Mind the TWEAKEY Schedule: Cryptanalysis on SKINNYe-64-256 *

Lingyue Qin[1,5,6], Xiaoyang Dong[2,5,6(✉)], Anyu Wang[2,4,5,6(✉)], Jialiang Hua[2(✉)], and Xiaoyun Wang[2,3,4,5,6(✉)]

[1] BNRist, Tsinghua University, Beijing, China
qinly@tsinghua.edu.cn
[2] Institute for Advanced Study, BNRist, Tsinghua University, Beijing, China
{xiaoyangdong,anyuwang,huajl18,xiaoyunwang}@tsinghua.edu.cn
[3] Key Laboratory of Cryptologic Technology and Information Security (Ministry of Education), School of Cyber Science and Technology, Shandong University, Qingdao, China
[4] Shangdong Institute of Blockchain, Jinan, China
[5] Zhongguancun Lab., Beijing, China
[6] National Financial Cryptography Research Center, Beijing, China

Abstract. Designing symmetric ciphers for particular applications becomes a hot topic. At EUROCRYPT 2020, Naito, Sasaki and Sugawara invented the threshold implementation friendly cipher SKINNYe-64-256 to meet the requirement of the authenticated encryption PFB_Plus. Soon, Thomas Peyrin pointed out that SKINNYe-64-256 may lose the security expectation due the new tweakey schedule. Although the security issue of SKINNYe-64-256 is still unclear, Naito *et al.* decided to introduce SKINNYe-64-256 v2 as a response.

In this paper, we give a formal cryptanalysis on the new tweakey schedule of SKINNYe-64-256 and discover unexpected differential cancellations in the tweakey schedule. For example, we find the number of cancellations can be up to 8 within 30 consecutive rounds, which is significantly larger than the expected 3 cancellations. Moreover, we take our new discoveries into rectangle, MITM and impossible differential attacks, and adapt the corresponding automatic tools with new constraints from our discoveries. Finally, we find a 41-round related-tweakey rectangle attack on SKINNYe-64-256 and leave a security margin of 3 rounds only.

As STK accepts arbitrary tweakey size, but SKINNY and SKINNYe-64-256 v2 only support up to $4n$ tweakey size. We introduce a new design of tweakey schedule for SKINNY-64 to further extend the supported tweakey size. We give a formal proof that our new tweakey schedule inherits the security requirement of STK and SKINNY. We also discuss possible ways to extend the tweakey size for SKINNY-128.

Keywords: SKINNY · TWEAKEY · Rectangle · Meet-in-the-middle · Impossible differential

* The full version of the paper is available at *https://eprint.iacr.org/2022/789*

1 Introduction

The design of symmetric cryptographic constructions for important security goals and practical applications becomes more and more popular. Typical algorithms including LowMC [3], MiMC [2], etc., provide efficient implementation for multi-party secure computing (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK). Another important topic is to design symmetric ciphers that can be efficiently implemented against side-channel attacks [28,12,47], especially because NIST lightweight cryptography competition optionally takes into account the security of the cryptographic modules against side-channel attack (SCA). Masking is by far the most common countermeasure against SCA [40,52]. Threshold implementation (TI) introduced by Nikova *et al.* [52] is a masking particularly popular for hardware implementation. Several TI-friendly Sboxes [13,36] are proposed. At TCHES 2020, Naito and Sugawara [51] discovered that for recently ciphers such as SKINNY [9] and GIFT [6], the complexity of TI for the linear key schedule function is significantly smaller than the nonlinear round function. With this asymmetry, Naito and Sugawara [51] proposed a TBC-based scheme PFB which is particularly efficient with TI. To further exploit this asymmetry, at EUROCRYPT 2020, Naito, Sasaki and Sugawara [48] invented tweakable block cipher (TBC) based AE modes PFB_Plus, PFBw, as well as a new TBC, i.e. SKINNYe-64-256, which are very efficient in threshold implementations.

At ASIACRYPT 2014, Jean, Nikolić and Peyrin introduced the TWEAKEY framework [42] with the goal to unify the design of tweakable block ciphers and allow to build a primitive with arbitrary tweak and key sizes. It treats the key input and the tweak input in the same way as the tweakey. Towards simplifying the security analysis when the tweakey size is large, Jean *et al.* identified a subclass of TWEAKEY, named as STK construction, which updates the round tweakey by the use of finite field multiplications on low hamming weight constants. SKINNY [9] is a well-known lightweight block cipher family proposed by Beierle *et al.* at CRYPTO 2016, which follows closely the STK construction [42]. However, instead of using multiplications by non-zero constants in a finite field adopted by STK construction, SKINNY updates the tweakey cells by the cheap 4-bit or 8-bit LFSRs (depending on the size of the cell) to minimize the hardware cost, while maintaining the cancellation behavior required by the STK construction: for a given position, $z-1$ cancellations can only happen every 15 rounds for TK-z[7].

As a concrete STK-like design, SKINNY only supports TK-1/-2/-3, while for STK construction, the size of tweakey can be of arbitrary length. However, in practical applications, tweakable block ciphers with large tweakeys may be required, such as the TI-friendly AE modes PFB_Plus and PFBw proposed by Naito, Sasaki and Sugawara [48]. Without TK-4 available for SKINNY, Naito *et al.* decided to build the SKINNYe-64-256 to support $zn = 4n$ tweakey with $n = 64$. In order to inherit the numerous cryptanalytic efforts on SKINNY-64 [37,31,46,4,30,54,24], SKINNYe-64-256 does not modify any components to real-

[7] For TK-z, if the size of internal state is n, the size of tweakey will be zn.

ize TK_1, TK_2, and TK_3, and only find a new LFSR for updating TK_4. With the expectation of keeping a similar security margin with 36-round SKINNY-64-128 and 40-round SKINNY-64-192, the authors decided to keep the same rate for increasing the number of rounds, namely 44 rounds for SKINNYe-64-256. However, Thomas Peyrin found that the security claim of SKINNYe-64-256 may not hold due to the tweakey schedule. Although the authors of SKINNYe-64-256 were unclear whether this issue causes some attacks against the whole cipher [50, Section 7], they proposed an updated version of SKINNYe-64-256, named as SKINNYe-64-256 v2 in Eprint 2020/542 [50].

Our Contributions. In this paper, we try to clarify the security issue of SKINNYe-64-256 [48] by delving into its new tweakey schedule. There are some previous works considered the relations of keys, such as the key-bridging technique [33,26]. The relations of subtweakeys for SKINNY and SKINNYe-64-256 are mostly dependent on the LFSR_m updating the cells of the tweakey states. For LFSR_2 used for TK_2 and LFSR_4 used for TK_4 of SKINNYe-64-256, both of them shift the 4-bit input to the left by 1 bit, while LFSR_2 updates 1 output bit with 1 XOR and LFSR_4 updates 2 output bits with 3 XORs. Suppose for a given cell of TK_2 and TK_4 with the initial value 0x8, then apply LFSR_2 and LFSR_4 respectively to the given cell for 14 times and we get two sequences, i.e.,

$$[\underline{0x8}, \underline{0x1}, \underline{0x2}, 0x4, \underline{0x9}, \underline{0x3}, 0x6, 0xd, \underline{0xa}, 0x5, \underline{0xb}, 0x7, 0xf, 0xe, 0xc],$$
$$[\underline{0x8}, \underline{0x1}, \underline{0x2}, 0x5, \underline{0x9}, \underline{0x3}, 0x7, 0xc, \underline{0xa}, 0x4, \underline{0xb}, 0x6, 0xe, 0xf, 0xd].$$

For example, run LFSR_2 or LFSR_4 on 0x8 for 3 times, we get LFSR_2^3(0x8)=0x4 and LFSR_4^3(0x8)=0x5, respectively. Intuitively, the longest common subsequence of the two sequences is [0x8,0x1,0x2,0x9,0x3,0xa,0xb] which is highlighted with underlines. In other words, when the initial values (or differences) for a given cell position of TK_2 and TK_4 are 0x8 and TK_1 and TK_3 are set to 0x0, the difference cancellations can happen 7 times within 15 LFSR applications.

In order to further clarify the cancellation property of the new tweakey schedule, we give a formal analysis of relations of subtweakeys. Since the tweakey schedule of SKINNYe-64-256 is linear, each cell of subtweakeys can be derived via multiplying some cells of the master tweakeys by certain binary matrix $\boldsymbol{A}$, which is determined by cell updating functions, i.e., LFSRs. The differential cancellation behavior means active input leads to zero output by multiplying $\boldsymbol{A}$. We analyze the properties of matrix $\boldsymbol{A}$, especially for the influence of its rank on the cancellations in the differential-like distinguishers, as well as the subtweakey guessing strategy in the key-recovery phase. For the differential cancellation behavior, we find the number of cancellations can be up to 8 within 30 consecutive rounds for SKINNYe-64-256 (a cell is updated by LFSR in every two rounds in SKINNY), which is significantly larger than the expected 3 cancellations. By exploring the properties of $\boldsymbol{A}$ in rectangle attack, meet-in-the-middle (MITM) attack and impossible differential attack, we discover unexpected distinguishers or key-recovery attacks:

- **Related-tweakey rectangle attacks.** The properties can not only extend the rectangle distinguisher significantly, but also improve the key-recovery phase. At EUROCRYPT 2022, Dong *et al.* [30] introduced the attacks on the 25-round SKINNY-64-128 with an 18-round distinguisher as well as the 31-round SKINNY-64-192 with a 22-round distinguisher. With our discoveries on SKINNYe-64-256, we find a 30-round rectangle distinguisher, where the gap between SKINNY-64-192 and SKINNYe-64-256 is significantly increased to 30-22=8 rounds comparing to 22-18=4 rounds between SKINNY-64-128 and SKINNY-64-192. Moreover, in the key-recovery phase, we explore the key relations in detail with the help of matrix $\boldsymbol{A}$, and finally perform a 41-round key-recovery attack on SKINNYe-64-256.

  In order to find the optimal configurations of the rectangle attack, we tweak Dong *et al.*'s automatic model by applying the properties of the new tweakey schedule into the model. Our attack leaves only a 3-round security margin for SKINNYe-64-256, which is significantly reduced comparing to the 11-round and 9-round security margins for SKINNY-64-128 and SKINNY-64-192.
- **MITM attacks in single-tweakey setting.** Not only the differential cancellation property can be used to improve attacks, but also the non-full rank property of $\boldsymbol{A}$. The MITM attack explores two independent chunks that overlap in a match point. Suppose $\boldsymbol{A}$ is of non-full rank, we compute the solution space of $\boldsymbol{Ax} = \boldsymbol{c}$ for given vector $\boldsymbol{c}$. In SKINNYe-64-256, $\boldsymbol{x}$ is the master tweakey bits and $\boldsymbol{c}$ is the subtweakey bits that will XORed into the internal state. Denote solution set as $\{\boldsymbol{x} : \boldsymbol{Ax} = \boldsymbol{c}\}$, if it is not empty, then its size will be $|\{\boldsymbol{x} : \boldsymbol{Ax} = \boldsymbol{c}\}| > 1$ due to non-full rank property of $\boldsymbol{A}$. In the MITM, those $\boldsymbol{x} \in \{\boldsymbol{x} : \boldsymbol{Ax} = \boldsymbol{c}\}$ will have the same effect on the internal states, i.e., the vector $\boldsymbol{c}$. When building independent forward and backward chunks in MITM, we may prefix $\boldsymbol{c}$ and $\boldsymbol{c}'$ for these two chunks, then the values in $\{\boldsymbol{x} : \boldsymbol{Ax} = \boldsymbol{c}\}$ and $\{\boldsymbol{y} : \boldsymbol{A}'\boldsymbol{y} = \boldsymbol{c}'\}$ will have independent effects.

  We adapt the previous automatic tools [7,29] for MITM attacks by taking the non-full rank properties of $\boldsymbol{A}$ into the model. Finally, we find 31-round MITM attack on SKINNYe-64-256, while previous MITM attacks on SKINNY-64-128 and SKINNY-64-192 reach 18 and 23 rounds, respectively. In other words, the gaps of the attacked rounds increase from 23-18=5 rounds between SKINNY-64-128 and SKINNY-64-192 to currently 31-23=8 rounds between SKINNY-64-192 and SKINNYe-64-256.
- **Related-tweakey impossible differential attack.** With the differential cancellation properties, we find a 21-round impossible differential for SKINNYe-64-256 based on a cancellation pattern, while previous impossible differential reaches 16 rounds [46] for SKINNY-64-192 and 15 rounds [56] for SKINNY-64-128, respectively.

Our cryptanalysis proves that SKINNYe-64-256 does not keep a similar security margin to SKINNY-64-128 and SKINNY-64-192 as expected by the designers. The non-trivial properties of the new tweakey schedule can be used to improve the attacks from the distinguishers to key-recovery.

In addition, we also analyze the updated version, i.e., SKINNYe-64-256 v2 [50], and obtain a 37-round related-tweakey rectangle attack, a 27-round MITM attack, as well as an 18-round impossible differential. Comparing to the attacks on SKINNY-64-128 and SKINNY-64-192, the attacked rounds on SKINNYe-64-256 v2 keep the same rate as expected by the designers. We summarize results on SKINNY-64 and SKINNYe-64-256 and its version 2 in Table 1 and Table 2.

Table 1: Rectangle attacks on SKINNY-64 and SKINNYe-64-256 and its version 2

Version	Rounds	Data	Time	Memory	Distinguisher	Setting	Ref.
SKINNY-64-128	23/36	$2^{60.54}$	$2^{120.7}$	$2^{60.9}$	19	RK	[37]
	24/36	$2^{61.67}$	$2^{96.83}$	2^{84}	18	RK	[54]
	25/36	$2^{61.67}$	$2^{118.43}$	$2^{64.26}$	18	RK	[30]
SKINNY-64-192	29/40	$2^{62.92}$	$2^{181.7}$	2^{80}	23	RK	[37]
	30/40	$2^{62.87}$	$2^{163.11}$	$2^{68.05}$	22	RK	[54]
	31/40	$2^{62.78}$	$2^{182.07}$	$2^{62.79}$	22	RK	[30]
SKINNYe-64-256	41/44	$2^{62.24}$	$2^{237.06}$	$2^{62.26}$	30	RK	Sect. 4.3
SKINNYe-64-256 v2	37/44	$2^{62.8}$	$2^{240.03}$	$2^{62.8}$	26	RK	Full Ver. [53]

Table 2: MITM attacks on SKINNY-64 and SKINNYe-64-256 and its version 2

Version	Rounds	Data	Time	Memory	Approach	Setting	Ref.
SKINNY-64-128	18/36	2^{16}	2^{124}	2^{4}	MITM	SK	[39]
SKINNY-64-192	23/40	2^{52}	2^{188}	2^{4}	MITM	SK	[29]
SKINNYe-64-256	31/44	2^{52}	2^{254}	2^{52}	MITM	SK	Full Ver. [53]
SKINNYe-64-256 v2	27/44	2^{52}	2^{252}	2^{52}	MITM	SK	Full Ver. [53]

Note that STK construction supports arbitrary length of tweakey, but SKINNY and SKINNYe-64-256 v2 supports upto $4n$-bit tweakey. As stated in [48, Page 5]: "... there is no consensus about the adequate tweak size to support". SKINNY with larger tweakey size may be useful in future applications, such as the TI-friendly AE modes PFB_Plus and PFBw with SKINNYe-64-256 v2. Therefore, as another contribution, we propose a uniformed design strategy for tweakey schedule of SKINNY-n-zn for positive integer $z \leq 14$. Our uniformed tweakey schedule satisfies the security requirements of the STK construction with a formal proof. Interestingly, our schedule will be reduced to SKINNY-64 when $z = 1, 2, 3$, and to SKINNYe-64-256 v2 when $z = 4$. In addition, we also discuss possible ways to extend the tweakey size for SKINNY-128.

2 Preliminaries

2.1 The TWEAKEY Framework

At ASIACRYPT 2014, Jean *et al.* [42] proposed a generic framework for tweakable block ciphers, named as the TWEAKEY framework. They consider the tweak and key inputs in a unified manner, i.e., tweakey, that can be used to design a tweakable block cipher with any key and any tweak sizes. The TWEAKEY framework uses the tweakey scheduling algorithm. The ciphertext is computed from the plaintext by applying the permutation f iteratively. Each round is composed of three parts, a sub-tweakey extraction function g from the tweakey state, an internal update permutation f and a tweakey state update function h. Based on the TWEAKEY framework, many designs of tweakable block ciphers are proposed, including Deoxys [43], SKINNY [9], and CRAFT [11], etc. Moreover, Jean *et al.* identified a subclass of tweakey for AES-like ciphers named as Superposition TWEAKEY (STK) construction shown in Figure 1. In the STK construction, the n-bit internal state and zn-bit tweakey state (denoted as TK-z) are partitioned into n/c and zn/c c-bit cells respectively. The functions g and h become:

- the function g simply XORs all the z n-bit words of the tweakey state to the internal state (AddRoundTweakey, denoted ART).
- the function h first applies the same cell position permutation function P to each of the z n-bit words of the tweakey state, and then multiply each c-bit cell of the j-th n-bit word by a nonzero coefficient α_j in the finite field $GF(2^c)$ (with $\alpha_i \neq \alpha_j$ for all $1 \leq i \neq j \leq z$).

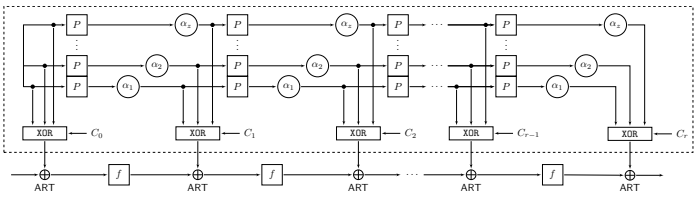

Fig. 1: The STK [42]. (Thanks to https://www.iacr.org/authors/tikz/)

2.2 SKINNY family and SKINNYe-64-256

SKINNY is a family of lightweight block cipher proposed by Beierle *et al.* at CRYPTO 2016 [9]. Following the TWEAKEY framework and STK construction [42], the round function of SKINNY that replaces the f function of STK in Figure 1 is given in Figure 2. There are six main versions SKINNY-n-zn: $n = 64, 128$, $z = 1, 2, 3$. The internal state is viewed as a 4×4 square arrays of cells. The tweakey state is viewed as z 4×4 square arrays of cells, denoted as (TK_1) when $z = 1$,

(TK_1, TK_2) when $z = 2$, and (TK_1, TK_2, TK_3) when $z = 3$. Denote the i-th cell of TK_m as $TK_{m,i}$ $(1 \le m \le z,\ 0 \le i \le 15)$. An important difference between the STK construction [42] and SKINNY is that in the tweakey schedule the cells of the tweakey are updated by LFSRs for SKINNY instead of multiplying α_j. As shown in Figure 2, the round function applies 5 transformations: SubCells (SC), AddConstants (AC), AddRoundTweakey (ART), ShiftRows (SR) and MixColumns (MC). For the details, please refer to [9].

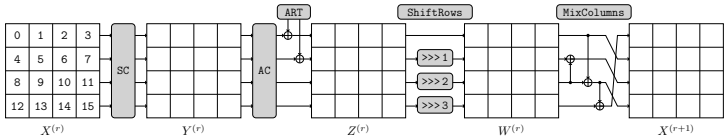

Fig. 2: Round function of SKINNY

For the block size $n = 64$, SKINNY supports the tweakey sizes up to 192 bits. At EUROCRYPT 2020, to support the TI-friendly AE modes PFB_Plus and PFBw, Naito, Sasaki, and Sugawara [48] extended the design of SKINNY-64 to support a 256-bit tweakey and derived SKINNYe-64-256, which applies the same round function of SKINNY but a new tweakey schedule. However, Thomas Peyrin found that the security claim of SKINNYe-64-256 may not hold due to the new tweakey schedule. In response, Naito *et al.* decided to propose an updated version of SKINNYe-64-256, i.e., SKINNYe-64-256 v2 in Eprint 2020/542 [50].

New Tweakey Schedule. The 256-bit tweakey state is viewed as 4 4×4 square arrays of nibbles as (TK_1, TK_2, TK_3, TK_4). Denote the tweakey arrays as $TK_1^{(r)}$, $TK_2^{(r)}$, $TK_3^{(r)}$ and $TK_4^{(r)}$ in round r $(r \ge 0)$, where $TK_m^{(0)} = TK_m$ $(1 \le m \le 4)$. For $r \ge 1$, $TK_m^{(r)}$ is generated in two steps.

First, apply the permutation $P = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$ on each nibble of all tweakey arrays:

$$TK_{m,i}^{(r)} \leftarrow TK_{m,P[i]}^{(r-1)},\ 1 \le m \le 4,\ 0 \le i \le 15, r \ge 1. \tag{1}$$

Then, apply LFSR_m to update each nibble of the first and second rows of $TK_m^{(r)}$ with $2 \le m \le 4$. The LFSR for $TK_4^{(r)}$ used in SKINNYe-64-256 and SKINNYe-64-256 v2 is different. The LFSRs are given in Table 3.

In the ART operation, only the first two rows of subtweakey $STK^{(r)}$ are xored to the internal state, where

$$STK_i^{(r)} = TK_{1,i}^{(r)} \oplus TK_{2,i}^{(r)} \oplus TK_{3,i}^{(r)} \oplus TK_{4,i}^{(r)}, 0 \le i \le 7,\ r \ge 0. \tag{2}$$

Lemma 1. *For any given* SKINNY *S-box S and any two non-zero differences δ_{in} and δ_{out}, the equation $S_i(y) \oplus S_i(y \oplus \delta_{in}) = \delta_{out}$ has one solution on average.*

Table 3: The LFSRs used in SKINNYe-64-256 and SKINNYe-64-256 v2

TK	LFSRs
TK_2	$(x_3\|x_2\|x_1\|x_0) \rightarrow (x_2\|x_1\|x_0\|x_3 \oplus x_2)$
TK_3	$(x_3\|x_2\|x_1\|x_0) \rightarrow (x_0 \oplus x_3\|x_3\|x_2\|x_1)$
TK_4	$(x_3\|x_2\|x_1\|x_0) \rightarrow (x_2\|x_1\|x_2 \oplus x_0\|x_3 \oplus x_2 \oplus x_1)$
TK_4 v2	$(x_3\|x_2\|x_1\|x_0) \rightarrow (x_1\|x_0\|x_3 \oplus x_2\|x_2 \oplus x_1)$

3 Properties of the Tweakey Schedule of SKINNYe-64-256

In round $r \geq 0$, each of the 64-bit tweakey $TK_m^{(r)}$ ($1 \leq m \leq 4$) of SKINNYe-64-256 can be represented as a 4×16 binary matrix $\boldsymbol{TK}_m^{(r)}$ $(1 \leq m \leq 4,\ r \geq 0)$ as

$$\boldsymbol{TK}_m^{(r)} = \begin{pmatrix} x_{m,0}^{(r)} & x_{m,4}^{(r)}, \ldots, x_{m,60}^{(r)} \\ x_{m,1}^{(r)} & x_{m,5}^{(r)}, \ldots, x_{m,61}^{(r)} \\ x_{m,2}^{(r)} & x_{m,6}^{(r)}, \ldots, x_{m,62}^{(r)} \\ x_{m,3}^{(r)} & x_{m,7}^{(r)}, \ldots, x_{m,63}^{(r)} \end{pmatrix},$$

with $x_{m,j}^{(r)} \in \{0,1\}$ $(0 \leq j \leq 63)$. Denote $\boldsymbol{TK}_m^{(r)}[*,i]$ as the i-th column of the binary matrix $\boldsymbol{TK}_m^{(r)}$. Then $\boldsymbol{TK}_m^{(r)}[*,i]$ is actually the i-th nibble of $TK_m^{(r)}$, *i.e.*, $TK_{m,i}^{(r)}$ $(0 \leq i \leq 15)$, which is denoted as a binary vector $\boldsymbol{tk}_{m,i}^{(r)} \in \mathbb{F}_2^4$,

$$\boldsymbol{tk}_{m,i}^{(r)} = [x_{m,4i}^{(r)}, x_{m,4i+1}^{(r)}, x_{m,4i+2}^{(r)}, x_{m,4i+3}^{(r)}]^T,\ 0 \leq i \leq 15,\ 1 \leq m \leq 4, r \geq 0.$$

Since $TK_m^{(0)} = TK_m$, we also write $\boldsymbol{tk}_{m,i}^{(0)} = [x_{m,4i}, x_{m,4i+1}, x_{m,4i+2}, x_{m,4i+3}]^T$ for simplicity. We can deduce the relations between the subtweakeys transformed from the same nibble of the master tweakey. For TK_1, only the permutation P is applied in each round. Assume P^r means to apply the permutation P for r times. We have $\boldsymbol{tk}_{1,i}^{(r)} = \boldsymbol{tk}_{1,P^r[i]}^{(0)},\ 0 \leq i \leq 15$.

For TK_2, TK_3 and TK_4, after applying the permutation, a LFSR is applied to update each cell of the 1st and 2nd rows in each round, which is equivalent to multiplying the cell by a 4×4 binary matrix. For SKINNYe-64-256 and its version 2, the LFSRs used for TK_2 and TK_3 are the same, whose corresponding matrices are denoted as $\boldsymbol{L}_2$ and $\boldsymbol{L}_3$. The LFSRs used in TK_4 for SKINNYe-64-256 and version 2 are different, which are denoted as $\boldsymbol{L}_4$ and $\tilde{\boldsymbol{L}}_4$. We have

$$\boldsymbol{L}_2 = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&1&0&0 \end{pmatrix},\ \boldsymbol{L}_3 = \begin{pmatrix} 1&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \end{pmatrix},\ \boldsymbol{L}_4 = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&1&0&1 \\ 1&1&1&0 \end{pmatrix},\ \tilde{\boldsymbol{L}}_4 = \begin{pmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&1&0&0 \\ 0&1&1&0 \end{pmatrix}.$$

Since only the first two rows of subtweakey are XORed to the internal state, the tweakey cells involved in the r-th round encryption will be involved again in the $(r+2)$-th round according to $P = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$. For simplicity, we first consider the formulas of subtweakeys for SKINNYe-64-256,

and for version 2, the formulas are different only for TK_4. Assume $\boldsymbol{L}_m^i$ represents the i-th power of matrix $\boldsymbol{L}_m$ in $GF(2)$ and $\boldsymbol{L}_m^0 = \boldsymbol{I}$ $(2 \le m \le 4)$. Note that the LFSRs for TK_2 and TK_3 in SKINNY and the new LFSR for TK_4 in SKINNYe-64-256 have the same cycle of 15, which lead to $\boldsymbol{L}_m^{15} = \boldsymbol{I}$ $(2 \le m \le 4)$. For SKINNYe-64-256 v2, although the update function for TK_4 is not a LFSR, it also has a cycle of 15, i.e., $\tilde{\boldsymbol{L}}_4^{15} = \boldsymbol{I}$. In the tweakey schedule, for each nibble of $TK_m^{(r)}$, the LFSR is applied in every two rounds, we deduce: $\forall m \in \{2,3,4\}$,

$$\begin{cases} \boldsymbol{tk}_{m,i}^{(r)} = \boldsymbol{L}_m^{\lceil r/2 \rceil} \cdot \boldsymbol{tk}_{m,P^r[i]}^{(0)}, \ 0 \le i \le 7, \\ \boldsymbol{tk}_{m,i}^{(r)} = \boldsymbol{L}_m^{\lfloor r/2 \rfloor} \cdot \boldsymbol{tk}_{m,P^r[i]}^{(0)}, \ 8 \le i \le 15. \end{cases}$$

Denote the nibble $STK_i^{(r)}$ $(0 \le i \le 7)$ as a binary vector $\boldsymbol{stk}_i^{(r)} = (y_{4i}^{(r)}, y_{4i+1}^{(r)}, y_{4i+2}^{(r)}, y_{4i+3}^{(r)})^T$. Then we obtain $\boldsymbol{stk}_i^{(r)} = \bigoplus_{m=1}^{4} \boldsymbol{tk}_{m,i}^{(r)}$ for $0 \le i \le 7$. Considering subtweakey cells $\boldsymbol{stk}_i^{(r)}$ derived from master tweakey, we get

$$\boldsymbol{stk}_i^{(r)} = [\boldsymbol{I} \ \boldsymbol{L_2}^{\lceil r/2 \rceil} \ \boldsymbol{L_3}^{\lceil r/2 \rceil} \ \boldsymbol{L_4}^{\lceil r/2 \rceil}] \cdot \left(\boldsymbol{tk}_{1,P^r[i]}^{(0)}, \boldsymbol{tk}_{2,P^r[i]}^{(0)}, \boldsymbol{tk}_{3,P^r[i]}^{(0)}, \boldsymbol{tk}_{4,P^r[i]}^{(0)}\right)^T. \quad (3)$$

Without losing generality, we analyze the subtweakeys in the even rounds, which are all transformed from the first two rows of master tweakeys. Let $\bar{P} = [8,9,10,11,\ 12,13,14,15,2,0,4,7,6,3,5,1]$ be the inverse permutation of P. For a set $\texttt{Index} = \{r_1, \cdots, r_t\}$ $(|\texttt{Index}| = t)$, which corresponding to a set of subtweakeys $\{STK^{(2r_1)}, STK^{(2r_2)} \cdots, STK^{(2r_t)}\}$, we can get a set of linear equations as

$$\begin{pmatrix} \boldsymbol{stk}_{\bar{P}^{2r_1}[i]}^{(2r_1)} \\ \boldsymbol{stk}_{\bar{P}^{2r_2}[i]}^{(2r_2)} \\ \vdots \\ \boldsymbol{stk}_{\bar{P}^{2r_t}[i]}^{(2r_t)} \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{L}_2^{r_1} & \boldsymbol{L}_3^{r_1} & \boldsymbol{L}_4^{r_1} \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_2} & \boldsymbol{L}_3^{r_2} & \boldsymbol{L}_4^{r_2} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_t} & \boldsymbol{L}_3^{r_t} & \boldsymbol{L}_4^{r_t} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{tk}_{1,i}^{(0)} \\ \boldsymbol{tk}_{2,i}^{(0)} \\ \boldsymbol{tk}_{3,i}^{(0)} \\ \boldsymbol{tk}_{4,i}^{(0)} \end{pmatrix}, \ 0 \le i \le 7. \quad (4)$$

Because the tweakey schedule only contains the permutation and LFSRs, Equation (4) is linear equation. Denote coefficient matrix as $\boldsymbol{A}$ and its rank as $rank(\boldsymbol{A}) = a$. The image space of $\boldsymbol{A}$ represents the solution space of $\{STK_{\bar{P}^{2r_1}[i]}^{(2r_1)}, STK_{\bar{P}^{2r_2}[i]}^{(2r_2)} \cdots, STK_{\bar{P}^{2r_t}[i]}^{(2r_t)}\}$ with arbitrary $\{\boldsymbol{tk}_{1,i}^{(0)}, \boldsymbol{tk}_{2,i}^{(0)}, \boldsymbol{tk}_{3,i}^{(0)}, \boldsymbol{tk}_{4,i}^{(0)}\}$, whose size is $|Im(\boldsymbol{A})| = 2^a$. Let the kernel space of $\boldsymbol{A}$ be $Ker(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{F}_2^{4t} : \boldsymbol{Ax} = 0\}$, then the size of the kernel space is $|Ker(\boldsymbol{A})| = 2^{16-a}$. For example, assuming $\texttt{Index} = \{0,1,2,3\}$, we can obtain the equations of $\{STK^{(0)}, STK^{(2)}, STK^{(4)},$

$STK^{(6)}\}$ as Equation (4). For $i = 0$, there is

$$\begin{pmatrix} \boldsymbol{stk}_0^{(0)} \\ \boldsymbol{stk}_2^{(2)} \\ \boldsymbol{stk}_4^{(4)} \\ \boldsymbol{stk}_6^{(6)} \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{L}_2^0 & \boldsymbol{L}_3^0 & \boldsymbol{L}_4^0 \\ \boldsymbol{I} & \boldsymbol{L}_2^1 & \boldsymbol{L}_3^1 & \boldsymbol{L}_4^1 \\ \boldsymbol{I} & \boldsymbol{L}_2^2 & \boldsymbol{L}_3^2 & \boldsymbol{L}_4^2 \\ \boldsymbol{I} & \boldsymbol{L}_2^3 & \boldsymbol{L}_3^3 & \boldsymbol{L}_4^3 \end{pmatrix} \begin{pmatrix} \boldsymbol{tk}_{1,0}^{(0)} \\ \boldsymbol{tk}_{2,0}^{(0)} \\ \boldsymbol{tk}_{3,0}^{(0)} \\ \boldsymbol{tk}_{4,0}^{(0)} \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \\ 1&0&0&0&0&1&0&0&1&0&0&1&0&1&0&0 \\ 0&1&0&0&0&0&1&0&1&0&0&0&0&0&1&0 \\ 0&0&1&0&0&0&0&1&0&1&0&0&0&1&0&1 \\ 0&0&0&1&1&1&0&0&0&0&1&0&1&1&1&0 \\ 1&0&0&0&0&0&1&0&1&0&1&1&0&0&1&0 \\ 0&1&0&0&0&0&0&1&1&0&0&1&0&1&0&1 \\ 0&0&1&0&1&1&0&0&1&0&0&0&1&1&0&0 \\ 0&0&0&1&0&1&1&0&0&1&0&0&0&0&1&1 \\ 1&0&0&0&0&0&0&1&1&1&1&1&0&1&0&1 \\ 0&1&0&0&1&1&0&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&0&1&0&1&1&0 \\ 0&0&0&1&0&0&1&1&1&0&0&0&1&0&1&1 \end{pmatrix} \begin{pmatrix} x_{1,0} \\ x_{1,1} \\ x_{1,2} \\ x_{1,3} \\ x_{2,0} \\ x_{2,1} \\ x_{2,2} \\ x_{2,3} \\ x_{3,0} \\ x_{3,1} \\ x_{3,2} \\ x_{3,3} \\ x_{4,0} \\ x_{4,1} \\ x_{4,2} \\ x_{4,3} \end{pmatrix}. \quad (5)$$

The rank of the coefficient matrix $\boldsymbol{A}$ in Equation (5) is 14. Therefore, the size of its kernel space and image space is $|Ker(\boldsymbol{A})| = 2^2$ and $|Im(\boldsymbol{A})| = 2^{14}$.

Let $\boldsymbol{A}_{r_j} = [\boldsymbol{I}\ \boldsymbol{L}_2^{r_j}\ \boldsymbol{L}_3^{r_j}\ \boldsymbol{L}_4^{r_j}]$, which is a 4×16 matrix. Then the coefficient matrix of Equation (4) can be represented as $\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}} = [\boldsymbol{A}_{r_1}^T\ \boldsymbol{A}_{r_2}^T\ \cdots\ \boldsymbol{A}_{r_t}^T]^T$, which is a $4t \times 16$ matrix. Since $\boldsymbol{L}_i^{15} = \boldsymbol{I}$ for $2 \le i \le 4$, we can assume that all subscripts of $\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}$ are mod 15. We call $\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}$ a full rank matrix if and only if $rank(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}) = \min\{4t, 16\}$. We find that when $t \ge 4$, certain sets of `Index` lead to non-full rank coefficient matrices. Let $\mathcal{K} = \{0, 1, 2, \cdots, 14\}$, for any subset $\{r_1, r_2, \cdots, r_t\} \subset \mathcal{K}$ and $0 \le r' \le 14$, we have

$$\begin{aligned} &\boldsymbol{A}_{\{r_1+r',r_2+r',\cdots,r_t+r'\}} \\ &= \begin{pmatrix} \boldsymbol{I} & \boldsymbol{L}_2^{r_1+r'} & \boldsymbol{L}_3^{r_1+r'} & \boldsymbol{L}_4^{r_1+r'} \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_2+r'} & \boldsymbol{L}_3^{r_2+r'} & \boldsymbol{L}_4^{r_2+r'} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_t+r'} & \boldsymbol{L}_3^{r_t+r'} & \boldsymbol{L}_4^{r_t+r'} \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{L}_2^{r_1} & \boldsymbol{L}_3^{r_1} & \boldsymbol{L}_4^{r_1} \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_2} & \boldsymbol{L}_3^{r_2} & \boldsymbol{L}_4^{r_2} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_t} & \boldsymbol{L}_3^{r_t} & \boldsymbol{L}_4^{r_t} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{I} & & & \\ & \boldsymbol{L}_2^{r'} & & \\ & & \boldsymbol{L}_3^{r'} & \\ & & & \boldsymbol{L}_4^{r'} \end{pmatrix} \quad (6) \\ &= \boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}} \cdot diag(\boldsymbol{I}, \boldsymbol{L}_2^{r'}, \boldsymbol{L}_3^{r'}\ \boldsymbol{L}_4^{r'}). \end{aligned}$$

Since $\boldsymbol{L}_2$, $\boldsymbol{L}_3$ and $\boldsymbol{L}_4$ are all 4×4 full rank matrices, $D_{r'} = diag(\boldsymbol{I}, \boldsymbol{L}_2^{r'}, \boldsymbol{L}_3^{r'}\ \boldsymbol{L}_4^{r'})$ is a 16×16 full rank matrix. Then we can deduce that

$$rank(\boldsymbol{A}_{\{r_1+r',r_2+r',\cdots,r_t+r'\}}) = rank(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}). \quad (7)$$

Since the rank of the coefficient matrix is our most concern, we introduce the concept of *rank-equivalent* as follows.

Definition 1 (rank-equivalent). *Given two subsets $x = \{r_1, r_2, \ldots, r_t\}$, $y = \{r'_1, r'_2, \ldots, r'_t\} \subset \mathcal{K}$, we say x and y are rank-equivalent if there exits an integer r' such that*

$$r_i \equiv r'_i + r' \bmod 15 \text{ for all } 1 \le i \le t.$$

The rank-equivalence class of the subset x is defined by

$$[x] := \{y \subset \mathcal{K} : x \text{ and } y \text{ are rank-equivalent}\}.$$

From Eq. (7), $rank(\boldsymbol{A}_x) = rank(\boldsymbol{A}_y)$ holds for any rank-equivalent subsets x and y.

Table 4: Rank-equivalence class of non-full rank coefficient matrix for SKINNYe-64-256

rank	t	Rank-equivalence class $[\{r_1, r_2, \cdots, r_t\}]$
14	4	[{0,1,2,3}],[{0,1,2,10}],[{0,1,3,4}],[{0,1,3,7}],[{0,1,3,13}],[{0,1,4,5}],[{0,1,4,12}], [{0,1,5,6}],[{0,1,5,8}],[{0,1,5,11}],[{0,1,6,7}],[{0,1,6,10}],[{0,1,6,12}],[{0,1,7,8}], [{0,1,7,9}],[{0,1,11,13}],[{0,2,4,6}],[{0,2,5,7}],[{0,2,5,12}],[{0,2,6,8}],[{0,2,6,11}], [{0,2,7,9}],[{0,2,7,10}],[{0,2,7,11}],[{0,2,9,12}],[{0,3,6,9}],[{0,3,7,10}],[{0,3,7,11}]
15	4	[{0,1,2,4}],[{0,1,2,5}],[{0,1,2,6}],[{0,1,2,7}],[{0,1,2,8}],[{0,1,2,9}],[{0,1,2,11}], [{0,1,2,12}],[{0,1,2,13}],[{0,1,3,5}],[{0,1,3,6}],[{0,1,3,8}],[{0,1,3,9}],[{0,1,3,10}], [{0,1,3,11}],[{0,1,3,12}],[{0,1,4,6}],[{0,1,4,7}],[{0,1,4,8}],[{0,1,4,9}],[{0,1,4,10}], [{0,1,4,11}],[{0,1,4,13}],[{0,1,5,7}],[{0,1,5,9}],[{0,1,5,10}],[{0,1,5,12}],[{0,1,5,13}], [{0,1,6,8}],[{0,1,6,9}],[{0,1,6,11}],[{0,1,6,13}],[{0,1,7,10}],[{0,1,7,11}],[{0,1,7,12}], [{0,1,7,13}],[{0,1,8,10}],[{0,1,8,11}],[{0,1,8,12}],[{0,1,8,13}],[{0,1,9,11}],[{0,1,9,12}], [{0,1,9,13}],[{0,1,10,12}],[{0,1,10,13}],[{0,2,4,7}],[{0,2,4,8}],[{0,2,4,9}],[{0,2,4,10}], [{0,2,4,11}],[{0,2,4,12}],[{0,2,5,8}],[{0,2,5,9}],[{0,2,5,10}],[{0,2,5,11}],[{0,2,6,9}], [{0,2,6,10}],[{0,2,6,12}],[{0,2,7,12}],[{0,2,8,11}],[{0,2,8,12}],[{0,3,6,10}],[{0,3,6,11}]
	5	[{0,1,2,3,7}],[{0,1,2,3,10}],[{0,1,2,3,11}],[{0,1,2,3,13}],[{0,1,2,4,5}],[{0,1,2,4,8}], [{0,1,2,4,10}],[{0,1,2,5,8}],[{0,1,2,5,10}],[{0,1,2,6,9}],[{0,1,2,6,10}],[{0,1,2,6,12}], [{0,1,2,7,10}],[{0,1,2,7,11}],[{0,1,2,7,13}],[{0,1,2,8,10}],[{0,1,2,9,10}],[{0,1,2,9,12}], [{0,1,2,10,11}],[{0,1,2,10,12}],[{0,1,2,10,13}],[{0,1,2,11,13}],[{0,1,3,4,7}],[{0,1,3,4,9}], [{0,1,3,5,6}],[{0,1,3,5,7}],[{0,1,3,5,8}],[{0,1,3,5,12}],[{0,1,3,6,7}],[{0,1,3,6,8}], [{0,1,3,6,12}],[{0,1,3,7,8}],[{0,1,3,7,9}],[{0,1,3,7,10}],[{0,1,3,7,11}],[{0,1,3,7,12}], [{0,1,3,7,13}],[{0,1,3,8,12}],[{0,1,3,10,11}],[{0,1,3,10,13}],[{0,1,3,11,13}],[{0,1,4,5,8}], [{0,1,4,5,10}],[{0,1,4,6,11}],[{0,1,4,6,12}],[{0,1,4,6,13}],[{0,1,4,7,9}],[{0,1,4,8,10}], [{0,1,4,11,13}],[{0,1,5,6,12}],[{0,1,5,7,8}],[{0,1,5,7,12}],[{0,1,5,8,9}],[{0,1,5,8,10}], [{0,1,5,8,11}],[{0,1,5,8,12}],[{0,1,5,8,13}],[{0,1,5,9,11}],[{0,1,5,9,13}],[{0,1,5,11,13}], [{0,1,6,7,12}],[{0,1,6,8,12}],[{0,1,6,9,12}],[{0,1,6,10,12}],[{0,1,6,11,13}],[{0,1,7,10,13}], [{0,1,7,11,13}],[{0,1,8,11,13}],[{0,1,9,11,13}],[{0,2,4,6,11}],[{0,2,4,7,11}],[{0,2,4,8,10}], [{0,2,4,9,12}],[{0,2,5,7,11}],[{0,2,5,8,10}],[{0,2,5,9,12}],[{0,2,6,9,12}]
	6	[{0,1,2,3,7,10}],[{0,1,2,3,7,11}],[{0,1,2,3,7,13}],[{0,1,2,3,10,11}],[{0,1,2,3,10,13}], [{0,1,2,3,11,13}],[{0,1,2,4,5,8}],[{0,1,2,4,5,10}],[{0,1,2,4,8,10}],[{0,1,2,5,8,10}], [{0,1,2,6,9,10}],[{0,1,2,6,9,12}],[{0,1,2,6,10,12}],[{0,1,2,7,10,11}],[{0,1,2,7,10,13}], [{0,1,2,7,11,13}],[{0,1,2,9,10,12}],[{0,1,2,10,11,13}],[{0,1,3,4,7,9}],[{0,1,3,5,6,8}], [{0,1,3,5,6,12}],[{0,1,3,5,7,8}],[{0,1,3,5,7,12}],[{0,1,3,5,8,12}],[{0,1,3,6,7,12}], [{0,1,3,6,8,12}],[{0,1,3,7,8,12}],[{0,1,3,7,10,11}],[{0,1,3,7,10,13}],[{0,1,3,7,11,13}], [{0,1,4,5,8,10}],[{0,1,4,6,11,13}],[{0,1,5,7,8,12}],[{0,1,5,8,11,13}],[{0,1,5,9,11,13}]
	7	[{0,1,2,3,7,10,11}],[{0,1,2,3,7,10,13}],[{0,1,2,3,7,11,13}],[{0,1,2,3,10,11,13}], [{0,1,2,4,5,8,10}],[{0,1,2,6,9,10,12}],[{0,1,2,7,10,11,13}],[{0,1,3,5,6,8,12}], [{0,1,3,5,7,8,12}]
	8	[{0,1,2,3,7,10,11,13}]

For SKINNYe-64-256, we compute all the rank-equivalence classes whose corresponding coefficient matrix is non-full rank with Algorithm 1 in Supplementary Material A in our full version paper [53] and list the results in Table 4.

Similarly, for SKINNYe-64-256 v2, we set $\tilde{\boldsymbol{A}}_{r_j} = [\boldsymbol{I}\ \boldsymbol{L_2}^{r_j}\ \boldsymbol{L_3}^{r_j}\ \tilde{\boldsymbol{L}}_{\boldsymbol{4}}^{r_j}]$, which is also a 4×16 matrix. Then the coefficient matrix of Equation (4) can be represented as $\tilde{\boldsymbol{A}}_{\{r_1,r_2,\cdots,r_t\}} = [\tilde{\boldsymbol{A}}_{r_1}^T\ \tilde{\boldsymbol{A}}_{r_2}^T\ \cdots\ \tilde{\boldsymbol{A}}_{r_t}^T]^T$, which is a $4t \times 16$ matrix. For arbitrary $\{r_1, r_2, \cdots, r_t\} \subset \mathcal{K}$, the matrix $\tilde{\boldsymbol{A}}_{\{r_1,r_2,\cdots,r_t\}}$ is full rank. That is, when $t \leq 4$, the rank of $\tilde{\boldsymbol{A}}_{\{r_1,r_2,\cdots,r_t\}}$ is $4t$, otherwise the rank is 16.

The Subtweakey Difference Cancellations. For a given active tweakey cell, $z-1$ subtweakey difference cancellation happens every 30 rounds for SKINNY-n-zn [9] with $z = 2, 3$. However, for SKINNYe-64-256, although $z = 4$, we have more cancellations than $z - 1 = 3$. Since the tweakey schedule is linear, the differences of subtweakeys can be computed by the differences injected in the master tweakey with Equation (4). Assume that there is at least one $1 \le m \le 4$ that $\Delta TK_{m,i} \neq 0$. Set $\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t\}]} \cdot [\boldsymbol{tk}^{(0)}_{1,i}, \boldsymbol{tk}^{(0)}_{2,i}, \boldsymbol{tk}^{(0)}_{3,i}, \boldsymbol{tk}^{(0)}_{4,i}]^T = \mathbf{0}$, which means the subtweakey difference cancellations happen at $\{STK^{(2r_1)}_{\bar{P}^{2r_1}[i]} \cdots, STK^{(2r_t)}_{\bar{P}^{2r_t}[i]}\}$ if $0 \le i \le 7$, or $\{STK^{(2r_1+1)}_{\bar{P}^{2r_1+1}[i]} \cdots, STK^{(2r_t+1)}_{\bar{P}^{2r_t+1}[i]}\}$ if $8 \le i \le 15$. When $rank(\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t\}]}) = 16$, the size of its kernel space is 1. Then $[\boldsymbol{tk}^{(0)}_{1,i}, \boldsymbol{tk}^{(0)}_{2,i}, \boldsymbol{tk}^{(0)}_{3,i}, \boldsymbol{tk}^{(0)}_{4,i}]$ has only one zero solution, which means $\Delta TK_{m,i} = 0$ for all $m = 1, 2, 3, 4$. When $rank(\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t\}]}) < 16$, we have non-zero solutions for $\Delta TK_{m,i}$, i.e., the subtweakey difference cancellations happen. Obviously, when $t \le 3$, $rank(\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t\}]}) = 4t \le 16$. For $t \ge 4$, we obtain all rank-equivalence classes whose corresponding coefficient matrices are non-full rank from Table 4. So each rank-equivalence class corresponds to a set of positions of the subtweakey difference cancellations. We find several properties of the rank-equivalence classes:

- When $t = 4$, we find the matrix $A_{\{r_1,r_2,r_3,r_4\}}$ with arbitrary $\{r_1, r_2, r_3, r_4\} \subset \mathcal{K}$ is non-full rank. That is, for the given active nibbles in the master key, the subtweakey difference cancellations can happen four times in arbitrary round for every 30 rounds. Especially for $rank(\boldsymbol{A}_{\{0,1,2,3\}}) = 14$ and $|Ker(\boldsymbol{A}_{\{0,1,2,3\}})| = 2^2$, there are 3 non-zero solutions of the difference for the active nibbles of the master tweakey. For SKINNYe-64-256, there can be nine consecutive rounds with fully inactive internal states.
- When $t \ge 5$, for all $[\{r_1, r_2, \cdots, r_t\}]$ in Table 4, $rank(\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t\}]}) = 15$. For $\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t]\}} \cdot [\boldsymbol{tk}^{(0)}_{1,i}, \boldsymbol{tk}^{(0)}_{2,i}, \boldsymbol{tk}^{(0)}_{3,i}, \boldsymbol{tk}^{(0)}_{4,i}]^T = \mathbf{0}$, there is only one nonzero solution. We find that for some different rank-equivalence classes, the solutions are the same. For example, for rank-equivalence classes $[\{0, 1, 2, 7, 10\}]$ and $[\{0, 1, 3, 11, 13\}]$, when $0 \le i \le 7$ we set

$$A_{[\{0,1,2,7,10\}]} \cdot [\boldsymbol{tk}^{(0)}_{1,i}, \boldsymbol{tk}^{(0)}_{2,i}, \boldsymbol{tk}^{(0)}_{3,i}, \boldsymbol{tk}^{(0)}_{4,i}]^T = \mathbf{0}, \tag{8}$$

$$A_{[\{0,1,3,11,13\}]} \cdot [\boldsymbol{tk}^{(0)}_{1,i}, \boldsymbol{tk}^{(0)}_{2,i}, \boldsymbol{tk}^{(0)}_{3,i}, \boldsymbol{tk}^{(0)}_{4,i}]^T = \mathbf{0}, \tag{9}$$

  where the cancellations happen at $\{STK^{(0)}_i, STK^{(2)}_{\bar{P}^2[i]}, STK^{(4)}_{\bar{P}^4[i]}, STK^{(14)}_{\bar{P}^{14}[i]}, STK^{(20)}_{\bar{P}^{20}[i]}\}$ for Equation (8) and $\{STK^{(0)}_i, STK^{(2)}_{\bar{P}^2[i]}, STK^{(6)}_{\bar{P}^6[i]}, STK^{(22)}_{\bar{P}^{22}[i]}, STK^{(26)}_{\bar{P}^{26}[i]}\}$ for Equation (9). The non-zero solutions of both two linear equations are $\boldsymbol{tk}^{(0)}_{1,i} = [0, 0, 0, 1]^T$, $\boldsymbol{tk}^{(0)}_{2,i} = [0, 1, 1, 1]^T$, $\boldsymbol{tk}^{(0)}_{3,i} = [0, 0, 0, 0]^T$, $\boldsymbol{tk}^{(0)}_{4,i} = [0, 1, 1, 0]^T$. Namely, the cancellations happen at $\{STK^{(0)}_i, STK^{(2)}_{\bar{P}^2[i]}, STK^{(4)}_{\bar{P}^4[i]}, STK^{(6)}_{\bar{P}^6[i]}, STK^{(14)}_{\bar{P}^{14}[i]}, STK^{(20)}_{\bar{P}^{20}[i]}, STK^{(22)}_{\bar{P}^{22}[i]}, STK^{(26)}_{\bar{P}^{26}[i]}\}$ at the same time, which corresponds to the rank-equivalence class $[\{0, 1, 2, 3, 7, 10, 11, 13\}]$.

The situation for $8 \leq i \leq 15$ is the same. Further, we find that for arbitrary $\{r_1, r_2, \cdots, r_t\} \subset \{0, 1, 2, 3, 7, 10, 11, 13\}$ $(t \geq 5)$, the solution of $\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t\}]} \cdot [\boldsymbol{tk}_{1,i}^{(0)}, \boldsymbol{tk}_{2,i}^{(0)}, \boldsymbol{tk}_{3,i}^{(0)}, \boldsymbol{tk}_{4,i}^{(0)}]^T = \mathbf{0}$ is the same to $A_{[\{0,1,2,3,7,10,11,13\}]} \cdot [\boldsymbol{tk}_{1,i}^{(0)}, \boldsymbol{tk}_{2,i}^{(0)}, \boldsymbol{tk}_{3,i}^{(0)}, \boldsymbol{tk}_{4,i}^{(0)}]^T = \mathbf{0}$, which means that there is only one difference cancellation behaviour for those rank-equivalence classes.

Remark. It is worth noting that there are some rank-equivalence classes $[\{r_1, r_2, \cdots, r_t\}]$ in Table 4, where $\{r_1, r_2, \cdots, r_t\}$ is not directly the subset of $\{0, 1, 2, 3, 7, 10, 11, 13\}$ but corresponds to the same difference cancellation behaviour. Taking the rank-equivalence class $[\{0, 1, 2, 6, 9\}]$ as an example, we can assume $A_{[\{0,1,2,6,9\}]} \cdot [\bar{\boldsymbol{tk}}_{1,i}^{(0)}, \bar{\boldsymbol{tk}}_{2,i}^{(0)}, \bar{\boldsymbol{tk}}_{3,i}^{(0)}, \bar{\boldsymbol{tk}}_{4,i}^{(0)}]^T = \mathbf{0}$, and obtain $\bar{\boldsymbol{tk}}_{1,i}^{(0)} = [0, 0, 0, 1]^T$, $\bar{\boldsymbol{tk}}_{2,i}^{(0)} = [1, 1, 1, 1]^T$, $\bar{\boldsymbol{tk}}_{3,i}^{(0)} = [0, 0, 0, 0]^T$, $\bar{\boldsymbol{tk}}_{4,i}^{(0)} = [1, 1, 1, 0]^T$. Applying the same solution, we can also deduce $A_{[\{0,1,2,6,9,10,12,14\}]} \cdot [\bar{\boldsymbol{tk}}_{1,i}^{(0)}, \bar{\boldsymbol{tk}}_{2,i}^{(0)}, \bar{\boldsymbol{tk}}_{3,i}^{(0)}, \bar{\boldsymbol{tk}}_{4,i}^{(0)}]^T = \mathbf{0}$. Similarly, for arbitrary $\{r_1, r_2, \cdots, r_t\} \subset \{0, 1, 2, 6, 9, 10, 12, 14\}$ $(t \geq 5)$, we deduce that there is only one difference cancellation behaviour. Further, due to rank-equivalence class in Definition 1, there is $[\{0, 1, 2, 3, 7, 10, 11, 13\}] = [\{0, 1, 2, 6, 9, 10, 12, 14\}]$. The two sets $\{0, 1, 2, 3, 7, 10, 11, 13\}$ and $\{0, 1, 2, 6, 9, 10, 12, 14\}$ only represent the difference cancellations starting from different rounds every 15 rounds for TK-z, and actually show the same difference cancellation behaviour.
In summary, there are only two kinds of the difference cancellation behaviours:

- For rank-equivalence class $[\{0, 1, 2, 4, 5, 8, 10\}]$, the subtweakey difference cancellations happen 7 times in the fixed positions for the given active nibble of the master key in every 30 rounds. Assuming $A_{[\{0,1,2,4,5,8,10\}]} \cdot [\boldsymbol{tk}_{1,i}^{(0)}, \boldsymbol{tk}_{2,i}^{(0)}, \boldsymbol{tk}_{3,i}^{(0)}, \boldsymbol{tk}_{4,i}^{(0)}]^T = \mathbf{0}$, we can compute the only one nonzero solution, where $\boldsymbol{tk}_{1,i}^{(0)} = [0, 0, 0, 0]^T$, $\boldsymbol{tk}_{2,i}^{(0)} = [1, 0, 0, 0]^T$, $\boldsymbol{tk}_{3,i}^{(0)} = [0, 0, 0, 0]^T$, $\boldsymbol{tk}_{4,i}^{(0)} = [1, 0, 0, 0]^T$.
- For rank-equivalence class $[\{0, 1, 2, 3, 7, 10, 11, 13\}]$, the subweakey difference cancellations happen 8 times in the fixed positions every 30 rounds. Assuming $A_{[\{0,1,2,3,7,10,11,13\}]} \cdot [\boldsymbol{tk}_{1,i}^{(0)}, \boldsymbol{tk}_{2,i}^{(0)}, \boldsymbol{tk}_{3,i}^{(0)}, \boldsymbol{tk}_{4,i}^{(0)}]^T = \mathbf{0}$, the nonzero solution is $\boldsymbol{tk}_{1,i}^{(0)} = [0, 0, 0, 1]^T$, $\boldsymbol{tk}_{2,i}^{(0)} = [0, 1, 1, 1]^T$, $\boldsymbol{tk}_{3,i}^{(0)} = [0, 0, 0, 0]^T$, $\boldsymbol{tk}_{4,i}^{(0)} = [0, 1, 1, 0]^T$.

For SKINNYe-64-256 v2, there is $rank(\tilde{\boldsymbol{A}}_{\{r_1,r_2,r_3,r_4\}}) = 16$ for arbitrary $\{r_1, r_2, r_3, r_4\} \subset \mathcal{K}$. That is, at most three difference cancellations can happen every 30 rounds for a given active tweakey nibble and there can be seven rounds of fully inactive internal states at most.

Key Guessing Strategy Based on the Relations of Subtweakeys. In key-recovery attacks, several rounds are added before and after the distinguisher and the involved subtweakeys should be guessed to recover the master tweakey. We can use the relations of subtweakeys to get more accurate and efficient key

guessing strategy following similar idea of the key-bridge technique [33,26]. For example, assume that a set of subtweakeys $\{\boldsymbol{stk}^{(2r_1)}_{\bar{P}^{2r_1}[i]}, \boldsymbol{stk}^{(2r_2)}_{\bar{P}^{2r_2}[i]} \cdots, \boldsymbol{stk}^{(2r_t)}_{\bar{P}^{2r_t}[i]}, \boldsymbol{stk}^{(2r_{t+1})}_{\bar{P}^{2r_{t+1}}[i]}\}$ derived from the same i-th ($0 \leq i \leq 7$) nibble of the master tweakey are involved in the key-recovery phase. Suppose $rank(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}) = a$ and $rank(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_{t+1}\}}) = b$ ($b > a$). The number of possible values for $\{\boldsymbol{stk}^{(2r_1)}_{\bar{P}^{2r_1}[i]}, \boldsymbol{stk}^{(2r_2)}_{\bar{P}^{2r_2}[i]} \cdots, \boldsymbol{stk}^{(2r_t)}_{\bar{P}^{2r_t}[i]}\}$ is $|Im(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}})| = 2^a$. After we guessed $\{\boldsymbol{stk}^{(2r_1)}_{\bar{P}^{2r_1}[i]}, \boldsymbol{stk}^{(2r_2)}_{\bar{P}^{2r_2}[i]} \cdots, \boldsymbol{stk}^{(2r_t)}_{\bar{P}^{2r_t}[i]}\} \in Im(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}})$, the number of possible guesses for the last nibble $\boldsymbol{stk}^{(2r_{t+1})}_{\bar{P}^{2r_{t+1}}[i]}$ will be 2^{b-a}.

4 Rectangle Attacks on SKINNYe-64-256 and Its Version 2

4.1 Preliminary for Boomerang and Rectangle Attacks

The boomerang attack proposed by Wagner [63] is a differential-based attack, which uses two short differential characteristics instead of one long characteristic as shown in Figure 3. The boomerang attack is developed into the amplified boomerang attack [44] and rectangle attack [17], which require only chosen plaintext queries. To clarify the probability of boomerang, Biryukov *et al.* [19] introduced the *boomerang switch* technique, which is generalized by Dunkelman *et al.* [34] as the *sandwich attack*. In the attack, the cipher E_d is considered as $\tilde{E}_1 \circ E_m \circ \tilde{E}_0$, where $\tilde{p}$ and $\tilde{q}$ are the probability of the differentials used for the r_0-round $\tilde{E}_0$ and r_1-round $\tilde{E}_1$. The middle part r_m-round E_m handles the dependence of the two short differentials. If the probability of generating a right quartet for E_m is ξ, the probability of the whole rectangle distinguisher is $2^{-n}\tilde{p}^2\tilde{q}^2\xi$. Then, Cid *et al.* [23] introduced the boomerang connectivity table (BCT) to clarify the probability around the boundary of boomerang and compute its probability more accurately. Further, various studies or improvements [21,61,64,24] on BCT technique enrich boomerang attacks.

Related-key boomerang and rectangle attacks were proposed by Biham *et al.* [18]. As shown in Figure 4, the cipher E is decomposed into $E_f \circ E_d \circ E_b$, where $E_d = E_1 \circ E_0$ is the related-key rectangle distinguisher and E_b and E_f are the extended rounds before and after the distinguisher. Assuming we use a related-key differential $\alpha \to \beta$ over E_0 under a key difference ΔK and $\delta \to \gamma$ over E_1 under a key difference ∇K. If the master key K_1 is known, the other three keys are all determined, where $K_2 = K_1 \oplus \Delta K$, $K_3 = K_1 \oplus \nabla K$, and $K_4 = K_1 \oplus \Delta K \oplus \nabla K$. Denote r_b as the number of unknown bits in the difference α' of plaintexts. Let k_b be the set of subkey bits that involved in E_b while encrypting the plaintext to the known difference α and decrypting to get the corresponding plaintext. Denote the number $m_b = |k_b|$. Similarly, we have r_f and $m_f = |k_f|$ for E_f.

There are several key-recovery frameworks of rectangle attacks [17,16,15,46] in both single-key setting and related-key setting. As shown by Biham *et al.* [15], when the key schedule is linear (e.g. SKINNY), the differences between the

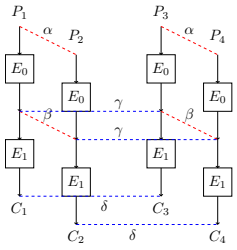

Fig. 3: Boomerang attack

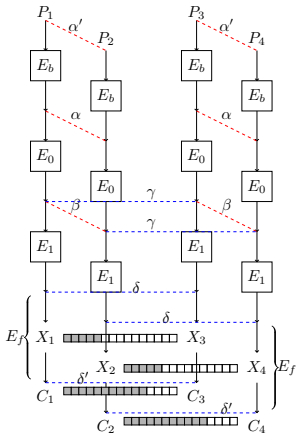

Fig. 4: Rectangle attack on E

.

subkeys of K_1, K_2, K_3 and K_4 are all determined in each round. Exploring this property, Dong *et al.* [30] proposed a new related-key rectangle attack for ciphers with linear key schedule (see Supplementary Material B.1 in our full version paper [53]). They try to guess all k_b and part of k_f, denoted as k'_f before generating quartets. Then with partial decryption, they may gain h_f inactive bits (or bits with fixed differences) from the internal state as filters. They also built a uniform automatic tool to search for the entire rectangle key-recovery attack on SKINNY, which is based on a series of automatic tools [37,24,54].

4.2 Automatic Search for Related-Tweakey Rectangle Attacks for SKINNYe-64-256 and its Version 2

We apply Dong *et al.*'s automatic tool [30] by modifying the constraints of the subtweakey to include more differential cancellation behaviours studied in Section 3. For simplicity, we put Dong *et al.*'s automatic tool in Supplementary Material B in our full version paper [53], and only list the differences of the modelling here.

In previous automatic models [9,24,37] for SKINNY-n-zn ($z = 1, 2, 3$), for a given cell position in the tweakey schedule, the number of cancellations can only be $z-1$ within 30 consecutive rounds. The constraints for the cancellations are given by the designers of SKINNY [10, Page 52], e.g., for 0-th nibble of the master tweakey within the 30 consecutive rounds:

$$\begin{aligned} &\mathrm{LANE}_0 - stk_0^{(0)} \geq 0,\ \mathrm{LANE}_0 - stk_{P^{2i}[0]}^{(2i)} \geq 0,\ 1 \leq i \leq 14, \\ &stk_0^{(0)} + stk_{P^2[0]}^{(2)} + \cdots + stk_{P^{28}[0]}^{(28)} - 15 \cdot \mathrm{LANE}_0 \geq -(z-1), \end{aligned} \tag{10}$$

where the binary variable LANE_0 is 0 only if $TK_{m,0} = 0$ for all $1 \le m \le z$, and the binary variable $stk^{(r)}_{P^r[0]}$ is 0 if and only if the nibble $STK^{(r)}_{P^r[0]}$ is inactive. Similar constraints are applied to other nibble positions.

However, for SKINNYe-64-256, although $z = 4$, we have more cancellations than $z - 1 = 3$ according to Section 3. The possible number and positions of cancellations are diverse, which needs to be modeled by new constraints for the upper and lower differentials besides Constraint (10). According to Section 3, the automatic models are divided into two cases according to different subtweakey difference cancellation behaviours to search for the distinguisher suitable for Dong *et al.*'s rectangle attack framework:

- $t \le 4$: When $t \le 3$, the rank of $\boldsymbol{A}_{\{r_1,\cdots,r_t\}}$ is $4t \le 16$. When $t = 4$, the matrix $\boldsymbol{A}_{\{r_1,r_2,r_3,r_4\}}$ is non-full rank. That is, when $t \le 4$, $rank(\boldsymbol{A}_{\{r_1,\cdots,r_t\}}) < 16$. For a given active nibble in the master key, the subtweakey difference cancellations can happen at most four times in arbitrary 30 rounds. In this case, we only need to modify the last constraint of Eq. (10) to be ($z = 4$):

$$stk^{(0)}_0 + stk^{(2)}_{P^2[0]} + \cdots + stk^{(28)}_{P^{28}[0]} - 15 \cdot \text{LANE}_0 \ge -z.$$

- $t > 4$: There are only two kinds of the difference cancellation behaviours in Section 3, i.e., $[\{0,1,2,4,5,8,10\}]$ and $[\{0,1,2,3,7,10,11,13\}]$. For the rank-equivalence class $[\{0,1,2,4,5,8,10\}]$, we fixed the positions of difference cancellations for the i-th active nibble of the master tweakey to build the model. For each $0 \le r' \le 14$, we set the subtweakey differences to 0 in $\{2r', 2(r'+1) \bmod 30, 2(r'+2) \bmod 30, 2(r'+4) \bmod 30, 2(r'+5) \bmod 30, 2(r'+8) \bmod 30, 2(r'+10) \bmod 30\}$ rounds when $0 \le i \le 7$, and in $\{2r'+1, (2(r'+1)+1) \bmod 30, (2(r'+2)+1) \bmod 30, (2(r'+4)+1) \bmod 30, (2(r'+5)+1) \bmod 30, (2(r'+8)+1) \bmod 30, (2(r'+10)+1) \bmod 30\}$ rounds when $8 \le i \le 15$ to run the model. Similar for case $[\{0,1,2,3,7,10,11,13\}]$.

Searching with different automatic models, we select a 30-round related-tweakey (RTK) boomerang distinguisher for SKINNYe-64-256 in Table 5, where the difference cancellation behaviour $[\{0,1,2,3,7,10,11,13\}]$ is used both in the upper and lower differentials. We also experimentally verify the probabilities of the middle part of the distinguishers, and list details of the distinguisher, the experimental results and full figures in Table 12, Table 14 and Figure 12 in Supplementary Material C.1 and I in our full version paper [53]. Our source codes are based on the open source in [24,30], which is provided in https://github.com/skinny64/Skinny64-256.

For SKINNYe-64-256 v2, we find a 26-round related-tweakey boomerang distinguisher in Table 11 and 13 in Supplementary Material C.1 in our full version paper [53].

4.3 Rectangle Attack on 41-round SKINNYe-64-256

We use the 30-round rectangle distinguisher for SKINNYe-64-256 in Table 5, whose probability is $2^{-n}\tilde{p}^2\xi\tilde{q}^2 = 2^{-64-56.47} = 2^{-120.47}$. The attack follows the

Table 5: The 30-round RTK boomerang distinguisher for SKINNYe-64-256.

$r_0 = 12$, $r_m = 5$, $r_1 = 13$, $\tilde{p} = 2^{-3.46}$, $\xi = 2^{-30.95}$, $\tilde{q} = 2^{-9.30}$, $\tilde{p}^2\xi\tilde{q}^2 = 2^{-56.47}$
$\Delta TK_1 =$ 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0
$\Delta TK_2 =$ 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 0, 0, 0, 0, 0, 0
$\Delta TK_3 =$ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
$\Delta TK_4 =$ 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0
$\Delta X^{(0)} =$ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4
$\nabla TK_1 =$ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1
$\nabla TK_2 =$ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8
$\nabla TK_3 =$ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
$\nabla TK_4 =$ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8
$\nabla X^{(30)} =$ 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1

Dong *et al.*'s rectangle attack framework [30], which is also given in Algorithm 2 in Supplementary Material B.1 in our full version paper [53]. Adding 4-round E_b and 7-round E_f, we attack 41-round SKINNYe-64-256, as illustrated in Figure 5. For simplicity, let $STK^{(i)}_{j_1,j_2}$ be the j_1-th and j_2-th nibble of the i-th round STK. In the first round, we use subtweakey $ETK^{(0)} = \mathtt{MC} \circ \mathtt{SR}(STK^{(0)})$ instead of $STK^{(0)}$, and there is $ETK^{(0)}_i = ETK^{(0)}_{i+4} = ETK^{(0)}_{i+12} = STK^{(0)}_i$ for $0 \le i \le 3$, and $ETK^{(0)}_8 = STK^{(0)}_7$, $ETK^{(0)}_9 = STK^{(0)}_4$, $ETK^{(0)}_{10} = STK^{(0)}_5$, $ETK^{(0)}_{11} = STK^{(0)}_6$. Construct the structures at $\bar{W}^{(0)}$ and $r_b = 12 \cdot 4 = 48$. The cells need to be guessed in E_b are $k_b = \{STK^{(2)}_{0,2,4}, STK^{(1)}_{0-3,5-7}, STK^{(0)}_{0-7}\}$ and $m_b = 18{\cdot}4 = 72$. In E_f, we have $r_f = 16{\cdot}4 = 64$ and $m_f = 45{\cdot}4 = 180$ where $k_f = \{STK^{(34)}_{3,7}, STK^{(35)}_{2-4,7}, STK^{(36)}_{1-7}, STK^{(37)}_{0-7}, STK^{(38)}_{0-7}, STK^{(39)}_{0-7}, STK^{(40)}_{0-7}\}$. The subtweakey cells guessed in advance are marked by red boxes, which are $k'_f = \{STK^{(37)}_{3,6,7}, STK^{(38)}_{0-2,4-7}, STK^{(39)}_{0-7}, STK^{(40)}_{0-7}\}$, and we have $m'_f = 26 \cdot 4 = 104$. Then, we get 7 cells in the internal states (marked by red boxes in $W^{(37)}$ and $W^{(36)}$) as additional filters with the guessed m'_f-bit key, i.e., $h_f = 7 \cdot 4 = 28$ as $\{W^{(36)}_{6,11,15}, W^{(37)}_{5,6,11,12}\}$.

Key bridges. To further accelerate our attack, we identify some tweakey relations in E_b and E_f according to the analysis in Section 3 . We list the subtweakeys transformed from the i-th ($0 \le i \le 15$) nibble of the master key $TK^{(0)}_m$ ($1 \le m \le 4$) in Table 6. For example in line 0 of Table 6, there are 5 subtweakeys in k_b and k_f transformed from the 0-th nibbles of $TK^{(0)}_m$, where $\left(\boldsymbol{stk}^{(0)}_0, \boldsymbol{stk}^{(2)}_2, \boldsymbol{stk}^{(36)}_4, \boldsymbol{stk}^{(38)}_6, \boldsymbol{stk}^{(40)}_5\right)^T = \boldsymbol{A}_{\{0,1,3,4,5\}} \cdot \left(\boldsymbol{tk}^{(0)}_{1,0}, \boldsymbol{tk}^{(0)}_{2,0}, \boldsymbol{tk}^{(0)}_{3,0}, \boldsymbol{tk}^{(0)}_{4,0}\right)^T$. Since $rank(\boldsymbol{A}_{\{0,1,3,4,5\}}) = 16$, the number of possible values of $\{ETK^{(0)}_0 = STK^{(0)}_0, STK^{(2)}_2, STK^{(36)}_4, STK^{(38)}_6, STK^{(40)}_5\}$ is $|Im(A_{\{0,1,3,4,5\}})| = 2^{16}$. Similarly, the number of possible values of $\{ETK^{(0)}_0, STK^{(2)}_2, STK^{(38)}_6, STK^{(40)}_5\} \in k_b \cup k'_f$ is $|Im(A_{\{0,1,4,5\}})| = 2^{14}$. In total, the key size involved in E_b and E_f is

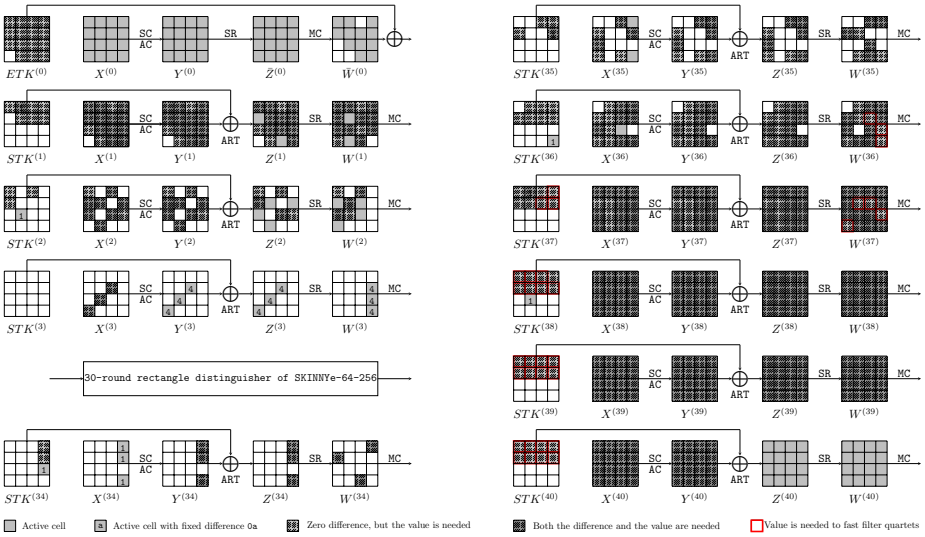

Fig. 5: The 41-round attack against SKINNYe-64-256.

only 224-bit due to the key relations although $m_b + m_f = 72 + 180 = 252$, denoted as $|k_b \cup k_f| = 2^{224}$. Similarly, we have $|k_b \cup k'_f| = 2^{170}$ although $m_b + m'_f = 72 + 104 = 176$.

The details of our attack are given as follows:

1. Construct $y = \sqrt{s} \cdot 2^{n/2-r_b}/\sqrt{\tilde{p}^2\xi\tilde{q}^2} = \sqrt{s} \cdot 2^{12.24}$ structures of $2^{r_b} = 2^{48}$ plaintexts each. For each structure, encrypt the 2^{48} plaintexts under the four related tweakeys K_1, K_2, K_3 and K_4 to get corresponding ciphertexts and store the plaintext-ciphertext pairs in L_1, L_2, L_3 and L_4. The data and memory complexity here is both $\sqrt{s} \cdot 2^{n/2+2}/\sqrt{\tilde{p}^2\xi\tilde{q}^2} = \sqrt{s} \cdot 2^{62.24}$.
2. Guess 2^x possible values of $k_b \cup k'_f$ ($2^x \leq |k_b \cup k'_f|$):
   (a) Initialize $|k_b \cup k_f|/2^x = 2^{224-x}$ counters with memory cost 2^{224-x}.
   (b) Guess all the remaining $|k_b \cup k'_f|/2^x = 2^{170-x}$ possible values in $k_b \cup k'_f$:
      i. For each structure, partially encrypt each plaintext P_1 under the guessed values of k_b to $Y^{(3)}_{6,9,12}$. After xoring the known difference α, partially decrypt it to get the plaintext P_2. Do the same for each P_3 to get P_4. Store the pairs in S_1 and S_2, whose sizes are $y \cdot 2^{r_b} = \sqrt{s} \cdot 2^{60.24}$.
      ii. For each element in S_1, partially decrypt (C_1, C_2) under guessed k'_f to get $W^{(36)}_{6,11,15} \| W^{(37)}_{5,6,11,12}$. Insert the element in S_1 into a hash table H indexed by the $h_f = 28$-bit $W^{(36)}_{6,11,15} \| W^{(37)}_{5,6,11,12}$ of C_1 and $h_f =$ 28-bit $\tilde{W}^{(36)}_{6,11,15} \| \tilde{W}^{(37)}_{5,6,11,12}$ of C_2. For each element in S_2, partially decrypt (C_3, C_4) under guessed k'_f to get the $2h_f = 56$ internal state bits, and check against H to find the pairs (C_1, C_2), where (C_1, C_3)

Table 6: Relations of the subtweakeys involved in the 41-round attack on SKINNYe-64-256, where the subtweakeys marked in bold are among k'_f.

i	k_b	k_f		
0	$ETK_0^{(0)}, STK_2^{(2)}$	$STK_4^{(36)}, \boldsymbol{STK_6^{(38)}}, \boldsymbol{STK_5^{(40)}}$	$\lvert Im(A_{\{0,1,3,4,5\}})\rvert = 2^{16}$	$\lvert Im(A_{\{0,1,4,5\}})\rvert = 2^{14}$
1	$ETK_1^{(0)}, STK_0^{(2)}$	$STK_2^{(36)}, \boldsymbol{STK_4^{(38)}}, \boldsymbol{STK_6^{(40)}}$	$\lvert Im(A_{\{0,1,3,4,5\}})\rvert = 2^{16}$	$\lvert Im(A_{\{0,1,4,5\}})\rvert = 2^{14}$
2	$ETK_2^{(0)}, STK_4^{(2)}$	$STK_6^{(36)}, \boldsymbol{STK_5^{(38)}}, \boldsymbol{STK_3^{(40)}}$	$\lvert Im(A_{\{0,1,3,4,5\}})\rvert = 2^{16}$	$\lvert Im(A_{\{0,1,4,5\}})\rvert = 2^{14}$
3	$ETK_3^{(0)}$	$STK_7^{(34)}, STK_1^{(36)}, \boldsymbol{STK_0^{(38)}}, \boldsymbol{STK_2^{(40)}}$	$\lvert Im(A_{\{0,2,3,4,5\}})\rvert = 2^{15}$	$\lvert Im(A_{\{0,4,5\}})\rvert = 2^{12}$
4	$ETK_9^{(0)}$	$STK_5^{(36)}, STK_3^{(38)}, \boldsymbol{STK_7^{(40)}}$	$\lvert Im(A_{\{0,3,4,5\}})\rvert = 2^{15}$	$\lvert Im(A_{\{0,5\}})\rvert = 2^{8}$
5	$ETK_{10}^{(0)}$	$STK_3^{(34)}, STK_7^{(36)}, \boldsymbol{STK_1^{(38)}}, \boldsymbol{STK_0^{(40)}}$	$\lvert Im(A_{\{0,2,3,4,5\}})\rvert = 2^{15}$	$\lvert Im(A_{\{0,4,5\}})\rvert = 2^{12}$
6	$ETK_{11}^{(0)}$	$STK_3^{(36)}, \boldsymbol{STK_7^{(38)}}, \boldsymbol{STK_1^{(40)}}$	$\lvert Im(A_{\{0,3,4,5\}})\rvert = 2^{15}$	$\lvert Im(A_{\{0,4,5\}})\rvert = 2^{12}$
7	$ETK_8^{(0)}$	$\boldsymbol{STK_2^{(38)}}, \boldsymbol{STK_4^{(40)}}$	$\lvert Im(A_{\{0,4,5\}})\rvert = 2^{12}$	$\lvert Im(A_{\{0,4,5\}})\rvert = 2^{12}$
8	$STK_2^{(1)}$	$STK_4^{(35)}, \boldsymbol{STK_6^{(37)}}, \boldsymbol{STK_5^{(39)}}$	$\lvert Im(A_{\{1,3,4,5\}})\rvert = 2^{15}$	$\lvert Im(A_{\{1,4,5\}})\rvert = 2^{12}$
9	$STK_0^{(1)}$	$STK_2^{(35)}, STK_4^{(37)}, \boldsymbol{STK_6^{(39)}}$	$\lvert Im(A_{\{1,3,4,5\}})\rvert = 2^{15}$	$\lvert Im(A_{\{1,5\}})\rvert = 2^{8}$
10		$STK_5^{(37)}, \boldsymbol{STK_3^{(39)}}$	$\lvert Im(A_{\{4,5\}})\rvert = 2^{8}$	$\lvert Im(A_{\{5\}})\rvert = 2^{4}$
11	$STK_7^{(1)}$	$STK_0^{(37)}, \boldsymbol{STK_2^{(39)}}$	$\lvert Im(A_{\{1,4,5\}})\rvert = 2^{12}$	$\lvert Im(A_{\{1,5\}})\rvert = 2^{8}$
12	$STK_6^{(1)}$	$\boldsymbol{STK_3^{(37)}}, \boldsymbol{STK_7^{(39)}}$	$\lvert Im(A_{\{1,4,5\}})\rvert = 2^{12}$	$\lvert Im(A_{\{1,4,5\}})\rvert = 2^{12}$
13	$STK_3^{(1)}$	$STK_7^{(35)}, STK_1^{(37)}, \boldsymbol{STK_0^{(39)}}$	$\lvert Im(A_{\{1,3,4,5\}})\rvert = 2^{15}$	$\lvert Im(A_{\{1,5\}})\rvert = 2^{8}$
14	$STK_5^{(1)}$	$STK_3^{(35)}, \boldsymbol{STK_7^{(37)}}, \boldsymbol{STK_1^{(39)}}$	$\lvert Im(A_{\{1,3,4,5\}})\rvert = 2^{15}$	$\lvert Im(A_{\{1,4,5\}})\rvert = 2^{12}$
15	$STK_1^{(1)}$	$STK_2^{(37)}, \boldsymbol{STK_4^{(39)}}$	$\lvert Im(A_{\{1,4,5\}})\rvert = 2^{12}$	$\lvert Im(A_{\{1,5\}})\rvert = 2^{8}$
			$\lvert k_b \cup k_f\rvert = 2^{224}$	$\lvert k_b \cup k'_f\rvert = 2^{170}$

and (C_2, C_4) collide at the $2h_f = 56$ bits. The time complexity here is $T_1 = \sqrt{s}\cdot 2^{|k_b\cup k'_f|+n/2+1}/\sqrt{\tilde{p}^2\xi\tilde{q}^2} = \sqrt{s}\cdot 2^{170+32+1+28.24} = \sqrt{s}\cdot 2^{231.24}$. We get $s\cdot 2^{|k_b\cup k'_f|-2h_f-n+2r_f}/(\tilde{p}^2\xi\tilde{q}^2) = s\cdot 2^{170-56-64+128+56.47} = s\cdot 2^{234.47}$ quartets.

iii. For each of the $s\cdot 2^{234.47}$ quartets, determine the key candidates step by step, whose time complexity is ε:

A: In round 38, guess 2^4 possible values of $STK_3^{(38)}$. As shown in Table 7, with other guessed k'_f together, we compute $Z_{0,12}^{(37)}$ and deduce $\Delta Y_0^{(37)}$ and $\Delta X_{12}^{(37)}$. For the 1st column of $X^{(37)}$ of (C_1, C_3), we obtain $\Delta X_0^{(37)} = \Delta X_{12}^{(37)}$ by property of MC, and deduce $STK_0^{(37)}$ by Lemma 1. Similarly, we deduce $STK_0'^{(37)}$ for (C_2, C_4). Then the fixed $\Delta STK_0^{(37)} = STK_0^{(37)} \oplus STK_0'^{(37)}$ is a 4-bit filter. $s\cdot 2^{234.47}\cdot 2^4\cdot 2^{-4} = s\cdot 2^{234.47}$ quartets remain.

B: In round 37, guessing 2^4 possible values of $STK_2^{(37)}$, following Table 7 we compute $Z_{3,15}^{(36)}$ and deduce $\Delta Y_3^{(36)}$ and $\Delta X_{15}^{(36)}$. For the 4-th column of $X^{(36)}$ of (C_1, C_3), we deduce $\Delta X_3^{(36)} = \Delta X_{15}^{(36)}$ by MC and deduce $STK_3^{(36)}$. Since the number of possible values[8] of $STK_3^{(36)}$ is only 2^3 as shown in Table 7, which acts as a filter of

[8] The number of possible values of $STK_3^{(36)}$ is computed via Table 6. For example, in line 6 of Table 6, $\{ETK_{11}^{(0)}, STK_7^{(38)}, STK_1^{(40)}\} \in k_b \cup k'_f$ derived from the 6-th nibble have already been guessed, so the number of possible values of $STK_3^{(36)}$ is $|Im(A_{\{0,3,4,5\}})|/|Im(A_{\{0,4,5\}})| = 2^{15-12} = 2^3$. Similarly, we compute all the number of possible values for subtweakey cells involved in the guess and filter procedure, which are listed in Table 7.

$2^3/2^4 = 2^{-1}$. Similarly, we deduce $STK_3'^{(36)}$ for (C_2, C_4). Then the fixed $\Delta STK_3^{(36)}$ is a 4-bit filter. $s \cdot 2^{234.47} \cdot 2^4 \cdot 2^{-1} \cdot 2^{-4} = s \cdot 2^{233.47}$ quartets remain.

C: Guessing 2^4 possible values of $STK_4^{(37)}$, we compute $Z_7^{(36)}$ and deduce $\Delta Y_7^{(36)}$. For the 4-th column of $X^{(36)}$ of (C_1, C_3), we can obtain $\Delta X_7^{36} = \Delta X_{15}^{(36)}$ by `MC`. With the known $\Delta X_{15}^{(36)}$ in **step B**, we deduce $STK_7^{(36)}$. The number of possible values of $STK_7^{(36)}$ is 2^3, which can act as a filter of $2^3/2^4 = 2^{-1}$. Similarly, we deduce $STK_7'^{(36)}$ for (C_2, C_4). Then the fixed $\Delta STK_7^{(36)}$ is a 4-bit filter. $s \cdot 2^{233.47} \cdot 2^4 \cdot 2^{-1} \cdot 2^{-4} = s \cdot 2^{232.47}$ quartets remain.

D: Guessing 2^4 possible values of $STK_1^{(37)}$, we compute $Z_{6,10,14}^{(36)}$. Then $\Delta Y_6^{(36)}$ and $\Delta X_{10,14}^{(36)}$ are deduced. For the 3rd column of $X^{(36)}$ of (C_1, C_3), we can obtain $\Delta X_6^{(36)} = \Delta X_{10}^{(36)} \oplus \Delta X_{14}^{(36)}$ by `MC` and deduce $STK_6^{(36)}$. The number of possible values of $STK_6^{(36)}$ is 2^2, which acts as a filter of $2^2/2^4 = 2^{-2}$. Similarly, we deduce $STK_6'^{(36)}$ for (C_2, C_4) and $\Delta STK_6^{(36)}$ can act as a 4-bit filter. $s \cdot 2^{232.47} \cdot 2^4 \cdot 2^{-2} \cdot 2^{-4} = s \cdot 2^{230.47}$ quartets remain.

E: In round 36, guessing $2^4 \times 2^2 \times 2^2$ possible values for $(STK_5^{(37)}, STK_2^{(36)}, STK_4^{(36)})$, we compute $Z_{3,7,15}^{(35)}$ and deduce $\Delta Y_{3,7}^{(35)}$ and $\Delta X_{15}^{(35)}$. For the 4-th column of $X^{(35)}$ of (C_1, C_3), we can obtain $\Delta X_3^{(35)} = \Delta X_7^{(35)} = \Delta X_{15}^{(35)}$ by `MC` and deduce $STK_3^{(35)}$ and $STK_7^{(35)}$. Both the numbers of possible values of $STK_3^{(35)}$ and $STK_7^{(35)}$ are 2^3, which acts as two filters of $2^3/2^4 = 2^{-1}$. Similarly, we deduce $STK_3'^{(35)}$ and $STK_7'^{(35)}$ for (C_2, C_4). Then the fixed $\Delta STK_3^{(35)}$ and $\Delta STK_7^{(35)}$ can act as two 4-bit filters. Thereafter, in round 34, we deduce $Z_3^{(34)}$ from $Z_7^{(35)}$ and $STK_7^{(35)}$. Since $STK_3^{(34)}$ only has one possible value[9], we deduce $X_3^{(34)}$. So $\Delta X_3^{(34)} =$ `0x1` acts a 4-bit filter both for (C_1, C_3) and (C_2, C_4). $s \cdot 2^{230.47} \cdot 2^8 \cdot 2^{-1} \cdot 2^{-1} \cdot 2^{-8} \cdot 2^{-8} = s \cdot 2^{220.47}$ quartets remain.

F: Guessing $2^3 \times 2^3 \times 2^3 \times 2^3$ possible values of $(STK_1^{(36)}, STK_5^{(36)}, STK_2^{(35)}, STK_4^{(35)})$, compute $Z_{7,15}^{(34)}$ and deduce $X_{15}^{(34)}$. Since $STK_7^{(34)}$ only has one possible value, we can deduce $X_7^{(34)}$. $\Delta X_7^{(34)} =$ `0x1` and $\Delta X_{15}^{(34)} =$ `0x1` are two 4-bit filters for both (C_1, C_3) and (C_2, C_4). $s \cdot 2^{220.47} \cdot 2^{12} \cdot 2^{-8} \cdot 2^{-8} = s \cdot 2^{216.47}$ quartets remain.

So for each quartet, $\varepsilon = 2^4 \cdot \frac{4}{41} + 2^4 \cdot \frac{4}{41} + 2^{-1} \cdot 2^4 \cdot \frac{4}{41} + 2^{-2} \cdot 2^4 \cdot \frac{4}{41} + 2^{-4} \cdot 2^8 \cdot \frac{4}{41} + 2^{-14} \cdot 2^{12} \cdot \frac{4}{41} \approx 2^{2.56}$ and $T_2 = s \cdot 2^{234.47} \cdot \varepsilon = s \cdot 2^{237.03}$.

[9] As shown in line 5 of Table 6, with $STK_7^{(36)}$ deduced in **step C** and other cells guessed in $k_b \cup k_f'$, the number of possible values is only 1 for $STK_3^{(34)}$.

(c) (Exhaustive search) Select the top $|k_b \cup k_f| \cdot 2^{-x-h} = 2^{224-x-h}$ hits in the counter as the key candidates. Guess the remaining $k - 224 = 32$-bit key to check the full key, and $T_3 = 2^{k-h}$.

Set $s = 1$, $h = 32$ and $x = 168$ ($x \leq 170$, $h \leq 224 - x$). We have $T_1 = 2^{231.24}$, $T_2 = 2^{237.03}$ and $T_3 = 2^{224}$. The memory complexity is $2^{62.24} + 2^{56} \approx 2^{62.26}$. In total, for the 41-round attack on SKINNYe-64-256, the data complexity is $2^{62.24}$, the memory complexity is $2^{62.26}$, and the time complexity is $2^{237.06}$. The success probability is about 70.6%.

In addition, for SKINNYe-64-256 v2 we give a 37-round related-tweakey rectangle attack (given in the Supplementary Material C.2 in our full version paper [53]) based on a 26-round related-tweakey boomerang distinguisher. The data complexity is $2^{62.8}$, the memory complexity is $2^{62.8}$, and the time complexity is $2^{240.03}$. The success probability is about 66.3%.

Table 7: Tweakey recovery for 41-round SKINNYe-64-256. The red cells are among k'_f or gained in the previous steps. D/G: deduced/guessed subtweakeys.

Step	State	Involved subtweakeys	Number of values
A	$Z_0^{(37)}$	$STK_4^{(38)}$, $STK_5^{(39)}$, $STK_{0,6,7}^{(40)}$	G: $STK_3^{(38)}$: 2^4
	$Z_{12}^{(37)}$	$STK_3^{(38)}$, $STK_{2,7}^{(39)}$, $STK_{1,4,6}^{(40)}$	D: $STK_0^{(37)}$: 2^4
B	$Z_3^{(36)}$	$STK_7^{(37)}$, $STK_4^{(38)}$, $STK_{3,5,6}^{(39)}$, $STK_{0-2,6,7}^{(40)}$	G: $STK_2^{(37)}$: 2^4
	$Z_{15}^{(36)}$	$STK_2^{(37)}$, $STK_{1,6}^{(38)}$, $STK_{0,5,7}^{(39)}$, $STK_{2-6}^{(40)}$	D: $STK_3^{(36)}$: 2^3
C	$Z_7^{(36)}$	$STK_4^{(37)}$, $STK_{3,5,6}^{(38)}$, $STK_{0-2,6,7}^{(39)}$, $STK_{0-7}^{(40)}$	G: $STK_4^{(37)}$: 2^4
			D: $STK_7^{(36)}$: 2^3
D	$Z_6^{(36)}$	$STK_7^{(37)}$, $STK_{2,4,5}^{(38)}$, $STK_{0,1,3,5,6}^{(39)}$, $STK_{0-7}^{(40)}$	G: $STK_1^{(37)}$: 2^4
	$Z_{10}^{(36)}$	$STK_4^{(37)}$, $STK_{3,5}^{(38)}$, $STK_{0,2,6,7}^{(39)}$, $STK_{1-4,6,7}^{(40)}$	D: $STK_6^{(36)}$: 2^2
	$Z_{14}^{(36)}$	$STK_1^{(37)}$, $STK_{0,5}^{(38)}$, $STK_{3,4,6}^{(39)}$, $STK_{1,2,4,5,7}^{(40)}$	
E	$Z_3^{(35)}$	$STK_7^{(36)}$, $STK_4^{(37)}$, $STK_{3,5,6}^{(38)}$, $STK_{0-2,6,7}^{(39)}$, $STK_{0-7}^{(40)}$	G: $STK_5^{(37)}$: 2^4
	$Z_7^{(35)}$	$STK_4^{(36)}$, $STK_{3,5,6}^{(37)}$, $STK_{0-2,6,7}^{(38)}$, $STK_{0-7}^{(39)}$, $STK_{0-7}^{(40)}$	G: $STK_2^{(36)}$: 2^2
	$Z_{15}^{(35)}$	$STK_2^{(36)}$, $STK_{1,6}^{(37)}$, $STK_{0,5,7}^{(38)}$, $STK_{2-6}^{(39)}$, $STK_{0-7}^{(40)}$	G: $STK_4^{(36)}$: 2^2
	$Z_3^{(34)}$	$STK_7^{(35)}$, $STK_4^{(36)}$, $STK_{3,5,6}^{(37)}$, $STK_{0-2,6,7}^{(38)}$, $STK_{0-7}^{(39)}$, $STK_{0-7}^{(40)}$	D: $STK_3^{(35)}$: 2^3
			D: $STK_7^{(35)}$: 2^3
			D: $STK_3^{(34)}$: 2^0
F	$Z_7^{(34)}$	$STK_4^{(35)}$, $STK_{3,5,6}^{(36)}$, $STK_{0-2,6,7}^{(37)}$, $STK_{0-7}^{(38)}$, $STK_{0-7}^{(39)}$, $STK_{0-7}^{(40)}$	G: $STK_1^{(36)}$: 2^3
	$Z_{15}^{(34)}$	$STK_2^{(35)}$, $STK_{1,6}^{(36)}$, $STK_{0,5,7}^{(37)}$, $STK_{2-6}^{(38)}$, $STK_{0-7}^{(39)}$, $STK_{0-7}^{(40)}$	G: $STK_5^{(36)}$: 2^3
			G: $STK_2^{(35)}$: 2^3
			G: $STK_4^{(35)}$: 2^3
			D: $STK_7^{(34)}$: 2^0

5 MITM and Impossible Differential Attacks on SKINNYe-64-256 and its Version 2

5.1 The Meet-in-the-Middle Attack

The three-subset meet-in-the-middle attack was proposed by Bogdanov and Rechberger [20] and was summarized by Isobe [41]. Several important tech-

niques significantly enhance and enrich the MITM methodology, including the *splice-and-cut* technique [5], initial structure [59,58], (indirect-)partial matching [59,58], sieve-in-the-middle [22], match-box technique [35], and dissection [27], etc. Recently, several automatic tools [25,57,7,8,60,38] on MITM attacks are presented. At CRYPTO 2021, Dong *et al.* [29] developed the MILP model for MITM key-recovery attack on SKINNY. Combining Dong *et al.*'s model and our new discoveries on tweakey schedule of SKINNYe-64-256, we develop MITM key-recovery attacks on 31-round SKINNYe-64-256 and 27-round SKINNYe-64-256 v2 in Supplementary Material D in our full version paper [53].

5.2 Related-Tweakey Impossible Differential

The impossible differential attack is proposed by Biham *et al.* [14] and Knudsen [45] independently. It uses a differential with probability zero to act as a distinguisher, named as the impossible differential. With several rounds appended before and after the impossible differential distinguisher, one partially encrypts/decrypts a given pair by a candidate key to the input and output of the distinguisher. The key candidate that leads to the impossible differential will be the wrong one and will be rejected. This technique provides a sieving of the key space and the remaining candidates can be tested by exhaustive search. There are several works analyzed the security of SKINNY family against the impossible differential attacks [46,62,4,56,31], in both single-tweakey and related-tweakey setting. We introduce related-tweakey impossible differentials on 21-round SKINNYe-64-256 and 18-round SKINNYe-64-256 v2 in Supplementary Material E in our full version paper [53].

6 A Proposal for Tweakey Schedule of SKINNY Family

At ASIACRYPT 2014, Jean *et al.* [42] introduced the STK construction as shown in Figure 1, which absorbs arbitrary length of tweakey. It updates each cell of the tweakey states by multiplying a non-zero α_j. For SKINNY-n-zn, the tweakey cells are updated by dedicated chosen lightweight LFSRs, which guarantees at most $z-1$ cancellations within 30 consecutive rounds. However, SKINNY family [9] only gives instances for $z = 1, 2, 3$. SKINNYe-64-256 [48] extends z to 4, but fails to satisfy its expected security claim[10]. In the updated version SKINNYe-64-256 v2 [50], the designers fixed the issue and claimed that the LFSR for TK_4 is the only one to ensure at most 3 cancellations after exhaustively testing 2^{16} choices. It is not trivial to extend SKINNY to support arbitrary length of tweakey with similar *subtweakey difference cancellation property* to STK construction: for a given cell position, $z-1$ cancellations can only happen every 15 rounds for TK-z (or every 30 rounds for SKINNY-n-zn).

[10] Similar issue happens to Lilliput-AE [1], one of the first-round candidates at the NIST competition, specifies TBCs with up to $z = 7$. However, they also ignored the rationale of the original tweakey framework to ensure the security, and were actually attacked practically [32].

As stated by Naito *et al.* [48, Page 5] that PFB_Plus "... give new insight to TBC designers considering that there is no consensus about the adequate tweak size to support". It is interesting to consider a uniformed tweakey schedule to extend SKINNY to support larger tweakey size, while obeying the property of STK construction, which may have potential application, such as SKINNYe-64-256 v2 in TI-friendly constructions.

For general $z \leq 14$, the output nibbles can be represented by linear combinations of the input nibbles as in equation (4), i.e.,

$$\begin{pmatrix} \boldsymbol{stk}^{(2\times 0)}_{\bar{P}^{2\times 0}[i]} \\ \boldsymbol{stk}^{(2\times 1)}_{\bar{P}^{2\times 1}[i]} \\ \vdots \\ \boldsymbol{stk}^{(2\times 14)}_{\bar{P}^{2\times 14}[i]} \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{L}_2^0 & \cdots & \boldsymbol{L}_z^0 \\ \boldsymbol{I} & \boldsymbol{L}_2^1 & \cdots & \boldsymbol{L}_z^1 \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{I} & \boldsymbol{L}_2^{14} & \cdots & \boldsymbol{L}_z^{14} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{tk}^{(0)}_{1,i} \\ \boldsymbol{tk}^{(0)}_{2,i} \\ \vdots \\ \boldsymbol{tk}^{(0)}_{z,i} \end{pmatrix}, \ 0 \leq i \leq 7. \tag{11}$$

To satisfy the subtweakey difference cancellation property, the coefficient matrix in (11) must satisfy the 'block-MDS' property [42], i.e.,

$$\det \begin{pmatrix} \boldsymbol{I} & \boldsymbol{L}_2^{r_1} & \cdots & \boldsymbol{L}_z^{r_1} \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_2} & \cdots & \boldsymbol{L}_z^{r_2} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_z} & \cdots & \boldsymbol{L}_z^{r_z} \end{pmatrix} \neq 0 \tag{12}$$

for all $0 \leq r_1 < r_2 < \cdots < r_z \leq 14$. In other words, the goal of our design is to choose $\boldsymbol{L}_i$'s such that the 'block-MDS' property is guaranteed. Although the coefficient matrix in (11) has a block Vandermonde form, there is no simple formula to compute the determinant of its squared sub-matrices for general $\boldsymbol{L}_i$'s. When the $\boldsymbol{L}_i$'s are pairwise commutable, a formula can be deduced for squared block Vandermonde matrices, which we refer to Supplementary Material F in our full version paper [53].

6.1 The Choice of $\boldsymbol{L_i}$

Our construction can be viewed as an extension of the generator matrices of Reed-Solomon codes to the block matrix form. Specifically, denoting $\boldsymbol{L}_1 = \boldsymbol{I}$, and we choose the $\boldsymbol{L}_i$'s to be consecutive powers of a matrix $\boldsymbol{L}$, i.e.,

$$\{\boldsymbol{L}_i\}_{1\leq i\leq z} = \{\boldsymbol{L}^{\alpha+1}, \cdots, \boldsymbol{L}^{\alpha+z}\} \tag{13}$$

for some integer $\alpha \in [-z, -1]$. Then we can show that the 'block-MDS' property is guaranteed if the matrix $\boldsymbol{L}$ satisfies specific property.

Proposition 1. *Suppose $\boldsymbol{L}$ is a 4×4 matrix over $GF(2)$ such that the characteristic polynomial $p_{\boldsymbol{L}}(\lambda)$ is a primitive polynomial of degree 4 over $GF(2)$. Then $\boldsymbol{L}$ has cycle 15, and for any integer α,*

$$\det \begin{pmatrix} (\boldsymbol{L}^{\alpha+1})^{r_1} & (\boldsymbol{L}^{\alpha+2})^{r_1} & \cdots & (\boldsymbol{L}^{\alpha+z})^{r_1} \\ (\boldsymbol{L}^{\alpha+1})^{r_2} & (\boldsymbol{L}^{\alpha+2})^{r_2} & \cdots & (\boldsymbol{L}^{\alpha+z})^{r_2} \\ \vdots & \vdots & \ddots & \vdots \\ (\boldsymbol{L}^{\alpha+1})^{r_z} & (\boldsymbol{L}^{\alpha+2})^{r_z} & \cdots & (\boldsymbol{L}^{\alpha+z})^{r_z} \end{pmatrix} \neq 0 \tag{14}$$

for all $0 \leq r_1 < r_2 < \cdots < r_z \leq 14$.

Proof. Let $\lambda_i, 1 \leq i \leq 4$, be the eigenvalues of $\boldsymbol{L}$, then λ_i is primitive in $GF(2^4)$ and $\boldsymbol{L}^r$ has eigenvalues $\lambda_i^r, 1 \leq i \leq 4$. For $1 \leq r < 15$, we have $\lambda_i^r \neq 1, 1 \leq i \leq 4$, and thus $\boldsymbol{L}^r \neq \boldsymbol{I}$. For $r = 15$, note that $p_{\boldsymbol{L}}(\lambda) \mid (\lambda^{15} - 1)$, and by the Cayley–Hamilton theorem (see Section 9 of [55]) we have $p_{\boldsymbol{L}}(\boldsymbol{L}) = \boldsymbol{0}$. Then it follows that $\boldsymbol{L}^{15} - \boldsymbol{I} = \boldsymbol{0}$.

To show the determinant is nonzero, we observe that

$$\begin{pmatrix} (\boldsymbol{L}^{\alpha+1})^{r_1} & \cdots & (\boldsymbol{L}^{\alpha+z})^{r_1} \\ (\boldsymbol{L}^{\alpha+1})^{r_2} & \cdots & (\boldsymbol{L}^{\alpha+z})^{r_2} \\ \vdots & \ddots & \vdots \\ (\boldsymbol{L}^{\alpha+1})^{r_z} & \cdots & (\boldsymbol{L}^{\alpha+z})^{r_z} \end{pmatrix} = \begin{pmatrix} \boldsymbol{L}^{\alpha r_1} & & & \\ & \boldsymbol{L}^{\alpha r_2} & & \\ & & \ddots & \\ & & & \boldsymbol{L}^{\alpha r_z} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{L}^{r_1} & \cdots & (\boldsymbol{L}^{r_1})^z \\ \boldsymbol{L}^{r_2} & \cdots & (\boldsymbol{L}^{r_2})^z \\ \vdots & \ddots & \vdots \\ \boldsymbol{L}^{r_z} & \cdots & (\boldsymbol{L}^{r_z})^z \end{pmatrix}. \tag{15}$$

Then it suffices to show that $\det\left((\boldsymbol{L}^{r_i})^j\right)_{1 \leq i,j \leq z} \neq 0$ for all $0 \leq r_1 < r_2 < \cdots < r_z \leq 14$, which we refer to Supplementary Material F in full version paper [53]. □

Construction of $\boldsymbol{L}$. One simple way to construct $\boldsymbol{L}$ is to take $\boldsymbol{L}$ to be the companion matrix of a primitive polynomial. For example, for the primitive polynomial $\lambda^4 + \lambda + 1$, we can take $\boldsymbol{L}$ to be the companion matrix

$$\boldsymbol{L} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}. \tag{16}$$

It can be readily checked that the characteristic polynomial $p_{\boldsymbol{L}}(\lambda) = \lambda^4 + \lambda + 1$ and thus the eigenvalues of $\boldsymbol{L}$ are distinct primitive elements in $GF(2^4)$. On the other hand, taking companion matrices of primitive polynomials is not the only way to obtain $\boldsymbol{L}$. In fact, we perform an exhaustive search of all binary 4×4 binary matrices, and find totally 1344 distinct $\boldsymbol{L}$ whose characteristic polynomial is primitive over $GF(2)$.

An Example for $z = 4$. Taking $\alpha = -2$ and $\boldsymbol{L}$ equals to that in (16), then

$$\{\boldsymbol{L}_i\}_{1 \leq i \leq 4} = \{\boldsymbol{L}^{-1}, \boldsymbol{L}^0, \boldsymbol{L}^1, \boldsymbol{L}^2\}. \tag{17}$$

Without loss of generality, let

$$\boldsymbol{L}_2 = \boldsymbol{L}^1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \boldsymbol{L}_3 = \boldsymbol{L}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \boldsymbol{L}_4 = \boldsymbol{L}^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}. \tag{18}$$

Considering the LFSRs defined by (18), we found that the LFSRs for TK_2 and TK_3 coincide with the original LFSRs in SKINNY, and the LFSRs for TK_4 coincides with that constructed in SKINNYe-64-256 v2. *From this point of view, our construction can be viewed as a natural extension of the original SKINNY-64 and SKINNYe-64-256 v2.*

For general $z \leq 14$, the 'block-MDS' property of our construction guarantees there are at most $z-1$ difference cancellations every 15 rounds for TK-z (or every 30 rounds SKINNY-n-zn). We derive the lower bounds of the number of active S-boxes for SKINNY-n-zn ($z \leq 14$) with our construction of the tweakey schedule (see Supplementary Material G in our full version paper [53]). The results (see Table 17 in our full version paper [53]) show that our new tweakey schedule for TK-z ($z \leq 14$) leads to a natural increase of the bounds compared to TK-1, TK-2 and TK-3 in [9] and TK-4 in [50].

Efficiency Considerations. How to choose $\boldsymbol{L}_i$'s to optimize the implementation efficiency is also an important issue. As pointed in [48], one direction of optimization is to minimize the total number of XORs required by the LFSRs. For $z = 4$, the LFSRs constructed through (18) require only 4 XORs totally, i.e., $\boldsymbol{L}_2$ and $\boldsymbol{L}_3$ require only 1 XOR respectively, and $\boldsymbol{L}_4$ requires 2 XORs. Note that in [48] it was proved that there is no secure LFSRs for TK_4 with only a single XOR, therefore the LFSRs constructed through (18) is optimal with respect to the number of XORs. For all $4 \leq z \leq 7$, we enumerate all possible $\boldsymbol{L}$ and α, and give the optimal number of XORs required in our construction in Table 8.

Table 8: Optimal number of XORs required in our construction.

z	$\boldsymbol{L}$	$\{\boldsymbol{L}_i\}_{2\leq i\leq z}$	Number of XORs	Total XORs
4	$\begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&1&0&0 \end{pmatrix}$	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}, \boldsymbol{L}^2\}$	$\{1, 1, 2\}$	4
5	$\begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&1&0&0 \end{pmatrix}$	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}, \boldsymbol{L}^2, \boldsymbol{L}^{-2}\}$	$\{1, 1, 2, 3\}$	7
6	$\begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&1&0&0 \end{pmatrix}$	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}, \boldsymbol{L}^2, \boldsymbol{L}^{-2}, \boldsymbol{L}^3\}$	$\{1, 1, 2, 3, 3\}$	10
7	$\begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&1&0&0 \end{pmatrix}$	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}, \boldsymbol{L}^2, \boldsymbol{L}^{-2}, \boldsymbol{L}^3, \boldsymbol{L}^4\}$	$\{1, 1, 2, 3, 3, 5\}$	15

Another direction of optimization is to minimize the circuit area of the LFSRs. In our construction, all $\boldsymbol{L}_i$'s are powers of a matrix $\boldsymbol{L}$, therefore a minimal area implementation can be supported by instantiating only one circuit of $\boldsymbol{L}$ and computing each $\boldsymbol{L}_i$ iteratively. For example, for $z = 4$ we take $\alpha = -1$ and $\boldsymbol{L}_2 = \boldsymbol{L}, \boldsymbol{L}_3 = \boldsymbol{L}^2, \boldsymbol{L}_4 = \boldsymbol{L}^3$. Then $\boldsymbol{L}_2, \boldsymbol{L}_3$ and $\boldsymbol{L}_4$ can be computed by repeating $\boldsymbol{L}$ in $1, 2$ and 3 times respectively, and the total latency is as 6 times as that of a single $\boldsymbol{L}$. On the other hand, we propose an area-latency trade-off to reduce the latency by slightly increasing the area. Again we take $z = 4$ and

$\boldsymbol{L}_2 = \boldsymbol{L}, \boldsymbol{L}_3 = \boldsymbol{L}^2$ and $\boldsymbol{L}_4 = \boldsymbol{L}^3$ for an example. In this case we instantiate a circuit of $\boldsymbol{L}$ and a circuit of $\boldsymbol{L}^2$. Then taking $\boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4 \in GF(2)^4$ as inputs, the output states $\boldsymbol{L}_2\boldsymbol{x}_2, \boldsymbol{L}_3\boldsymbol{x}_3, \boldsymbol{L}_4\boldsymbol{x}_4$ can be computed in two steps, i.e., firstly compute $\boldsymbol{L}\boldsymbol{x}_2$ and $\boldsymbol{L}^2\boldsymbol{x}_4$, then compute $\boldsymbol{L}(\boldsymbol{L}^2\boldsymbol{x}_4)$ and $\boldsymbol{L}^2\boldsymbol{x}_3$. As a result, the total latency is reduced by a third at the cost of double area[11]. In Table 9 we list the area-latency trade-off for our construction for $4 \leq z \leq 7$.

A More Scalable Construction. Our construction can be naturally extended to choose $c \times c$ ($c \geq 4$) matrices $\boldsymbol{L}_i$'s such that the 'block-MDS' property in (12) is satisfied. The discussion is given in Supplementary Material H in our full version paper [53], where possible ways to extend the tweakey size for SKINNY-128 are introduced. Similar methods can also be applied to Deoxys-BC to extend its tweakey size.

Table 9: The area-latency trade-off for our construction.

z	$\{\boldsymbol{L}_i\}_{2\leq i\leq z}$	Instantiated circuit	Area	Latency
4	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3\}$	$\{\boldsymbol{L}\}$	1	6
	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3\}$	$\{\boldsymbol{L}, \boldsymbol{L}^2\}$	2	2
5	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4\}$	$\{\boldsymbol{L}\}$	1	10
	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}, \boldsymbol{L}^2, \boldsymbol{L}^{-2}\}$	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}\}$	2	3
	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4\}$	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3\}$	3	2
6	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4, \boldsymbol{L}^5\}$	$\{\boldsymbol{L}\}$	1	15
	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4, \boldsymbol{L}^5\}$	$\{\boldsymbol{L}, \boldsymbol{L}^2\}$	2	4
	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4, \boldsymbol{L}^5\}$	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^4\}$	3	3
	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4, \boldsymbol{L}^5\}$	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4\}$	4	2
7	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4, \boldsymbol{L}^5, \boldsymbol{L}^6\}$	$\{\boldsymbol{L}\}$	1	21
	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}, \boldsymbol{L}^2, \boldsymbol{L}^{-2}, \boldsymbol{L}^3, \boldsymbol{L}^{-3}\}$	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}\}$	2	6
	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^3, \boldsymbol{L}^4, \boldsymbol{L}^5, \boldsymbol{L}^6\}$	$\{\boldsymbol{L}, \boldsymbol{L}^2, \boldsymbol{L}^4\}$	3	3
	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}, \boldsymbol{L}^2, \boldsymbol{L}^{-2}, \boldsymbol{L}^3, \boldsymbol{L}^{-3}\}$	$\{\boldsymbol{L}, \boldsymbol{L}^{-1}, \boldsymbol{L}^2, \boldsymbol{L}^{-2}\}$	4	2

7 Conclusion

The unexpected cancellations in the new tweakey schedule of SKINNYe-64-256 significantly enhances several attacks on SKINNYe-64-256 when compared to that on SKINNY-64-128 and SKINNY-64-192, and leaves a security margin of 3 rounds in related-tweakey setting. Moreover, we give some cryptanalysis results on the updated version 2, which indicates that the current version satisfies the security claims of the designers. At last, we introduce a uniformed design strategy

[11] The area of the trade-off implementation mainly includes the circuit for $\boldsymbol{L}$ and $\boldsymbol{L}^2$ and two 4-bit registers. In area optimization implementation, the area is the circuit of $\boldsymbol{L}$ and one 4-bit register. Assume the registers bound the area, we can say trade-off method costs double area.

for the tweakey schedule of SKINNY-n-zn ($z \leq 14$), and prove that it satisfies the security requirements of the STK construction.

At CRYPTO 2022, Naito, Sasaki, Sugawara further introduced a new tweakable block cipher SKINNYee [49] based on SKINNYe-64-256 version 2. It supports 128-bit key and a (256+3)-bit tweak with a 64-bit plaintext block. The method to extend the tweakey size is different from what we suggest in Section 6. It is an interesting open problem to explore its security margin.

Acknowledgments

We would like to thank the anonymous reviewers from ASIACRYPT 2022 for their valuable comments. This work is supported by National Key R&D Program of China (2018YFA0704701), the Major Program of Guangdong Basic and Applied Research (2019B030302008), Natural Science Foundation of China (62272257, 61902207, 62072270, 62072207), Major Scientific and Technological Innovation Project of Shandong Province, China (2020ZLYS09 and 2019JZZY010133), Natural Science Foundation of Shanghai (19ZR1420000), and Open Foundation of Network and Data Security Key Laboratory of Sichuan Province (University of Electronic Science and Technology of China).

References

1. Alexandre Adomnicai, Thierry P. Berger, Christophe Clavier, Julien Francq, Paul Huynh, Virginie Lallemand, Kévin Le Gouguec, Marine Minier, Léo Reynaud, and Gëel Thomas. Lilliput-AE: a new lightweight tweakable block cipher for authenticated encryption with associated data. *Submission to NIST Lightweight Cryptography Project*, 2019.
2. Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In *ASIACRYPT 2016, Proceedings, Part I*, volume 10031 of *LNCS*, pages 191–219.
3. Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. Ciphers for MPC and FHE. In *EUROCRYPT 2015, Proceedings, Part I*, volume 9056 of *LNCS*, pages 430–454.
4. Ralph Ankele, Subhadeep Banik, Avik Chakraborti, Eik List, Florian Mendel, Siang Meng Sim, and Gaoli Wang. Related-key impossible-differential attack on reduced-round SKINNY. In *ACNS 2017*, volume 10355, pages 208–228.
5. Kazumaro Aoki and Yu Sasaki. Preimage attacks on one-block MD4, 63-step MD5 and more. In *SAC 2008*, volume 5381 of *LNCS*, pages 103–119.
6. Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A small present - towards reaching the limit of lightweight encryption. In *CHES 2017, Proceedings*, volume 10529, pages 321–345.
7. Zhenzhen Bao, Xiaoyang Dong, Jian Guo, Zheng Li, Danping Shi, Siwei Sun, and Xiaoyun Wang. Automatic search of meet-in-the-middle preimage attacks on aes-like hashing. In *EUROCRYPT 2021, Part I*, volume 12696, pages 771–804.
8. Zhenzhen Bao, Jian Guo, Danping Shi, and Yi Tu. Superposition Meet-in-the-Middle attacks: Updates on fundamental security of AES-like hashing. In *CRYPTO 2022*.

9. Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In *CRYPTO 2016, Proceedings, Part II*, pages 123–153.
10. Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. Cryptology ePrint Archive, Report 2016/660, 2016.
11. Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks. *IACR Transactions on Symmetric Cryptology*, 2019(1):5–45.
12. Davide Bellizia, Francesco Berti, Olivier Bronchain, Gaëtan Cassiers, Sébastien Duval, Chun Guo, Gregor Leander, Gaëtan Leurent, Itamar Levi, Charles Momin, Olivier Pereira, Thomas Peters, François-Xavier Standaert, Balazs Udvarhelyi, and Friedrich Wiemer. Spook: Sponge-based leakage-resistant authenticated encryption with a masked tweakable block cipher. *IACR Transactions on Symmetric Cryptology*, 2020(S1):295–349.
13. Tim Beyne and Begül Bilgin. Uniform first-order threshold implementations. In *SAC 2016*, volume 10532 of *LNCS*, pages 79–98.
14. Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In *EUROCRYPT '99, Proceeding*, volume 1592 of *LNCS*, pages 12–23.
15. Eli Biham, Orr Dunkelman, and Nathan Keller. New cryptanalytic results on IDEA. In *ASIACRYPT 2006, Proceedings*, pages 412–427.
16. Eli Biham, Orr Dunkelman, and Nathan Keller. New results on boomerang and rectangle attacks. In *FSE 2002, Revised Papers*, volume 2365, pages 1–16.
17. Eli Biham, Orr Dunkelman, and Nathan Keller. The rectangle attack - rectangling the serpent. In *EUROCRYPT 2001, Proceeding*, volume 2045, pages 340–357.
18. Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In *EUROCRYPT 2005, Proceedings*, volume 3494, pages 507–525.
19. Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In *ASIACRYPT 2009*, volume 5912, pages 1–18.
20. Andrey Bogdanov and Christian Rechberger. A 3-subset meet-in-the-middle attack: Cryptanalysis of the lightweight block cipher KTANTAN. In *SAC 2010*, volume 6544 of *LNCS*, pages 229–240.
21. Christina Boura and Anne Canteaut. On the boomerang uniformity of cryptographic sboxes. *IACR Transactions on Symmetric Cryptology*, 2018(3):290–310.
22. Anne Canteaut, María Naya-Plasencia, and Bastien Vayssière. Sieve-in-the-middle: Improved MITM attacks. In *CRYPTO 2013, Part I*, volume 8042, pages 222–240.
23. Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In *EUROCRYPT 2018, Proceedings, Part II*, volume 10821, pages 683–714.
24. Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. Catching the fastest boomerangs application to SKINNY. *IACR Transactions on Symmetric Cryptology*, 2020(4):104–129.
25. Patrick Derbez and Pierre-Alain Fouque. Automatic search of Meet-in-the-Middle and Impossible Differential attacks. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016 Proceedings, Part II*, volume 9815, pages 157–184.
26. Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved key recovery attacks on reduced-round AES in the single-key setting. In *EUROCRYPT 2013*, volume 7881, pages 371–387.

27. Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Efficient dissection of composite problems, with applications to cryptanalysis, knapsacks, and combinatorial search problems. In *CRYPTO 2012*, volume 7417, pages 719–740.
28. Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, and Thomas Unterluggauer. ISAP - towards side-channel secure authenticated encryption. *IACR Transactions on Symmetric Cryptology*, 2017(1):80–105, 2017.
29. Xiaoyang Dong, Jialiang Hua, Siwei Sun, Zheng Li, Xiaoyun Wang, and Lei Hu. Meet-in-the-middle attacks revisited: Key-recovery, collision, and preimage attacks. In *CRYPTO 2021, Proceedings, Part III*, volume 12827 of *LNCS*, pages 278–308.
30. Xiaoyang Dong, Lingyue Qin, Siwei Sun, and Xiaoyun Wang. Key guessing strategies for linear key-schedule algorithms in rectangle attacks. In *EUROCRYPT 2022, Proceedings, Part III*, volume 13277 of *LNCS*, pages 3–33, 2022.
31. Orr Dunkelman, Senyang Huang, Eran Lambooij, and Stav Perle. Single tweakey cryptanalysis of reduced-round SKINNY-64. In *CSCML 2020, Proceedings*, volume 12161, pages 1–17. Springer, 2020.
32. Orr Dunkelman, Nathan Keller, Eran Lambooij, and Yu Sasaki. A practical forgery attack on Lilliput-AE. *J. Cryptol.*, 33(3):910–916, 2020.
33. Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. In *ASIACRYPT 2010, Proceedings*, pages 158–176.
34. Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. *J. Cryptology*, 27(4):824–849, 2014.
35. Thomas Fuhr and Brice Minaud. Match box meet-in-the-middle attack against KATAN. In *FSE 2014*, volume 8540 of *LNCS*, pages 61–81.
36. Si Gao, Arnab Roy, and Elisabeth Oswald. Constructing TI-friendly substitution boxes using shift-invariant permutations. In *CT-RSA 2019, Proceedings*, volume 11405 of *LNCS*, pages 433–452.
37. Hosein Hadipour, Nasour Bagheri, and Ling Song. Improved rectangle attacks on SKINNY and CRAFT. *IACR Transactions on Symmetric Cryptology*, 2021(2):140–198.
38. Jialiang Hua, Xiaoyang Dong, Siwei Sun, Zhiyu Zhang, Lei Hu, and Xiaoyun Wang. Improved MITM cryptanalysis on Streebog. *IACR Trans. Symmetric Cryptol.*, 2022(2):63–91, 2022.
39. Jialiang Hua, Tai Liu, Yulong Cui, Lingyue Qin, Xiaoyang Dong, and Huiyong Cui. Low-data cryptanalysis on SKINNY block cipher. *The Computer Journal*, 2022.
40. Yuval Ishai, Amit Sahai, and David A. Wagner. Private circuits: Securing hardware against probing attacks. In *CRYPTO 2003*, volume 2729, pages 463–481.
41. Takanori Isobe. A single-key attack on the full GOST block cipher. In *FSE 2011*, volume 6733 of *LNCS*, pages 290–305.
42. Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In *ASIACRYPT 2014*, volume 8874, pages 274–288.
43. Jérémy Jean, Ivica Nikolić, Thomas Peyrin, and Yannick Seurin. Submission to CAESAR : Deoxys v1.41, October 2016.
44. John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In *FSE 2000*, volume 1978, pages 75–93.
45. L. R. Knudsen. DEAL - a 128-bit block cipher. *Complexity*, 1998.
46. Guozhen Liu, Mohona Ghosh, and Ling Song. Security analysis of SKINNY under related-tweakey settings. *IACR Transactions on Symmetric Cryptology*, 2017(3):37–72.

47. Bart Mennink. Beyond birthday bound secure fresh rekeying: Application to authenticated encryption. In *ASIACRYPT 2020*, volume 12491, pages 630–661.
48. Yusuke Naito, Yu Sasaki, and Takeshi Sugawara. Lightweight authenticated encryption mode suitable for threshold implementation. In *EUROCRYPT 2020, Proceedings, Part II*, volume 12106 of *LNCS*, pages 705–735.
49. Yusuke Naito, Yu Sasaki, and Takeshi Sugawara. Secret can be public: Low-memory AEAD mode for high-order masking. In *CRYPTO 2022*.
50. Yusuke Naito, Yu Sasaki, and Takeshi Sugawara. Lightweight authenticated encryption mode suitable for threshold implementation. *Cryptol. ePrint Arch.*, 2020.
51. Yusuke Naito and Takeshi Sugawara. Lightweight authenticated encryption mode of operation for tweakable block ciphers. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(1):66–94, 2020.
52. Svetla Nikova, Christian Rechberger, and Vincent Rijmen. Threshold implementations against side-channel attacks and glitches. In *ICICS 2006, Proceedings*, volume 4307 of *LNCS*, pages 529–545.
53. Lingyue Qin, Xiaoyang Dong, Anyu Wang, Jialiang Hua, and Xiaoyun Wang. Mind the tweakey schedule: Cryptanalysis on skinnye-64-256. Cryptology ePrint Archive, Paper 2022/789, 2022. https://eprint.iacr.org/2022/789.
54. Lingyue Qin, Xiaoyang Dong, Xiaoyun Wang, Keting Jia, and Yunwen Liu. Automated search oriented to key recovery on ciphers with linear key schedule applications to boomerangs in SKINNY and ForkSkinny. *IACR Transactions on Symmetric Cryptology*, 2021(2):249–291.
55. Joseph J Rotman. *Advanced modern algebra*. American Mathematical Soc., 2010.
56. Sadegh Sadeghi, Tahereh Mohammadi, and Nasour Bagheri. Cryptanalysis of reduced round SKINNY block cipher. *IACR Transactions on Symmetric Cryptology*, 2018(3):124–162, 2018.
57. Yu Sasaki. Integer linear programming for three-subset meet-in-the-middle attacks: Application to GIFT. In *IWSEC 2018*, volume 11049, pages 227–243.
58. Yu Sasaki. Meet-in-the-middle preimage attacks on AES hashing modes and an application to whirlpool. In *FSE 2011*, volume 6733 of *LNCS*, pages 378–396.
59. Yu Sasaki and Kazumaro Aoki. Finding preimages in full MD5 faster than exhaustive search. In *EUROCRYPT 2009*, volume 5479, pages 134–152.
60. André Schrottenloher and Marc Stevens. Simplified MITM modeling for permutations: New (quantum) attacks. In *CRYPTO 2022*.
61. Ling Song, Xianrui Qin, and Lei Hu. Boomerang connectivity table revisited. application to SKINNY and AES. *IACR Transactions on Symmetric Cryptology*, 2019(1):118–141.
62. Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef. Impossible differential cryptanalysis of reduced-round SKINNY. In *AFRICACRYPT 2017, Proceedings*, volume 10239, pages 117–134.
63. David A. Wagner. The boomerang attack. In *FSE '99*, volume 1636, pages 156–170.
64. Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. application to AES variants and Deoxys. *IACR Transactions on Symmetric Cryptology*, 2019(1):142–169.