Tight Security of TNT Reinforcing Khairallah's Birthday-bound Attack

Ashwin Jha¹, Mridul Nandi², and Abishanka Saha²

¹CISPA Helmholtz Center for Information Security, Saarbrücken, Germany ashwin.jha@cispa.de ²Indian Statistical Institute, Kolkata, India mridul.nandi@gmail.com,sahaa.1993@gmail.com

Abstract. In a recent paper, Khairallah demonstrated a birthday-bound attack on TNT, thereby invalidating its (beyond-the-birthday-bound) CCA security claims. In this short note, we reestablish a birthday-bound CCA security bound for TNT. Furthermore, using a minor variant of Khairallah's attack, we show that our security bound is tight. We provide a rigorous and complete attack advantage calculations to further enhance the confidence in Khairallah's proposed attack strategy.

Keywords: TNT, LRW1, tight security, birthday-bound attack

1 Introduction

The TWEAK-AND-TWEAK or **TNT** construction is a block cipher mode of operation introduced [1] by Bao et al. at Eurocrypt 2020. Given $E : \{0,1\}^{\kappa} \times \{0,1\}^{n} \rightarrow \{0,1\}^{n}$ — a block cipher family indexed by κ -bit secret key — the **TNT** construction gives a family of tweakable block cipher (TBC) $\mathsf{TNT}[E] : \{0,1\}^{3\kappa} \times \{0,1\}^{n} \times \{0,1\}^{n} \rightarrow \{0,1\}^{n}$, indexed by a 3κ -bit secret key and an *n*-bit public tweak.



Fig. 1: The Tweak-aNd-Tweak Construction.

Formally, for any key triple $K := (K_1, K_2, K_3) \in \{0, 1\}^{3\kappa}$, the cipher is defined (also see Figure 1) by the mapping

$$(T, M) \xrightarrow{\mathsf{TNT}[E]_K} E_{K_3}(T \oplus E_{K_2}(T \oplus E_{K_1}(M))).$$

The construction is highly appreciated in the community for its simple design and high provable security guarantee. It can be viewed as a cascaded extension of LRW1, one of the seminal TBC designs [6] by Liskov et al. However, unlike LRW1, which achieves security up to roughly $2^{n/2}$ queries and that too just against chosen-plaintext attacks (CPA), TNT has been proved [1] to be secure up to roughly $2^{2n/3}$ chosen-plaintext and chosen-ciphertext attack (CCA) queries. In fact, Guo et al. have further shown [3] that the security is guaranteed up to roughly $2^{3n/4}$ CPA queries. In [9], Zhang et al. studied a more general problem. They employed the coupling technique to show that an arbitrary $r \geq 2$ -round cascading of LRW1, defined by the mapping

$$(T, M) \xrightarrow{r-\mathsf{LRW1}_K} E_{K_r}(T \oplus \ldots E_{K_2}(T \oplus E_{K_1}(M)) \ldots),$$

is secure up to roughly $2^{\frac{r-1}{r+1}n}$ CCA queries, where $K = (K_1, \ldots, K_r) \in \{0, 1\}^{r\kappa}$ is the $r\kappa$ -bit key of the construction. Note that, TNT is equivalent to 3-LRW1, and thus, guaranteed by the Zhang et al. bound to be CCA secure up to roughly $2^{n/2}$ queries — a significant degradation as compared to the original analysis.

1.1 Khairallah's Birthday-Bound CCA Attack on TNT

Recently, Khairallah proposed [5] an elegant CCA attack on TNT that requires roughly $2^{n/2}$ queries. This completely invalidates the existing CCA security analysis [1] on TNT. At a high level, the attack works in three main steps:

1. For some fixed choice of $\Delta \neq 0^n \in \{0,1\}^n$, choose a set of carefully crafted tweak values

$$\{T_1,\ldots,T_q,T_1\oplus\Delta,\ldots,T_q\oplus\Delta\}$$

such that $T_i \neq T_j$ and $T_i \neq T_j \oplus \Delta$ for all $1 \leq i \neq j \leq q$. 2. For some fixed choice of $M \in \{0,1\}^n$, for all $1 \leq i \leq q$:

- (a) Make encryption query (T_i, M) and suppose the response is C_i .
- (b) Make decryption query $(T_i \oplus \Delta, C_i)$ and suppose the response is M'_i .
- 3. Count the number of colliding $(M'_i = M'_j)$ pairs (i, j).
- 4. If the count is more than the expected number of collisions for a with replacement sampling of size q, then return 1.

The tweak values are chosen in such a way that ensures tweak-distinctness at each query. This ensures that for any uniform tweakable random permutation of $\{0,1\}^n$, each of the output is chosen uniformly at random from $\{0,1\}^n$ and independent of all other outputs.

In the real world, however, since the output of an encryption query is directly fed to a decryption query, the effect of the third block cipher E_{k_3} is effectively canceled. This helps in compressing the construction and identifying two different sources of collisions, each roughly following the collision distribution of a with replacement sampling, leading to nearly twice as many collisions as expected in the ideal world.

1.2 Our Contributions

Our contributions are twofold.

First, in section 3, we provide a simple proof of birthday-bound CCA security for TNT.

Note that, Khairallah specifically mentions [5] that the CCA security bound [9] of r-LRW1 implies birthday-bound security for TNT = 3-LRW1. While this seems to be the case in an asymptotic sense, the general coupling-based analysis introduces some unnecessary constant factors in the concrete advantage. On the other hand, our H-coefficients based proof is much more compact and gives cleaner bound. Besides, given the recent invalidation of TNT's security claims, we think that multiple security proofs using different techniques will lead to a greater confidence in the revised security claim.

We remark that the attack analysis in [5] is somewhat incomplete. So, as a second contribution, in section 4, we provide a detailed attack algorithm (based on Khairallah's attack) coupled with a careful analysis of the attack advantage. In the course of this rigorous exercise, we also identify a special condition¹ on the choice of tweak values that is sufficient (and probably necessary) for the successful accomplishment of the attack.

2 Preliminaries

NOTATIONS: Throughout, we fix a positive integer n, and $N := 2^n$. For any $0 < r \le m$, $(m)_r := m(m-1) \dots (m-r+1)$ denotes the r falling factorial of m. For any positive integer q, x^q denotes a q-tuple (x_1, \dots, x_q) . For any finite set $\mathcal{X}, X \leftarrow \mathcal{X}$ denote the uniform at random sampling of X from \mathcal{X} . We write $X_1, \dots, X_q \xleftarrow{\text{wor}} \mathcal{S}$ to denote WOR (without replacement sampling). More precisely, $(X_1, \dots, X_q) \leftarrow \{x^q \in \mathcal{S}^q : x_i\}$ are distinct}.

DISTINGUISHER AND ITS ADVANTAGE: Let \mathbf{F} and \mathbf{G} be two oracles and \mathcal{A} be a distinguisher aiming to distinguish the oracles \mathbf{F} and \mathbf{G} . The distinguisher works in two steps.

- 1. The algorithm $\mathcal{A}^{\mathcal{O}}$ obtains a transcript $\tau := \tau(\mathcal{A}^{\mathcal{O}}) = (x^q, y^q)$ after interacting with its oracle \mathcal{O} .
- 2. After all interaction is over, it returns a bit based on the transcript τ .

We now define the *distinguishing advantage* as

$$\varDelta_{\mathcal{A}}(\mathbf{F} \ ; \ \mathbf{G}) := \big| \mathsf{Pr} \left(\mathcal{A}^{\mathbf{F}} \to 1 \right) - \mathsf{Pr} \left(\mathcal{A}^{\mathbf{G}} \to 1 \right) \big|.$$

An extended oracle provides some additional values to the distinguisher after all interaction is over. Let S and S' be the additional values provided by **F** and **G** respectively. If S is sampled from a set S then (**F**, S) is called an S-extended oracle. The final response of a distinguisher \mathcal{A} interacting with an extended

¹ This condition is missing in Khairallah's analysis.

oracle is based on the extended transcript. Note that, the extended transcripts are defined as

$$\bar{\tau}(\mathcal{A}^{\mathbf{F}}) = (\tau(\mathcal{A}^{\mathbf{F}}), \mathsf{S}), \ \bar{\tau}(\mathcal{A}^{\mathbf{G}}) = (\tau(\mathcal{A}^{\mathbf{G}}), \mathsf{S}').$$

2.1 Tweakable Block Cipher and Its Security

A tweakable random permutation $\widetilde{E} : \{0,1\}^{\kappa} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is keyed family of permutations of $\{0,1\}^n$ indexed by a κ -bit key and a n-bit tweak, i.e., for all $(K,T) \in \{0,1\}^{\kappa} \times \{0,1\}^n$, $\widetilde{E}_K(T,\cdot) := \widetilde{E}(K,T,\cdot)$ is a permutation of $\{0,1\}^n$. We write $\widetilde{E}_K^{-1}(T,\cdot)$ to denote the inverse of $\widetilde{E}_K(T,\cdot)$.

Definition 1. Let $\tilde{\pi}$ denote a random tweakable permutation of $\{0,1\}^n$ with nbit tweak values. If the distinguisher has access to both forward and backward queries, we write the system as $\tilde{\pi}^{\pm}$ (similar notation for any system).

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{tprp}}(\mathcal{A}) = \varDelta_{\mathcal{A}}(\widetilde{E}_{K} \ ; \ \widetilde{\boldsymbol{\pi}}), \qquad \mathbf{Adv}_{\widetilde{E}}^{\mathrm{tsprp}}(\mathcal{A}) = \varDelta_{\mathcal{A}}(\widetilde{E}_{K}^{\pm} \ ; \ \widetilde{\boldsymbol{\pi}}^{\pm}),$$

where K is chosen uniformly at random.

When tweak space has size 1, the random tweakable permutation is essentially the same as the random permutation.

2.2 H-Technique

We describe the extended version (see [4]) of the H-technique. The basic or standard version, also called the H-coefficients technique [8], is a simple instantiation of the extended version (viewing the adjoined random variable as a degenerated or fixed constant).

Lemma 1 (Extended H-technique). Suppose $\overline{\mathbf{F}} := (\mathbf{F}, \mathsf{S})$ and $\overline{\mathbf{G}} := (\mathbf{G}, \mathsf{S}')$ are two S-extended oracles. Suppose there is a set of extended transcripts $\mathcal{V}_{\mathsf{bad}}$ such that for all $(x^q, y^q, s) \notin \mathcal{V}_{\mathsf{bad}}$, $\mathsf{Pr}(\mathbf{G}(x^q) = y^q, \mathsf{S}' = s) > 0$, and

$$\frac{\Pr\left(\mathbf{F}(x^q) = y^q, \mathbf{S} = s\right)}{\Pr\left(\mathbf{G}(x^q) = y^q, \mathbf{S}' = s\right)} \ge (1 - \epsilon)$$

for some $\epsilon \geq 0$. Then, for any distinguisher \mathcal{A} ,

$$\Delta_{\mathcal{A}}(\mathbf{F}; \mathbf{G}) \le \Pr\left(\left(\tau(\mathcal{A}^{\mathbf{G}}), \mathsf{S}'\right) \in \mathcal{V}_{\mathsf{bad}}\right) + \epsilon.$$
(1)

A proof of the (extended) H-technique is available in multiple sources, including [8,7,2,4].

3 TNT and Its Security

Hereafter, we only consider the TNT construction in information-theoretic setting. A computational equivalent of all the subsequent results can be easily obtained by the boilerplate hybrid argument.

Accordingly, we instantiate TNT based on three independent random permutations π_1 , π_2 , and π_3 of $\{0,1\}^n$. Recall that, the TNT construction is defined by the mapping

$$(T, M) \xrightarrow{\mathsf{INI}} \pi_3(T \oplus \pi_2(T \oplus \pi_1(M)))$$

and additionally, for $r \ge 2$, the r-LRW1 construction is defined by the mapping

$$(T, M) \xrightarrow{r-\mathsf{LRW1}} \pi_r(T \oplus \ldots \pi_2(T \oplus \pi_1(M)) \ldots)$$

where π_1, \ldots, π_r are mutually independent uniform random permutations of $\{0, 1\}^n$. Clearly, TNT is equivalent to 3-LRW1.

3.1 Birthday-bound Security of TNT

In [5], Khairallah relies on the TSPRP bound by Zhang et al. to demonstrate the tightness of his attack. However, we observe that the generic bound in [9] introduces some constant factors, and in general, an independent security proof, using a different proof technique, will instill greater confidence in the revised security claims of TNT.

In light of the above discussion, it is clear that the security of TNT is in a limbo. Here, we salvage a birthday-bound security for TNT based on three independent random permutations π_1 , π_2 , and π_3 of $\{0,1\}^n$. For an oracle \mathcal{O} , we abuse the $\mathcal{O}(x^q) = y^q$ to denote $\mathcal{O}(x_1) = y_1, \ldots, \mathcal{O}(x_q) = y_q$.

Theorem 1. For all $q \ge 1$ we have

$$\mathbf{Adv}_{\mathsf{TNT}}^{\mathsf{tsprp}}(q) \le \frac{q^2}{2^n}.$$

Proof. The statement is vacuously true for $q \ge 2^{n/2}$. We will use the extended H-technique to prove the statement for $1 \le q < 2^{n/2}$.

EXTENDED SYSTEMS. Let **F** be the response system corresponding to TNT and $\tilde{\pi}$ be the system corresponding to a tweakable random permutation. If $(\mathsf{T}_i, \mathsf{M}_i)$ is the encryption query with a tweak T_i we write the response as C_i . Similarly, if $(\mathsf{T}_i, \mathsf{C}_i)$ is the decryption query with a tweak T_i we write the response as M_i . After all queries have been made, the transcript τ is defined as the tuple $(\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q)$.

We now define $(\{0,1\}^n)^{2q}$ -extended response systems by adjoining two internal values X^q and Y^q. In the case of **F**, X^q and Y^q correspond to the output of π_1 and input of π_2 , respectively, and thus they are well defined from the definition of TNT. In the ideal system $\tilde{\pi}$, we sample X^q, Y^q as follows for all $i \in [q]$: 1. $X_i = X_j$ whenever $M_j = M_i$ for j < i. Otherwise (for all j < i, $M_j \neq M_i$), we sample

 $\mathsf{X}_i \leftarrow \{0,1\}^n \setminus \{x \in \{0,1\}^n : \exists j < i, \mathsf{X}_j = x\};$

2. $Y_i = Y_j$ whenever $C_j = C_i$ for j < i. Otherwise (for all j < i, $C_j \neq C_i$), we sample

 $\mathsf{Y}_i \leftarrow \$ \{0,1\}^n \setminus \{y \in \{0,1\}^n : \exists j < i, \mathsf{Y}_j = y\};$

We denote the extended transcript as $\bar{\tau}(\tilde{\pi}) = (\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q, \mathsf{X}^q, \mathsf{Y}^q)$ if follow the ideal world sampling. Similarly, $\bar{\tau}(\mathbf{F})$ denotes the extended transcript for the real-world interaction.

BAD TRANSCRIPT AND ITS ANALYSIS. An extended transcript $(t^q, m^q, c^q, x^q, y^q)$ is called *bad* if and only if (i) there is a collision among u^q values where $u_i = x_i + t_i$ or (ii) there is a collision among v^q values where $v_i = y_i + t_i$. Let $\mathcal{V}_{\mathsf{bad}}$ denote the set of all bad extended transcripts. Now, $\bar{\tau}(\tilde{\pi}) \in \mathcal{V}_{\mathsf{bad}}$ if either for some i < j, $X_i + \mathsf{T}_i = \mathsf{X}_j + \mathsf{T}_j$ or $\mathsf{Y}_i + \mathsf{T}_i = \mathsf{Y}_j + \mathsf{T}_j$. Now, it is easy to see that for any fixed i < j, $\mathsf{Pr}(\mathsf{X}_i + \mathsf{T}_i = \mathsf{X}_j + \mathsf{T}_j) \leq (2^n - 1)^{-1}$ and similarly for the other case. So, by using the union bound,

$$\Pr\left(\bar{\tau}(\widetilde{\pmb{\pi}}) \in \mathcal{V}_{\mathsf{bad}}\right) \leq \frac{q(q-1)}{2^n - 1} \leq \frac{q^2}{2^n}.$$

ANALYSIS OF GOOD TRANSCRIPTS. For a good transcript $\bar{\tau} = (t^q, m^q, c^q, x^q, y^q)$, we know that (m^q, x^q) , (y^q, c^q) , and (u^q, v^q) are permutation consistent and hence for the real world we have

$$\begin{split} \Pr\left(\bar{\tau}(\mathbf{F}) = \bar{\tau}\right) &= \Pr\left(\mathbf{\pi}_1(m^q) = x^q\right) \times \Pr\left(\mathbf{\pi}_2(u^q) = v^q\right) \times \Pr\left(\mathbf{\pi}_3(y^q) = c^q\right) \\ &= \frac{1}{(2^n)_m} \times \frac{1}{(2^n)_q} \times \frac{1}{(2^n)_c} \end{split}$$

where m and c denote the number of distinct values present in m^q and c^q respectively. In the ideal world, we have,

$$\begin{split} \Pr\left(\bar{\tau}(\widetilde{\pmb{\pi}}) = \bar{\tau}\right) &= \Pr\left(\widetilde{\pmb{\pi}}(t^q, m^q) = c^q\right) \times \frac{1}{(2^n)_m} \times \frac{1}{(2^n)_c} \\ &\leq \frac{1}{(2^n)_q} \times \frac{1}{(2^n)_m} \times \frac{1}{(2^n)_c}, \end{split}$$

where the final inequality follows from the fact that $\Pr(\tilde{\pi}(t^q, m^q) = c^q)$ maximizes when $t_i = t_j$ for all $1 \le i < j \le q$. The result follows from the extended H-technique Lemma 1.

4 Cryptanalysis of TNT

4.1 Attack Algorithm \mathcal{A}^*

Fix a message $M \in \{0,1\}^n$, a subspace $\mathcal{T} \subseteq \{0,1\}^n$ of size q (assuming q is a power of 2), and a $\Delta \notin \mathcal{T}$. We write $\mathcal{T} = \{T_1, \ldots, T_q\}$. Let $\pi_1(M) = \hat{M}$ (unknown secret). For all $T_i \in \mathcal{T}$:

- 1. Make encryption query (T_i, M) and suppose the response is C_i .
- 2. Make decryption query $(T_i \oplus \Delta, C_i)$ and suppose the response is X_i . 3. Return 1, if for some $j < i, X_i = X_j$.

4.2Advantage Calculation



Fig. 2: Cancellation of π_3 .



Fig. 3: The π_{Δ} permutation.

Ideal world collision probability. The ideal world probability of obtaining a collision can be derived as follows

$$\begin{split} &\Pr_{\mathsf{Id}}[\exists i,j\in[q]:X_i=X_j]=1-\mathsf{Pr}\left(\forall i,j\in[q]:X_i\neq X_j\right)\\ &=1-\frac{(N)_q}{N^q} \end{split}$$

We denote this ideal probability as $\mathbf{cp}(q) := 1 - \frac{(N_q)}{N^q}$ for future use.

Real world collision probability. Note that since the same message M is used in every query by the attacker we have $U_i \oplus U_j = T_i \oplus T_j$ for all $i, j \in [q]$. If two responses collide, i.e., $X_i = X_j$ then we must have $V_i \oplus V_j = T_i \oplus T_j$. Therefore there will be a collision in the *i*-th and *j*-th responses if and only if $U_i \oplus V_i = U_j \oplus V_j$.

From Fig. 3 we can observe that $U_i \oplus V_i = U_j \oplus V_j$, or equivalently $U_i \oplus V'_i = U_j \oplus V'_i$, holds if and only if:

- Either $\widehat{U}_i \oplus \widehat{U}_j = \Delta$
- Or $(\widehat{U}_i \oplus \widehat{U}_j \neq \Delta) \land \left(\pi_2^{-1} (\widehat{U}_i \oplus \Delta) \oplus U_i = \pi_2^{-1} (\widehat{U}_j \oplus \Delta) \oplus U_j \right)$

Let us define the following three events

$$\begin{split} \mathbf{E}_{0} &:= \left(\exists i, j \in [q] : U_{i} \oplus V_{i} = U_{j} \oplus V_{j}\right) \\ \mathbf{E}_{1} &:= \left(\exists i, j \in [q] : \widehat{U}_{i} \oplus \widehat{U}_{j} = \Delta\right) \\ \mathbf{E}_{2} &:= \left(\exists i, j \in [q] : \boldsymbol{\pi}_{2}^{-1}(\widehat{U}_{i} \oplus \Delta) \oplus U_{i} = \boldsymbol{\pi}_{2}^{-1}(\widehat{U}_{j} \oplus \Delta) \oplus U_{j}\right) \end{split}$$

The above observation says that $E_0 \Leftrightarrow E_1 \cup E_2$. Then we can write

$$\Pr(\mathbf{E}_0) = \Pr(\mathbf{E}_1) + \Pr(\mathbf{E}_1^c \wedge \mathbf{E}_2)$$
(2)

Calculating $\Pr(\mathbf{E}_1^c)$. Assuming the underlying permutation π_2 as a random permutation, $\Pr(\mathbf{E}_1^c)$ is same as the probability that $\widehat{U}_i \oplus \widehat{U}_j \neq \Delta$, $\forall i, j \in [q]$, where $\widehat{U}_1, \ldots, \widehat{U}_q \stackrel{\text{wor}}{\longleftarrow} \{0, 1\}^n$. Suppose $\widehat{U}_1, \ldots, \widehat{U}_t$ is chosen such that

$$(\widehat{U}_i \oplus \widehat{U}_j \neq \Delta) \land (\widehat{U}_i \neq \widehat{U}_j), \ \forall i, j \in [t]$$
(3)

Then the possible choices for \widehat{U}_{t+1} are exactly $\{0,1\}^n \setminus \mathcal{S}_t$, where

$$\mathcal{S}_t := \{\widehat{U}_1, \dots, \widehat{U}_t\} \cup \{\widehat{U}_1 \oplus \Delta, \dots, \widehat{U}_t \oplus \Delta\}.$$

Since $\widehat{U}_1, \ldots, \widehat{U}_t$ satisfies condition (3) we have $|\mathcal{S}_t| = 2t$. Thus total number of ways of selecting $\widehat{U}_1, \ldots, \widehat{U}_q$ is $N(N-2) \cdots (N-2q)$. Hence we have,

$$\Pr\left(\mathbf{E}_{1}^{c}\right) = \frac{N(N-2)\cdots(N-2q+2)}{(N)_{q}}$$
$$\leq \frac{(N)_{q}}{N^{q}} = (1 - \mathbf{cp}(q)) \tag{4}$$

Hence, $\Pr(\mathbf{E}_1) \geq \mathbf{cp}(q)$. So, we get that the probability of collision of responses in the real world is bounded as follows

$$\begin{aligned} \Pr_{\mathsf{Re}} \left(\exists i, j \in [q] : X_i = X_j \right) &= \Pr\left(\mathsf{E}_0\right) \\ &= \Pr\left(\mathsf{E}_1\right) + \Pr\left(\mathsf{E}_1^c \wedge \mathsf{E}_2\right) \\ &\geq \mathbf{cp}(q) + \Pr\left(\mathsf{E}_1^c \wedge \mathsf{E}_2\right) \\ &= \Pr_{\mathsf{Id}} \left(\exists i, j \in [q] : X_i = X_j \right) + \Pr\left(\mathsf{E}_1^c \wedge \mathsf{E}_2\right) \end{aligned}$$

Hence the advantage of our distinguisher \mathcal{A}^* will be

$$\mathbf{Adv}_{\mathsf{TNT}}^{\mathsf{tsprp}}(\mathcal{A}^*) \ge \mathsf{Pr}\left(\mathsf{E}_1^c \wedge \mathsf{E}_2\right) \tag{5}$$

So, it is sufficient to provide a lower bound for $\Pr(E_1^c \wedge E_2)$ which is the same as $\Pr(E_2 \mid E_1^c) \times \Pr(E_1^c)$.

$$\Pr\left(\mathbf{E}_{1}^{c}\right) = \frac{N(N-2)\cdots(N-2q+2)}{(N)_{q}}$$

$$= (1-\mathbf{cp}(q))\prod_{i=1}^{q-1}\left(1-\frac{i^{2}}{(N-i)^{2}}\right)$$

$$\geq (1-\mathbf{cp}(q))\prod_{i=1}^{q-1}\left(1-\frac{i^{2}}{(N-q)^{2}}\right)$$

$$\geq (1-\mathbf{cp}(q))\left(1-\frac{q(q-1)(2q-1)}{6(N-q)^{2}}\right)$$

$$\geq (1-\mathbf{cp}(q))(1-\frac{2q^{3}}{N^{2}})$$
(6)

In the last inequality, we assume that $q \leq N/2$.

Calculating $\Pr(\mathbf{E}_2|\mathbf{E}_1^c)$. Given the condition that $\widehat{U}_i \oplus \Delta \neq \widehat{U}_j$, $\forall i, j \in [q]$, we have that $\boldsymbol{\pi}_2^{-1}(\widehat{U}_i \oplus \Delta) \notin \mathcal{U} := \{U_1, \ldots, U_q\}$. Note that the set $\mathcal{U} = \mathcal{T} \oplus \boldsymbol{\pi}_1(M)$ is the affine space obtained from the subspace \mathcal{T} by translating it by $\boldsymbol{\pi}_1(M)$. Now, declaring the variables $\widehat{V}_i := \boldsymbol{\pi}_2^{-1}(\widehat{U}_i \oplus \Delta)$ and noting that $U_i \oplus U_j = T_i \oplus T_j$, we have that $(\mathbf{E}_2|\mathbf{E}_1^c)$ is same as the event,

$$\bigvee_{i\neq j\in[q]} \left(\widehat{V}_i \oplus \widehat{V}_j = T_i \oplus T_j\right), \text{ where } \widehat{V}_1, \dots, \widehat{V}_q \stackrel{\text{wor}}{\leftarrow} \mathcal{U}^c := \{0,1\}^n \setminus \mathcal{U}_i$$

For every $i \neq j \in [q]$, we define the events $\mathsf{E}_{\{i,j\}} = (\widehat{V}_i \oplus \widehat{V}_j = T_i \oplus T_j)$ where $\widehat{V}_1, \ldots, \widehat{V}_q \xleftarrow{\text{wor}} \mathcal{U}^c$. Note that for any distinct i, j,

$$\widehat{V}_i, \widehat{V}_j \stackrel{\text{wor}}{\leftarrow} \mathcal{U}^c.$$

In general, any subset follows WOR distribution. Using this observation we have $\Pr(\mathsf{E}_{\{i,j\}}) = (N - q - 1)^{-1}$. This is true because any choice of \widehat{V}_i from the set \mathcal{U}^c , we have $\widehat{V}_i \oplus T_i \oplus T_j \notin \mathcal{U}$. By using a similar argument, one can show that

$$\Pr\left(\mathbb{E}_{\{i,j\}} \wedge \mathbb{E}_{\{k,\ell\}}\right) \le \frac{1}{(N-q-1)(N-q-3)}.$$

Hence, by using Bonferroni's inequality and denoting $\alpha = \frac{\binom{q}{2}}{N-q-1}$ we have

$$\Pr\left(\bigvee_{i \neq j \in [q]} \mathbf{E}_{\{i,j\}}\right) \ge \frac{\binom{q}{2}}{N-q-1} - \frac{\binom{q}{2}^2}{2(N-q-1)(N-q-3)} \\ = \alpha \left(1 - \frac{\binom{q}{2}}{2(N-q-3)}\right) \\ \ge \alpha \left(1 - \frac{\alpha}{2}\left(1 + \frac{2}{(N-q-3)}\right)\right)$$
(7)

Note that $\mathbf{cp}(q) \leq \alpha$ (by union bound). Thus, using Equations (5)-(7), we have

$$\mathbf{Adv}_{\mathsf{TNT}}^{\mathrm{tsprp}}(\mathcal{A}^*) \geq \alpha(1-\alpha)(1-\frac{\alpha}{2}-\frac{\alpha}{N-q-3})(1-\frac{2q^3}{N^2})$$

Let q_0 be the number for which $\alpha = 1/2$. Clearly, $q_0 = O(2^{n/2})$. So, if the attacker chooses $q = \lceil q_0 \rceil$, $\mathbf{Adv}_{\mathsf{TNT}}^{\mathrm{tsprp}}(\mathcal{A}^*) \geq \frac{1}{8} - \lambda(n)$, where $\lambda(n) = O(\frac{q_0^3}{N^2}) = O(2^{-n/2})$ is negligible for large n.

5 Conclusion

In this short note, we established the tight birthday bound security for TNT. Our attack algorithm is a minor variant of Khairallah's attack [5], albeit with a more rigorous treatment and detailed advantage calculations.

ACKNOWLEDGMENTS: The authors would like to thank Mustafa Khairallah for his valuable comments. Ashwin Jha carried out this work in the framework of the French-German-Center for Cybersecurity, a collaboration of CISPA and LORIA.

References

- Zhenzhen Bao, Chun Guo, Jian Guo, and Ling Song. TNT: How to Tweak a Block Cipher. In Advances in Cryptology - EUROCRYPT 2020, Proceedings, Part II, pages 641–673, 2020.
- Shan Chen and John P. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In Advances in Cryptology - EUROCRYPT 2014, Proceedings, pages 327– 350, 2014.
- 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, Proceedings, Part I, pages 567–597, 2020.
- Ashwin Jha and Mridul Nandi. A Survey on Applications of H-Technique: Revisiting Security Analysis of PRP and PRF. *Entropy*, 24(4):462, 2022.
- 5. Mustafa Khairallah. $CLRW1^3$ is not Secure Beyond the Birthday Bound Breaking TNT with $O(2^{n/2})$ Queries. *IACR Cryptol. ePrint Arch.*, page 1212, 2023.

- Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable Block Ciphers. In Advances in Cryptology - CRYPTO 2002, Proceedings, pages 31–46, 2002.
- Mridul Nandi. A Simple and Unified Method of Proving Indistinguishability. In Progress in Cryptology - INDOCRYPT 2006, Proceedings, pages 317–334, 2006.
- Jacques Patarin. The "Coefficients H" Technique. In Selected Areas in Cryptography - SAC 2008, Revised Selected Papers, pages 328–345, 2008.
- Zhongliang Zhang, Zhen Qin, and Chun Guo. Just tweak! Asymptotically optimal security for the cascaded LRW1 tweakable blockcipher. *Des. Codes Cryptogr.*, 91(3):1035–1052, 2023.