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

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

[1]BNRist, Tsinghua University, Beijing, China
[2]Institute for Advanced Study, BNRist, Tsinghua University, Beijing, China
[3]Key Laboratory of Cryptologic Technology and Information Security (Ministry of Education), School of Cyber Science and Technology, Shandong University, Qingdao, China
[4]National Financial Cryptography Research Center, Beijing, China
[5]Zhongguancun Lab., Beijing, China

December 4, 2022

Outline

Outline

Background

- The TWEAKEY framework , Jean et al. [JNP14]

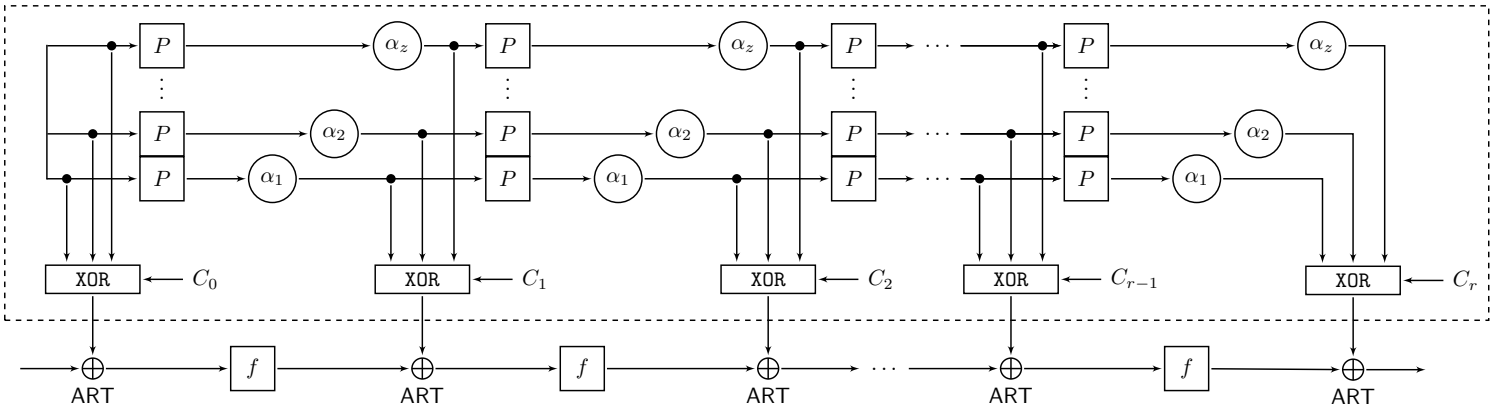
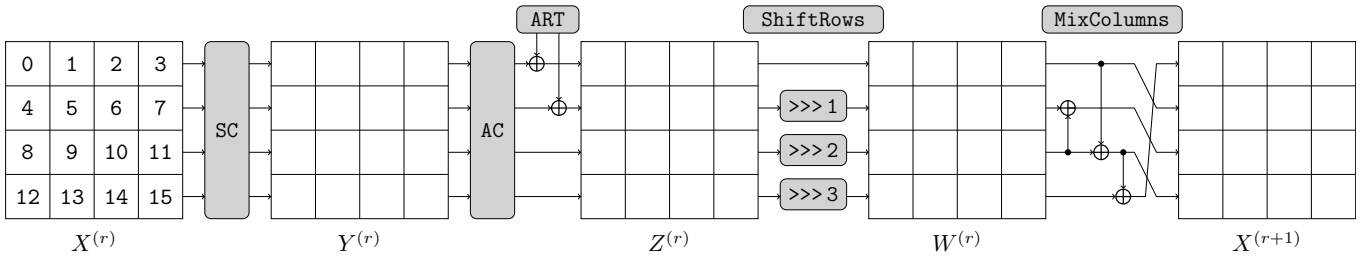


Figure: The STK construction.

SKINNY family and SKINNYe-64-256

- The SKINNY family: proposed by Beierle et al. [BJK+16]
  - SKINNY-*n*-*zn*: $n \in \{64, 128\}$, $z = 1, 2, 3$



- SKINNYe-64-256: Naito et al. [NSS20a]
  - same round function, new tweakey schedule?
  - SKINNYe-64-256 version 2 [NSS20b]

Our contribution

- Give a formal analysis of properties of the new tweakey schedule
- Cryptanalysis on SKINNYe-64-256
  - Rectangle attack in related-tweakey setting (41/44 rounds)
  - MITM attack in single-tweakey setting (37/44 rounds)
  - Impossible differential attack in related-tweakey setting
- Propose a uniformed design strategy for tweakey schedule of SKINNY-n-zn ($z \leq 14$)

Outline

Tweakey schedule for SKINNYe-64-256

- 256-bit tweakey $(TK_1,\ TK_2,\ TK_3,\ TK_4)$
  - $TK^{(r)}_{m,i} \leftarrow LFSR_m(TK^{(r-1)}_{m,P[i]})$
  - $STK^{(r)}_i = TK^{(r)}_{1,i} \oplus TK^{(r)}_{2,i} \oplus TK^{(r)}_{3,i} \oplus TK^{(r)}_{4,i}$
- For a set of subtweakeys $\{STK^{(2r_1)}, STK^{(2r_2)} \cdots, STK^{(2r_t)}\}$

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

  - $\boldsymbol{A}_{r_j} = [\boldsymbol{I}\ \boldsymbol{L}_2^{r_j}\ \boldsymbol{L}_3^{r_j}\ \boldsymbol{L}_4^{r_j}]$, $\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}} = [\boldsymbol{A}_{r_1}^T\ \boldsymbol{A}_{r_2}^T\ \cdots\ \boldsymbol{A}_{r_t}^T]^T$

Tweakey schedule for SKINNYe-64-256

- $rank(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}) = a$
  - $|Im(\boldsymbol{A})| = 2^a$: solution space of $\{STK^{(2r_1)}_{\bar{P}^{2r_1}[i]}, STK^{(2r_2)}_{\bar{P}^{2r_2}[i]} \cdots, STK^{(2r_t)}_{\bar{P}^{2r_t}[i]}\}$
  - $|Ker(\boldsymbol{A})| = 2^{16-a}$: $Ker(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{F}_2^{4t} : \boldsymbol{A}\boldsymbol{x} = 0\}$
- Example: $[\boldsymbol{stk}_0^{(0)}, \boldsymbol{stk}_2^{(2)}, \boldsymbol{stk}_4^{(4)}, \boldsymbol{stk}_6^{(6)}]^T = \boldsymbol{A}_{\{0,1,2,3\}} \cdot [\boldsymbol{tk}_{1,i}^{(0)}, \boldsymbol{tk}_{2,i}^{(0)}, \boldsymbol{tk}_{3,i}^{(0)}, \boldsymbol{tk}_{4,i}^{(0)}]^T$

$$\begin{pmatrix} \boldsymbol{stk}_0^{(0)} \\ \boldsymbol{stk}_2^{(2)} \\ \boldsymbol{stk}_4^{(4)} \\ \boldsymbol{stk}_6^{(6)} \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \\ 1&0&0&0&0&1&0&0&1&0&0&1&0&1&0&0 \\ 0&1&0&0&0&0&1&0&1&0&0&0&0&0&1&0 \\ 0&0&1&0&0&0&0&1&0&1&0&0&0&1&0&1 \\ 0&0&0&1&1&1&0&0&0&0&1&0&1&1&1&0 \\ 1&0&0&0&0&0&1&0&1&0&1&1&0&0&1&0 \\ 0&1&0&0&0&0&0&1&1&0&0&1&0&1&0&1 \\ 0&0&1&0&1&1&0&0&1&0&0&0&1&1&0&0 \\ 0&0&0&1&0&1&1&0&0&1&0&0&0&0&1&1 \\ 1&0&0&0&0&0&0&1&1&1&1&1&0&1&0&1 \\ 0&1&0&0&1&1&0&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&0&1&0&1&1&0 \\ 0&0&0&1&0&0&1&1&1&0&0&0&1&0&1&1 \end{pmatrix} \cdot \begin{pmatrix} x_{1,0} \\ x_{1,1} \\ x_{1,2} \\ x_{1,3} \\ x_{2,0} \\ x_{2,1} \\ x_{2,2} \\ x_{2,3} \\ x_{3,0} \\ x_{3,1} \\ x_{3,2} \\ x_{3,3} \\ x_{4,0} \\ x_{4,1} \\ x_{4,2} \\ x_{4,3} \end{pmatrix}$$

- $rank(\boldsymbol{A}_{\{0,1,2,3\}}) = 14 \Longrightarrow$ image space 2^{14}, kernel space 2^2

Properties of the tweakey schedule

- $\boldsymbol{A}_{\{r_1+r',r_2+r',\cdots,r_t+r'\}} = \boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}} \cdot diag(\boldsymbol{I}, \boldsymbol{L}_2^{r'}, \boldsymbol{L}_3^{r'}\ \boldsymbol{L}_4^{r'})$

$$\begin{pmatrix} \boldsymbol{I} & \boldsymbol{L}_2^{r_1+r'} & \boldsymbol{L}_3^{r_1+r'} & \boldsymbol{L}_4^{r_1+r'} \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_2+r'} & \boldsymbol{L}_3^{r_2+r'} & \boldsymbol{L}_4^{r_2+r'} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_t+r'} & \boldsymbol{L}_3^{r_t+r'} & \boldsymbol{L}_4^{r_t+r'} \end{pmatrix} = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{L}_2^{r_1} & \boldsymbol{L}_3^{r_1} & \boldsymbol{L}_4^{r_1} \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_2} & \boldsymbol{L}_3^{r_2} & \boldsymbol{L}_4^{r_2} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{I} & \boldsymbol{L}_2^{r_t} & \boldsymbol{L}_3^{r_t} & \boldsymbol{L}_4^{r_t} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{I} & & & \\ & \boldsymbol{L}_2^{r'} & & \\ & & \boldsymbol{L}_3^{r'} & \\ & & & \boldsymbol{L}_4^{r'} \end{pmatrix}$$

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

Definition (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

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

Rank-equivalence class for SKINNYe-64-256

- Rank-equivalence class: $[x] := \{y \subset \mathcal{K} : x \text{ and } y \text{ are rank-equivalent}\}$
  - $rank(\boldsymbol{A}_x) = rank(\boldsymbol{A}_y)$
- $rank(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}) = \min\{4t, 16\} \Longleftrightarrow \boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}$ is a full rank matrix

rank	t	Rank-equivalence class $[\{r_1, r_2, \cdots, r_t\}]$	Num.
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}], ...	28
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},] ...	63
	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}], ...	77
	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}], ...	35
	7	[{0,1,2,3,7,10,11}],[{0,1,2,3,7,10,13}],[{0,1,2,3,7,11,13}], ...	9
	8	[{0,1,2,3,7,10,11,13}]	1

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

The subtweakey difference cancellations

- SKINNY-*n*-*zn* ($z = 2, 3$): for given active cell, $z - 1$ subtweakey difference cancellations happen in every 30 rounds
- SKINNYe-64-256: applying rank-equivalence class of non-full rank
- $\boldsymbol{A}_{[\{r_1, r_2, \cdots, r_t\}]} \cdot [\Delta \boldsymbol{tk}_{1,i}^{(0)}, \Delta \boldsymbol{tk}_{2,i}^{(0)}, \Delta \boldsymbol{tk}_{3,i}^{(0)}, \Delta \boldsymbol{tk}_{4,i}^{(0)}]^T = \boldsymbol{0}$
  - cancellations happen in $\{STK_{\bar{P}^{2r_1}[i]}^{(2r_1)} \cdots, STK_{\bar{P}^{2r_t}[i]}^{(2r_t)}\}$
  - $rank(\boldsymbol{A}_{[\{r_1, r_2, \cdots, r_t\}]}) = 16$, there has only zero solution
  - $rank(\boldsymbol{A}_{[\{r_1, r_2, \cdots, r_t\}]}) < 16$, there has non-zero solution

Difference cancellation behaviour of rank-equivalence class

- $t = 4$: $\boldsymbol{A}_{\{r_1,r_2,r_3,r_4\}}$ is non-full rank
  - for given nibble, 4 cancellations happen in arbitrary rounds
- $t \geq 5$: $rank(\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t\}]}) = 15$, $|Ker(\boldsymbol{A}_{[\{r_1,r_2,\cdots,r_t\}]})| = 2$
  - different rank-equivalence classes corresponds to same non-zero solution

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

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

$\boldsymbol{tk}_{1,i}^{(0)} = [0,0,0,1]^T$, $\boldsymbol{tk}_{2,i}^{(0)} = [0,1,1,1]^T$,
$\boldsymbol{tk}_{3,i}^{(0)} = [0,0,0,0]^T$, $\boldsymbol{tk}_{4,i}^{(0)} = [0,1,1,0]^T$

  - two kinds of difference cancellation behaviours
    - $[\{0,1,2,4,5,8,10\}]$, $[\{0,1,2,3,7,10,11,13\}]$
    - 7 or 8 cancellations in fixed positions every 30 rounds

Key guessing strategy based on the relations

- similar idea of the key-bridge technique
- a set of $\{\boldsymbol{stk}^{(2r_1)}_{\bar{P}^{2r_1}[i]}, \boldsymbol{stk}^{(2r_2)}_{\bar{P}^{2r_2}[i]} \cdots, \boldsymbol{stk}^{(2r_t)}_{\bar{P}^{2r_t}[i]}, \boldsymbol{stk}^{(2r_{t+1})}_{\bar{P}^{2r_{t+1}}[i]}\}$
  - $rank(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}}) = a$, $rank(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t,r_{t+1}\}}) = b$
  - solution space of $\{\boldsymbol{stk}^{(2r_1)}_{\bar{P}^{2r_1}[i]}, \boldsymbol{stk}^{(2r_2)}_{\bar{P}^{2r_2}[i]} \cdots, \boldsymbol{stk}^{(2r_t)}_{\bar{P}^{2r_t}[i]}\}$: $|Im(\boldsymbol{A}_{\{r_1,r_2,\cdots,r_t\}})| = 2^a$
  - $\boldsymbol{stk}^{(2r_{t+1})}_{\bar{P}^{2r_{t+1}}[i]}$: 2^{b-a} guessing

Outline

Boomerang and Rectangle attacks

- Boomerang attack, Wagner [Wag99]
  - $E = E_f \circ \underbrace{E_1}_{\gamma \xrightarrow{q} \delta} \circ \underbrace{E_0}_{\alpha \xrightarrow{p} \beta} \circ E_b$
- Rectangle attack [BDK01]
  - several key-recovery frameworks [BDK01, BDK02, BDK06, LGS17]
  - Dong *et al.*'s related-key rectangle framework for ciphers with linear key schedule [DQSW22]

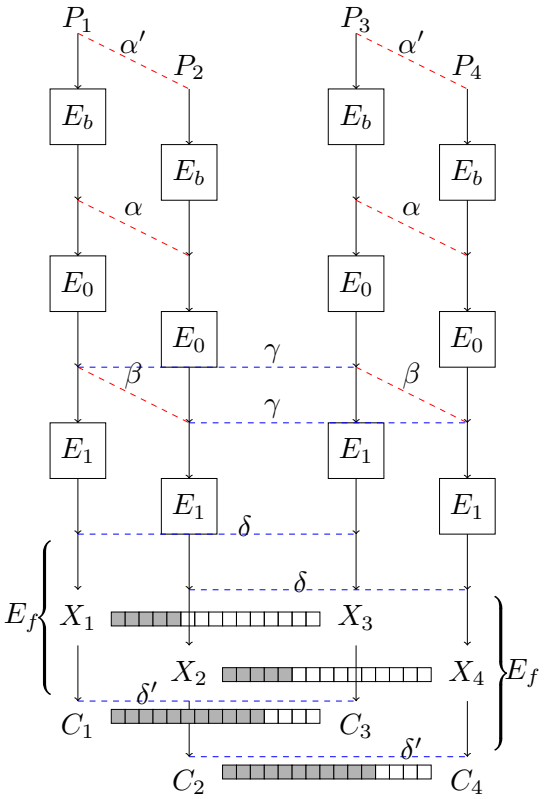
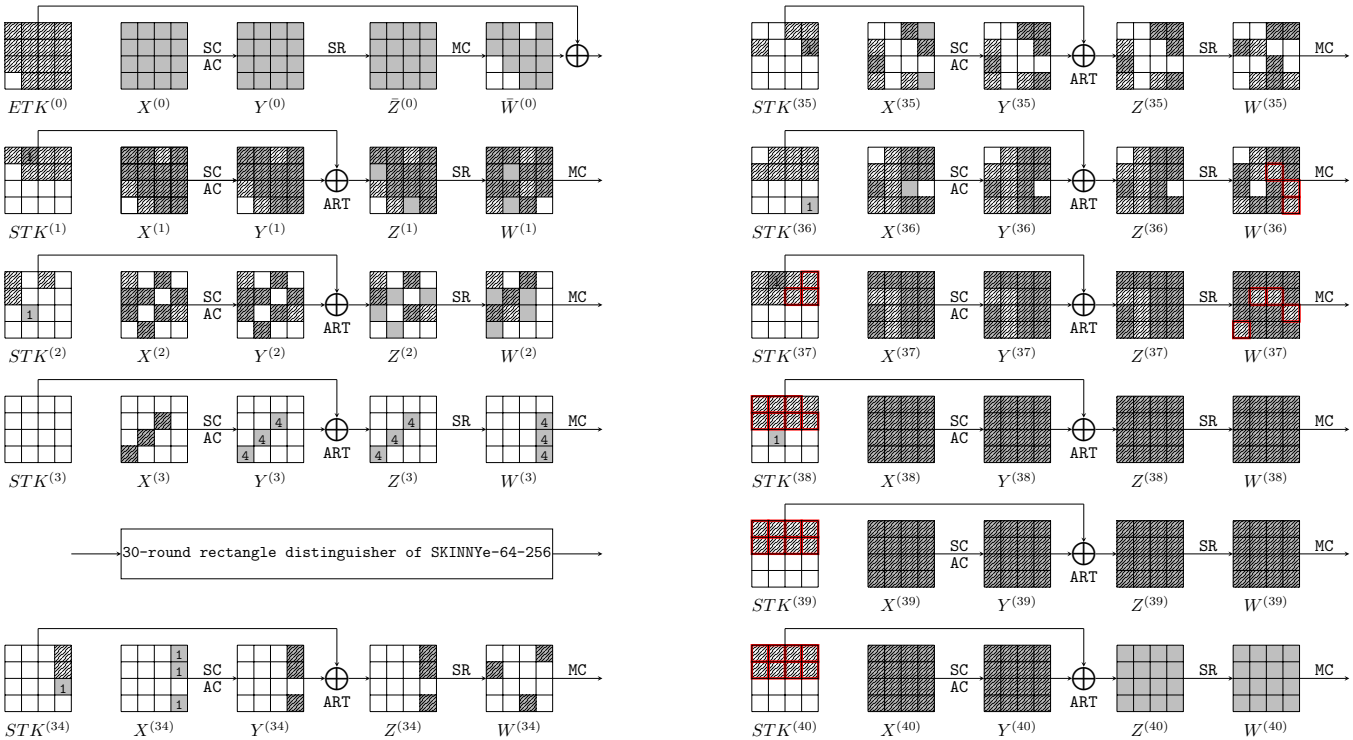


Figure: [DQSW22]

Rectangle attacks on SKINNYe-64-256

- Dong *et al.*'s rectangle attack framework: search the entire $(N_b + N_d + N_f)$-round attack [DQSW22]
- Constraints of different subtweakey difference cancellations:
  - $t \leq 4$: $stk_0^{(0)} + stk_{P^2[0]}^{(2)} + \cdots + stk_{P^{28}[0]}^{(28)} - 15 \cdot \mathrm{LANE}_0 \geq -4$
  - $t > 4$: fixed the positions of difference cancellation with rank-equivalence class $[\{0, 1, 2, 4, 5, 8, 10\}]$ and $[\{0, 1, 2, 3, 7, 10, 11, 13\}]$
- 30-round distinguisher following $[\{0, 1, 2, 3, 7, 10, 11, 13\}]$

Related-key rectangle attack on 41-round SKINNYe-64-256



- 41-round attack: 4-round E_b + 30-round E_d + 7-round E_f
  - key relations in the key-recovery phase

MITM and impossible differential attacks on SKINNYe-64-256

- Meet-in-the-Middle attack [BR10, Iso11]
  - MILP model for MITM key-recovery attack on SKINNY [DHS+21]
  - MITM key-recovery attacks on 31-round SKINNYe-64-256 in single-tweakey setting
- Impossible differential attack [BBS99, Knu98]
  - 21-round impossible differential on SKINNYe-64-256 in related-tweakey setting

Attacks on SKINNY-64 and SKINNYe-64-256 and its version 2

Version	Rounds	Data	Time	Memory	Approach	Setting	Ref.
SKINNY-64-128	23/36	$2^{60.54}$	$2^{120.7}$	$2^{60.9}$	Rectangle	RK	[HBS21]
	24/36	$2^{61.67}$	$2^{96.83}$	2^{84}	Rectangle	RK	[QDW+21]
	25/36	$2^{61.67}$	$2^{118.43}$	$2^{64.26}$	Rectangle	RK	[DQSW22]
SKINNY-64-192	29/40	$2^{62.92}$	$2^{181.7}$	2^{80}	Rectangle	RK	[HBS21]
	30/40	$2^{62.87}$	$2^{163.11}$	$2^{68.05}$	Rectangle	RK	[QDW+21]
	31/40	$2^{62.78}$	$2^{182.07}$	$2^{62.79}$	Rectangle	RK	[DQSW22]
SKINNYe-64-256	41/44	$2^{62.24}$	$2^{237.06}$	$2^{62.26}$	Rectangle	RK	Ours
SKINNYe-64-256 v2	37/44	$2^{62.8}$	$2^{240.03}$	$2^{62.8}$	Rectangle	RK	Ours
SKINNY-64-128	18/36	2^{16}	2^{124}	2^{4}	MITM	SK	[HLC+22]
SKINNY-64-192	23/40	2^{52}	2^{188}	2^{4}	MITM	SK	[DHS+21]
SKINNYe-64-256	31/44	2^{52}	2^{254}	2^{52}	MITM	SK	Ours
SKINNYe-64-256 v2	27/44	2^{52}	2^{252}	2^{52}	MITM	SK	Ours

Outline

A proposal for tweakey schedule of SKINNY family

- SKINNY-n-zn $(1 \leq z \leq 14)$
  - *Subtweakey difference cancellation property* (similar to STK)
  - for a given cell, $z-1$ cancellations in every 15 rounds for TK-z

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

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

The choice of L_i

- $\boldsymbol{L}_1 = \boldsymbol{I}$,$\{\boldsymbol{L}_i\}_{1\le i\le z} = \{\boldsymbol{L}^{\alpha+1}, \cdots, \boldsymbol{L}^{\alpha+z}\}$ $(\alpha \in [-z, -1])$

Proposition

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*,*

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

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

Construction of L

- L: the companion matrix of a primitive polynomial
  - Example: primitive polynomial $\lambda^4 + \lambda + 1$

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

- Example $z = 4$: $\{L^{-1}, L^0, L^1, L^2\}$, $L_2 = L^1$, $L_3 = L^{-1}$, $L_4 = L^2$

$$L_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, L_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, L_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Efficiency considerations

- Implementation optimization of minimizing the total number of XORs required by the LFSRs

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

Table: Optimal number of XORs required in our construction

Efficiency considerations

- Optimization of minimizing the circuit area of the LFSRs

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

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

Thanks for Your Attention!

Reference I


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, 1999.


Eli Biham, Orr Dunkelman, and Nathan Keller.
The rectangle attack - rectangling the serpent.
In *EUROCRYPT 2001, Proceeding*, volume 2045, pages 340–357, 2001.


Eli Biham, Orr Dunkelman, and Nathan Keller.
New results on boomerang and rectangle attacks.
In *FSE 2002, Revised Papers*, volume 2365, pages 1–16, 2002.


Eli Biham, Orr Dunkelman, and Nathan Keller.
New cryptanalytic results on IDEA.
In *ASIACRYPT 2006, Proceedings*, pages 412–427, 2006.


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, 2016.

Reference II


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, 2010.


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, 2021.


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.


Hosein Hadipour, Nasour Bagheri, and Ling Song.
Improved rectangle attacks on SKINNY and CRAFT.
IACR Transactions on Symmetric Cryptology, 2021(2):140–198, 2021.

Reference III


Jialiang Hua, Tai Liu, Yulong Cui, Lingyue Qin, Xiaoyang Dong, and Huiyong Cui.
Low-data cryptanalysis on SKINNY block cipher.
The Computer Journal, 2022.


Takanori Isobe.
A single-key attack on the full GOST block cipher.
In *FSE 2011*, volume 6733 of *LNCS*, pages 290–305, 2011.


Jérémy Jean, Ivica Nikolic, and Thomas Peyrin.
Tweaks and keys for block ciphers: The TWEAKEY framework.
In *ASIACRYPT 2014*, volume 8874, pages 274–288, 2014.


L. R. Knudsen.
DEAL - a 128-bit block cipher.
Complexity, 1998.


Guozhen Liu, Mohona Ghosh, and Ling Song.
Security analysis of SKINNY under related-tweakey settings.
IACR Transactions on Symmetric Cryptology, 2017(3):37–72, 2017.

Reference IV


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, 2020.


Yusuke Naito, Yu Sasaki, and Takeshi Sugawara.
Lightweight authenticated encryption mode suitable for threshold implementation.
Cryptol. ePrint Arch., 2020.


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, 2021.


David A. Wagner.
The boomerang attack.
In *FSE '99, Proceedings*, volume 1636, pages 156–170, 1999.