Cascading Four Round LRW1 is Beyond Birthday Bound Secure

Nilanjan Datta, Shreya Dey, Avijit Dutta, Sougata Mandal

Institute for Advancing Intelligence, TCG CREST.
nilanjan.datta@tcgcrest.org, exhilarant.shreya.dey@gmail.com,
avirocks.dutta13@gmail.com, sougatamandal2014@gmail.com

Abstract. In CRYPTO'02, Liskov et al. have introduced a new symmetric key primitive called tweakable block cipher. They have proposed two constructions of designing a tweakable block cipher from block ciphers. The first proposed construction is called LRW1 and the second proposed construction is called LRW2. Although, LRW2 has been extended in later works to provide beyond birthday bound security (e.g., cascaded LRW2 in CRYPTO'12 by Landecker et al.), but extension of the LRW1 has received no attention until the work of Bao et al. in EUROCRYPT'20, where the authors have shown that one round extension of LRW1, i.e., masking the output of LRW1 with the given tweak and then re-encrypting it with the same block cipher, gives security up to $2^{2n/3}$ queries. Recently, Khairallah has shown a birthday bound distinguishing attack on the construction and hence invalidated the security claim of Bao et al. This has led to the open research question, that *how many round are required for cascading* LRW1 *to achieve beyond birthday bound security ?*
In this paper, we have shown that cascading LRW1 up to four rounds is sufficient for ensuring beyond the birthday bound security. In particular, we have shown that CLRW1^4 provides security up to $2^{3n/4}$ queries. Security analysis of our construction is based on the recent development of the mirror theory technique for tweakable random permutations under the framework of the Expectation Method.

Keywords: Tweakable Block Cipher, Mirror Theory, Block Cipher, Expectation Method, TNT

1 Introduction

A block cipher is a family of permutations that is indexed via a secret key. While block ciphers, over the years, have received a widespread adoption as a fundamental cryptographic object, they inherently lack flexibility as applicability of block ciphers in different mode of operations strictly limits the variability of the cipher. As a result, many applications of block ciphers are either implicitly or explicitly designed from a tweakable block cipher. A tweakable block cipher is an another fundamental cryptographic primitive that introduces the variability in the

cipher. 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 notion of tweakable block ciphers were formalized by Liskov, Rivest, and Wagner [LRW02] and find a broad range of its applications in the direction of designing authenticated encryption schemes such as OCB [RBB03], AEZ [HKR15], Deoxys [JNPS21], in designing disk encryption schemes like XTS [Mar10], and designing numerous MAC schemes such as ZMAC [IMPS17], tweakable block cipher based PMAC_Plus [Yas11] etc. However, in recent years, due to the development of authenticated encryption schemes in CAESAR competition [CAE14] and the NIST lightweight cryptography competition [NIS18], usage of tweakable block ciphers have gained a significant boost in designing various cryptographic algorithms.

There are two different ways to construct tweakable block ciphers. One approach is the *modular approach* and the other one is the *dedicated approach*. In the modular approach, tweakable block ciphers are built from classical block ciphers via various modular constructions, and the security of the designed tweakable block cipher is ensured by a reduction to that of the underlying block ciphers. On the other hand, one could directly design tweakable block ciphers from scratch using various heuristic algorithms, and their security guarantees come from comprehensive cryptanalysis.

1.1 Designing Tweakable Block Ciphers Using Modular Approach

Tweakable block ciphers are designed from classical block ciphers in a black-box fashion. However,one can further subdivide this modular approach of designing tweakable block ciphers into two categories: (a) in the first approach, tweakable block ciphers are designed from classical block ciphers by assuming that the underlying block ciphers are *psuedorandom permutations*. This design approach was introduced by Liskov et al. [LRW02]. (b) The other approach, introduced by Mennink [Men15], is about designing tweakable block ciphers from classical block ciphers by assuming that the underlying block cipher are *ideal ciphers*. These two distinct design approaches not only deviate in their security assumptions, but also in their design philosophies. For example, pseudorandom permutation based constructions do not employ tweak-dependent rekeying technique which in-turn reduces the computational cost of the cipher, but introduces hybrid security loss in their security bounds. On the other hand, such a security loss is not incurred in the ideal cipher based constructions, which is leveraged by many constructions for achieving good security bounds and efficiency at the same time. In fact, ideal cipher-based tweakable block cipher constructions achieve more than n-bit security 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 pseduorandomness assumption of the underlying block cipher. In this regard, we revisit to the original Liskov et al.'s proposed constructions [LRW02], which were later renamed to LRW1 and LRW2 by Landecker et al. [LST12]. The first proposed construction, 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:

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

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:

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

Authors [LRW02] have proved that $\mathsf{LRW2}$ achieves a tight CCA security upto $2^{n/2}$ queries. However, compared to $\mathsf{LRW1}$, $\mathsf{LRW2}$ requires a single block cipher invocation and a hash function evaluation to process n-bit message and variable length tweak.

$\mathsf{LRW2}$ 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]. Later 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 done on the security analysis of cascading $\mathsf{LRW2}$ construction, but no extension of the $\mathsf{LRW1}$ construction has been made until the work of Bao et al. [BGGS20]. 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 $\mathsf{E} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, indexed by n-bit secret key, the construction $\mathsf{CLRW1}^3$ gives a family of tweakable block cipher $\mathsf{CLRW1}^3[\mathsf{E}](T, M) : \{0,1\}^{3n} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, indexed by a $3n$-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 shown 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 construction achieves $3n/4$-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 adopted the idea of the coupling technique to show that $\mathsf{CLRW1}^r$ achieves CCA security up to $2^{(r-2)n/r}$ queries, for $r \geq 2$. In addition, the construction achieves an improved security up to $2^{(r-1)n/(r+1)}$ queries, when r is odd.

In a recent work Khairallah [Kha23] has demonstarted a birthday bound CCA distinguishing attack on the $\mathsf{CLRW1}^3$ construction, and thereby invalidated the security claim of Bao et al. [BGGS20] and Guo et al. [GGLS20]. Now, as the things stand, $\mathsf{CLRW1}^3$ achieves a tight CCA security up to $2^{n/2}$ queries by virtue of the result by Zhang et al. [ZQG22] by plugging-in the value $r = 3$. In a very recent work, Jha et al. [JNS23] have shown an alternative tight birthday bound security proof on the construction using the standard H-Coefficient technique that removes the unnecessary constant factors arises due to the general coupling-based security analysis on $\mathsf{CLRW1}^r$.

This recent progress on the security of cascaded $\mathsf{LRW1}$ opens the direction to investigate about the number of rounds necessary for cascading $\mathsf{LRW1}$ to achieve beyond the birthday bound security against chosen-plaintext chosen-ciphertext adversaries. Note that, by the virtue of the result of Zhang et al. [ZQG22], we already know that 5-round cascaded $\mathsf{LRW1}$ achieves a beyond birthday bound CCA security, as with $r = 5$, it yields CCA security upto $2^{2n/3}$ queries. On the other hand, with $r = 4$, as per the bound obtained by Zhang et al., 4-round cascaded $\mathsf{LRW1}$ provides CCA security upto $2^{n/2}$ queries. However, the result of Zhang et al. [ZQG22] on the security bound of 4-round cascaded $\mathsf{LRW1}$ is not tight as no matching attack have been reported on the construction. Therefore, it remains an interesting open avenue to ask whether we have a birthday bound CCA attack on the 4-round cascaded $\mathsf{LRW1}$ construction or does it achieve a beyond birthday bound security? An answer to this question will essentially solve the following open problem:

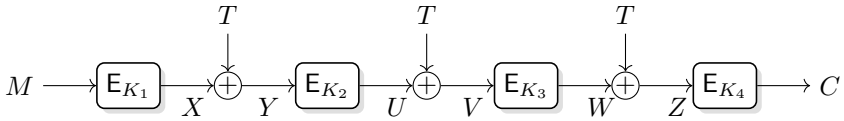
How many rounds are required for $\mathsf{CLRW1}$ *to achieve BBB security?*

1.3 Our Contribution

In this paper, we answer the above question affirmatively and show that 4 rounds for cascading $\mathsf{LRW1}$ are sufficient to cross the birthday bound barrier. We define the 4-round cascading $\mathsf{LRW1}$ 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, proof of which is deferred until Sect. 3

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

$$\mathbf{Adv}^{\mathrm{tsprp}}_{\mathsf{CLRW1}^4[\mathsf{E}]}(\mathsf{A}) \leq 4\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{E}}(\mathsf{A}') + \frac{6q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n} + \frac{38q^4}{2^{3n}}.$$

Security analysis of our construction is based on the recent development of the mirror theory technique for tweakable random permutation coupled with the framework of Expectation Method [HT16]. Concurrent to this work, Jha et al. [JKNS23] have indepedently studied the security of 4-round cascaded $\mathsf{LRW1}$ and have shown a similar CCA security bound, i.e., $3n/4$-bit, as that of ours.

2 Preliminaries

NOTATIONS: For $q \in \mathbb{N}$, we write $[q]$ to denote the set $\{1,\ldots,q\}$. 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, we write (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 set $\mathcal{X}$, $\mathsf{X} \leftarrow\!\!\$\ \{0,1\}^n$ denotes that X is sampled uniformly at random from $\{0,1\}^n$. For a tuple of random

variables $(X_1, \ldots, X_q)$, 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 $y^q = (y_1, y_2, \ldots, y_q)$, where each $x_i, y_i \in \{0,1\}^n$, denoted as $x^q \overset{\mathsf{P}}{\mapsto} y^q$ if for all $i \in [q]$, we have $\mathsf{P}(x_i) = y_i$. We say that tuple x^q is *permutation compatible* with tuple y^q, 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 is not permutation compatible with y^q, then we denote it as $x^q \overset{\times}{\leftrightsquigarrow} y^q$. 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 $K \in \{0,1\}^k$ 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. However, we will not be concerned about it. 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 and we assume that $\kappa = n$ throughout the paper.

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.

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 indistinguishabilty 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:

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

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 Twekable 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

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

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 $\mathtt{t}$.

2.4 Expectation Method

The Expectation Method, 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]. 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 X_{re} and X_{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., $\mathsf{Pr}[\mathsf{X}_{\mathrm{id}} = \tau]$) 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., $\mathsf{Pr}[\mathsf{X}_{\mathrm{id}} = \tau] > 0$). We denote the set of all attainable transcripts by Ω. Following these notations, we state the main result of 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 $\tau \in \Omega_{\mathsf{good}}$, let*

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

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

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

2.5 Mirror Theory For Tweakable Random Permutations

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 $\mathscr{L}$ of the form

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

where X^q and Y^q are unknonws 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 a 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 states that

> the number of solutions $(x_1, x_2, \ldots, x_{q_X}, y_1, y_2, \ldots, y_{q_Y})$ to the given system of linear equations $\mathcal{L}$ such that the corresponding equation graph $\mathcal{L}(G)$ satisfies the above three conditions, denoted as $h(q)$, is at least
>
> $$h(q) \geq \frac{(2^n)_{q_X}(2^n)_{q_Y}}{2^{nq}}.$$

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. Only recently, due to the work of Cogliati et al. [CDN+23], the above lower bound has been achieved with zero error term as long as $\xi_{\max} \leq 2^{n/4}/\sqrt{n}$.

Mirror theory fundamentally works for bounding the pseudorandomness of sum of permutations [Pat10, BI99, HWKS98, DHT17] with respect to a random function. However, the traditional setup of 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 H-Coefficient technique, the real interpolation probability is

$$\frac{h(q)}{(2^n)_{q_X}(2^n)_{q_Y}}$$

and the ideal interpolation probability is 2^{-nq}. Therefore, by canceling out the term 2^{nq} in the ratio of real to ideal interpolation probability, we obtain the lower bound of the ratio for a good transcript. However, this is not true for the

setting when the ideal world is *tweakable random permutation* because, in that case the ideal intepolation probability is

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

Hence, in this case, the ratio of real to ideal interpolation probability becomes

$$\frac{\prod\limits_{T \in T^q} (2^n)_{\mu_T}}{2^{nq}}.$$

Notice that, when μ_T, denoted as multi-collision of tweak T, reaches q, the ratio becomes $(1 - q^2/2^n)$, a bound deterimental for constructions achieving beyond birthday bound security.

To get rid of this bottlneck, 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 call a component $\mathcal{C}$ is *star* if $\xi_{\mathcal{C}} \geq 3$ 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, 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 atmost 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*

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

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 for establishing the security bound shown in Theorem 1. Our proof approach closely follows that of [JN20]. We fix a (q, t) adversary A against the strong tweakable pseudorandom permutation security of $\mathsf{CLRW1}^4[\mathsf{E}]$ and we let

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

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

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

where $t' = t$. We replace successively $\mathsf{E}_{k_1}, \mathsf{E}_{k_2}, \mathsf{E}_{k_3}$ and E_{k_4} by a random permutation, each time constructing an hybrid SPRP-adversary, and we consider the best of the four adversaries). Our goal is now to upper bound δ^*. Note that, we have

$$\delta^* \leq \max_{\mathsf{A}} \left| \Pr[\mathsf{P} \in \mathsf{Perm}(n)^4 : \mathsf{A}^{\mathsf{CLRW1}^4[\mathsf{P}]} = 1] - \Pr[\widetilde{\mathsf{P}} \in \mathsf{TP}(\{0,1\}^n, n) : \mathsf{A}^{\widetilde{\mathsf{P}}} = 1] \right|,$$

where the maximum is taken over non-trivial adversaries. Hence, we see that δ^* cannot be larger than the advantage of the best non-trivial distinguisher between the two oracle $\mathsf{CLRW1}^4[\mathsf{P}]$ 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 H-coefficients technique.

We fix a non-trivial distinguisher A and assume that A is computationally bounded 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 $i \in [q]$ such that 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 also 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

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

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 good or bad. We call 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. $\mathtt{Bad}_2$: $\{(i,j) \in [q]^2 : Y_i = Y_j\} \geq q^{2/3}$.
3. $\mathtt{Bad}_3$: $\{(i,j) \in [q]^2 : W_i = W_j\} \geq q^{2/3}$.
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. $\texttt{Bad}_5$ (W-Y-W path of length 4): $\exists i, j, k, l \in [q]$ such that the following holds: $W_i = W_j, Y_j = Y_k, W_k = W_l$

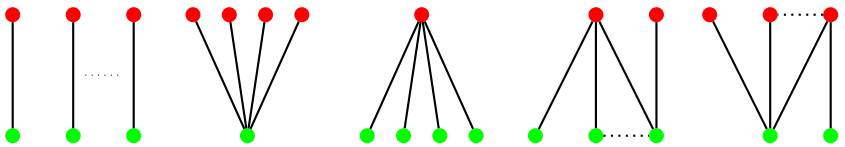
If the sampled tuple (X^q, Z^q) is bad, then U^q and V^q values are sampled degenerately, i.e., $U_i = V_i = 0$ for all $i \in [q]$. That is, we sample without maintaining any specific conditions, which may lead to inconsistencies. However, if the sampled tuple (X^q, Z^q) is good, then we study a graph 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. The proof of the lemma follows from a basic observation of the structure of the random transcript graph $\mathcal{G}(Y^q, W^q)$ and hence we omit it.

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

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

Fig. 1: Type-I is a graph of isolated edges, type-II is a star graph with Y being the centered vertex, type-III is a star graph with W being the centered vertex. Type-4 and type-5 are graphs that are not isolated edges or stars. It can have degree 2 vertices in both Y and W.



(a) type-1. (b) type-2. (c) type-3. (d) type-4. (e) type-5.

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 five types of possible random transcript graphs for good tuple (X^q, Z^q), which we denote as $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3, \mathcal{G}_4$ and $\mathcal{G}_5$ respectively. Therefore, we define for each $b \in [5]$,

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

Since, the collection of sets $\mathcal{I}_b$ are disjoint, we have $[q] = \mathcal{I}_1 \sqcup \mathcal{I}_2 \sqcup \mathcal{I}_3 \sqcup \mathcal{I}_4 \sqcup \mathcal{I}_5$. Moreover, we have $\mathcal{I} = \mathcal{I}_1 \sqcup \mathcal{I}_2 \sqcup \mathcal{I}_3$. 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:

- $(U^{\mathcal{I}}, V^{\mathcal{I}}) \xleftarrow{\$} \mathcal{S}$, i.e., it uniformly samples one valid solution from the set of all valid solutions
- We consider the graph $\mathcal{G}' := \mathcal{G} \setminus (\mathcal{G}_1 \sqcup \mathcal{G}_2 \sqcup \mathcal{G}_3)$, i.e., the collection of all subgraphs that contains path length 3. Now, for each component $\mathcal{C}$ of $\mathcal{G}'$, 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, i.e., it is type-4 $\mathcal{G}_4$ or type-5 graph $\mathcal{G}_5$. Then, we have $U_i \xleftarrow{\$} \{0,1\}^n$ 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 $(Y_j, W_j) \in \mathcal{C}$. Therefore, it implies that the edge (Y_i, W_i) belongs to either type-2 graph $\mathcal{G}_2$ or type-3 graph $\mathcal{G}_3$. 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:

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

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 withing 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 $\mathcal{G}$.

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 $(M^q, T^q) \leftrightsquigarrow (C^q, T^q)$. Now, we will discuss what specific events constitute a bad condition.

- Consider the event occurs while sampling $(U^{\mathcal{I}}, V^{\mathcal{I}})$, where recall that $\mathcal{I}$ encodes the edges that belongs to either type-1 or type-2 or type-3 graphs, $Y^{\mathcal{I}} \overset{\times}{\rightsquigarrow} U^{\mathcal{I}}$ or $W^{\mathcal{I}} \overset{\times}{\rightsquigarrow} V^{\mathcal{I}}$. 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 $Y^q \overset{\times}{\rightsquigarrow} U^q$ or $W^q \overset{\times}{\rightsquigarrow} V^q$

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

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

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

$$\mathtt{Bad} := \mathtt{Bad}_1 \cup \mathtt{Bad}_2 \cup \mathtt{Bad}_3 \cup \mathtt{Bad}_4 \cup \mathtt{Bad}_5.$$

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., $Y^q \overset{\times}{\rightsquigarrow} U^q$ or $W^q \overset{\times}{\rightsquigarrow} V^q$. 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 $\alpha \in [5]$ and $\beta \in [\alpha, 5]$, we have

- $\mathtt{Ucoll}_{\alpha\beta}$: $\exists i \in \mathcal{I}_\alpha$, $j \in \mathcal{I}_\beta$ such that $Y_i \neq Y_j$ and $U_i = U_j$.
- $\mathtt{Vcoll}_{\alpha\beta}$: $\exists i \in \mathcal{I}_\alpha$, $j \in \mathcal{I}_\beta$ 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 30 conditions, but due to the sampling mechanism of (U^q, V^q), some of them could be immediately thrown out. For example, $\mathtt{Ucoll}_{11}, \mathtt{Ucoll}_{12}, \mathtt{Ucoll}_{13}, \mathtt{Ucoll}_{22}, \mathtt{Ucoll}_{23}, \mathtt{Ucoll}_{33}$ does not get satisfied. Similarly, for $\mathtt{Vcoll}_{\alpha\beta}$, where $\alpha \in [3]$ and $\beta \in [\alpha, 3]$. For the sake of completeness, we listed out all the 30 conditions and combine them in a single event as follows:

$$\mathsf{Bad\text{-}samp} := \bigcup_{\substack{\alpha \in [5] \\ \beta \in [\alpha, 5]}} (\mathtt{Ucoll}_{\alpha,\beta} \cup \mathtt{Vcoll}_{\alpha,\beta}). \tag{5}$$

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.

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 Bad or $\mathsf{Bad\text{-}samp}$ occur. Therefore, we have

$$\begin{aligned}\epsilon_{\mathrm{bad}} = \Pr[\mathsf{X}_{\mathrm{id}} \in \Omega_{\mathrm{bad}}] &= \Pr_{\mathsf{X}_{\mathrm{id}}}[\mathsf{Bad} \vee \mathsf{Bad\text{-}samp}] \\ &\leq \Pr_{\mathsf{X}_{\mathrm{id}}}[\mathsf{Bad}] + \Pr_{\mathsf{X}_{\mathrm{bad}}}[\mathsf{Bad\text{-}samp}]. \end{aligned} \tag{6}$$

The following two lemmas establishes an upper bound on the probability of the event Bad and $\mathsf{Bad\text{-}samp}$ under the ideal world distribution.

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

$$\Pr_{\mathsf{X}_{\mathrm{id}}}[\mathsf{Bad}] \leq \frac{4q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n}.$$

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

$$\Pr_{\mathsf{X}_{\mathrm{bad}}}[\mathsf{Bad\text{-}samp}] \leq \frac{9q^4}{2^{3n}}.$$

Following Lemma 2, Lemma 3 and Eqn. (6), we obtain the probaility of bad transcripts as

$$\Pr[\mathsf{X}_{\mathrm{id}} \in \Omega_{\mathrm{bad}}] \leq \frac{4q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n} + \frac{9q^4}{2^{3n}}. \tag{7}$$

Proof of Lemma 2 Recall that $\mathsf{Bad} = \mathtt{Bad}_1 \cup \mathtt{Bad}_2 \cup \mathtt{Bad}_3 \cup \mathtt{Bad}_4 \cup \mathtt{Bad}_5$. 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 Bad.

□ **Bounding $\mathtt{Bad}_1$.** 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

$$\Pr[\mathtt{Bad}_1] \leq \frac{4q^2}{2^{2n}}, \tag{8}$$

□ **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

$$\Pr[\mathtt{Bad}_2] = \Pr[\exists (i,j) \in [q]^2 :\ Y_i = Y_j] \leq \frac{q^2}{2^n} \times \frac{1}{q^{2/3}} = \frac{q^{4/3}}{2^n}. \tag{9}$$

Using a similar argument as used in bounding $\mathtt{Bad}_3$, we have

$$\Pr[\mathtt{Bad}_3] \leq \frac{q^{4/3}}{2^n}. \tag{10}$$

□ **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,

$$\Pr[\mathtt{Bad}_4 \wedge \overline{\mathtt{Bad}_2}] \leq \frac{q^{4/3}}{2^n}. \tag{11}$$

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

$$\Pr[\mathtt{Bad}_5 \wedge \overline{\mathtt{Bad}_3}] \leq \frac{q^{4/3}}{2^n}. \tag{12}$$

Finally, by combining Eqn. (8), Eqn. (9), and Eqn. (10), Eqn. (11), and Eqn. (12), we obtain the result.

Proof of Lemma 3 Recall that from Eq. 5 we have

$$\begin{aligned}\Pr_{\mathsf{X}_{\mathrm{bad}}}[\mathsf{Bad\text{-}Samp}] &\leq \mathsf{Pr}\left[\bigcup_{\substack{\alpha\in[5]\\ \beta\in[\alpha,5]}} (\mathtt{Ucoll}_{\alpha,\beta} \cup \mathtt{Vcoll}_{\alpha,\beta})\right] \\ &\leq \sum_{\alpha\in[5]} \sum_{\beta\in\{\alpha,\ldots,5\}} \Pr[\mathtt{Ucoll}_{\alpha,\beta} \cup \mathtt{Vcoll}_{\alpha,\beta}]. \end{aligned} \tag{13}$$

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

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

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

Hence,

$$\sum_{\alpha\in[3]} \sum_{\beta\in\{\alpha,\ldots,3\}} \Pr[\mathtt{Ucoll}_{\alpha,\beta} \cup \mathtt{Vcoll}_{\alpha,\beta}] = 0. \tag{14}$$

□ Case 2: $\alpha \in [3], \beta \in \{4,5\}$: For this case we will analyse the probability for for $\alpha = 1 \wedge \beta = 4$ and other twelve cases will follow the same bound by same approach. Moreover bounding the probaililty of $\texttt{Vcoll}_{\alpha,\beta}$ is similar to bounding $\texttt{Ucoll}_{\alpha,\beta}$. Hence we have to bound only $\texttt{Ucoll}_{1,4}$. 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 atleast one of these Y_j and W_j have degree ≥ 2. Let us consider following conditions:

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

$$\mathtt{E}_1 :\ Y_k = Y_j \wedge W_j = W_l.$$

(ii) $\mathsf{deg}(X_j) \geq 2$ and $\mathsf{deg}(U_j) = 1$: 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

$$\mathtt{E}_2 :\ Y_k = Y_j \wedge W_k = W_l.$$

(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

$$\mathtt{E}_3 := Y_l = Y_k \wedge W_k = W_j.$$

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

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

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

$$\begin{aligned}
\Pr[\texttt{Ucoll}_{1,4}] &= \Pr[\exists i \in \mathcal{I}_1, \exists j,k,l \in \mathcal{I}_4 :\ U_i = U_j \wedge (\mathtt{E}_1 \vee \mathtt{E}_2 \vee \mathtt{E}_3)] \\
&\leq \sum_{i \in \mathcal{I}_1} \sum_{j \neq k \neq l \in \mathcal{I}_4} \Pr[U_i = U_j] \times \Pr[\mathtt{E}_1 \vee \mathtt{E}_2 \vee \mathtt{E}_3] \\
&\leq q \times \binom{q}{3} \times \frac{1}{2^n} \times \frac{3}{2^{2n}} \\
&\leq \frac{q^4}{2^{3n+1}}. \qquad (15)
\end{aligned}$$

As stated before following similar approach we can achieve the same bound for other 11 cases $\texttt{Ucoll}_{2,4}, \texttt{Ucoll}_{2,4}, \texttt{Vcoll}_{1,4}, \texttt{Ucoll}_{\alpha,5}, \texttt{Vcoll}_{\alpha,4}, \texttt{Vcoll}_{\alpha,5}$. Hence

$$\sum_{\alpha \in [3]} \sum_{\beta \in \{4,5\}} \Pr[\texttt{Ucoll}_{\alpha,\beta} \cup \texttt{Vcoll}_{\alpha,\beta}] \leq \frac{6.q^4}{2^{3n}}. \qquad (16)$$

□ Case 3: $\alpha \in \{4,5\}, \beta \in \{\alpha,5\}$: For this case we will follow the similar approach as previous case. Here we will bound the probability of $\texttt{Ucoll}_{4,5}$ and other five cases will follow the same bound by similar approach. Moreover, bounding the probabilility of $\texttt{Vcoll}_{\alpha,\beta}$ is similar to bounding $\texttt{Ucoll}_{\alpha,\beta}$. Hence, we have to bound only $\texttt{Ucoll}_{4,5}$. Recall that

$$\texttt{Ucoll}_{4,5} := \exists i \in \mathcal{I}_4,\ j \in \mathcal{I}_5 \text{ such that } Y_i \neq Y_j \text{ and } U_i = U_j.$$

Since $j \in \mathcal{I}_5$, so $Y_j - W_j$ is an edge in some component of $\mathcal{I}_5$ say C. This C is a connected component having a path of length 3. Hence atleast 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 $j \neq k \neq l \in \mathcal{I}_5$. Then we will have the same final bound

$$\Pr[\texttt{Ucoll}_{4,5}] \leq \frac{q^4}{2^{3n+1}}.$$

Moreover, we will have same bound for other five cases $\texttt{Ucoll}_{4,4}, \texttt{Vcoll}_{4,4}, \texttt{Vcoll}_{4,5}, \texttt{Ucoll}_{5,5}$, $\texttt{Vcoll}_{5,5}$. Hence, we have

$$\sum_{\alpha \in \{4,5\}} \sum_{\beta \in \{\alpha,5\}} \Pr[\texttt{Ucoll}_{\alpha,\beta} \cup \texttt{Vcoll}_{\alpha,\beta}] \leq \frac{3.q^4}{2^{3n}}. \tag{17}$$

The result follows by combining Eqn. (14), Eqn. (16), and Eqn. (17).

3.3 Analysis of Good Transcripts

In this section, we fix a 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, 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. **??**. 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 $e_i(\tau) = \xi_i(\tau)$ 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 they are understood from the context. Recall that m denotes the distinct number of plaintexts and c denotes the distinct number of ciphertexts.

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 $e_1 + \xi_2 + e_3 + 2\xi_4 + (e_5 - \xi_5)$ and P_3 is called exactly $e_1 + \xi_3 + e_2 + 2\xi_5 + (e_4 - \xi_4)$. 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 U^*-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 V^*-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

$$\Pr[\mathsf{X}_{\mathrm{re}} = \tau] = \frac{1}{(2^n)_m} \frac{1}{(2^n)_c} \frac{1}{(2^n)_{e_1+\xi_2+e_3+2\xi_4+(e_5-\xi_5)}} \frac{1}{(2^n)_{e_1+\xi_3+e_2+2\xi_5+(e_4-\xi_4)}} \tag{18}$$

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

$$\Pr[\widetilde{\mathsf{P}}(T^q, M^q) = C^q] = \prod_{i=1}^{r} \frac{1}{(2^n)_{d_i}} \tag{19}$$

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, we have

$$\Pr[(X^q, Z^q) = (x^q, z^q)] = \frac{1}{(2^n)_m} \frac{1}{(2^n)_c}. \tag{20}$$

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 hae 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. Consider the set $\mathcal{I} = \mathcal{I}_1 \sqcup \mathcal{I}_2 \sqcup \mathcal{I}_3$ and the following system of equations

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

  Let $(T_1, T_2, \ldots, T_s)$ denotes the tuple of distinct tweaks in $T^{\mathcal{I}}$, and for all $i \in [s]$, we denote $g_i = \mu(T^{\mathcal{I}}, T_i)$. Note that, as the transcript is good, the system of equations $\mathcal{E}$ does not contain any cycle and non-degenarate. Moreover, the maximum component size $\xi_{\max}(\mathcal{E})$ is at most $q^{2/3}$. Therefore, we apply Theorem 3 to lower bound on the number of valid solutions, $|\mathcal{S}|$ for $\mathcal{E}$. Since, we sample $(U^{\mathcal{I}}, V^{\mathcal{I}}) \xleftarrow{\$} \mathcal{S}$ and by the virtue of Theorem 3, we

have

$$\Pr[(U^{\mathcal{I}}, V^{\mathcal{I}}) = (u^{\mathcal{I}}, v^{\mathcal{I}})] \leq \frac{\prod_{i=1}^{s} (2^n)_{g_i}}{\Delta \cdot (2^n)_{e_1+\xi_2+e_3} (2^n)_{e_1+e_2+\xi_3}}, \tag{21}$$

where $\Delta = \left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=e_1+1}^{\xi_2+\xi_3} \zeta_i^2\right) \frac{4q^2}{2^{2n}}\right)$.

- **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

$$\Pr[(U^{[q]\setminus\mathcal{I}}, V^{[q]\setminus\mathcal{I}}) = (u^{[q]\setminus\mathcal{I}}, v^{[q]\setminus\mathcal{I}})] = \frac{1}{(2^n)^{(\xi_4+\xi_5)}}, \tag{22}$$

By combining Eqn. (19), Eqn. (20), Eqn. (21), and Eqn. (22), we have

$$\Pr[\mathsf{X}_{\mathrm{id}} = \tau] \leq \prod_{i=1}^{r} \frac{1}{(2^n)_{d_i}} \cdot \frac{1}{(2^n)_m} \cdot \frac{1}{(2^n)_c} \cdot \frac{\prod_{i=1}^{s} (2^n)_{g_i}}{\Delta \cdot (2^n)_{e_1+\xi_2+e_3} (2^n)_{e_1+e_2+\xi_3}} \cdot \frac{1}{(2^n)^{(\xi_4+\xi_5)}}. \tag{23}$$

Ratio of Real to Ideal Interpolation Probability By taking the ratio of Eqn. (18) to Eqn. (23), we have the following:

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

Following the analysis of [JN20], we have $\mathsf{X} \geq 1$, and by following the lower bound on Δ, we have

$$\frac{\Pr[\mathsf{X}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{X}_{\mathrm{id}} = \tau]} \geq \left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=e_1+1}^{\xi_2+\xi_3} \zeta_i^2\right) \frac{4q^2}{2^{2n}}\right). \tag{24}$$

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 be the random variable denotes

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 $\nu'_i = |\mathsf{F}_i|$. Therefore,

$$\mathbf{E}\left[\sum_{i=e_1+1}^{\xi_2+\xi_3} \zeta_i^2\right] \overset{(1)}{\leq} \mathbf{E}\left[\sum_{i=1}^{y} \nu_i^2\right] + \mathbf{E}\left[\sum_{i=1}^{w} \nu_i'^2\right] \overset{(2)}{\leq} \frac{4q^2}{2^n}, \tag{25}$$

where (1) follows from the fact that X^q and Z^q are independently sampled and (2) follows from Lemma 4.3 of [JN20]. Finally, by combining Eqn. (7), Eqn. (24), Eqn. (25), and by following the Expectation Method, we have

$$\begin{aligned}\delta^* &\leq \left(\frac{4q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n} + \frac{9q^4}{2^{3n}}\right) + \left(\frac{13q^4}{2^{3n}} + \frac{2q^2}{2^{2n}} + \mathbf{E}\left[\left(\sum_{i=e_1+1}^{\xi_2+\xi_3} \zeta_i^2\right)\right]\frac{4q^2}{2^{2n}}\right) \\ &\leq \frac{6q^2}{2^{2n}} + \frac{4q^{4/3}}{2^n} + \frac{38q^4}{2^{3n}}. \end{aligned} \tag{26}$$

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]. As we already mentioned that Zhang et al. [ZQG22] have studied the security of general r-round cascading of LRW1 construction. However, their proven bound is not tight. Therefore, an another interesting open problem is to explore in establishing a tight secrurity 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`.

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

[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.

[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.

[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.

[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.

[Pat10] 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.