://doi.org/10.1145/12130.12167
36. Luykx, A., Preneel, B., Tischhauser, E., Yasuda, K.: A mac mode for lightweight block ciphers. In: Peyrin, T. (ed.) Fast Software Encryption. pp. 43–59. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
37. Luykx, A., Preneel, B., Tischhauser, E., Yasuda, K.: A MAC mode for lightweight block ciphers. In: Peyrin, T. (ed.) Fast Software Encryption – FSE 2016.

Lecture Notes in Computer Science, vol. 9783, pp. 43–59. Springer, Heidelberg, Germany, Bochum, Germany (Mar 20–23, 2016). https://doi.org/10.1007/978-3-662-52993-5_3
38. Mennink, B.: Towards tight security of cascaded LRW2. In: Beimel, A., Dziembowski, S. (eds.) Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11240, pp. 192–222. Springer (2018). https://doi.org/10.1007/978-3-030-03810-6_8, https://doi.org/10.1007/978-3-030-03810-6_8
39. Mennink, B., Neves, S.: Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. In: Advances in Cryptology - CRYPTO 2017. Proceedings, Part III. pp. 556–583 (2017)
40. Mennink, B., Neves, S.: Encrypted Davies-Meyer and its dual: Towards optimal security using mirror theory. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017, Part III. Lecture Notes in Computer Science, vol. 10403, pp. 556–583. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 2017). https://doi.org/10.1007/978-3-319-63697-9_19
41. Nachef, V., Patarin, J., Volte, E.: Feistel ciphers. Cham: Springer International Publishing (2017)
42. Naito, Y.: Blockcipher-based macs: Beyond the birthday bound without message length. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017. pp. 446–470. Springer International Publishing, Cham (2017)
43. Patarin, J.: Pseudorandom permutations based on the des scheme. In: International Symposium on Coding Theory and Applications (held in Europe). pp. 193–204. Springer (1990)
44. Patarin, J.: Etude des Générateurs de Permutations Pseudo-aléatoires Basés sur le Schéma du DES. Ph.D. thesis, Université de Paris (1991)
45. Patarin, J.: Security of random Feistel schemes with 5 or more rounds. In: Franklin, M. (ed.) Advances in Cryptology – CRYPTO 2004. Lecture Notes in Computer Science, vol. 3152, pp. 106–122. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 15–19, 2004). https://doi.org/10.1007/978-3-540-28628-8_7
46. Patarin, J.: The "coefficients H" technique. In: Selected Areas in Cryptography - SAC 2008. Revised Selected Papers. pp. 328–345 (2008)
47. Patarin, J.: Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. IACR Cryptol. ePrint Arch. p. 287 (2010), http://eprint.iacr.org/2010/287
48. Piret, G.: Luby–rackoff revisited: On the use of permutations as inner functions of a feistel scheme. Designs, Codes and Cryptography **39**, 233–245 (2006)
49. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher clefia (extended abstract). In: Biryukov, A. (ed.) Fast Software Encryption. pp. 181–195. Springer Berlin Heidelberg, Berlin, Heidelberg (2007)
50. Taylor, R.: An integrity check value algorithm for stream ciphers. In: Stinson, D.R. (ed.) Advances in Cryptology – CRYPTO'93. Lecture Notes in Computer Science, vol. 773, pp. 40–48. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 22–26, 1994). https://doi.org/10.1007/3-540-48329-2_4
51. Yasuda, K.: The sum of cbc macs is a secure prf. In: Pieprzyk, J. (ed.) Topics in Cryptology - CT-RSA 2010. pp. 366–381. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
52. Yasuda, K.: A new variant of pmac: Beyond the birthday bound. In: Rogaway, P. (ed.) Advances in Cryptology – CRYPTO 2011. pp. 596–609. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)

53. Zhang, L., Wu, W., Sui, H., Wang, P.: 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In: Wang, X., Sako, K. (eds.) Advances in Cryptology – ASIACRYPT 2012. pp. 296–312. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)