Cascading Four Round LRW1 is Beyond Birthday Bound Secure

Nilanjan Datta[1], Shreya Dey[1], Avijit Dutta[1], Sougata Mondal[1]

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 necessary for cascading* LRW1 *to achieve beyond birthday bound security ?*
In this paper, we have shown that cascading LRW1 up to four rounds are necessary for ensuring beyond the birthday bound security. In particular, we have shown that $\mathsf{CLRW1}^4$ provides security up to $2^{2n/3}$ queries. Security analysis of our construction is based on the recent development of the mirror theory technique for tweakable random permutations under the H-Coefficient framework.

Keywords: Tweakable Block Cipher, Mirror Theory, Block Cipher, H-Coefficient Technique, TNT

1 Introduction

Liskov et al. have introduced a new symmetric key primitive called tweakable block cipher in [15]. They have proposed two constructions of desigining a tweakable block cipher from block ciphers. The first proposed construction is called LRW1 and the second proposed construction is called LRW2. 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.,

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

Therefore, LRW1 requires two block cipher calls to process an n-bit message and n-bit ciphertex. On the other hand, LRW2 transforms a block cipher into a tweakable block cipher by masking the input and output of the block cipher with hash of the given tweak, i.e.,

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

Therefore, this construction requires a single block cipher call and a hash function evaluation to process n-bit message and variable length tweak. It has been shown in [15] that both LRW1 and LRW2 achieves birthday bound CCA security.

Although, LRW2 has been extended in later works to provide beyond birthday bound security (e.g., cascaded LRW2 by Landecker et al. [14]), but no extension of the LRW1 construction has been made until the work of Bao et al. [1] where the authors have considered the 3-round cascading of the LRW1 construction, called TNT (abbreviated as *"The Tweak-aNd-Tweak"* construction. TNT is the extension of the basic LRW1 construction by masking its output with the given tweak and then it is re-encrypted with an independent block cipher to produce the ciphertext. 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 TNT gives a family of tweakable block cipher $\mathsf{TNT}[\mathsf{E}] : \{0,1\}^{3n} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, indexed by a $3n$-bit secret key and an n-bit public tweak as follows:

$$\mathsf{TNT}_{K_1,K_2,K_3}[\mathsf{E}] := \mathsf{E}_{K_3}(T \oplus \underbrace{\mathsf{E}_{K_2}(T \oplus \mathsf{E}_{K_1}(M))}_{\mathsf{LRW1}_{K_1,K_2}}).$$

TNT has been proven to be secured roughly up to $2^{2n/3}$ chosen-plaintext and chosen-ciphertext queries. Later in [8], Guo et al. have shown that TNT achieves $3n/4$-bit security bound against all possible information theoretic CPA adversaries. In [21], Zhang et al. have studied the security analysis of the generalization of LRW1 construction, called CLRW1$-r$ to denote r-round cascading of the basic LRW1 constuction, defined as follows:

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

To prove the security of the construction, authors have adopted the idea of the coupling technique to show that CLRW1-r achieves CCA security up to $2^{(r-1)n/(r+1)}$ queries, when r is odd and $r \geq 2$. On the other hand, it achieves CCA security up to $2^{(r-2)n/r}$ queries, when r is even and $r \geq 2$.

Despite of establishing beyond birthday security bound on TNT, a recent work of Khairallah [12] has shown a birthday bound chosen ciphertext distinguishing attack on the TNT construction and hence, invalidated the security claim of Bao et al. [1] and Guo et al. [8]. Therefore, by virtue of the result by Zhang et al. [21], TNT achieves a tight birthday bound security [1]. However, very recently, Jha et

[1] Note that for TNT, $r = 3$. Therefore, by plugging-in the value of r into the security bound of CLRW1-r [21] yields security upto $2^{n/2}$ queries.

al. [11] have shown an alternative birthday bound security proof on TNT using the standard H-Coefficient technique that removes the unnecessary constant factors arises due to the general coupling-based security analysis on CLRW1-r.

The above recent progresses on the security of cascaded LRW1 opens the direction to investigate about the number of rounds necessary for cascading LRW1 to achieve beyond birthday bound security. Note that, by the virtue of the result of Zhang et al. [21], we already know that 5 rounds are sufficient to achieve the CCA security of the construction as with $r = 5$, it yields CCA security upto $2^{2n/3}$ queries. On the other hand, with $r = 4$, Zhang et al. results provides CCA security of 4-round cascaded LRW1 upto $2^{n/2}$ queries. However, the security bound on 4 round cascading LRW1 is not tight as there is no birthday bound attack on the construction. Therefore, it remains an interesting open avenue to ask whether we have a birthday bound CCA attack? or it achieves a beyond birthday bound security? An answer to this question will essentially solve the following open problem:

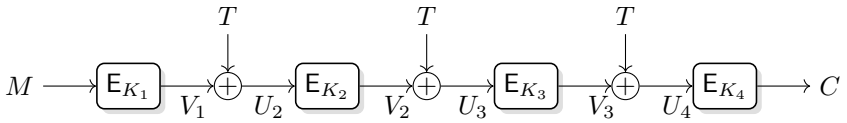
How many rounds are necessary for cascading LRW1 *to achieve BBB security ?*

1.1 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. In particular, we consider the 4 round cascading LRW1 construction dub as $\mathsf{CLRW1}^4$.Given a block cipher family $\mathsf{E} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, indexed by n-bit secret key, the $\mathsf{CLRW1}^4$ construction gives a family of tweakable block cipher: $\mathsf{CLRW1}^4[\mathsf{E}] : \{0,1\}^{4n} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, indexed by a $4n$-bit secret key and an n-bit public tweak, given as follows:

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

The pictorial description of the construction is given below.



In this paper, we have shown that the construction $\mathsf{CLRW1}^4$ provides security up to $2^{2n/3}$ 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*

$$\mathbf{Adv}^{\mathrm{tsprp}}_{\mathsf{CLRW1}^4[\mathsf{E}]}(\mathsf{A}) \leq 4\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{E}}(\mathsf{A}') + \frac{13q^4}{2^{3n}} + \frac{4q^2}{2^{2n}} + \frac{28q^3}{2^{2n}}.$$

Security analysis of our construction is based on the recent development of the mirror theory technique for tweakable random permutation coupled with the H-Coefficient technique.

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 $(x_i, y_i)_{i\in[q]}$ 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 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 is permutation compatible with tuple y^q if for all $i \in [q]$, $x_i = x_j \Leftrightarrow y_i = y_j, i \neq j \in [q]$. 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:

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

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 H-Coefficient Technique

H-Coefficient technique developed by Patarin, 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 H-Coefficient technique in Theorem 2. The proof of this theorem can be found in [18].

Theorem 2. *Let $\Omega = \Omega_{\mathsf{good}} \sqcup \Omega_{\mathsf{bad}}$ be a partition of the set of attainable transcripts. Suppose there exists $\epsilon_{\mathrm{good}} \geq 0$ such that for any good transcript $\tau \in \Omega_{\mathsf{good}}$, we have*

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

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

$$\Delta_{\mathsf{A}}[\mathcal{O}_1; \mathcal{O}_0] \leq \epsilon_1 + \epsilon_2. \tag{3}$$

2.5 Mirror Theory For Tweakable Random Permutations

Mirror theory, as introduced by Patarin [20], 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 correspondinf 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 [6, 7, 13, 16] have shown only a loose lower bound with a non-zero error term ϵ. Only recently, due to the work of Cogliati et al. [4], 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 [2,5,9,19] 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

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

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 [17] 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 [10] 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 [17], their result [10] 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 ofboth 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 [10] 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:

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*

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

where e_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. 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 a tweakable random permutation $\widetilde{\mathsf{P}} \leftarrow\!\!\$\, \mathsf{TP}(\{0,1\}^n, n)$, making at most q queries, and outputting a single bit. Let

$$\tau := \{(M_1, T_1, C_1), (M_2, T_2, C_2), \ldots, (M_q, T_q, C_q)\}$$

be the list of queries of A and corresponding answers. As defined before, we call a transcript τ *attainable* (with respect to distinguisher A) if the probability to obtain this transcript in the ideal world is non-zero. As before, we denote Ω the set of attainable transcripts and X_{re} (resp. X_{id}), the probability distribution of the transcript τ induced by the real world, (resp. the ideal world). Recall that, we have partitioned the set of attainable transcripts into two disjopint sets: set of bad transcripts, denoted as Ω_{bad} and the set of good transcripts, denoted as Ω_{good}. For the purpose of the security analysis of our construction, we set $\Omega_{\mathrm{bad}} = \emptyset$.

3.1 Analysis of Good Transcripts

In this section, we fix a transcript $\tau = \{(M_1, T_1, C_1), (M_2, T_2, C_2), \ldots, (M_q, T_q, C_q)\}$ and we have to lower bound

$$p(\tau) = \Pr[\mathsf{P} \in \mathsf{Perm}(n)^4 : \mathsf{CLRW1}^4[\mathsf{P}] \mapsto \tau].$$

The proof will proceed in two steps: first, we will lower bound the probability that permutations P_1 and P_4 satisfy some conditions given in the definition below, and then, assuming $(\mathsf{P}_1, \mathsf{P}_4)$ is good, we will lower bound the probability, over the choice of P_2 and P_3, that $\mathsf{CLRW1}^4[\mathsf{P}] \mapsto \tau$. For this second step, we will directly appeal to mirror theory result for tweakable random permutation [11] as stated in Theorem 3 that lower bounds the number of solutions of a given system of bivariate affine equations.
We start by giving the conditions defining good pairs of permutations $(\mathsf{P}_1, \mathsf{P}_4)$. We stress that these conditions cannot be accommodated in the definition of bad transcripts since they depend on values of P_1 and P_4 which do not appear in the queries transcript, so that they cannot be defined from the transcript τ alone.

Definition 1. *A pair of permutations* $(\mathsf{P}_1, \mathsf{P}_4)$ *is said to be* **bad** *if at least one of the following conditions is fulfilled*

1. $\mathtt{Bad}_1$*: There exists* $i, j \in [1, q]$ *such that* $\mathsf{P}_1(M_i) \oplus T_i = \mathsf{P}_1(M_j) \oplus T_j$ *and* $\mathsf{P}_4^{-1}(C_i) \oplus T_i = \mathsf{P}_4^{-1}(C_i) \oplus T_i$ *holds.*
2. $\mathtt{Bad}_2$*: There exists* $i, j, k \in [1, q]$ *such that* $\mathsf{P}_1(M_i) \oplus T_i = \mathsf{P}_1(M_j) \oplus T_j$ *and* $\mathsf{P}_4^{-1}(C_i) \oplus T_i = \mathsf{P}_4^{-1}(C_k) \oplus T_k$ *holds.*

3. $\mathtt{Bad}_3$*: There exists* $i, j, k \in [1, q]$ *such that* $\mathsf{P}_1(M_i) \oplus T_i = \mathsf{P}_1(M_j) \oplus T_j$ *and* $\mathsf{P}_1(M_i) \oplus T_i = \mathsf{P}_1(M_k) \oplus T_k$ *holds.*
4. $\mathtt{Bad}_4$*: There exists* $i, j, k \in [1, q]$ *such that* $\mathsf{P}_4^{-1}(C_i) \oplus T_i = \mathsf{P}_4^{-1}(C_j) \oplus T_j$ *and* $\mathsf{P}_4^{-1}(C_i) \oplus T_i = \mathsf{P}_4^{-1}(C_k) \oplus T_k$ *holds.*

Otherwise we say that $(\mathsf{P}_1, \mathsf{P}_4)$ *is good. We denote* Π_{good}*, resp.* Π_{bad} *the set of good, resp. bad pairs of permutations* $(\mathsf{P}_1, \mathsf{P}_4)$*.*

The first step towards studying good transcripts will be to upper bound the probability that the pair $(\mathsf{P}_1, \mathsf{P}_4)$ is bad.

Lemma 1. *For any integer* q *such that* $q \leq 2^{n-2}$*, one has*

$$\Pr[(\mathsf{P}_1, \mathsf{P}_4) \in \Pi_{\text{bad}}] \leq \frac{12q^3}{2^{2n}} + \frac{2q^2}{2^{2n}}.$$

Proof. For bounding the probability of a pair $(\mathsf{P}_1, \mathsf{P}_4)$ being **bad**, we individually bound the probability of each of the above events defined in definition 1 and then we derive the probability that a pair of randomly sampled permutation is bad by summing up the individual bound due to the virtue of the union bound. In order to do this, we make the following observations:

Observation 1: Consider a pair of query response tuple (M_i, T_i, C_i) and (M_j, T_j, C_j) such that $T_i = T_j$. Since, we have considered non-trivial adversary, we must have $M_i \neq M_j$ and hence $C_i \neq C_j$. Therefore, we have

$$\Pr[\mathsf{P}_1(M_i) \oplus T_i = \mathsf{P}_1(M_j) \oplus T_j] = \Pr[\mathsf{P}_4^{-1}(C_i) \oplus T_i = \mathsf{P}_4^{-1}(C_j) \oplus T_j] = 0$$

Observation 2: Consider a pair of query response tuple (M_i, T_i, C_i) and (M_j, T_j, C_j) such that $T_i \neq T_j$. Let us consider $M_i = M_j$. In this case, we have

$$\Pr[\mathsf{P}_1(M_i) \oplus T_i = \mathsf{P}_1(M_j) \oplus T_j] = 0.$$

Similarly, if we consider $C_i = C_j$, then we have

$$\Pr[\mathsf{P}_4^{-1}(C_i) \oplus T_i = \mathsf{P}_4^{-1}(C_j) \oplus T_j] = 0.$$

Observation 3: Consider a pair of query response tuple (M_i, T_i, C_i) and (M_j, T_j, C_j) such that $T_i \neq T_j$ and also $M_i \neq M_j$. In this case, we have

$$\Pr[\mathsf{P}_1(M_i) \oplus T_i = \mathsf{P}_1(M_j) \oplus T_j] \leq 2^{-n},$$

due to the randomness of the permutation P_1. Similarly, if we consider $C_i \neq C_j$, then we have

$$\Pr[\mathsf{P}_4^{-1}(C_i) \oplus T_i = \mathsf{P}_4^{-1}(C_j) \oplus T_j] \leq 2^{-n},$$

due to the randomness of the permutation P_1. Now, it remains to bound the probability of the individual bad events.

I. Bounding $\mathtt{Bad}_1$**.** We fix a pair of indices $i \neq j \in [q]$ and consider the following pair of query-response tuple $(M_i, T_i, C_i), (M_j, T_j, C_j) \in \tau$. Now, let us consider

the following two possibilities: (a) if $T_i = T_j$, then due to the observation 1, the probability of the event $\texttt{Bad}_1 = 0$. (b) On the other hand, if $T_i \neq T_j$, but $M_i = M_j$ or $C_i = C_j$ leads to probability of the event $\texttt{Bad}_1 = 0$. Finally, if $T_i \neq T_j$, and both $M_i \neq M_j$ and $C_i \neq C_j$, we have the probability of the above event is at most $1/(2^n - q)(2^n - q - 1) \leq 4/2^{2n}$ assuming $q \leq 2^{n-1} - 1$. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\texttt{Bad}_1] \leq \frac{2q^2}{2^{2n}}. \tag{5}$$

II. Bounding $\texttt{Bad}_2$. We fix a triplet of indices $i, j, k \in [q]$ such that $i \neq j$, and $i \neq k$. Now, we consider the following triplet of query-response tuple $(M_i, T_i, C_i), (M_j, T_j, C_j), (M_k, T_k, C_k) \in \tau$. Now, let us consider the following two possibilities: (a) if $T_i = T_j$ or $T_i = T_k$, then due to the observation 1, the probability of the event $\texttt{Bad}_2 = 0$. (b) On the other hand, if $T_i \neq T_j$ and $T - i \neq T_k$, but $M_i = M_j$ or $C_i = C_j$ leads to probability of the event $\texttt{Bad}_2 = 0$. Finally, if $T_i \neq T_j$, and $T_i \neq T_k$ and both $M_i \neq M_j$ and $C_i \neq C_j$, we have the probability of the above event is at most $1/(2^n - q)(2^n - q - 1) \leq 4/2^{2n}$ assuming $q \leq 2^{n-1} - 1$. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\texttt{Bad}_2] \leq \frac{4q^3}{2^{2n}}. \tag{6}$$

III. Bounding $\texttt{Bad}_3$. We fix a triplet of indices $i, j, k \in [q]$ such that $i \neq j \neq k$. Now, we consider the following triplet of query-response tuple $(M_i, T_i, C_i), (M_j, T_j, C_j)$, $(M_k, T_k, C_k) \in \tau$. Now, let us consider the following two possibilities: (a) if $T_i = T_j$ or $T_i = T_k$, then due to the observation 1, the probability of the event $\texttt{Bad}_3 = 0$. (b) On the other hand, if $T_j = T_k$, then as $M_j \neq M_k$, the probability of the event $\texttt{Bad}_3 = 0$. (c) Moreover, if T_i, T_j, T_k are all distinct, then either $M_i = M_j$, or $M_i = M_k$, or $M_j = M_k$ leads to the probability of the above event to 0. Finally, if T_i, T_j, T_k are all distinct, and M_i, M_j, M_k are also distinct, then we have the probability of the above event is at most $1/(2^n - q)(2^n - q - 1) \leq 4/2^{2n}$ assuming $q \leq 2^{n-1} - 1$. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\texttt{Bad}_3] \leq \frac{4q^3}{2^{2n}}. \tag{7}$$

IV. Bounding $\texttt{Bad}_4$. We fix a triplet of indices $i, j, k \in [q]$ such that $i \neq j \neq k$. Now, we consider the following triplet of query-response tuple $(M_i, T_i, C_i), (M_j, T_j, C_j)$, $(M_k, T_k, C_k) \in \tau$. Now, let us consider the following two possibilities: (a) if $T_i = T_j$ or $T_i = T_k$, then due to the observation 1, the probability of the event $\texttt{Bad}_4 = 0$. (b) On the other hand, if $T_j = T_k$, then as $C_j \neq C_k$, the probability of the event $\texttt{Bad}_4 = 0$. (c) Moreover, if T_i, T_j, T_k are all distinct, then either $C_i = C_j$, or $C_i = C_k$, or $C_j = C_k$ leads to the probability of the above event to 0. Finally, if T_i, T_j, T_k are all distinct, and C_i, C_j, C_k are also distinct, then we have the probability of the above event is at most $1/(2^n - q)(2^n - q - 1) \leq 4/2^{2n}$ assuming $q \leq 2^{n-1} - 1$. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\texttt{Bad}_4] \leq \frac{4q^3}{2^{2n}}. \tag{8}$$

By summing up the individual bounds of the above bad events, we obtain the result. □

We are now ready for the second step of the reasoning.

Definition 2. *Fix any pair of permutations* $(\mathsf{P}_1, \mathsf{P}_4)$*. We define a new query transcript* τ' *depending on* $(\mathsf{P}_1, \mathsf{P}_4)$ *as*

$$\tau' = \{(T, \mathsf{P}_1(M) \oplus T, \mathsf{P}_4^{-1}(C) \oplus T) : (T, M, C) \in \tau\}.$$

We also denote

$$p'(\tau, \mathsf{P}_1, \mathsf{P}_4) = \Pr[\mathsf{P}_2, \mathsf{P}_3 \leftarrow\!\!\$\, \mathsf{Perm}(n) : \mathsf{CLRW1}^4[\mathsf{P}_2, \mathsf{P}_3] \mapsto \tau']$$

.
Therefore, we have

Lemma 2. *One has*

$$\frac{\Pr[\mathsf{X}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{X}_{\mathrm{re}} = \tau]} \geq \sum_{(\mathsf{P}_1, \mathsf{P}_4) \in \Pi_{\mathrm{good}}} \frac{p'(\tau, \mathsf{P}_1, \mathsf{P}_4)}{((2^n)!)^2 \prod\limits_{T \in T^q} (1/2^n)_{\mu_T}},$$

where μ_T *is the multi-collision of tweak* T *in* T^q*.*

Proof. It is easy to see that, once P_1 and P_4 is fixed, $\mathsf{CLRW1}^4[\mathsf{P}] \mapsto \tau$ is equivalent to $\mathsf{CLRW1}^4[\mathsf{P}_2, \mathsf{P}_3] \mapsto \tau'$. Therefore,

$$\begin{aligned} p(\tau) &= \sum_{(\pi_1, \pi_4) \in \mathsf{Perm}(n)^2} \Pr[(\mathsf{P}_1, \mathsf{P}_4) \leftarrow\!\!\$\, \mathsf{Perm}(n)^2 : \mathsf{P}_1 = \pi_1, \mathsf{P}_4 = \pi_4] \cdot p'(\tau, \pi_1, \pi_4) \\ &\geq \sum_{(\pi_1, \pi_4) \in \Pi_{\mathrm{good}}} \Pr[(\mathsf{P}_1, \mathsf{P}_4) \leftarrow\!\!\$\, \mathsf{Perm}(n)^2 : \mathsf{P}_1 = \pi_1, \mathsf{P}_4 = \pi_4] \cdot p'(\tau, \pi_1, \pi_4) \\ &\geq \sum_{(\pi_1, \pi_4) \in \Pi_{\mathrm{good}}} \frac{p'(\tau, \pi_1, \pi_4)}{((2^n)!)^2}. \end{aligned} \tag{9}$$

Moreover, the ideal interpolation probability for transcript τ, where the ideal world is a tweakable random permutation, is precisely $1/(2^n)_{q_1} \cdot 1/(2^n)_{q_2} \cdots 1/(2^n)_{q_\mu}$, where μ is the distinct number of tweaks in q queries and q_i is the number of queries with tweak T_i, which is nothing but

$$\prod_{T \in T^q} (1/2^n)_{\mu_T}.$$

By taking the ratio of the real to ideal interpolation probability, the result follows. □

Now, we will lower bound $p'(\tau, \pi_1, \pi_4)$ for any good pair of permutations $(\pi_1, \pi_4) \in \Pi_{\mathrm{good}}$. Note that, $p'(\tau, \mathsf{P}_1, \mathsf{P}_4) = \Pr[\mathsf{P}_2, \mathsf{P}_3 \leftarrow\!\!\$\, \mathsf{Perm}(n) : \mathsf{CLRW1}^4[\mathsf{P}_2, \mathsf{P}_3] \mapsto \tau'$ which is equivalent to say that for a pair of randomly chosen permutations $\mathsf{P}_2, \mathsf{P}_3$,

we are interested to lower bound the probability that the following system of bivariate affine equations hold:

$$\mathcal{L} = \begin{cases} \mathsf{P}_2(V_1^1 \oplus T_1) \oplus \mathsf{P}_3^{-1}(U_1^4 \oplus T_1) = T_1 \\ \mathsf{P}_2(V_2^1 \oplus T_2) \oplus \mathsf{P}_3^{-1}(U_2^4 \oplus T_2) = T_2 \\ \vdots \quad \vdots \quad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ \mathsf{P}_2(V_q^1 \oplus T_q) \oplus \mathsf{P}_3^{-1}(U_q^4 \oplus T_q) = T_q \end{cases}$$

Therefore, we have

$$p'(\tau, \mathsf{P}_1, \mathsf{P}_4) = \Pr[(\mathsf{P}_2, \mathsf{P}_3) \xleftarrow{\$} \mathsf{Perm}(n)^2 : \mathcal{L} \text{ holds}].$$

To lower bound the above probability, we need to count the number of solutions of such a system of bivariate affine equations $\mathcal{L}$. To do this, we cast the above system of equations in a graph $\mathcal{L}(G)$ having q many edges by represeting each variable of the equations as a vertex and we connect two vertices if the corresponding variables are part of the same equation. Since, (π_1, π_4) is good, the associated equation graph is nice in the sense that it does not contain any cycle, otherwise it would satisfy event $\mathtt{Bad}_1$. Similarly, each component is either a $\mathcal{P}_2$-type star graph or $\mathcal{P}_3$-type star graph such that each star graph has exactly 3 vertices, otherwise it would satisfy either of the events $\mathtt{Bad}_2, \mathtt{Bad}_3$ or $\mathtt{Bad}_4$. Let α be the number of components having isolated edges, β be the number of components of $\mathcal{P}_2$-type, and γ be the number of components of $\mathcal{P}_3$-type. Moreover, q_1 denotes the number of equations of isolated types, q_2 be the number of equations of $\mathcal{P}_2$-type, and q_3 be the number of equations of $\mathcal{P}_3$-type. Therefore $\alpha = q_1$ and hence, we plug-in the result of mirror theory, i.e., Theorem 3 to lower bound the above probability, i.e., we have

$$\begin{aligned} p'(\tau, \mathsf{P}_1, \mathsf{P}_4) &= \frac{h(q)}{(2^n)_{q_1+\beta+q_3}(2^n)_{q_1+q_2+\gamma}} \\ &\geq \underbrace{\left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=1}^{\beta+\gamma} e_{\alpha+i}^2\right)\frac{4q^2}{2^{2n}}\right)}_{\Delta_g} \cdot \prod_{T \in T^q} \frac{1}{(2^n)_{\mu_T}} \end{aligned} \tag{10}$$

Recall that, T^q denotes the set of distinct tweaks queried among q queries, μ_T denotes the multi-collision of tweak T, and e_j denotes the number of edges in the j-th component for $j \in [\alpha+\beta+\gamma]$. Since, the equation graph for our construction is nice, we have $e_j = 2$. Therefore, we have

$$\Delta_g = \left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \frac{16q^2(\beta+\gamma)}{2^{2n}}\right) \tag{11}$$

From Eqn. (9) and Eqn. (10), we have

$$\begin{aligned} p(\tau) &= \Delta_g \cdot \prod_{T \in T^q} \frac{1}{(2^n)_{\mu_T}} \Pr[(\mathsf{P}_1, \mathsf{P}_4) \leftarrow\!\!\$\, \mathsf{Perm}(n)^2 : (\mathsf{P}_1, \mathsf{P}_4) \in \Pi_{\text{good}}] \\ &= \Delta_g \cdot \prod_{T \in T^q} \frac{1}{(2^n)_{\mu_T}} 1 - \Pr[(\mathsf{P}_1, \mathsf{P}_4) \leftarrow\!\!\$\, \mathsf{Perm}(n)^2 : (\mathsf{P}_1, \mathsf{P}_4) \in \Pi_{\text{bad}}] \\ &= \Delta_g \cdot \prod_{T \in T^q} \frac{1}{(2^n)_{\mu_T}} \underbrace{\left(1 - \frac{12q^3}{2^{2n}} - \frac{2q^2}{2^{2n}}\right)}_{\Delta_b}, \end{aligned} \tag{12}$$

where Eqn. (12) follows from Lemma 1. As the ideal interpolation probability is

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

by taking the ratio of the real to ideal interpolation probability, we have

$$\frac{\Pr[\mathsf{X}_{\text{re}} = \tau]}{\Pr[\mathsf{X}_{\text{id}} = \tau]} \geq \Delta_g \Delta_b \geq \left(1 - \frac{13q^4}{2^{3n}} - \frac{4q^2}{2^{2n}} - \frac{28q^3}{2^{2n}}\right),$$

where the last inequality follows from the fact that $(1-a)(1-b) \geq (1-a-b)$ when $a, b \leq 1$. Moreover, we have substituted the value $\beta + \gamma = q$ into Eqn. (11) to derive the final lower bound on the ratio of the real to ideal interpolation probability. □

4 Conclusion

In this paper, we have shown that 4 rounds are neccessary for cascading LRW1 to achieve beyond birthday bound security. Our security analysis is heavily influnced on the result of mirror theory tailored for tweakable random permutations [10]. However, the tightness of its security bound remains open. Likewise the tight security analysis of key-alternating cipher [3], a similar research direction is to study the tight secrity analysis of r-round cascaded LRW1.

References

1. 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.
2. 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`.

3. Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 327–350. Springer, 2014.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. Ashwin Jha and Mridul Nandi. Tight security of cascaded LRW2. *J. Cryptol.*, 33(3):1272–1317, 2020.
11. 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`.
12. 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`.
13. 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.

14. Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable block-ciphers 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. Jacques Patarin. Mirror theory and cryptography. *Appl. Algebra Eng. Commun. Comput.*, 28(4):321–338, 2017.
21. 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.