IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2023, No. 4, pp. 365–390. DOI:10.46586/tosc.v2023.i4.365-390

Cascading Four Round LRW1 is Beyond Birthday Bound Secure

Nilanjan Datta[1], Shreya Dey[1,2], Avijit Dutta[1] and Sougata Mandal[1,2]

[1] Institute for Advancing Intelligence, TCG CREST, Kolkata, India
[2] Ramakrishna Mission Vivekananda Educational and Research Institute, India
<name>.<surname>@tcgcrest.org

Abstract. In CRYPTO'02, Liskov et al. introduced the concept of a tweakable block cipher, a novel symmetric key primitive with promising applications. They put forth two constructions for designing such tweakable block ciphers from conventional block ciphers: LRW1 and LRW2. While subsequent efforts extended LRW2 to achieve security beyond the birthday bound (e.g., cascaded LRW2 in CRYPTO'12 by Landecker et al.), the extension of LRW1 remained unexplored until Bao et al.'s work in EUROCRYPT'20 that considered cascaded LRW1, a one-round extension of LRW1 - entailing masking the LRW1 output with the given tweak and re-encrypting it with the same block cipher. They showed that CLRW1 offers security up to $2^{2n/3}$ queries. However, this result was challenged by Khairallah's recent birthday bound distinguishing attack on cascaded LRW1, effectively refuting the security claim of Bao et al. Consequently, a pertinent research question emerges: *How many rounds of cascaded LRW1 are required to obtain security beyond the birthday bound?* This paper addresses this question by establishing that cascading LRW1 for four rounds suffices to ensure security beyond the birthday bound. Specifically, we demonstrate that 4 rounds of CLRW1 guarantees security for up to $2^{3n/4}$ queries. Our security analysis is based from recent advancements in the mirror theory technique for tweakable random permutations, operating within the framework of the Expectation Method.

Keywords: Tweakable Block Cipher · Cascaded LRW1 · Beyond Birthday Bound Security · Mirror Theory · Expectation Method

1 Introduction

A block cipher is a family of permutations that is indexed via a secret key. Over time, block ciphers have gained widespread acceptance as a fundamental cryptographic object. However, their applicability is somewhat constrained due to the specific utilization of block ciphers within various modes of operation. Consequently, the adaptability of the cipher itself is limited. To address this limitation, a significant number of applications that involve block ciphers are either implicitly or explicitly designed from a tweakable block cipher. The tweakable block cipher, as an additional fundamental cryptographic building block, serves to introduce variability within the cipher's structure. It is defined as a family of permutations $\widetilde{\mathsf{E}} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$, indexed by secret key $k \in \mathcal{K}$ and public tweak $t \in \mathcal{T}$. The concept of tweakable block ciphers was formally introduced by Liskov, Rivest, and Wagner [LRW02]. Tweakable block ciphers have found diverse applications, notably in designing of authenticated encryption schemes like OCB [RBB03], AEZ [HKR15], Deoxys [JNPS21]. They have also been instrumental in crafting disk encryption systems such as XTS [Mar10], as well as multiple message authentication codes including ZMAC [IMPS17], tweakable block cipher based PMAC_Plus [Yas11], etc. More recently, the emergence of authenticated encryption schemes in the CAESAR competition [CAE14] and the NIST

Licensed under Creative Commons License CC-BY 4.0.
Received: 2023-09-01 Accepted: 2023-11-01 Published: 2023-12-08

lightweight cryptography competition [NIS18] has significantly propelled the usage of tweakable block ciphers in the design of various cryptographic algorithms.

Tweakable block ciphers are constructed through two different ways: the *modular approach* and the *dedicated approach*. In the modular approach, tweakable block ciphers are built from classical block ciphers via various modular constructions. The security of the resulting tweakable block cipher is established from the security of the underlying block ciphers [LRW02, Men15, JLM+17, LL18, WGZ+16]. Conversely, the dedicated approach involves the direct design of tweakable block ciphers using heuristic algorithms. The security assurances for these tweakable block ciphers stem from thorough cryptanalysis [JNP14, JNPS21, BJK+16, CDJ+21].

1.1 Designing Tweakable Block Ciphers Using Modular Approach

Tweakable block ciphers can be designed from classical block ciphers in a black-box fashion. Nonetheless, this modular design approach can be further divided into two distinctive categories: (a) In the first approach, tweakable block ciphers are designed from classical block ciphers by assuming that the underlying block ciphers are *pseudorandom permutations*. This design strategy was introduced by Liskov et al. [LRW02]. (b) The second approach, as proposed by Mennink [Men15], involves designing tweakable block ciphers from classical block ciphers while assuming that the underlying block ciphers function as *ideal ciphers*. These two design methodologies not only differ in their security assumptions but also in their design principles. For instance, pseudorandom permutation-based constructions do not employ the tweak-dependent rekeying technique. This reduces the computational overhead of the cipher but introduces a hybrid security loss in their security bounds. Conversely, such a trade-off is absent in ideal cipher-based constructions. This particular phenomenon is utilized by numerous designs to attain good security bounds and efficiency simultaneously. In fact, tweakable block cipher constructions based on ideal ciphers achieve security beyond n-bits using only 1 or 2 block cipher calls [JLM+17, LL18, WGZ+16].

In this work, our objective is to study tweakable block cipher constructions based on the pseudorandomness assumption of the underlying block cipher. In this regard, we delve into the original constructions proposed by Liskov et al. [LRW02], subsequently renamed to $\mathsf{LRW1}$ and $\mathsf{LRW2}$ by Landecker et al. [LST12]. The first proposed construction, $\mathsf{LRW1}$ transforms a block cipher into a tweakable block cipher by masking the encryption output of the input message with the given tweak which is again re-encrypted to produce the ciphertext, i.e., for a given block cipher E with key space $\{0,1\}^n$ and message space $\{0,1\}^n$, $\mathsf{LRW1}$ construction is defined as follows:

$$\mathsf{LRW1}[\mathsf{E}]_K(T, M) \overset{\Delta}{=} \mathsf{E}_K(\mathsf{E}_K(M) \oplus T),$$

where $T \in \{0,1\}^n$ is the tweak and $M \in \{0,1\}^n$ is the input message. It has been proved that $\mathsf{LRW1}$ achieves a tight CPA security upto $2^{n/2}$ queries [LRW02]. Moreover, it requires two block cipher calls to process an n-bit message and n-bit tweak. To achieve CCA security, Liskov et al. [LRW02] have proposed the second construction based on block cipher E and an almost-xor universal keyed hash function H, called $\mathsf{LRW2}$. It transforms a block cipher into a tweakable block cipher by masking the input and output of the given block cipher with hash of the given tweak, i.e., for a given block cipher E with key space $\{0,1\}^n$ and message space $\{0,1\}^n$, and for a given almost-xor-universal keyed hash function H, $\mathsf{LRW2}$ construction is defined as follows:

$$\mathsf{LRW2}_{K,K'}[\mathsf{E}, H](T, M) \overset{\Delta}{=} \mathsf{E}_K(M \oplus H_{K'}(T)) \oplus H_{K'}(T).$$

The authors of [LRW02] have proved that $\mathsf{LRW2}$ achieves a tight CCA security up to $2^{n/2}$ queries. However, in contrast to $\mathsf{LRW1}$, $\mathsf{LRW2}$ demands only a single invocation of the

Table 1: Comparison Table for $\mathsf{LRW2}$ based Tweakable Block Ciphers. # BC refers to the number of block cipher invocations. # Hash refers to the number of hash function evaluations. Tweak length for $\mathsf{LRW2}$ based constructions are arbitrary. Security bounds are expressed in terms of number of bits. † denotes the corresponding bound is tight.

Constructions	# BC	# keys	# Hash	CPA Sec.	CCA Sec.
$\mathsf{LRW2}$	1	2	1	$n/2$ [LRW02]	† $n/2$ [LRW02]
$\mathsf{CLRW2}$	2	2	2	$3n/4$ [JN20]	† $3n/4$ [JN20]
$\mathsf{CLRW2}^r$ (r: odd)	r	r	r	$\frac{(r-1)n}{r+1}$ [LS13]	$\frac{(r-1)n}{r+1}$ [LS13]
$\mathsf{CLRW2}^r$ (r: even)	r	r	r	$\frac{rn}{r+2}$ [LS13]	$\frac{rn}{r+2}$ [LS13]

block cipher and an evaluation of a hash function to process an n-bit message along with a tweak of variable length. $\mathsf{LRW2}$ has later been extended by Landecker et al. to provide beyond birthday bound security. In particular, Landecker et al. [LST12] have shown two-round cascading of $\mathsf{LRW2}$, called $\mathsf{CLRW2}$, achieves $2n/3$-bit CCA security, which was later improved to a tight $3n/4$-bit security bound [Men18, JN20]. In [LS13], Lampe and Seurin have shown that r-round cascading of $\mathsf{LRW2}$ achieves CCA security upto $2^{rn/r+2}$ adversarial queries. Although a number of works have been conducted on the security analysis of cascading the $\mathsf{LRW2}$ construction, no extension of the $\mathsf{LRW1}$ construction had been made until the work of Bao et al. [BGGS20]. We present the existing and updated security bounds of various $\mathsf{LRW2}$ based tweakable block cipher constructions in Table 1. In the next subsection, we discuss all the recent results on the security of Cascading $\mathsf{LRW1}$.

1.2 Recent Developments on the Security of Cascading LRW1

In Eurocrypt'20, Bao et al. [BGGS20] considered the 3-round cascading of the $\mathsf{LRW1}$ construction $\mathsf{CLRW1}^3$ (also known as TNT as an abbreviation of *"The Tweak-aNd-Tweak"*) and showed that the construction achieves security beyond the birthday bound. $\mathsf{CLRW1}^3$ is the extension of the basic $\mathsf{LRW1}$ construction by masking its output with the given tweak and then it is re-encrypted with an independent keyed block cipher to produce the ciphertext, i.e., for a given block cipher family $\mathsf{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$, indexed by κ-bit secret key, the construction $\mathsf{CLRW1}^3$ gives a family of tweakable block cipher $\mathsf{CLRW1}^3[\mathsf{E}](T, M) : \{0,1\}^{3\kappa} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, indexed by a 3κ-bit secret key and an n-bit public tweak as follows:

$$\mathsf{CLRW1}^3_{K_1,K_2,K_3}[\mathsf{E}](T, M) \triangleq \mathsf{E}_{K_3}(T \oplus \underbrace{\mathsf{E}_{K_2}(T \oplus \mathsf{E}_{K_1}(M))}_{\mathsf{LRW1}_{K_1,K_2}}).$$

The authors have proved that $\mathsf{CLRW1}^3$ achieves security up to $2^{2n/3}$ chosen-plaintext and chosen-ciphertext queries. Later in [GGLS20], Guo et al. have shown that the $\mathsf{CLRW1}^3$ construction based on three independent random permutation achieves a tight $3n/4$-bit security bound against all possible information theoretic CPA adversaries.

In [ZQG22], Zhang et al. have studied the security analysis of the r-round cascading of the basic $\mathsf{LRW1}$ construction, called $\mathsf{CLRW1}^r$, which is defined as follows:

$$\mathsf{CLRW1}^r_{K_1,K_2,\ldots,K_r}[\mathsf{E}](T, M) \triangleq \mathsf{E}_{K_r}(T \oplus \underbrace{\mathsf{E}_{K_{r-1}}(T \oplus \cdots (T \oplus \mathsf{E}_{K_2}(T \oplus \mathsf{E}_{K_1}(M))))}_{\mathsf{CLRW1}^{r-1}_{K_1,K_2,\ldots,K_{r-1}}}).$$

The authors have incorporated the coupling technique to show that $\mathsf{CLRW1}^r$ achieves

CCA security up to $2^{(r-2)n/r}$ queries, with $r \geq 2$. Furthermore, when r is odd, the construction attains enhanced security for up to $2^{(r-1)n/(r+1)}$ queries.

In a recent work, Khairallah [Kha23] successfully presented a birthday bound CCA distinguishing attack on the $\mathsf{CLRW1}^3$ construction. As a result, the previously asserted security claim of Bao et al. [BGGS20] has been rendered invalid. As things currently stand, $\mathsf{CLRW1}^3$ achieves a tight CCA security up to $2^{n/2}$ queries, owing to the result by Zhang et al. [ZQG22]. In a very recent work, Jha et al. [JNS23] have presented an alternative tight birthday bound security proof for the construction using the standard H-Coefficient technique. This method effectively eliminates the unnecessary constant factors that arise due to the general coupling-based security analysis on $\mathsf{CLRW1}^r$.

This recent advancement in the security of cascaded LRW1 constructions paves the way to explore the optimal number of rounds required to achieve CCA security beyond the birthday bound. It's worth mentioning that, leveraging the insights of Zhang et al. [ZQG22], it's already established that a 5-round cascaded LRW1 achieves a beyond birthday bound security against chosen-ciphertext adversaries; this is accomplished with the round number r set to 5, which results in CCA security for up to $2^{2n/3}$ queries. Conversely, for $r = 4$, as indicated by Zhang et al.'s established bound, a 4-round cascaded LRW1 provides CCA security up to $2^{n/2}$ queries. It's important to note, however, that this security bound established by Zhang et al. is not tight, as no matching attack against this construction has been reported. This brings us to an intriguing and unresolved question: Can a birthday bound CCA attack be found against the 4-round cascaded LRW1 construction, or does it indeed achieve security beyond the birthday bound? Answering this question would potentially solve the following related open problem:

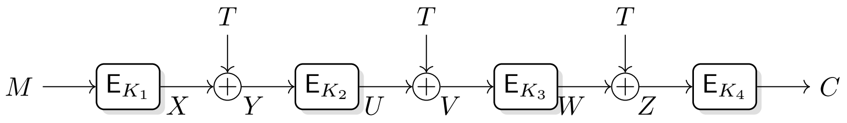
How many rounds are required for CLRW1 *to achieve BBB security against all adaptive CCA adversaries?*

1.3 Our Contribution

In this paper, we answer the above question affirmatively and show that 4 rounds for cascading LRW1 are sufficient to cross the birthday bound barrier. We define the 4-round cascading LRW1 construction, dubbed as $\mathsf{CLRW1}^4$, as follows:

$$\mathsf{CLRW1}^4_{K_1,K_2,K_3,K_4}[\mathsf{E}](T,M) \triangleq \mathsf{E}_{K_4}(T \oplus \underbrace{\mathsf{E}_{K_3}(T \oplus \mathsf{E}_{K_2}(T \oplus \mathsf{E}_{K_1}(M)))}_{\mathsf{CLRW1}^3_{K_1,K_2,K_3}[\mathsf{E}]}).$$

Note that, an equivalent way of visualizing the $\mathsf{CLRW1}^4$ construction is the encryption of the masked $\mathsf{CLRW1}^3$ construction, where the tweak is used as the mask. The construction is depicted below.



In this paper, we have shown that the construction $\mathsf{CLRW1}^4$ provides security up to $2^{3n/4}$ queries. In particular, we have the following security result, the proof of which is deferred until Sect. 3.

Theorem 1. *Let* $\mathsf{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ *be a block cipher. Then, for any* (q,t) *adversary* A[1] *against the strong tweakable pseudorandom permutation security of* $\mathsf{CLRW1}^4[\mathsf{E}]$

[1] A (q,t) adversary A is one that makes a total of q queries to the oracle with running time of at most t steps.

with $q \leq 2^{2n/3}$, there exists a (q, t') adversary A' against the strong pseudorandom permutation security of E, where $t' = t$, such that

$$\mathbf{Adv}^{\text{tsprp}}_{\mathsf{CLRW1}^4[\mathsf{E}]}(\mathsf{A}) \leq 4\mathbf{Adv}^{\text{sprp}}_{\mathsf{E}}(\mathsf{A}') + \frac{6q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n} + \frac{33q^4}{2^{3n}}.$$

To the best of our knowledge, this is the first work that confirms that 4 rounds are sufficient for cascaded LRW1 to obtain security beyond the birthday bound against CCA adversaries. We tabulate all the existing and updated security results on LRW1 based constructions in Table 2.

Remarks: Concurrent to this work, Jha et al. [JKNS23] have independently studied the security bound of 4-round cascaded LRW1 and have also shown that it achieves $3n/4$-bit CCA security bound.

1.4 Proof Approach

The security analysis of our construction is rooted in the recent advancements of the mirror theory technique for tweakable random permutation framework, coupled with the Expectation Method [HT16] framework. In the distinguishing game, we reveal the intermediate variables $(X_i, Y_i, U_i, V_i, W_i, Z_i)$, for $i \in [q]$, to the adversary after it makes q queries to the oracle and received the corresponding responses. In particular, in the real world, the oracle reveals the actual intermediate variables, while in the ideal world, these intermediate variables are sampled in a manner that maintains permutation compatibility. After revealing all the intermediate variables, the adversary obtains a complete query-response transcript. Based on the sampling of the intermediate random variables, we obtain a number of unfavorable conditions, defined as *bad events* (refer to Sect. 3.1). A transcript satisfying any one of these bad events is referred as a *bad transcript.* We have shown that the probability of obtaining a bad transcript in the ideal world is upper bounded by $q^4/2^{3n}$. For *good transcripts*, we lower bound the real interpolation probability and upper bound the ideal interpolation probability. To lower bound the former, we counted the number of times each permutation is invoked. Meanwhile, in determining the ideal interpolation probability, we leverage the mirror theory results for the tweakable permutation environment. Finally, the distinguishing advantage of the construction is obtained by applying the result of the Expectation Method [HT16].

2 Preliminaries

NOTATIONS: For $q \in \mathbb{N}$, we write $[q]$ to denote the set $\{1, \ldots, q\}$. For two natural numbers a and b such that $a \leq b$, we write $[a, b]$ to denote the set $\{a, a+1, \ldots, b\}$. For a natural number n, $\{0,1\}^n$ denotes the set of all binary strings of length n and $\{0,1\}^*$ denotes the set of all binary strings of arbitrary length. For $x, y \in \{0,1\}^n$, we write $z = x \oplus y$ to denote xor of x and y. For two strings x, y, we write $x \| y$ to denote the concatenation of x followed by y. Often we write $(x, y) \in \{0,1\}^{2n}$ to denote the $2n$-bit string $x \| y$. For a natural number n and q, we write x^q to denote a q-tuple $(x_1, x_2, \ldots, x_q)$ where each $x_i \in \{0,1\}^n$. We write $\widehat{x}^q$ to denote the set $\{x_i : i \in [q]\}$. By an abuse of notation, we also write x^q to denote the multiset $\{x_i : i \in [q]\}$ and $\mu(x^q, x)$ denotes the multiplicity of $x \in x^q$. We also write μ_x to denote the multiplicity of $x \in x^q$, when the multiset x^q is understood from the context. For a set $\mathcal{I} \subseteq [q]$ and a q-tuple x^q, we write $x^{\mathcal{I}}$ to denote the sub-tuple $(x_i)_{i \in \mathcal{I}}$. We write a 2-ary tuple (x^q, y^q) to denote the q tuple $((x_1, y_1), (x_2, y_2), \ldots, (x_q, y_q))$, where each $x_i, y_i \in \{0,1\}^n$. We write $x \leftarrow y$ to denote the assignment of the variable y into x. For a random variable X, $\mathsf{X} \leftarrow\!\!\$ \{0,1\}^n$ denotes that X is sampled uniformly at random from $\{0,1\}^n$. We use bold letter to denote random variable and small letter to denote a particular element. For a tuple of random variables

Table 2: Comparison table for all LRW1 based tweakable block ciphers. # BC refers to the number of block cipher invocations. Security bounds of the constructions are expressed in terms of the number of bits. † denotes the corresponding security bound is tight.

Constructions	# BC	CPA Sec.	CCA Sec.
LRW1	2	(†) $n/2$ (CPA) [LRW02]	$\times$
CLRW1^3	3	(†) $3n/4$ (CPA) [GGLS20]	(†) $n/2$ (CCA) [JNS23]
CLRW1^r (r: odd)	r	$\frac{(r-1)n}{r+1}$ (CPA) [ZQG22]	$\frac{(r-1)n}{r+1}$ (CCA) [ZQG22]
CLRW1^r (r: even)	r	$\frac{(r-2)n}{r}$ (CPA) [ZQG22]	$\frac{(r-2)n}{r}$ (CCA) [ZQG22]
CLRW1^4	4	$3n/4$ (CPA) [This Paper]	$3n/4$ (CCA) [This Paper]

$(X_1,\ldots,X_q)$, we write $(X_1,\ldots,X_q) \leftarrow\!\!\$ \ \{0,1\}^n$ to denote that each X_i is sampled uniformly from $\{0,1\}^n$ and independent to all other previously sampled random variables. Similarly, we write $(X_1,\ldots,X_q) \xleftarrow{\text{wor}} \{0,1\}^n$ to denote that each X_i is sampled uniformly from $\{0,1\}^n \setminus \{X_1,\ldots,X_{i-1}\}$. The set of all permutations over $\mathcal{X}$ is denoted as $\mathsf{Perm}(\mathcal{X})$. When $\mathcal{X} = \{0,1\}^n$, then we omit $\mathcal{X}$ and simply write $\mathsf{Perm}(n)$ to denote the set of all permutations over $\{0,1\}^n$. We say that an n-bit permutation $\mathsf{P} \in \mathsf{Perm}$ maps a q-tuple $x^q = (x_1,x_2,\ldots,x_q)$ to $y^q = (y_1,y_2,\ldots,y_q)$, denote it as $x^q \overset{\mathsf{P}}{\mapsto} y^q$, if for all $i \in [q]$, we have $\mathsf{P}(x_i) = y_i$, where each $x_i, y_i \in \{0,1\}^n$. We say that a 2-ary tuple (x^q, y^q) is *permutation compatible*, denoted as $x^q \leftrightsquigarrow y^q$, if there exists at least one permutation $\mathsf{P} \in \mathsf{Perm}$ such that $x^q \overset{\mathsf{P}}{\mapsto} y^q$. In other words, $x^q \leftrightsquigarrow y^q$ if for all $i \in [q]$, $x_i = x_j \Leftrightarrow y_i = y_j, i \neq j \in [q]$. Moreover, if (x^q, y^q) is not permutation compatible, then we denote it as $x^q \overset{\times}{\leftrightsquigarrow} y^q$. For three tuples $x^q = (x_1,x_2,\ldots,x_q)$, $y^q = (y_1,y_2,\ldots,y_q)$, and $\lambda^q = (\lambda_1,\lambda_2,\ldots,\lambda_q)$ of q n-bit elements, we write $x^q \oplus y^q = \lambda^q$, if for all $i \in [q]$, it holds that $x_i \oplus y_i = \lambda_i$. For integers $1 \leq b \leq a$, we write $(a)_b$ to denote $a(a-1)\ldots(a-b+1)$, where $(a)_0 = 1$ by convention.

2.1 Block Cipher

Let $n, \kappa \in \mathbb{N}$ be two natural numbers. A block cipher $\mathsf{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ is a function that takes as input a key $K \in \{0,1\}^\kappa$ and an n-bit string $x \in \{0,1\}^n$ and outputs an element $y \in \{0,1\}^n$ such that for each $k \in \{0,1\}^\kappa$, the function E_k is bijective from $\{0,1\}^n$ to $\{0,1\}^n$. Due to the bijectivity of the function E_k, its inverse function E_k^{-1} exists. We fix positive even integers n and κ to denote the *block size* and the *key size* of the block cipher respectively in terms of number of bits.

2.2 Tweakable Block Cipher

Let $n, \kappa, t \in \mathbb{N}$ be three natural numbers. A *tweakable block cipher* (TBC) is a mapping $\widetilde{\mathsf{E}} : \{0,1\}^\kappa \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$, where $\{0,1\}^\kappa$ is called the key space and $\{0,1\}^t$ is called the tweak space, such that for all key $k \in \{0,1\}^\kappa$ and for all tweak $T \in \{0,1\}^t$, $\widetilde{\mathsf{E}}_k^T$ is a permutation over $\{0,1\}^n$. We denote $\mathsf{TBC}(\{0,1\}^\kappa, \{0,1\}^t, \{0,1\}^n)$, the set of all tweakable block ciphers with key space $\{0,1\}^\kappa$, tweak space $\{0,1\}^t$ and message space $\{0,1\}^n$. A *tweakable permutation* with tweak space $\{0,1\}^t$ and domain $\{0,1\}^n$ is a mapping $\widetilde{\mathsf{P}} : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ such that for all tweak $T \in \{0,1\}^t$, $\widetilde{\mathsf{P}}^T$ is a permutation over $\{0,1\}^n$. We write $\mathsf{TP}(\{0,1\}^t, n)$ to denote the set of all tweakable permutations with tweak space $\{0,1\}^t$ and n-bit messages. We say a pair of q-tuples (M^q, T^q) is *tweakable permutation compatible* with another pair of q-tuples (C^q, T^q), if there exists a tweakable permutation $\widetilde{\mathsf{P}} \in \mathsf{TP}(\{0,1\}^t, n)$ such that for each $i \in [q]$, $\widetilde{\mathsf{P}}^T(M_i) = C_i$.

2.3 Security Definitions

A distinguisher A is an algorithm that tries to distinguish between two oracles $\mathcal{O}_1$ and $\mathcal{O}_0$ via black box interaction with one of them. At the end of interaction it returns a bit $b \in \{0,1\}$. We write $\mathsf{A}^{\mathcal{O}} = b$ to denote the output of A at the end of its interaction with $\mathcal{O}$. The distinguishing advantage of A against $\mathcal{O}_1$ and $\mathcal{O}_0$ is defined as

$$\Delta_{\mathsf{A}}[\mathcal{O}_1; \mathcal{O}_0] = \left|\mathsf{Pr}[\mathsf{A}^{\mathcal{O}_1} = 1] - \mathsf{Pr}[\mathsf{A}^{\mathcal{O}_0} = 1]\right|, \tag{1}$$

where the probabilities depend on the random coins of $\mathcal{O}_1$ and $\mathcal{O}_0$ and the random coins of the distinguisher A. The time complexity of the adversary is defined over the usual RAM model of computations.

I. Security Definition of Block Cipher. We capture the security notion of a block cipher E with key size κ and block size n in terms of indistinguishability advantage from an uniform random permutation. More formally, we define the pseudorandom permutation (prp) advantage of E with respect to a distinguisher A as follows:

$$\mathbf{Adv}^{\mathrm{prp}}_{\mathsf{E}}(\mathsf{A}) \overset{\Delta}{=} \Delta_{\mathsf{A}}[\mathsf{E}_K; \mathsf{P}] = \left|\mathsf{Pr}[\mathsf{A}^{\mathsf{E}_K} = 1] - \mathsf{Pr}[\mathsf{A}^{\mathsf{P}} = 1]\right|,$$

where the first probability is calculated over the randomness of $K \leftarrow\!\!\$ \ \{0,1\}^{\kappa}$ and the second probability is calculated over the randomness of $\mathsf{P} \leftarrow\!\!\$ \ \mathsf{Perm}(n)$. We say that E is $(q, \mathtt{t}, \epsilon)$ secure if the maximum pesudorandom permutation advantage of E is ϵ where the maximum is taken over all distinguishers A that makes q queries to its oracle and runs for time at most $\mathtt{t}$.

II. Security Definition of Tweakable Block Cipher. An adversary A for tweakable block cipher has access to the oracle in either of the two world: in the real world, it has access to the oracle $(\widetilde{\mathsf{E}}_k(\cdot,\cdot))$ for some fixed key $k \in \{0,1\}^{\kappa}$. In the ideal world, it has access to the oracle $(\widetilde{\mathsf{P}}(\cdot,\cdot))$ oracles for some $\widetilde{\mathsf{P}} \in \mathsf{TP}(\{0,1\}^t, n)$. Adversary A queries to the oracle in an adaptive way and after the interaction is over, it outputs a single bit b. We assume that A does not repeat any query to the oracle. We call such an adversary A, a *non-trivial* $(q, \mathtt{t})$ adaptive adversary, where A makes total q many queries with running time at most $\mathtt{t}$.

Let $\widetilde{\mathsf{E}} \in \mathsf{TBC}(\{0,1\}^{\kappa}, \{0,1\}^t, \{0,1\}^n)$ be a tweakable block cipher and A be a non-trivial $(q, \mathtt{t})$ adaptive adversary with oracle access to a tweakable permutation and its inverse with tweak space $\{0,1\}^t$ and domain $\{0,1\}^n$. The advantage of A in breaking the strong tweakable pseudorandom permutation (*STPRP*) security of $\widetilde{\mathsf{E}}$ is defined as

$$\mathbf{Adv}^{\mathrm{STPRP}}_{\widetilde{\mathsf{E}}}(\mathsf{A}) \overset{\Delta}{=} |\Pr[\mathsf{A}^{\widetilde{\mathsf{E}}_K, \widetilde{\mathsf{E}}_K^{-1}} = 1] - \Pr[\mathsf{A}^{\widetilde{\mathsf{P}}, \widetilde{\mathsf{P}}^{-1}} = 1]|, \tag{2}$$

where the first probability is calculated over the randomness of $K \leftarrow\!\!\$ \ \{0,1\}^{\kappa}$ and the second probability is calculated over the randomness of $\widetilde{\mathsf{P}} \leftarrow\!\!\$ \ \mathsf{TP}(\{0,1\}^t, n)$. When the adversary is given access only to the tweakable permutation and not its inverse, then we say the tweakable pseudorandom permutation *(TPRP)* advantage of A against $\widetilde{\mathsf{E}}$. We say that $\widetilde{\mathsf{E}}$ is $(q, \mathtt{t}, \epsilon)$ secure if the maximum strong tweakable pesudorandom permutation advantage of $\widetilde{\mathsf{E}}$ is ϵ where the maximum is taken over all distinguishers A that makes a total of q queries to its oracle and runs for time at most $\mathtt{t}$. We assume throughout the paper the tweak size t of the tweakable block cipher is equal to its block size n.

2.4 Expectation Method

The Expectation Method was introduced by Hoang and Tessaro [HT16] to derive a tight multi-user security bound of the key-alternating cipher. Subsequently, this technique has been used for bounding the distinguishing advantage of various cryptographic constructions [HT17, BHT18, DNT19]. The Expectation Method is a generalization of the H-Coefficient technique developed by Patarin [Pat08], which serves as a "systematic" tool to upper bound the distinguishing advantage of any deterministic and computationally unbounded distinguisher A in distinguishing the real oracle $\mathcal{O}_1$ (construction of interest) from the ideal oracle $\mathcal{O}_0$ (idealized version). The collection of all the queries and responses that A made and received to and from the oracle, is called the *transcript* of A, denoted as τ. Sometimes, we allow the oracle to release more internal information to A only after A completes all its queries and responses, but before it outputs its decision bit. Note that, revealing extra informations will only increase the advantage of the distinguisher.

Let $\mathsf{X}_{\rm re}$ and $\mathsf{X}_{\rm id}$ denote the transcript random variable induced by the interaction of A with the real oracle and the ideal oracle respectively. The probability of realizing a transcript τ in the ideal oracle (i.e., $\mathsf{Pr}[\mathsf{X}_{\rm id} = \tau]$) is called the *ideal interpolation probability.* Similarly, one can define the *real interpolation probability.* A transcript τ is said to be *attainable* with respect to A if the ideal interpolation probability is non-zero (i.e., $\mathsf{Pr}[\mathsf{X}_{\rm id} = \tau] > 0$). We denote the set of all attainable transcripts by Ω. Following these notations, we state the main result of the Expectation Method in Theorem 2. The proof of this theorem can be found in [HT16].

Theorem 2. *Let $\Omega = \Omega_{\mathsf{good}} \sqcup \Omega_{\mathsf{bad}}$ be a partition of the set of attainable transcripts. Let $\Phi : \Omega \to [0, \infty)$ be a non-negative real valued function. For any attainable good transcript $\tau \in \Omega_{\mathsf{good}}$, assume that*

$$\frac{\mathsf{Pr}[\mathsf{X}_{\rm re} = \tau]}{\mathsf{Pr}[\mathsf{X}_{\rm id} = \tau]} \geq 1 - \Phi(\tau),$$

and there exists $\epsilon_{\rm bad} \geq 0$ such that $\mathsf{Pr}[\mathsf{X}_{\rm id} \in \Omega_{\mathsf{bad}}] \leq \epsilon_{\rm bad}$. Then,

$$\Delta_{\mathsf{A}}[\mathcal{O}_1; \mathcal{O}_0] \leq \mathbf{E}[\Phi(\mathsf{X}_{\rm id})] + \epsilon_{\rm bad}. \tag{3}$$

2.5 Mirror Theory For Tweakable Random Permutations

The Mirror theory, as introduced by Patarin [Pat17], is a combinatorial technique to estimate the number of solutions of a linear systems of equalities and linear non equalities in finite groups. Let there exists a set of linear equation $\mathcal{L}$ of the form

$$\mathcal{L} = \{X_1 \oplus Y_1 = \lambda_1, X_2 \oplus Y_2 = \lambda_2, \ldots, X_q \oplus Y_q = \lambda_q\},$$

where X^q and Y^q are unknowns and $\lambda^q \in (\{0,1\}^n)^q$ are knowns. However, there are equalities and non-equalities restriction on X^q and Y^q which uniquely determines the distinct set of variables in the given system of equations $\mathcal{L}$, which is denoted as $\widetilde{X}^q$ and $\widetilde{Y}^q$ respectively. Without loss of generality, we assume that $[q_X]$ and $[q_Y]$ are two index sets which are used to index the elements of $\widetilde{X}^q$ and $\widetilde{Y}^q$ respectively. Given such an ordering, we view the two sets $\widetilde{X}^q$ and $\widetilde{Y}^q$ as ordered sets $\widetilde{X}^q = \{X'_1, X'_2, \ldots, X'_{q_X}\}$ and $\widetilde{Y}^q = \{Y'_1, Y'_2, \ldots, Y'_{q_Y}\}$ respectively. Now, we define two surjective index mappings: $\phi_X : [q] \to [q_X]$ such that $i \mapsto j$ if and only if $X_i = X'_j$. Similarly, $\phi_Y : [q] \to [q_Y]$ such that $i \mapsto j$ if and only if $Y_i = Y'_j$. Therefore, $\mathcal{L}$ is uniquely determined by the triplet $(\phi_X, \phi_Y, \lambda^q)$.

Given such a system of linear equations $\mathcal{L} = (\phi_X, \phi_Y, \lambda^q)$, we associate an edge-labeled bipartite graph, called *equation-graph*, denoted as $\mathcal{L}(G) = ([q_X] \cup [q_Y], \mathcal{E}, L)$, where $\mathcal{E} = \{(\phi_X(i), \phi_Y(i)) : i \in [q]\}$ and L is an edge labeling function defined as $L((\phi_X(i), \phi_Y(i))) = \lambda_i$, i.e., each labeled edge of the graph corresponds to an unique equation in $\mathcal{L}$.

Now, we list out three properties of an equation graph as follows: (a) **cycle-freeness:** which asserts that $\mathcal{L}$ is cycle-free if and only if $\mathcal{L}(G)$ is acylic. (b) $\xi_{\max}$ **component:**

which gives an upper bound on the maximum size of a component of $\mathcal{L}(G)$ and finally (c) **non-degeneracy:** which says that the there does not exist any even length path of length at least 2 in $\mathcal{L}(G)$ such that the sum of the labels of its edges become zero. Under these three conditions, the fundamental theorem of mirror theory [CDN+23, NPV17] states that

> the number of solutions $(x_1, x_2, \dots, x_{q_X}, y_1, y_2, \dots, y_{q_Y})$ to the given system of linear equations $\mathcal{L}$ such that the corresponding equation graph $\mathcal{L}(G)$ satisfies (a) **cycle-freeness**, (b) $\xi_{\max}$ **component** and (c) **non-degeneracy** condition, denoted as $h(q)$, is at least
> $$h(q) \geq \frac{(2^n)_{q_X}(2^n)_{q_Y}}{2^{nq}}.$$

For $\xi \geq 2$ and $\epsilon \geq 0$, we write (ξ, ϵ)-restricted mirror theory to denote the mirror theory result in which the number of solutions, h_q for a system of equations with $\xi_{\max} = \xi$, satisfies

$$h(q) \geq \frac{(2^n)_{q_X}(2^n)_{q_Y}}{2^{nq}}\left(1 - \epsilon\right). \tag{4}$$

Note that the fundamental theorem of mirror theory is basically $(\xi, 0)$-restricted mirror theory. Over the past several years, a number of studies [Luc00, DDNY18, DNT19, KLL20] have shown only a loose lower bound with a non-zero error term ϵ. For example, [Pat10a, DNT19, DDNY18] used the $(3, q^3/2^{2n})$-restricted mirror theory. In [KLL20, DDD21, DDNT23], authors have used the $(\xi, q^4/2^{3n})$-restricted mirror theory, for $\xi \leq 2^n/2q$. Mennink [Men18] have used the $(4, 3q/2^n)$-restricted mirror theory. Recently, Cogliati et al. [CDN+23] have proved the $(\xi, 0)$-restricted mirror theory result as long as $q \leq 2^n/12\xi_{\max}^2$.

The Mirror theory fundamentally works for bounding the pseudorandomness of sum of permutations [Pat10b, BI99, HWKS98, DHT17] with respect to a random function. However, the traditional setup of the mirror theory is not suited for bounding the pseudorandomness of tweakable block ciphers with respect to tweakable random permutation. This is because, ideally, in sum of permutation based constructions, coupled with the H-Coefficient technique, the real interpolation probability is

$$\frac{h(q)}{(2^n)_{q_X}(2^n)_{q_Y}} \overset{(1)}{\geq} \left(1 - \epsilon\right),$$

where inequality (1) follows from Eqn. (4). Moreover, the ideal interpolation probability is 2^{-nq}. Therefore, by canceling out the term 2^{nq} from the ratio of the real to ideal interpolation probability, we obtain the lower bound of the ratio for a good transcript as $(1 - \epsilon)$. However, it does not hold true when the ideal world is a *tweakable random permutation* because, in that case the ideal intepolation probability becomes

$$\Pr[\mathsf{X}_{\text{id}} = \tau] = \prod_{T \in T^q} \frac{1}{(2^n)_{\mu_T}},$$

where $\mu_T := |\{i \in [q] : T_i = T\}|$. Hence, in this case, the ratio of real to ideal interpolation probability becomes

$$\frac{\prod_{T \in T^q} (2^n)_{\mu_T}}{2^{nq}}\left(1 - \epsilon\right).$$

Notice that, when μ_T reaches q, the ratio becomes $(1 - q^2/2^n)$, a bound detrimental for constructions achieving beyond birthday bound security.

To get rid of this bottleneck, Mennink [Men18] used the idea of limiting the maximum number of tweak repetitions upto $2^{n/4}$ times, which was in turn used in the context of proving $3n/4$-bit security of cascaded LRW2 construction. Later, Jha and Nandi [JN20] developed a variant of mirror theory result that is suited for tweakable block cipher based constructions when the ideal world is tweakable random permutation. In fact, unlike [Men18], their result [JN20] is not dependent on the maximum number of repetitions of tweak.

General Set Up: For a given system of linear equations $\mathcal{L}$, we associate an edge-labeled bipartite graph $\mathcal{L}(G) = (\mathcal{X} \cup \mathcal{Y}, \mathcal{E})$ with the labeling function L, an edge (x, y) with label λ is called an *isolated-edge* if the degree of both x and y is 1. We say that a component $\mathcal{C}$ is a *star* if $\xi_{\mathcal{C}} \geq 3$, where $\xi_{\mathcal{C}}$ denotes the number of vertices in component $\mathcal{C}$, and there exists an unique vertex, called *center vertex*, with degree $\xi_{\mathcal{C}} - 1$ and all the other vertices have degree exactly 1. A component $\mathcal{C}$ is called $\mathcal{X}$-type (resp. $\mathcal{Y}$-type) if the center vertex of the component $\mathcal{C}$ lies in $\mathcal{X}$ (resp. $\mathcal{Y}$).

For a given system of linear equations $\mathcal{L}$ and its corresponding associated equation graph $\mathcal{L}(G)$, we write α (resp. β, γ) to denote the number of isolated edges (resp. number of components of $\mathcal{X}$-type and number of components of $\mathcal{Y}$-type). Similarly, q_1 denotes the number of equations such that none of its variables have collided with any other variables. q_2 denotes the number of equations of $\mathcal{X}$-type and q_3 denotes the number of equations of $\mathcal{Y}$-type. Note that $\alpha = q_1$. Jha and Nandi [JN20] have given a lower bound on the number of solutions for a given system of linear equations $\mathcal{L}$ such that X'_i values are pairwise distinct and Y'_i values are pairwise distinct. Formally, we have the following result, the proof of which can be found in [JN20].

Theorem 3. *Let $\mathcal{L}$ be an system of linear equation as defined above with $q \leq 2^{n-2}$ and any component of $\mathcal{L}(G)$ have at most 2^{n-1} edge. Then the number of tuple of solution $(x_1, x_2, \ldots, x_{q_X}, y_1, y_2, \ldots, y_{q_Y})$ of $\mathcal{L}$, denoted by $h(q)$, where $x_i \neq x_j$ and $y_i \neq y_j$, for all $i \neq j$, satisfies*

$$h(q) \geq \left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=\alpha+1}^{\beta+\gamma} \zeta_i^2\right) \frac{4q^2}{2^{2n}}\right) \times \frac{(2^n)_{q_1+\beta+q_3} \times (2^n)_{q_1+q_2+\gamma}}{\prod_{\lambda \in \lambda^q} (2^n)_{\mu_\lambda}} \tag{5}$$

where ζ_i denote the number of edge in i-th component $\forall i \in [\alpha + \beta + \gamma]$.

3 Proof of Theorem 1

This section is entirely devoted to establish the security bound shown in Theorem 1. We fix a (q, t) adversary A against the strong tweakable pseudorandom permutation security of $\mathsf{CLRW1}^4[\mathsf{E}]$ and we let

$$\delta = \mathbf{Adv}^{\text{tsprp}}_{\mathsf{CLRW1}^4[\mathsf{E}]}(\mathsf{A}).$$

The first step of the proof consists in replacing the four independent keyed block ciphers $\mathsf{E}_{k_1}, \mathsf{E}_{k_2}, \mathsf{E}_{k_3}$ and E_{k_4} used in the construction with four independently sampled n-bit random permutations $\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3$ and P_4 at the cost of the strong pseudorandom permutation advantage of the underlying block cipher and denote the resulting construction as $\mathsf{CLRW1}^4[\mathsf{P}]$, where $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3, \mathsf{P}_4)$. Therefore, we have

$$\delta \leq 4\mathbf{Adv}^{\text{sprp}}_{\mathsf{E}}(\mathsf{A}') + \underbrace{\mathbf{Adv}^{\text{tsprp}}_{\mathsf{CLRW1}^4[\mathsf{P}]}(\mathsf{A})}_{\delta^*},$$

where A' is a (q, t') adversary such that $t' = t$. Our goal is now to upper bound δ^*. Note that, we have

$$\delta^* \leq \max_{\mathsf{A}} \left| \Pr[\mathsf{A}^{\mathsf{CLRW1}^4[\mathsf{P}], \mathsf{CLRW1}^4[\mathsf{P}]^{-1}} = 1] - \Pr[\mathsf{A}^{\widetilde{\mathsf{P}}, \widetilde{\mathsf{P}}^{-1}} = 1] \right|,$$

where the first probability is computed over the randomness of $\mathsf{P} \leftarrow\!\!\$\ \mathsf{Perm}(n)^4$ and the second probability is computed over the randomness of $\widetilde{\mathsf{P}} \leftarrow\!\!\$\ \mathsf{TP}(\{0,1\}^n, n)$. Moreover, the maximum is taken over non-trivial adversaries [2]. Hence, we see that δ^* cannot be larger than the advantage of the best non-trivial distinguisher between the two oracles $\mathsf{CLRW1}^4[\mathsf{P}]$ for a tuple of n-bit random permutations $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3, \mathsf{P}_4)$ and the tweakable random permutation $\widetilde{\mathsf{P}} \leftarrow\!\!\$\ \mathsf{TP}(\{0,1\}^n, n)$. This formulation of the problem now allows us to use the Expectation Method.

We fix a non-trivial distinguisher A and assume that A is computationally unbounded and hence without loss of generality a deterministic distinguisher. A interacts either with the real world $\mathsf{CLRW1}^4[\mathsf{P}]$ for a tuple of n-bit random permutations $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3, \mathsf{P}_4)$, or with the ideal world. In the initial phase of the interaction with the real world, it responds with C corresponding to the encryption query (M, T) such that $C = \mathsf{CLRW1}^4[\mathsf{P}](M, T)$. Similarly, it responds with M corresponding to the decryption query (C, T) such that $M = (\mathsf{CLRW1}^4[\mathsf{P}])^{-1}(C, T)$. Therefore, the initial query-response transcript of the adversary is (M^q, T^q, C^q) for all $i \in [q]$, where T_i is the i-th tweak value, M_i is the i-th plaintext value and C_i is the i-th ciphertext value. At the end of the query-response phase, the real world releases some internal information $(X^q, Y^q, U^q, V^q, W^q, Z^q)$, where for all $i \in [q]$, the following holds:

- (M_i, X_i) is the i-th input-output pair of P_1
- (Y_i, U_i) is the i-th input-output pair of P_2
- (V_i, W_i) is the i-th input-output pair of P_3
- (Z_i, C_i) is the i-th input-output pair of P_4

3.1 Description of the Ideal World

The ideal world consists of two stages: in the first stage, which we call the *online stage*, the ideal world simulates a random tweakable permutation $\widetilde{P}$, i.e., for each encryption query (M, T), it returns $\widetilde{\mathsf{P}}(M, T)$. Similarly, for each decryption query (C, T), it returns $\widetilde{\mathsf{P}}^{-1}(C, T)$. Since the real world releases some additional information, the ideal world must generate these values as well. The ideal transcript random variable X_{id} is a 9-ary q-tuple

$$(M^q, T^q, C^q, X^q, Y^q, U^q, V^q, W^q, Z^q)$$

defined below. However, the probability distribution of these additional random variables would be determined from their definitions. The initial transcript consists of (M^q, T^q, C^q), where for all $i \in [q]$, T_i is the i-th tweak value, M_i is the i-th plaintext value, and C_i is the i-th ciphertext value. Once the query-response phase is over, the next stage of the ideal world begins, which we call the *offline stage.* In the offline stage, the ideal world samples the intermediate random variables as follows: let us define the following two sets:

$$\mathbb{M}(M^q) = \{x : x = M_i, i \in [q]\},\ \mathbb{C}(C^q) = \{z : z = C_i, i \in [q]\}.$$

Let us assume that $m := |\mathbb{M}(M^q)|$ be the distinct number of plaintexts and $c := |\mathbb{C}(C^q)|$ denotes the distinct number of ciphertexts. Then, it samples

$$X_{x_1}, X_{x_2}, \ldots, X_{x_m} \xleftarrow{\text{wor}} \{0,1\}^n,$$

where $(x_1, x_2, \ldots, x_m)$ is an arbitrary ordering of the set $\mathbb{M}(M^q)$. Similarly, we sample

$$Z_{z_1}, Z_{z_2}, \ldots, Z_{z_c} \xleftarrow{\text{wor}} \{0,1\}^n,$$

[2] A non-trivial adversary is one who does not repeat queries.

where $(z_1, z_2, \ldots, z_c)$ is an arbitrary ordering of the set $\mathbb{C}(C^q)$ such that X_{x_i} is independently distributed with Z_{z_j}. From these sampled random variables $(X_{x_1}, X_{x_2}, \ldots, X_{x_m})$ and $(Z_{z_1}, Z_{z_2}, \ldots, Z_{z_c})$, we define two q-tuples X^q and Z^q as follows: $X^q = (X_1, X_2, \ldots, X_q)$ such that $X_i = X_{M_i}$. Similarly, $Z^q = (Z_1, Z_2, \ldots, Z_q)$ such that $Z_i = Z_{C_i}$. Having defined the pair of q-tuple of random variables X^q and Z^q, we define two q-tuples (Y^q, W^q) as follows: for each $i \in [q]$, $Y_i = X_i \oplus T_i$ and $W_i = Z_i \oplus T_i$. Given this partial transcript

$$\mathsf{X}'_{\mathrm{id}} = (M^q, T^q, C^q, X^q, Y^q, W^q, Z^q),$$

we wish to define whether the sampled value X^q and Z^q is good or bad. We say that a tuple (X^q, Z^q) is **bad** if one of the following predicates hold:

1. $\mathtt{Bad}_1$ (cycle of length 2): $\exists i, j \in [q]$ such that the following holds: $Y_i = Y_j, W_i = W_j$
2. $\mathtt{Bad}_2$: $|\{(i,j) \in [q]^2 : i \neq j, Y_i = Y_j\}| \geq q^{2/3}$.
3. $\mathtt{Bad}_3$: $|\{(i,j) \in [q]^2 : i \neq j, W_i = W_j\}| \geq q^{2/3}$.
4. $\mathtt{Bad}_4$ (Y-W-Y path of length 4): $\exists i, j, k, l \in [q]$ such that the following holds: $Y_i = Y_j, W_j = W_k, Y_k = Y_l$
5. $\mathtt{Bad}_5$ (W-Y-W path of length 4): $\exists i, j, k, l \in [q]$ such that the following holds: $W_i = W_j, Y_j = Y_k, W_k = W_l$

If the sampled tuple (X^q, Z^q) is bad, then U^q and V^q values are sampled degenerately, i.e., $U_i = V_i = 0$ for all $i \in [q]$. That is, we sample without maintaining any specific conditions, which may lead to inconsistencies. However, if the sampled tuple (X^q, Z^q) is good, then we study a graph associated to (Y^q, W^q). In particular, we consider the random transcript graph $\mathcal{G}(Y^q, W^q)$ defined as follows: the set of vertices of the graph is $Y^q \sqcup W^q$. Moreover, we put a labeled edge between Y_i and W_i with label T_i. For two distinct indices $i \neq j$, if $Y_i = Y_j$, then we merge the corresponding vertices. Similarly, for two distinct indices, if $W_i = W_j$, then we merge the corresponding vertices. Therefore, the random transcript graph $\mathcal{G}(Y^q, W^q)$ is a labeled bipartite graph. Now, we have the following lemma which asserts that the random transcript graph $\mathcal{G}(Y^q, W^q)$ is **nice** if (X^q, Z^q) is good.

Lemma 1. *The transcript graph $\mathcal{G} := \mathcal{G}(Y^q, W^q)$ generated by a good tuple (X^q, Z^q) is nice, i.e., it satisfies the following properties:*

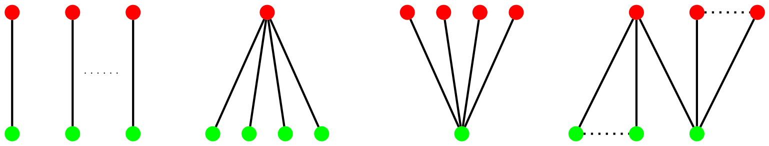
- *$\mathcal{G}$ is simple, acyclic, and has no isolated vertices.*
- *$\mathcal{G}$ has no adjacent edges such that their labels are equal.*
- *maximum component size of $\mathcal{G}$ is $2q^{2/3}$.*
- *every component of G is either a star graph, or isolated edges or contains a path of length 3.*

Proof. It is easy to see that the random transcript graph $\mathcal{G}(Y^q, W^q)$ is constructed in such a way that it contains no isolated vertices. Here we briefly justify the other properties of $\mathcal{G}$ as follows:

- By virtue of $\overline{\mathtt{Bad}_4} \wedge \overline{\mathtt{Bad}_5}$, the maximum possible length of any path of $\mathcal{G}$ is three.
- Due to $\overline{\mathtt{Bad}_1}$, $\mathcal{G}$ contains no multiple edge or a cycle of length two. So, $\mathcal{G}$ being a bipartite graph, the above conditions imply $\mathcal{G}$ is simple and acyclic.
- The construction of the transcript graph $\mathcal{G}$ implies it has no adjacent edges with equal label.

- Owing to $\overline{\texttt{Bad}_2} \wedge \overline{\texttt{Bad}_3}$, the maximum component size of $\mathcal{G}$ is $2q^{2/3}$. The maximum occurs when any component has a Y vertex and a W vertex linked by a edge and both of them have maximum possible degree $q^{2/3}$. □

We depict the type of subgraphs generated from a good tuple (X^q, Z^q) in Fig. 1.



(a) type-1. **(b)** type-2. **(c)** type-3. **(d)** type-4.

Figure 1: Type-1 is a graph of isolated edges, and the maximum path length of Type-1 graph is one. Type-2 is a star graph with Y being the centered vertex, and Type-3 is also a star graph with W being the centered vertex. The maximum path length of Type-2 and Type-3 graphs is two. Type-4 is a connected graph that is not an isolated edge or a star. It can have degree 2 vertices in both Y and W. The maximum path length of Type-4 graph is three.

Having described the possible structure of random transcript graphs, we define the sampling of (U^q, V^q) when (X^q, Z^q) is good. Note that, from Fig. 1, we have four types of possible random transcript graphs for good tuple (X^q, Z^q), which we denote as $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ and $\mathcal{G}_4$ respectively, where $\mathcal{G}_i$ is a type-i graph, for $i \in [4]$, and

- $\mathcal{G}_1$ is the union of isolated edges.
- $\mathcal{G}_2$ is the union of star components containing Y as centered vertex. That is, every component has a Y vertex with deg ≥ 2 and all other vertices are of degree one.
- $\mathcal{G}_3$ is the union of star components containing W as centered vertex. That is, every component has a W vertex with deg ≥ 2 and all other vertices are of degree one.
- $\mathcal{G}_4$ is the union of components containing at least one path of length three. That is, every component has exactly one Y and one W vertex both with deg ≥ 2 and all other vertices are of degree one.

Therefore, we define for each $b \in [4]$,

$$\mathcal{I}_b = \{i \in [q] : (Y_i, W_i) \in \mathcal{G}_b\}.$$

Since, the collection of sets $\mathcal{I}_b$ are disjoint, we have $[q] = \mathcal{I}_1 \sqcup \mathcal{I}_2 \sqcup \mathcal{I}_3 \sqcup \mathcal{I}_4$. We define $\mathcal{I} = \mathcal{I}_1 \sqcup \mathcal{I}_2 \sqcup \mathcal{I}_3$. Now, we consider the following system of equations

$$\mathcal{E} = \{U_i \oplus V_i = T_i : i \in \mathcal{I}\},$$

where $U_i = U_j$ if and only if $Y_i = Y_j$. Similarly, $V_i = V_j$ if and only of $W_i = W_j$ for all $i \neq j \in [q]$. Thus, the solution set of $\mathcal{E}$ is

$$\mathcal{S} = \{(u^{\mathcal{I}}, v^{\mathcal{I}}) : u^{\mathcal{I}} \leftrightsquigarrow Y^{\mathcal{I}}, v^{\mathcal{I}} \leftrightsquigarrow W^{\mathcal{I}}, u^{\mathcal{I}} \oplus v^{\mathcal{I}} = T^{\mathcal{I}}\}.$$

Having defined the solution set for $\mathcal{E}$, we now define the sampling of the random variables (U^q, V^q) in the ideal world as follows:

- $(U^{\mathcal{I}}, V^{\mathcal{I}}) \leftarrow\!\!\$\; \mathcal{S}$, i.e., it uniformly samples one valid solution from the set of all valid solutions

- For each component $\mathcal{C}$ of $\mathcal{G}_4$, let $(Y_i, W_i) \in \mathcal{C}$ corresponds to an edge in the component $\mathcal{C}$ such that the degree of both Y_i and W_i is at least 2. Then, we sample $U_i \leftarrow\$ \{0,1\}^n$ and set $V_i = U_i \oplus T_i$.

- The final possibility is that for each edge $(Y_i, W_i) \in \mathcal{C}$ such that $(Y_i, W_i) \neq (Y_j, W_j)$, where $(Y_j, W_j) \in \mathcal{C}$. Suppose, $Y_i = Y_j$, then $U_i = U_j$ and $V_i = U_i \oplus T_i$. Similarly, if $W_i = W_j$, then $V_i = V_j$ and $U_i = V_i \oplus T_i$.

Therefore, we completely define the random variable represents the ideal world transcript as follows:

$$\mathsf{X}_{\text{id}} = (M^q, T^q, C^q, X^q, Y^q, U^q, V^q, W^q, Z^q).$$

In this way, we achieve both the consistency of the equations in the form $\{U_i \oplus V_i = T_i\}$ and the permutation compatibility within each component of the graph $\mathcal{G}$ when the tuple (X^q, Z^q) is good. However, one must need to anticipate collisions among U values or V values across different components of the random transcript graph $\mathcal{G}$, which we will discuss in detail in the next section.

3.2 Definitition and Probability of Bad Transcripts

Given the description of the transcript random variable in the ideal world, we define the set of all attainable transcripts Ω as the set of all q tuples

$$\tau = (M^q, T^q, C^q, X^q, Y^q, U^q, V^q, W^q, Z^q),$$

where $T^q, M^q, C^q, X^q, Y^q, U^q, V^q, W^q, Z^q \in (\{0,1\}^n)^q$, $Y^q = X^q \oplus T^q$, $W^q = Z^q \oplus T^q$ and (M^q, T^q) is *tweakable permutation compatible* with (C^q, T^q). Now, we will discuss what specific events constitute a bad condition.

- Consider the event $Y^{\mathcal{I}} \overset{\times}{\leftrightsquigarrow} U^{\mathcal{I}}$ or $W^{\mathcal{I}} \overset{\times}{\leftrightsquigarrow} V^{\mathcal{I}}$ that occurs while sampling $(U^{\mathcal{I}}, V^{\mathcal{I}})$, where $\mathcal{I}$ encodes the edges that belongs to either type-1 or type-2 or type-3 graphs. However, this condition cannot arise as we sample a valid solution from the set of all valid solutions $\mathcal{S}$.

- Due to the sampling of (U^q, V^q), it may so happen that $Y^q \overset{\times}{\leftrightsquigarrow} U^q$ or $W^q \overset{\times}{\leftrightsquigarrow} V^q$

We define transcripts to be bad depending upon the characterization of the pair of q-tuples (X^q, Z^q). Following the ideal world description, we say that a pair of q-tuples (X^q, Z^q) is bad, if and only if the following predicate is true:

$$\texttt{Bad}_1 \vee \texttt{Bad}_2 \vee \texttt{Bad}_3 \vee \texttt{Bad}_4 \vee \texttt{Bad}_5.$$

We say that a transcript τ is *tuple-induced* bad transcript if (X^q, Z^q) is bad, which we denote as

$$\texttt{Bad} := \texttt{Bad}_1 \vee \texttt{Bad}_2 \vee \texttt{Bad}_3 \vee \texttt{Bad}_4 \vee \texttt{Bad}_5.$$

The other type of events that we need to discard, arise due to the bad sampling of (U^q, V^q) which causes permutation incompatibility, i.e., $Y^q \overset{\times}{\leftrightsquigarrow} U^q$ or $W^q \overset{\times}{\leftrightsquigarrow} V^q$. To bound such bad events, we need to enumerate all the conditions that results to the above inconsistencies. Note that, when the tuple (X^q, Z^q) is bad, then the transcript is trivially inconsistent as we sample (U^q, V^q) degenerately. Therefore, for a good tuple (X^q, Z^q), if $Y_i = Y_j$ or $W_i = W_j$, then we always have $U_i = U_j$ or $V_i = V_j$ respectively and hence in that case permutation inconsistencies won't arise. Therefore, we say that a transcript τ is *sampling induced* bad transcript if one of the following conditions hold: for $\alpha \in [4]$ and $\beta \in [\alpha, 4]$, we have

- $\texttt{Ucoll}_{\alpha\beta}$: $\exists i \in \mathcal{I}_\alpha$, $j \in \mathcal{I}_\beta$ such that $Y_i \neq Y_j$ and $U_i = U_j$.

- $\texttt{Vcoll}_{\alpha\beta}$: $\exists i \in \mathcal{I}_\alpha$, $j \in \mathcal{I}_\beta$ such that $W_i \neq W_j$ and $V_i = V_j$.

Note that, by varying α and β over all possible choices, we would have obtained 20 conditions, but due to the sampling mechanism of (U^q, V^q), some of them could be immediately thrown out. For example, $\texttt{Ucoll}_{11}, \texttt{Ucoll}_{12}, \texttt{Ucoll}_{13}, \texttt{Ucoll}_{22}, \texttt{Ucoll}_{23}, \texttt{Ucoll}_{33}$ does not get satisfied. Similarly, for $\texttt{Vcoll}_{\alpha\beta}$, where $\alpha \in [3]$ and $\beta \in [\alpha, 3]$. For the sake of completeness, we listed out all the 20 conditions and combine them in a single event as follows:

$$\textsf{Bad-samp} := \bigcup_{\substack{\alpha\in[4] \\ \beta\in[\alpha,4]}} (\texttt{Ucoll}_{\alpha,\beta} \cup \texttt{Vcoll}_{\alpha,\beta}). \tag{6}$$

Finally, we consider a transcript $\tau \in \Omega_{\text{bad}}$ if τ is either *tuple-induced* bad or it is *sampling-induced* bad. All other transcripts $\tau \in \Omega_{\text{good}} := \Omega \setminus \Omega_{\text{bad}}$ are good and it is easy to see that all good transcripts are attainable one.

3.2.1 Bad Transcript Analysis

Now, we analyze the probability of realizing a bad transcript in the ideal world. From the above discussion, it follows that analyzing the probability of realizing a bad transcript is possible if and only if either of the following two conditions $\textsf{Bad}$ or $\textsf{Bad-samp}$ occur. Therefore, we have

$$\begin{aligned} \epsilon_{\text{bad}} = \Pr[\textsf{X}_{\text{id}} \in \Omega_{\text{bad}}] &= \Pr[\textsf{Bad} \vee \textsf{Bad-samp}] \\ &\leq \Pr[\textsf{Bad}] + \Pr[\textsf{Bad-samp}], \end{aligned} \tag{7}$$

where these two probabilities are calculated using the ideal world distribution of the random variables. The following two lemmas establishes an upper bound on the probability of the event $\textsf{Bad}$ and $\textsf{Bad-samp}$ under the ideal world distribution.

Lemma 2. *Let* $\textsf{X}_{\text{id}}$ *and the event* $\textsf{Bad}$ *be defined as above. Then, for any integer* q *such that* $q \leq 2^{n-2}$*, one has*

$$\Pr[\textsf{Bad}] \leq \frac{4q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n}.$$

Lemma 3. *Let* $\textsf{X}_{\text{id}}$ *and the event* $\textsf{Bad-samp}$ *be defined as above. Then, for any integer* q *such that* $q \leq 2^{n-2}$*, one has*

$$\Pr[\textsf{Bad-samp}] \leq \frac{4q^4}{2^{3n}}.$$

Following Lemma 2, Lemma 3 and Eqn. (7), we obtain the probaility of bad transcripts as

$$\Pr[\textsf{X}_{\text{id}} \in \Omega_{\text{bad}}] \leq \frac{4q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n} + \frac{4q^4}{2^{3n}}. \tag{8}$$

3.2.2 Proof of Lemma 2

Recall that $\textsf{Bad} = \texttt{Bad}_1 \cup \texttt{Bad}_2 \cup \texttt{Bad}_3 \cup \texttt{Bad}_4 \cup \texttt{Bad}_5$. In this section, we bound the probability of the individual events and then by the virtue of the union bound, we sum up the individual bounds to obtain the overall bound of the probability of the event $\textsf{Bad}$.

□ **Bounding $\texttt{Bad}_1$.** Here we need to consider only the case when $T_i \neq T_j$. Note that if $T_i = T_j$ then $M_i \neq M_j$ and $C_i \neq C_j$, and hence the probability of the event is 0. Now, when $T_i \neq T_j$, using the randomness of V_i and W_i, the probability of the above event can be bounded by $1/(2^n - m)(2^n - c)$. Therefore, by varying over all possible choices of indices, and by assuming $q \leq 2^{n-1}$, we have

$$\Pr[\texttt{Bad}_1] \leq \frac{4q^2}{2^{2n}}, \tag{9}$$

□ **Bounding $\mathtt{Bad}_2$ and $\mathtt{Bad}_3$.** We first bound the probability of the event $\mathtt{Bad}_2$. For a fixed choice of indices, we define an indicator random variable $\mathbb{I}_{i,j}$ which takes the value 1 if $Y_i = Y_j$, and 0 otherwise. Let $\mathbb{I} = \sum_{i \neq j} \mathbb{I}_{i,j}$. By linearity of expectation,

$$\mathbf{E}[\mathbb{I}] = \sum_{i \neq j} \mathbf{E}[\mathbb{I}_{i,j}] = \sum_{i \neq j} \Pr[Y_i = Y_j] \leq \frac{q^2}{2^n}.$$

Applying Markov's inequality, we have

$$\Pr[\mathtt{Bad}_2] = \Pr[|\{(i,j) \in [q]^2 : Y_i = Y_j\}| \geq q^{2/3}] \leq \frac{q^2}{2^n} \times \frac{1}{q^{2/3}} = \frac{q^{4/3}}{2^n}. \tag{10}$$

Using a similar argument as used in bounding $\mathtt{Bad}_2$, we have

$$\Pr[\mathtt{Bad}_3] \leq \frac{q^{4/3}}{2^n}. \tag{11}$$

□ **Bounding** $(\mathtt{Bad}_4 \wedge \overline{\mathtt{Bad}_2})$ **and** $(\mathtt{Bad}_5 \wedge \overline{\mathtt{Bad}_3})$ Let us consider the event $(\mathtt{Bad}_4 \wedge \overline{\mathtt{Bad}_2})$. Due to $\overline{\mathtt{Bad}_2}$, the number of $(i,j),(k,l)$ pairs such that $Y_i = Y_j$ and $Y_k = Y_l$ holds is at most $q^{4/3}$. For each such choices of i,j,k,l, the probability of the event $W_j = W_k$, i.e., $Z_j \oplus Z_k = T_j \oplus T_k$ holds with at most 2^{-n}. This is due to the randomness of Z values. Therefore,

$$\Pr[\mathtt{Bad}_4 \wedge \overline{\mathtt{Bad}_2}] \leq \frac{q^{4/3}}{2^n}. \tag{12}$$

Using a similar argument as used above and using the randomness of X values, we can obtain

$$\Pr[\mathtt{Bad}_5 \wedge \overline{\mathtt{Bad}_3}] \leq \frac{q^{4/3}}{2^n}. \tag{13}$$

Finally, by combining Eqn. (9), Eqn. (10), and Eqn. (11), Eqn. (12), and Eqn. (13), we obtain the result.

3.2.3 Proof of Lemma 3

Recall that from Eqn. (6) we have

$$\begin{aligned}\Pr[\textsf{Bad-Samp}] &\leq \textsf{Pr}\left[\bigcup_{\substack{\alpha\in[4]\\ \beta\in[\alpha,4]}} (\mathtt{Ucoll}_{\alpha,\beta} \cup \mathtt{Vcoll}_{\alpha,\beta})\right] \\ &\leq \sum_{\alpha\in[4]} \sum_{\beta\in\{\alpha,\ldots,4\}} \Pr[\mathtt{Ucoll}_{\alpha,\beta} \cup \mathtt{Vcoll}_{\alpha,\beta}]. \end{aligned} \tag{14}$$

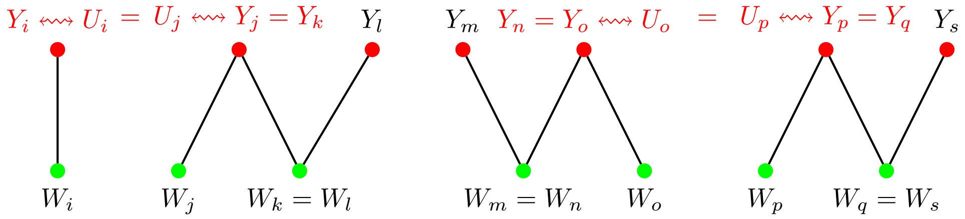
Now we will bound the probability for different value of (α, β) as follows:

□ Case 1: $\alpha \in [3], \beta \in [\alpha, 3]$: In the ideal case we have done all the sampling of U and V consistently for all three $\mathcal{I}_1, \mathcal{I}_2$ and $\mathcal{I}_3$. Recall that, $\mathcal{I} = \mathcal{I}_1 \cup \mathcal{I}_2 \cup \mathcal{I}_3$. Now for any $\alpha \in [3], \beta \in [\alpha, 3]$, we have

$$\Pr[\mathtt{Ucoll}_{\alpha,\beta} \cup \mathtt{Vcoll}_{\alpha,\beta}] = 0.$$

Hence,

$$\sum_{\alpha\in[3]} \sum_{\beta\in[\alpha,3]} \Pr[\mathtt{Ucoll}_{\alpha,\beta} \cup \mathtt{Vcoll}_{\alpha,\beta}] = 0. \tag{15}$$


$Y_i \leftrightsquigarrow U_i = U_j \leftrightsquigarrow Y_j = Y_k$
Y_l
W_i
W_j
$W_k = W_l$
Y_m
$Y_n = Y_o \leftrightsquigarrow U_o = U_p \leftrightsquigarrow Y_p = Y_q$
Y_s
$W_m = W_n$
W_o
W_p
$W_q = W_s$

(a) Example 1. **(b)** Example 2.

Figure 3: These are two events where Bad-samp occurs. Example-1 indicates the event $\texttt{Ucoll}_{1,4}$ i.e. $\exists\ i \in \mathcal{I}_1,\ j \in \mathcal{I}_4,$ such that $Y_i \neq Y_j$ and $U_i = U_j$. Example-2 indicates the event $\texttt{Ucoll}_{4,4}$ i.e. $\exists\ o\ \&\ p \in \mathcal{I}_4,$ such that $Y_o \neq Y_p$ and $U_o = U_p$.

□ Case 2: $\alpha \in [3], \beta = 4$: For this case we will analyse the probability for $\alpha = 1 \wedge \beta = 4$ and other five cases will attain the same bound by the same approach as bounding the probability of $\texttt{Vcoll}_{\alpha,\beta}$ is similar to bounding that of $\texttt{Ucoll}_{\alpha,\beta}$. Hence we have to bound only $\texttt{Ucoll}_{1,4}$. Example 1 in Fig. 3 illustrates the event $\texttt{Ucoll}_{1,4}$. Recall that

$$\texttt{Ucoll}_{1,4} := \exists i \in \mathcal{I}_1,\ j \in \mathcal{I}_4,\ \text{such that } Y_i \neq Y_j \text{ and } U_i = U_j.$$

Since $j \in \mathcal{I}_4$, so $Y_j - W_j$ is an edge in some component of $\mathcal{I}_4$ say C. This C is a connected component having a path of length 3. Hence, at least one of these Y_j and W_j have degree ≥ 2. Let us consider following conditions:

(i) $\mathsf{deg}(Y_j) \geq 2$ and $\mathsf{deg}(W_j) \geq 2$: These two vertices of degree-2 clearly implies that there exist $k, l \neq j$ such that $W_k - (Y_k = Y_j) - (W_j = W_l) - Y_l$ forms a path of length 3 in C. To satisfy this case, we need

$$\texttt{E}_1 := (Y_k = Y_j \wedge W_j = W_l).$$

(ii) $\mathsf{deg}(Y_j) \geq 2$ and $\mathsf{deg}(W_j) = 1$: In this case having a 3-length path implies that there exists $k, l \neq j$ such that $Y_l - (W_l = W_k) - (Y_k = Y_j) - W_j$ path exists in C. Hence, we need

$$\texttt{E}_2 := (Y_k = Y_j \wedge W_k = W_l).$$

(iii) $\mathsf{deg}(Y_j) = 1$ and $\mathsf{deg}(W_j) \geq 2$: In this case having a 3-length path implies existence of $k, l \neq j$ such that $W_l - (Y_l = Y_k) - (W_k = W_j) - Y_j$ is path in C. Hence, we need

$$\texttt{E}_3 := (Y_l = Y_k \wedge W_k = W_j).$$

Clearly from random sampling of Y's and W's we have

$$\forall a, b, c \in [q],\ \ \Pr[Y_a = Y_b \wedge W_b = W_c] \leq \frac{1}{2^{2n}}.$$

Now clearly from the definition of $\texttt{Ucoll}_{1,4}$ we have

$$\begin{aligned}
\Pr[\texttt{Ucoll}_{1,4}] &= \Pr[\exists i \in \mathcal{I}_1, \exists j, k, l \in \mathcal{I}_4 :\ U_i = U_j \wedge (\texttt{E}_1 \vee \texttt{E}_2 \vee \texttt{E}_3)] \\
&\leq \sum_{i \in \mathcal{I}_1} \sum_{j \neq k \neq l \in \mathcal{I}_4} \Pr[U_i = U_j] \times \Pr[\texttt{E}_1 \vee \texttt{E}_2 \vee \texttt{E}_3] \\
&\leq q \times \binom{q}{3} \times \frac{1}{2^n} \times \frac{3}{2^{2n}} \\
&\leq \frac{q^4}{2^{3n+1}}. \qquad (16)
\end{aligned}$$

As stated before following similar approach we can achieve the same bound for other five cases $\texttt{Ucoll}_{2,4}, \texttt{Ucoll}_{3,4}, \texttt{Vcoll}_{\alpha,4}$, where $\alpha = [3]$. Hence

$$\sum_{\alpha \in [3]} \sum_{\beta=4} \Pr[\texttt{Ucoll}_{\alpha,\beta} \cup \texttt{Vcoll}_{\alpha,\beta}] \leq \frac{3q^4}{2^{3n}}. \tag{17}$$

□ Case 3: $\alpha = 4, \beta = 4$: For this case we will follow the similar approach as previous case. Here we will bound the probability of $\texttt{Ucoll}_{4,4}$ and other case will attain the same bound by a similar approach as bounding the probabilility of $\texttt{Vcoll}_{4,4}$ is similar to that of bounding $\texttt{Ucoll}_{4,4}$. Hence, we have to bound only $\texttt{Ucoll}_{4,4}$. Example 2 in Fig. 3 illustrates the event $\texttt{Ucoll}_{4,4}$. Recall that

$$\texttt{Ucoll}_{4,4} := \exists i \& j \in \mathcal{I}_4, \text{ such that } Y_i \neq Y_j \text{ and } U_i = U_j.$$

Since $j \in \mathcal{I}_4$, so $Y_j - W_j$ is an edge in some component of $\mathcal{I}_4$ say C. This C is a connected component having a path of length three. Hence at least one of these Y_j and W_j have degree ≥ 2. Now, following the same approach as previous case, we will have same $\texttt{E}_1, \texttt{E}_2, \texttt{E}_3$ for some $j \neq k \neq l \in \mathcal{I}_4$. Then we will have the same final bound

$$\Pr[\texttt{Ucoll}_{4,4}] \leq \frac{q^4}{2^{3n+1}}.$$

Moreover, we will have same bound for other case $\texttt{Vcoll}_{4,4}$. Hence, we have

$$\Pr[\texttt{Ucoll}_{4,4} \cup \texttt{Vcoll}_{4,4}] \leq \frac{q^4}{2^{3n}}. \tag{18}$$

The result follows by combining Eqn. (15), Eqn. (17), and Eqn. (18).

3.3 Analysis of Good Transcripts

In this section, we fix a good transcript $\tau = (M^q, T^q, C^q, X^q, Y^q, U^q, V^q, W^q, Z^q)$ and we have to lower bound the real interpolation probability and upper bound the ideal interpolation probability. Since the transcript τ is good, we know that the corresponding transcript graph $\mathcal{G}$ is a nice graph and it is composed of the collection of components depicted in Fig. 1. From the definition of bad transcript in Sect. 3.2, we know that for a good transcript τ, one must have

$$(M^q, T^q) \leftrightsquigarrow (C^q, T^q), Y^q \leftrightsquigarrow U^q, W^q \leftrightsquigarrow V^q, U^q \oplus V^q = T^q.$$

For $i \in [5]$, we define $\xi_i(\tau)$ and $e_i(\tau)$ to denote the number of components and number of indices (coresponding to the edges), respectively, of type-i graphs in τ. Therefore, we have $e_1(\tau) = \xi_1(\tau)$ and $e_i(\tau) \geq 2\xi_i(\tau)$ for $i \in \{2, 3\}$ and $e_i(\tau) \geq 3\xi_i(\tau)$ for $i \in \{4, 5\}$. However, we have $q = e_1(\tau) + e_2(\tau) + e_3(\tau) + e_4(\tau) + e_5(\tau)$. In our subsequent discussions, we will omit the parameter τ whenever it is understood from the context. Recall that m denotes the distinct number of plaintexts and c denotes the distinct number of ciphertexts.

3.3.1 Real Interpolation Probability

In the real world, P_1 is called exactly m times and P_4 is called exactly c times, Moreover, P_2 is called exactly $e_1 + \xi_2 + e_3 + 2\xi_4 + (e_5 - \xi_5)$ times and P_3 is called exactly $e_1 + \xi_3 + e_2 + 2\xi_5 + (e_4 - \xi_4)$ times. This is because, type-1 graph is only isolated edges. Therefore, for each one of the isolated edges, P_2, P_3 is invoked once. Type-2 graphs is a Y^*-star graph, which means that P_2 is invoked once for every type-2 components. However, P_3 is invoked for each edges present in each of the type-2 components. Similarly, for type-3 graphs, which are W^*-star graph, P_3 is invoked once for every type-3 components. However, P_2 is invoked for each edges present in each of the type-3 components. For every type-4 components, one can similarly see that P_2 is invoked twice, but P_3 is invoked $(e_4 - \xi_4)$ times. Similarly, for every type-5 components, one can similarly see that P_3 is invoked twice, but P_2 is invoked $(e_5 - \xi_5)$ times. Therefore, the real interpolation probability is

$$\Pr[\mathsf{X}_{\text{re}} = \tau] = \frac{1}{(2^n)_m} \frac{1}{(2^n)_c} \frac{1}{(2^n)_{e_1+\xi_2+e_3+2\xi_4+(e_5-\xi_5)}} \frac{1}{(2^n)_{e_1+\xi_3+e_2+2\xi_5+(e_4-\xi_4)}} \tag{19}$$

3.3.2 Ideal Interpolation Probability

In the ideal world, the sampling of the random variables are done in three parts: in the first part, i.e., in the online stage of the sampling algorithm, it simulates a tweakable random permutation. Let $(T_1, T_2, \ldots, T_r)$ denotes the tuple of distinct tweaks in T^q and for all $i \in [r]$, we have $d_i = \mu(T^q, T_i)$, i.e., $r \leq q$ and we have $\sum_{i=1}^{r} d_i = q$. Then, we have

$$\Pr[\widetilde{\mathsf{P}}(T^q, M^q) = C^q] = \prod_{i=1}^{r} \frac{1}{(2^n)_{d_i}} \tag{20}$$

In the next stage of the sampling process, it samples the intermediate random variables. First it samples the tuple (X^q, Z^q) in without replacement manner, i.e., $X_i = X_j$ if and only if $M_i = M_j$. Similarly, $Z_i = Z_j$ if and only if $C_i = C_j$. Since, there are m distinct plaintexts and c distinct ciphertexts. Therefore, for any pair of q-tuples (x^q, z^q), we have

$$\Pr[(X^q, Z^q) = (x^q, z^q)] = \frac{1}{(2^n)_m} \frac{1}{(2^n)_c}. \tag{21}$$

Now, we sample the intermediate random variables (U^q, V^q) in the following two stages:

- **Type-1, type-2, type-3 Sampling:** Recall that, we have defined three sets $\mathcal{I}_1, \mathcal{I}_2$, and $\mathcal{I}_3$ such that $i \in \mathcal{I}_b$ implies the edge (Y_i, W_i) belongs to type-b graph, for $b \in \{1, 2, 3\}$. Recall that, we have defined the set $\mathcal{I} = \mathcal{I}_1 \sqcup \mathcal{I}_2 \sqcup \mathcal{I}_3$ and the following system of equations
$$\mathcal{E} = \{U_i \oplus V_i = \lambda_i : i \in \mathcal{I}\}.$$
Let $(\lambda_1, \lambda_2, \ldots, \lambda_s)$ denotes the tuple of distinct elements in $\lambda^{\mathcal{I}}$, and for all $i \in [s]$, we denote $g_i = \mu(\lambda^{\mathcal{I}}, \lambda_i)$. Note that, as the transcript is good, the system of equations $\mathcal{E}$ does not contain any cycle and is non-degenarate. Moreover, the maximum component size $\xi_{\max}(\mathcal{E})$ is at most $q^{2/3}$ due to $\overline{\mathtt{Bad}_2}$ and $\overline{\mathtt{Bad}_3}$. Therefore, we apply Theorem 3 to lower bound on the number of valid solutions, $|\mathcal{S}|$ for $\mathcal{E}$. Since, we sample $(U^{\mathcal{I}}, V^{\mathcal{I}}) \leftarrow\!\!\$\ \mathcal{S}$ and by virtue of Theorem 3, we have
$$\Pr[(U^{\mathcal{I}}, V^{\mathcal{I}}) = (u^{\mathcal{I}}, v^{\mathcal{I}})] \leq \frac{\prod_{i=1}^{s} (2^n)_{g_i}}{\Delta \cdot (2^n)_{e_1+\xi_2+e_3} (2^n)_{e_1+e_2+\xi_3}}, \tag{22}$$
where
$$\Delta \triangleq \left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=e_1+1}^{\xi_2+\xi_3} \zeta_i^2\right) \frac{4q^2}{2^{2n}}\right). \tag{23}$$

- **Typ-4 and type-5 Sampling:** For the indices belongs to $\mathcal{I}_4$ and $\mathcal{I}_5$, a single value is sampled uniformly for each of the components, i.e., we have
$$\Pr[(U^{[q]\setminus\mathcal{I}}, V^{[q]\setminus\mathcal{I}}) = (u^{[q]\setminus\mathcal{I}}, v^{[q]\setminus\mathcal{I}})] = \frac{1}{(2^n)^{(\xi_4+\xi_5)}}, \tag{24}$$

By combining Eqn. (20), Eqn. (21), Eqn. (22), and Eqn. (24), we have

$$\Pr[\mathsf{X}_{\text{id}} = \tau] \leq \prod_{i=1}^{r} \frac{1}{(2^n)_{d_i}} \cdot \frac{1}{(2^n)_m} \cdot \frac{1}{(2^n)_c} \cdot \frac{\prod_{i=1}^{s} (2^n)_{g_i}}{\Delta \cdot (2^n)_{e_1+\xi_2+e_3} (2^n)_{e_1+e_2+\xi_3}} \cdot \frac{1}{(2^n)^{(\xi_4+\xi_5)}}. \quad (25)$$

3.3.3 Ratio of Real to Ideal Interpolation Probability

By taking the ratio of Eqn. (19) to Eqn. (25), we have the following:

$$\begin{aligned}
\frac{\Pr[\mathsf{X}_{\text{re}} = \tau]}{\Pr[\mathsf{X}_{\text{id}} = \tau]} &\geq \frac{\prod_{i=1}^{r} (2^n)_{d_i} \cdot \Delta \cdot (2^n)_{e_1+\xi_2+e_3} (2^n)_{e_1+e_2+\xi_3} (2^n)^{\xi_4+\xi_5}}{\prod_{i=1}^{s} (2^n)_{g_i} (2^n)_{e_1+\xi_2+e_3+2\xi_4+(e_5-\xi_5)} (2^n)_{e_1+e_2+\xi_3+2\xi_5+(e_4-\xi_4)}} \\
&\geq \frac{\prod_{i=1}^{r} (2^n)_{f_i} \prod_{i=1}^{r} (2^n - f_i)_{d_i - f_i} \cdot \Delta \cdot (2^n)_{e_1+\xi_2+e_3} (2^n)_{e_1+e_2+\xi_3} (2^n)^{\xi_4+\xi_5}}{\prod_{i=1}^{s} (2^n)_{g_i} (2^n)_{e_1+\xi_2+e_3+2\xi_4+(e_5-\xi_5)} (2^n)_{e_1+e_2+\xi_3+2\xi_5+(e_4-\xi_4)}} \\
&\overset{(1)}{\geq} \Delta \cdot \underbrace{\frac{\prod_{i=1}^{r} (2^n - f_i)_{d_i - f_i}}{(2^n - e_1 - \xi_2 - e_3 - \xi_4)_{\xi_4+(e_5-\xi_5)} (2^n - e_1 - e_2 - \xi_3 - \xi_5)_{\xi_5+(e_4-\xi_4)}}}_{\mathsf{X}},
\end{aligned}$$

where $f_i = \mu(T^{\mathcal{I}}, T^i), i \in [r]$. As the number of distinct internal masking values λ_i is at most the number of distinct tweaks T_i which implies that $r \geq s$ and by the virtue of the Definition 2.1 of [JN20], $\widehat{T}^{\mathcal{I}}$ compresses [3] to $\widehat{\lambda}^{\mathcal{I}}$. Hence, following Proposition 1 of [JN20], inequality (1) holds.

Proposition 1 ([JN20]). *For $r \geq s$, let $a = (a_i)_{i\in[r]}$ and $b = (b_i)_{i\in[s]}$ be two sequences over $\mathbb{N}$ such that a compresses to b. Then, for any n, such that, $2^n \geq \sum_{i=1}^{r} a_i$ holds, we have $\prod_{i=1}^{r} (2^n)_{a_i} \geq \prod_{j=1}^{s} (2^n)_{b_j}$.*

Moreover, from the following claim, we have $\mathsf{X} \geq 1$. Finally, by plugging-in the value of Δ from Eqn. (23), we have

$$\frac{\Pr[\mathsf{X}_{\text{re}} = \tau]}{\Pr[\mathsf{X}_{\text{id}} = \tau]} \geq \left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=e_1+1}^{\xi_2+\xi_3} \zeta_i^2\right) \frac{4q^2}{2^{2n}}\right). \quad (26)$$

Claim 1. *With the notations defined above, $\mathsf{X} \geq 1$.*

Proof. Note that, f_i denotes the multiplicity of the i-th tweak in the tuple $T^{\mathcal{I}}$. Hence, by definition, the multiplicity cannot be more than the number of components of type-I, type-II, and type-III graph as each of the component of type-II and type-III graphs have distinct tweak values. Therefore, $f_i \leq e_1 + \xi_2 + \xi_3 \leq e_1 + \xi_2 + e_3 + \xi_4$. Similarly, $f_i \leq \xi_1 + \xi_2 + \xi_3 \leq e_1 + e_2 + \xi_3 + \xi_5$. Note that, d_i denotes the multiplicity of the i-th tweak in the tuple T^q. Therefore, d_i cannot be more than the number of components of type-I, type-II, and type-III graph and twice that of the number of components of type-IV and type-V graphs. Therefore,

$$\begin{aligned}
d_i &\leq \xi_1 + \xi_2 + \xi_3 + 2\xi_4 + 2\xi_5 \leq e_1 + \xi_2 + e_3 + 2\xi_4 + e_5 - \xi_5, \\
d_i &\leq e_1 + e_2 + \xi_3 + e_4 - \xi_4 + 2\xi_5.
\end{aligned}$$

[3] Definition 2.1 of [JN20] says that a sequence $(a_i)_{i\in[r]}$ compresses to an another sequence $(b_i)_{i\in[s]}$, where both the sequences are defined over $\mathbb{N}$ if there exists a partition $\mathcal{P}$ of $[r]$ such that it contains exactly s classes $\mathcal{P}_1, \ldots, \mathcal{P}_s$ and for all $i \in [s]$, we have $b_i = \sum_{j\in\mathcal{P}_i} a_j$

Moreover, it is easy to verify that $\sum_{i=1}^{r}(d_i - f_i) = e_4 + e_5$ as the total multiplicity of tweaks $T \in T^{[q]\setminus\mathcal{I}}$ is exactly the number of edges in components of type-IV and type-V graphs. Therefore, we have the condition that

$$\begin{aligned}
f_i &\leq e_1 + \xi_2 + e_3 + \xi_4 \\
f_i &\leq e_1 + e_2 + \xi_3 + \xi_5 \\
d_i &\leq e_1 + \xi_2 + e_3 + 2\xi_4 + e_5 - \xi_5 \\
d_i &\leq e_1 + e_2 + \xi_3 + e_4 - \xi_4 + 2\xi_5 \\
\sum_{i=1}^{r}(d_i - f_i) &= \xi_4 + (e_5 - \xi_5) + \xi_5 + (e_4 - \xi_4) = e_4 + e_5.
\end{aligned}$$

The above conditions satisfy the conditions given in Proposition 2 of [JN20] and hence by the virtue of Propsition 2 of [JN20], the result follows. □

Proposition 2 ([JN20]). *For $r \geq 2$, let $c = (c_i)_{i\in[r]}$ and $d = (d_i)_{i\in[r]}$ be two sequences over $\mathbb{N}$. Let $a_1, a_2, b_1, b_2 \in \mathbb{N}$ such that $c_i \leq a_j, c_i + d_i \leq a_j + b_j$ for all $i \in [r], j \in [2]$, and $\sum_{i=1}^{r} d_i = b_1 + b_2$. Then, for any $n \in \mathbb{N}$, such that $a_j + b_j \leq 2^n$ for $j \in [2]$, we have*

$$\prod_{i=1}^{r}(2^n - c_i)_{d_i} \geq (2^n - a_1)_{b_1}(2^n - a_2)_{b_2}.$$

Let $\sim_Y$ be the equivalence relation over $[q]$ defined as $i \sim_Y j$ if and only if $Y_i = Y_j$. Similarly, $\sim_W$ be the equivalence relation over $[q]$ defined as $i \sim_W j$ if and only if $W_i = W_j$. Note that, each ζ_i is the random variable that corresponds to the cardinality of some non-singleton equivalence classes corresponding to the equivalence relation $\sim_Y$ or $\sim_W$. Let $\mathsf{E}_1, \mathsf{E}_2, \ldots, \mathsf{E}_y$ be the equivalence classes corresponding to the equivalence relation $\sim_Y$. Similarly, $\mathsf{F}_1, \mathsf{F}_2, \ldots, \mathsf{F}_w$ be the equivalence classes corresponding to the equivalence relation $\sim_W$. For every $i \in [y]$, let $\nu_i = |\mathsf{E}_i|$ and for every $i \in [w]$, let $\nu'_i = |\mathsf{F}_i|$. In other words, ν_i denotes the number of occurences of Y_i and ν'_i denotes the number of occurences of W_i. We define coll_Y to denote the number of colliding pairs in Y^q. Similarly, we define coll_W to denote the number of colliding pairs in W^q. Then, we have the following lemma:

Lemma 4 ([JN20]). *Since $\mathbf{E}[\mathsf{coll}_Y] \leq \frac{\binom{q}{2}}{2^n}$ and $\mathbf{E}[\mathsf{coll}_W] \leq \frac{\binom{q}{2}}{2^n}$, it holds that*

$$\begin{aligned}
\mathbf{E}\left[\sum_{i=1}^{y}\nu_i^2\right] &= 2.\mathbf{E}[\mathsf{coll}_Y] + \sum_{i=1}^{y}\nu_i \leq 4\mathbf{E}[\mathsf{coll}_Y] \leq 2q^2/2^n \\
\mathbf{E}\left[\sum_{i=1}^{w}\nu_i'^2\right] &= 2.\mathbf{E}[\mathsf{coll}_W] + \sum_{i=1}^{w}\nu'_i \leq 4\mathbf{E}[\mathsf{coll}_W] \leq 2q^2/2^n
\end{aligned}$$

It is easy to see that the expected number of colliding pairs in Y^q is $\binom{q}{2}/2^n$, as for a fixed choice of pairs (i, j), the probability that $Y_i = Y_j$ holds with probability at most 2^{-n} due to the randomness of P_1. Similarly, the expected number of colliding pairs in W^q is $\binom{q}{2}/2^n$, as for a fixed choice of pairs (i, j), the probability that $W_i = W_j$ holds with probability at most 2^{-n} due to the randomness of P_4^{-1}. Therefore, due to the fact that X^q and Z^q are independently sampled (justifies inequality (2)) and from Lemma 4 (justifies inequality (3)), the following holds.

$$\mathbf{E}\left[\sum_{i=e_1+1}^{\xi_2+\xi_3}\zeta_i^2\right] \overset{(2)}{\leq} \mathbf{E}\left[\sum_{i=1}^{y}\nu_i^2\right] + \mathbf{E}\left[\sum_{i=1}^{w}\nu_i'^2\right] \overset{(3)}{\leq} \frac{4q^2}{2^n}, \tag{27}$$

Finally, by combining Eqn. (8), Eqn. (26), Eqn. (27), and by following the Expectation Method, we have

$$\begin{aligned}\delta^* &\leq \left(\frac{4q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n} + \frac{4q^4}{2^{3n}}\right) + \left(\frac{13q^4}{2^{3n}} + \frac{2q^2}{2^{2n}} + \mathbf{E}\left[\left(\sum_{i=e_1+1}^{\xi_2+\xi_3} \zeta_i^2\right)\right]\frac{4q^2}{2^{2n}}\right) \\ &\leq \frac{6q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n} + \frac{33q^4}{2^{3n}}. \qquad (28)\end{aligned}$$

4 Conclusion

In this paper, we have shown that 4-rounds cascading LRW1 is secure up to $2^{3n/4}$ queries. However, we do not know whether the bound is tight or not. Therefore, it remains an interesting research problem to find a matching attack for CLRW1^4. We have already mentioned that Zhang et al. [ZQG22] have conducted a study on the security of the general r-round cascading of the LRW1 construction, but their proven bound is not tight. Therefore, another interesting open problem is to explore in establishing a tight security bound on the general r-round cascading of LRW1 construction.

References

[BGGS20] Zhenzhen Bao, Chun Guo, Jian Guo, and Ling Song. Tnt: How to tweak a block cipher. In *Advances in Cryptology – EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II*, page 641–673, Berlin, Heidelberg, 2020. Springer-Verlag.

[BHT18] Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, pages 468–499, 2018.

[BI99] M. Bellare and R. Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to prp to prf conversion. Cryptology ePrint Archive, Paper 1999/024, 1999. https://eprint.iacr.org/1999/024.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[CAE14] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, 2014. http://competitions.cr.yp.to/caesar.html.

[CDJ+21] Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-López, Mridul Nandi, and Yu Sasaki. Elastic-tweak: A framework for short tweak tweakable block cipher. In Avishek Adhikari, Ralf Küsters, and Bart Preneel, editors, *Progress in Cryptology - INDOCRYPT 2021 - 22nd International Conference on Cryptology in India, Jaipur, India, December 12-15, 2021, Proceedings*, volume 13143 of *Lecture Notes in Computer Science*, pages 114–137. Springer, 2021.

[CDN$^+$23] Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and Abishanka Saha. Proof of mirror theory for a wide range of $\xi _{\max }$. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV*, volume 14007 of *Lecture Notes in Computer Science*, pages 470–501. Springer, 2023.

[DDD21] Nilanjan Datta, Avijit Dutta, and Kushankur Dutta. Improved security bound of (E/D)WCDM. *IACR Trans. Symmetric Cryptol.*, 2021(4):138–176, 2021.

[DDNT23] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Tight multi-user security bound of dbhts. *IACR Trans. Symmetric Cryptol.*, 2023(1):192–223, 2023.

[DDNY18] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based MAC. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I*, pages 631–661, 2018.

[DHT17] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 497–523. Springer, 2017.

[DNT19] Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond birthday bound secure MAC in faulty nonce model. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I*, pages 437–466, 2019.

[GGLS20] Chun Guo, Jian Guo, Eik List, and Ling Song. Towards closing the security gap of tweak-and-tweak (tnt). In *Advances in Cryptology – ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I*, page 567–597, Berlin, Heidelberg, 2020. Springer-Verlag.

[HKR15] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust authenticated-encryption AEZ and the problem that it solves. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 15–44. Springer, 2015.

[HT16] Viet Tung Hoang and Stefano Tessaro. Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 3–32, 2016.

[HT17] Viet Tung Hoang and Stefano Tessaro. The multi-user security of double encryption. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, pages 381–411, 2017.

[HWKS98] Chris Hall, David Wagner, John Kelsey, and Bruce Schneier. Building prfs from prps. In Hugo Krawczyk, editor, *Advances in Cryptology — CRYPTO '98*, pages 370–389, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[IMPS17] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A fast tweakable block cipher mode for highly secure message authentication. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 34–65. Springer, 2017.

[JKNS23] Ashwin Jha, Mustafa Khairallah, Mridul Nandi, and Abishanka Saha. Tight security of tnt and beyond: Attacks, proofs and possibilities for the cascaded lrw paradigm. Cryptology ePrint Archive, Paper 2023/1272, 2023. https://eprint.iacr.org/2023/1272.

[JLM$^+$17] Ashwin Jha, Eik List, Kazuhiko Minematsu, Sweta Mishra, and Mridul Nandi. XHX - A framework for optimally secure tweakable block ciphers from classical block ciphers and universal hashing. In Tanja Lange and Orr Dunkelman, editors, *Progress in Cryptology - LATINCRYPT 2017 - 5th International Conference on Cryptology and Information Security in Latin America, Havana, Cuba, September 20-22, 2017, Revised Selected Papers*, volume 11368 of *Lecture Notes in Computer Science*, pages 207–227. Springer, 2017.

[JN20] Ashwin Jha and Mridul Nandi. Tight security of cascaded LRW2. *J. Cryptol.*, 33(3):1272–1317, 2020.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In Palash Sarkar and Tetsu Iwata, editors, *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*, volume 8874 of *Lecture Notes in Computer Science*, pages 274–288. Springer, 2014.

[JNPS21] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. The deoxys AEAD family. *J. Cryptol.*, 34(3):31, 2021.

[JNS23] Ashwin Jha, Mridul Nandi, and Abishanka Saha. Tight security of tnt: Reinforcing khairallah's birthday-bound attack. Cryptology ePrint Archive, Paper 2023/1233, 2023. https://eprint.iacr.org/2023/1233.

[Kha23] Mustafa Khairallah. Clrw1^3 is not secure beyond the birthday bound: Breaking tnt with $O(2^{n/2})$ queries. Cryptology ePrint Archive, Paper 2023/1212, 2023. https://eprint.iacr.org/2023/1212.

[KLL20] Seongkwang Kim, ByeongHak Lee, and Jooyoung Lee. Tight security bounds for double-block hash-then-sum macs. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International*

Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I, volume 12105 of *Lecture Notes in Computer Science*, pages 435–465. Springer, 2020.

[LL18] ByeongHak Lee and Jooyoung Lee. Tweakable block ciphers secure beyond the birthday bound in the ideal cipher model. In *Lecture Notes in Computer Science*, pages 305–335. Springer International Publishing, 2018.

[LRW02] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In Moti Yung, editor, *Advances in Cryptology — CRYPTO 2002*, pages 31–46, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[LS13] Rodolphe Lampe and Yannick Seurin. Tweakable blockciphers with asymptotically optimal security. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 133–151. Springer, 2013.

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 14–30. Springer, 2012.

[Luc00] Stefan Lucks. The sum of prps is a secure PRF. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 470–484. Springer, 2000.

[Mar10] Luther Martin. XTS: A mode of AES for encrypting hard disks. *IEEE Secur. Priv.*, 8(3):68–69, 2010.

[Men15] Bart Mennink. Optimally secure tweakable blockciphers. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 428–448. Springer, 2015.

[Men18] Bart Mennink. Towards tight security of cascaded lrw2. In *Theory of Cryptography: 16th International Conference, TCC 2018, Panaji, India, November 11–14, 2018, Proceedings, Part II*, page 192–222, Berlin, Heidelberg, 2018. Springer-Verlag.

[NIS18] NIST. Lightweight cryptography, 2018. Online: https://csrc.nist.gov/Projects/Lightweight-Cryptography. Accessed: August 01, 2019.

[NPV17] Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers - Security Proofs and Cryptanalysis*. Springer, 2017.

[Pat08] Jacques Patarin. The "coefficients h" technique. In *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, pages 328–345, 2008.

[Pat10a] Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *IACR Cryptology ePrint Archive*, 2010:287, 2010.

[Pat10b] Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *IACR Cryptol. ePrint Arch.*, 2010:287, 2010.

[Pat17] Jacques Patarin. Mirror theory and cryptography. *Appl. Algebra Eng. Commun. Comput.*, 28(4):321–338, 2017.

[RBB03] Phillip Rogaway, Mihir Bellare, and John Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Trans. Inf. Syst. Secur.*, 6(3):365–403, 2003.

[WGZ$^+$16] Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, and Dawu Gu. How to build fully secure tweakable blockciphers from classical blockciphers. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 455–483, 2016.

[Yas11] Kan Yasuda. A new variant of pmac: Beyond the birthday bound. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, pages 596–609, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[ZQG22] Zhongliang Zhang, Zhen Qin, and Chun Guo. Just tweak! asymptotically optimal security for the cascaded lrw1 tweakable blockcipher. *Des. Codes Cryptography*, 91(3):1035–1052, oct 2022.