Cryptanalysis of Reduced round SKINNY Block Cipher

Sadegh Sadeghi[1], Tahereh Mohammadi[2] and Nasour Bagheri[2,3]

[1] Department of Mathematics, Faculty of Mathematical Sciences and Computer, Kharazmi University, Tehran, Iran, S.Sadeghi.Khu@gmail.com

[2] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran, {T.Mohammadi,Nabgheri}@sru.ac.ir

[3] School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran, Na.bagheri@gmail.com

Outline

- A brief description of SKINNY
- Zero-Correlation Linear Cryptanalysis of SKINNY
- MILP model for SKINNY64 cipher
  - Using MILP in Impossible differential cryptanalysis
- Searching Related-tweakey Impossible Differential Characteristics of SKINNY
- The related-tweakey Impossible Differential attack of SKINNY
- Conclusion
  - Cryptanalytic Results

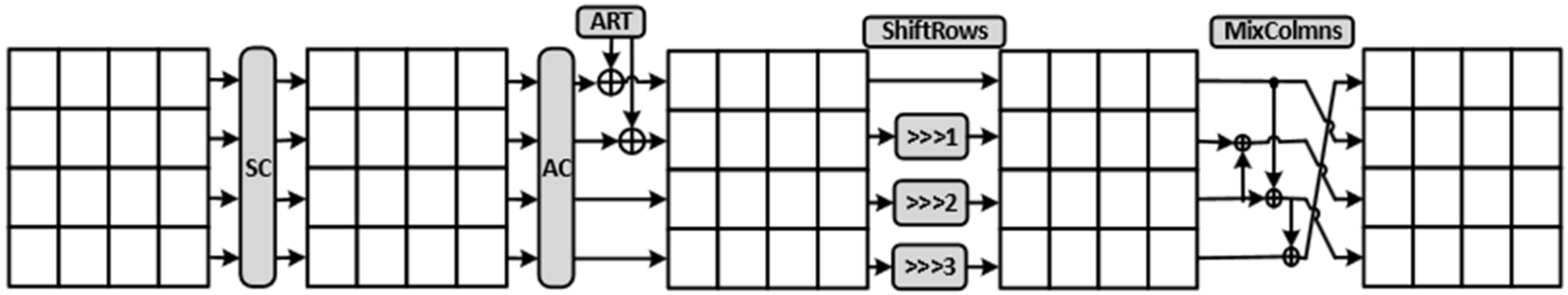
A brief description of SKINNY

- SKINNY was introduced in CRYPTO'16. The variants of SKINNY are denoted as SKINNY-n-t, $t \in \{n, 2n, 3n\}$ (or TK1, TK2 and TK3).

- Two main versions, SKINNY64 and SKINNY128, i.e., SKINNY-64-64/128/192 and SKINNY-128-128/256/384.

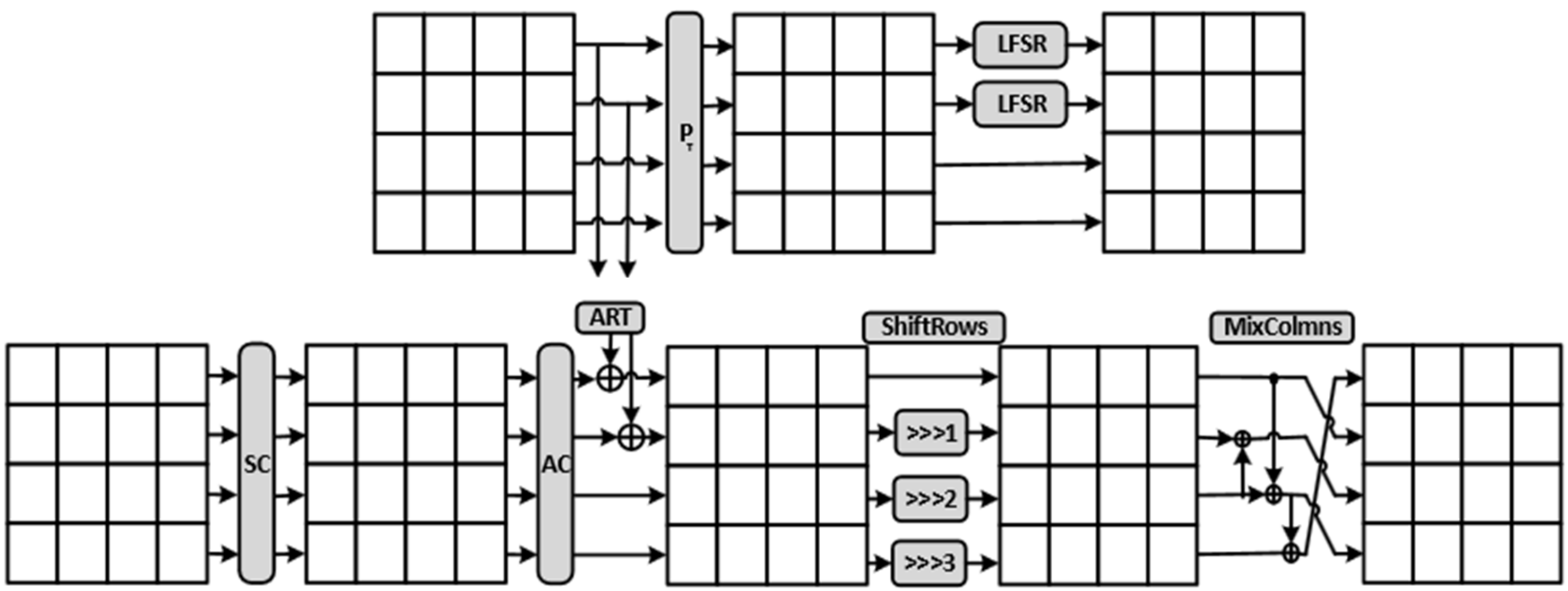
- Each state is represented by a 4×4 square array where each cell is either a nibble or a byte.

- Each round consists of 5 steps, i.e., SubCells(SC), AddConstants(AC), AddRoundTweakey(ART), ShiftRows(SR), MixColumns(MC)



A brief description of SKINNY

- The key is updated with a permutation and the tweak is updated with a LFSR transformation additionally
- Note that, no LFSR is used in TK-1 or single key case.



Outline

- A brief description of SKINNY
- Zero-Correlation Linear Cryptanalysis of SKINNY
- MILP model for SKINNY64 cipher
  - Using MILP in Impossible differential cryptanalysis
- Searching Related-tweakey Impossible Differential Characteristics of SKINNY
- The related-tweakey Impossible Differential attack of SKINNY
- Conclusion
  - Cryptanalytic Results

- For f-function $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ with input variable $x \in \mathbb{F}_2^n$, if we call v and u as the input and output masks, respectively, the linear approximation is defined as follows:

$$x \longmapsto v.x \oplus u.f(x)$$

- Its probability can be defined as:

$$p(v,u) = pr(v.x \oplus uf(x) = 0)$$

- The correlation is:

$$C_f(v,u) = 2p(v,u) - 1$$

- The correlation of an approximation will be equal to zero if the probability of approximation is $\frac{1}{2}$.

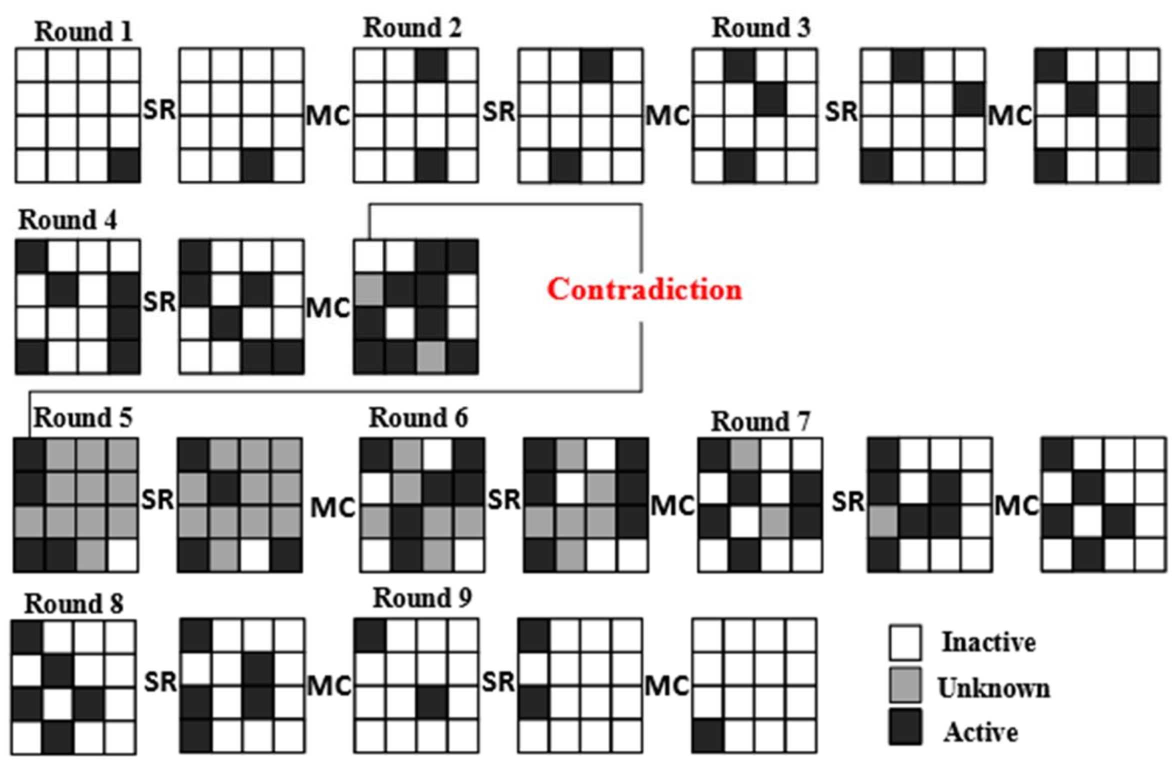
- In zero-correlation linear cryptanalysis, we look for a linear approximation with zero correlation for all keys.

9-round Zero-correlation linear distinguishers for SKINNY

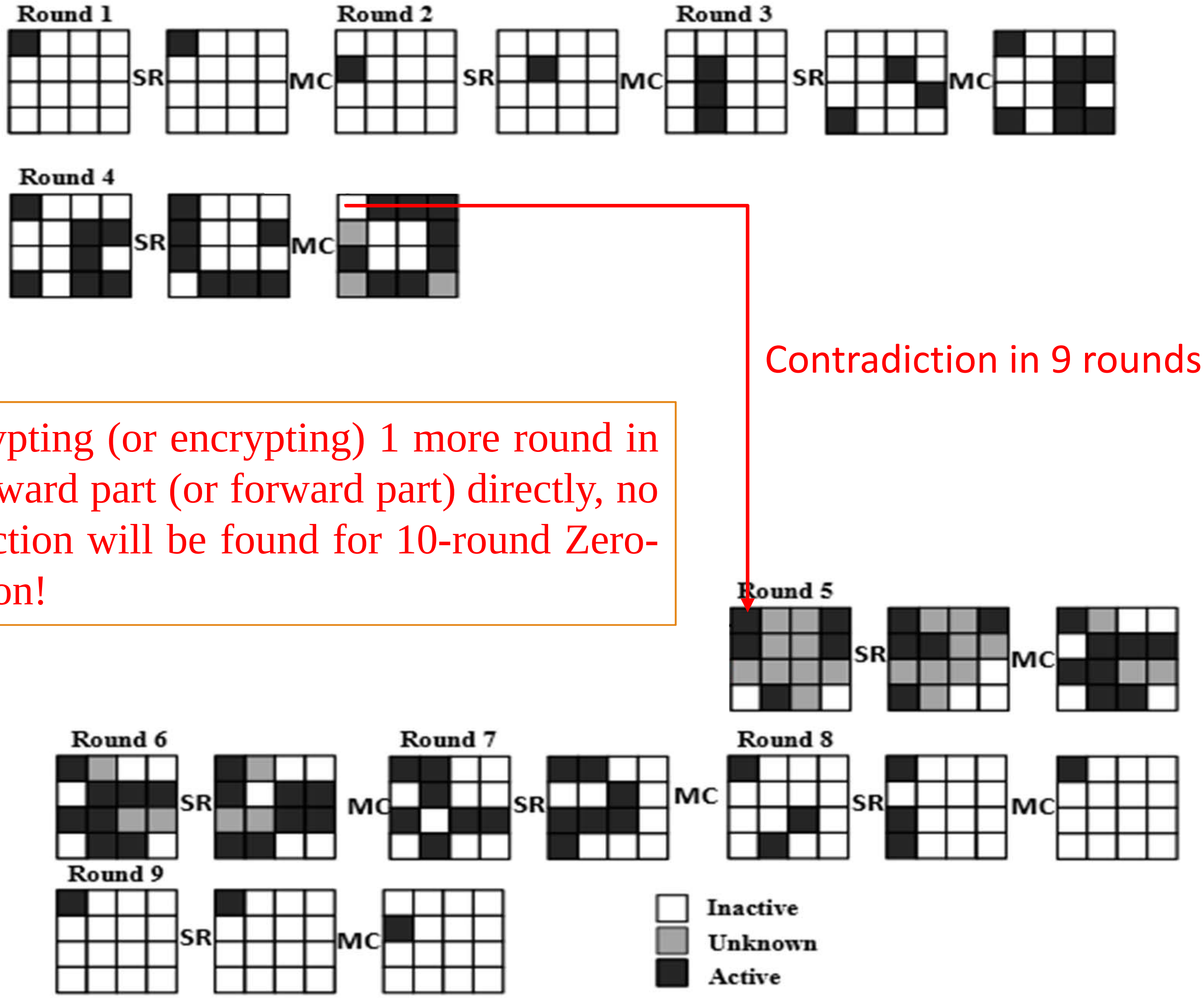
- $\Gamma_{in}^{i} \nrightarrow \Gamma_{out}^{j}$ show that the correlation of linear approximation of r-round SKINNY with input mask Γ_{in}^{i} (i-th nibble of input) to output mask Γ_{out}^{j} (j-th nibble of output) is zero.

For example:

$$(\Gamma_{in}^{15}) \overset{9}{\nrightarrow} (\Gamma_{out}^{12}).$$

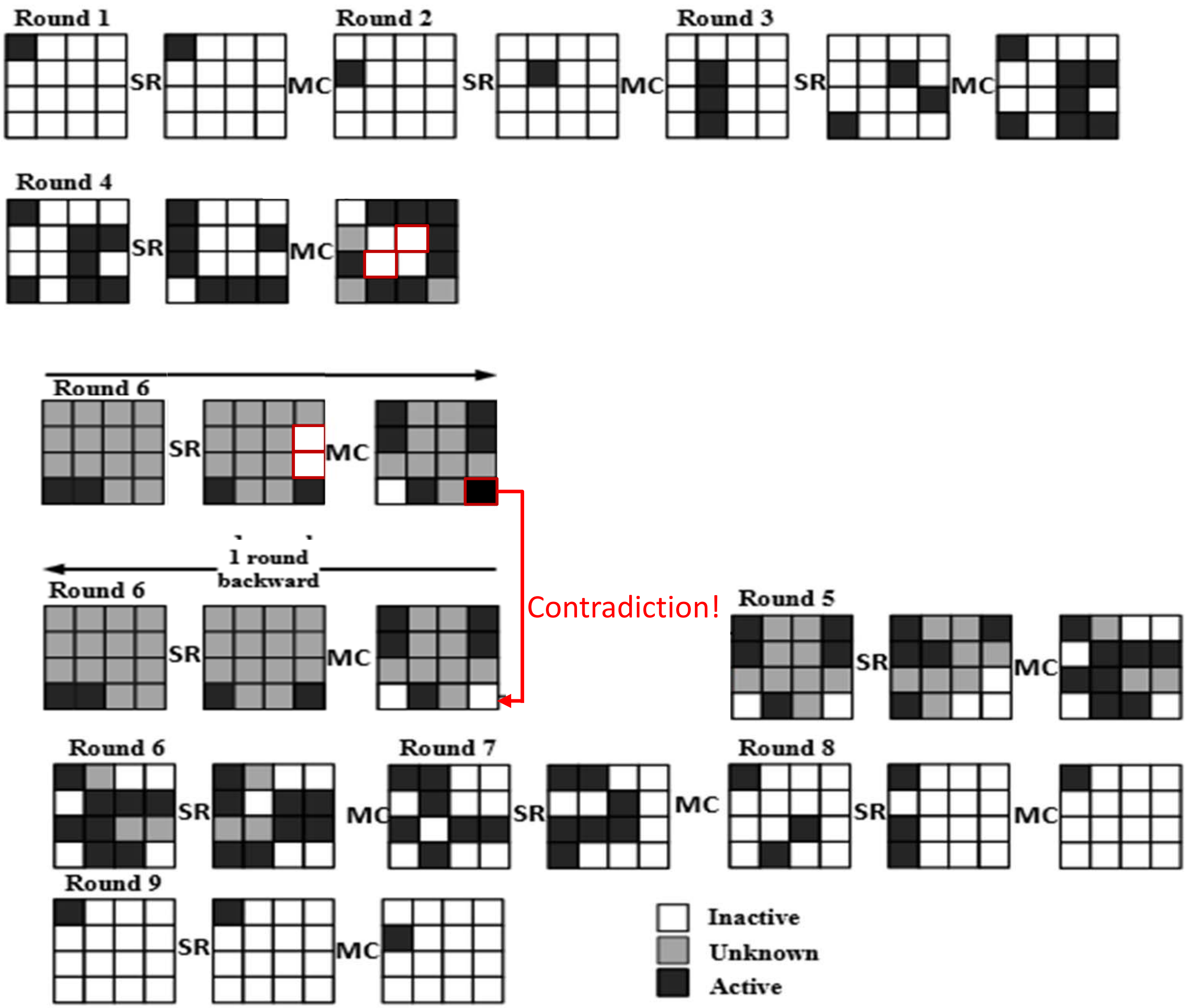


10-round Zero-correlation linear distinguishers for SKINNY



By decrypting (or encrypting) 1 more round in the backward part (or forward part) directly, no contradiction will be found for 10-round Zero-correlation!

10-round Zero-correlation linear distinguishers for SKINNY



Summary of the main results of Zero-correlation attacks on SKINNY

Vers.	#Rounds	$log_2(Time)$	$log_2(Data)$	$log_2(Memory)$
64(64)	14	62	62.58	64
64(128)	18	126	62.68	64

Outline

- A brief description of SKINNY
- Zero-Correlation Linear Cryptanalysis of SKINNY
- MILP model for SKINNY64 cipher
  - Using MILP in Impossible differential cryptanalysis
- Searching Related-tweakey Impossible Differential Characteristics of SKINNY
- The related-tweakey Impossible Differential attack of SKINNY
- Conclusion
  - Cryptanalytic Results

MILP Model for SKINNY64 Cipher

Mouha et al. at Inscrypt 2011:

Problem of finding optimal differential (linear) trail → **Convert** → Optimization problem in MILP

Optimize objective function within the solution range satisfying all the constraints.

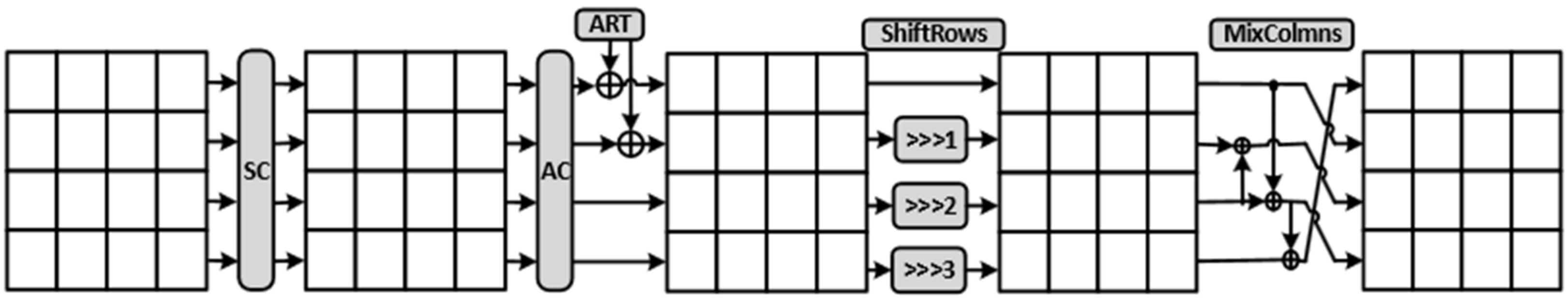
$$\min \quad f = \sum_i c_i x_i$$

$$S.t \quad x \in S = \{\ Ax \leq b, x \geq 0\}$$

$$x \in \mathbb{Z}^k \times \mathbb{R}^{n-k} \subseteq \mathbb{R}^n$$

MILP Model for SKINNY64 Cipher

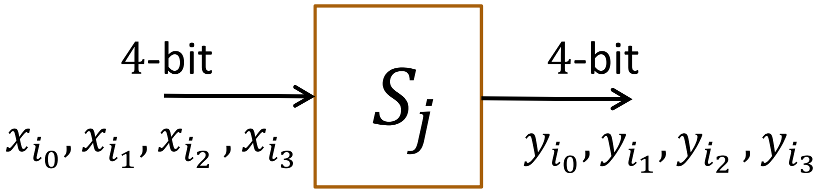
To make the MILP model, define a binary variable $x_i \in \{0,1\}$ for each round;
$x_i = 0$ denotes the bit has no difference.
$x_i = 1$ denotes the bit has difference.



For the input of the S-boxes in the i-th round, we define 16×4 binary variables: $x_{i_0}, x_{i_1}, \dots, x_{i_{63}}$

For the output of the S-boxes in the i-th round, we define 16×4 binary variables : $y_{i_0}, y_{i_1}, \dots, y_{i_{63}}$

MILP Model for SKINNY64 Cipher



$$A_j = \begin{cases} 1 & \text{If } j\text{-th Sbox is active} \\ 0 & \text{If } j\text{-th Sbox is not active} \end{cases}$$

$$x_{i_0} + x_{i_1} + x_1 + x_{i_1} - A_j \geq 0$$

$$A_j - x_{i_0} \geq 0$$

$$A_j - x_{i_1} \geq 0$$

$$A_j - x_{i_2} \geq 0$$

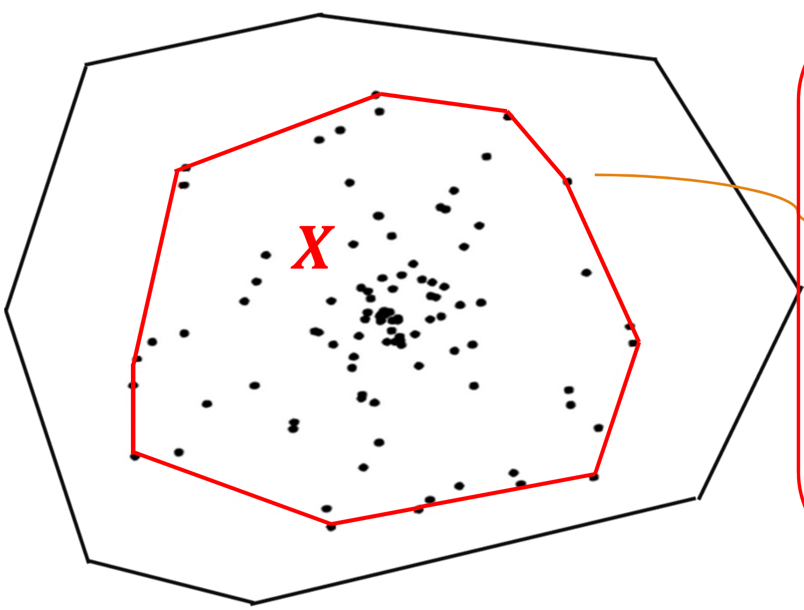
$$A_j - x_{i_3} \geq 0$$

Objective Function: $\min \sum_j A_j$

Differential Distribution Table (DDT)

We compute the probability that Δx propagates to Δy for each $(\Delta x, \Delta y)$.

Define $\boldsymbol{X} = \{(\Delta x, \Delta y) | \Pr(\Delta x \rightarrow \Delta y) \neq 0\}$



Computing H-representation of convex hull with SAGE math tool and greedy algorithm:

$$H_{conv(X)} \begin{cases} \lambda_{0,0}x_0 + \cdots + \lambda_{0,n-1}x_n + \lambda_{0,n} \geq 0 \\ \cdots \\ \vdots \\ \gamma_{0,0}x_0 + \cdots + \gamma_{0,n-1}x_n + \gamma_{0,n} = 0 \\ \cdots \end{cases}$$

$$\lambda_{i,j}\ , \gamma_{i,j} \epsilon R$$

$a \oplus b = c$ can be modeled with 1 inequality by removing each impossible (a, b, c)

$$a + b + c = 2 \times d$$

a, b, c and d are binary and d is a dumy variable.

$$a + b + c = 2 \times d \implies \begin{cases} (a, b, c) \neq (0,0,1) \\ (a, b, c) \neq (0,1,0) \\ (a, b, c) \neq (1,0,0) \\ (a, b, c) \neq (1,1,1) \end{cases}$$

Using MILP in Impossible differential cryptanalysis

- Cui et al. proposed a method for searching impossible differential characteristic and zero-correlation linear distinguisher based on Mixed-Integer Linear Programming (MILP).

- Sasaki et al. proposed a new impossible differential search tool from the design and cryptanalysis aspects in using MILP. They presented an approach for evaluating s-boxes, including 8×8 s-boxes, in impossible differential cryptanalysis which was missing in Cui et al.'s paper.

Technique is simple.

- ❑ Input and output differences are fixed to specific values.

- ❑ MILP search whether or not there are propagations from input to output differences.

- ❑ If MILP model is infeasible, the pair is impossible.

Outline

- A brief description of SKINNY
- Zero-Correlation Linear Cryptanalysis of SKINNY
- MILP model for SKINNY64 cipher
  - Using MILP in Impossible differential cryptanalysis
- Searching Related-tweakey Impossible Differential Characteristics of SKINNY
- The related-tweakey Impossible Differential attack of SKINNY
- Conclusion
  - Cryptanalytic Results

Notations:

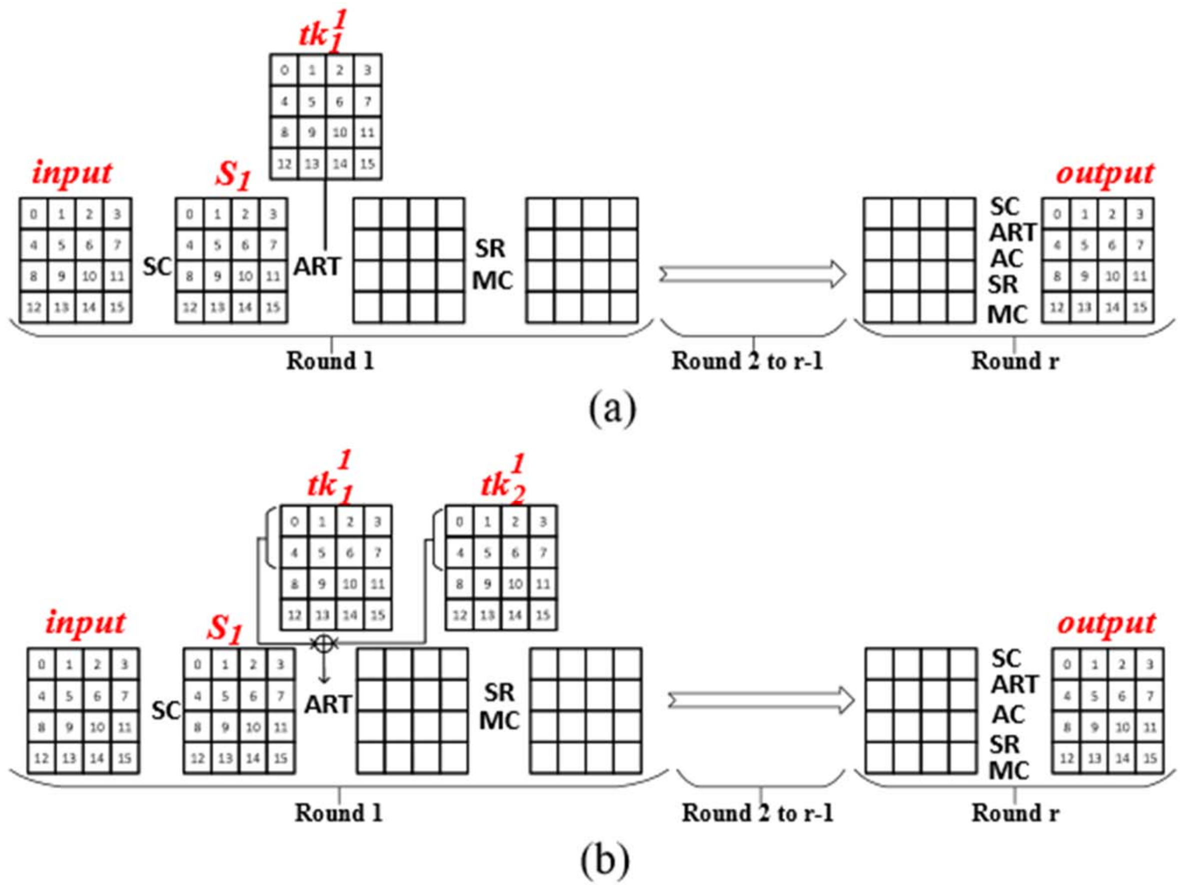


Figure 2: r-round of SKINNY in (a): TK1 model (b):TK2 model.

Searching Related-tweakey ID Characteristics of SKINNY-n-n and SKINNY-n-2n

A summary of the known related-tweakey impossible differential characteristics for SKINNY in both TK-1 and TK-2 model.

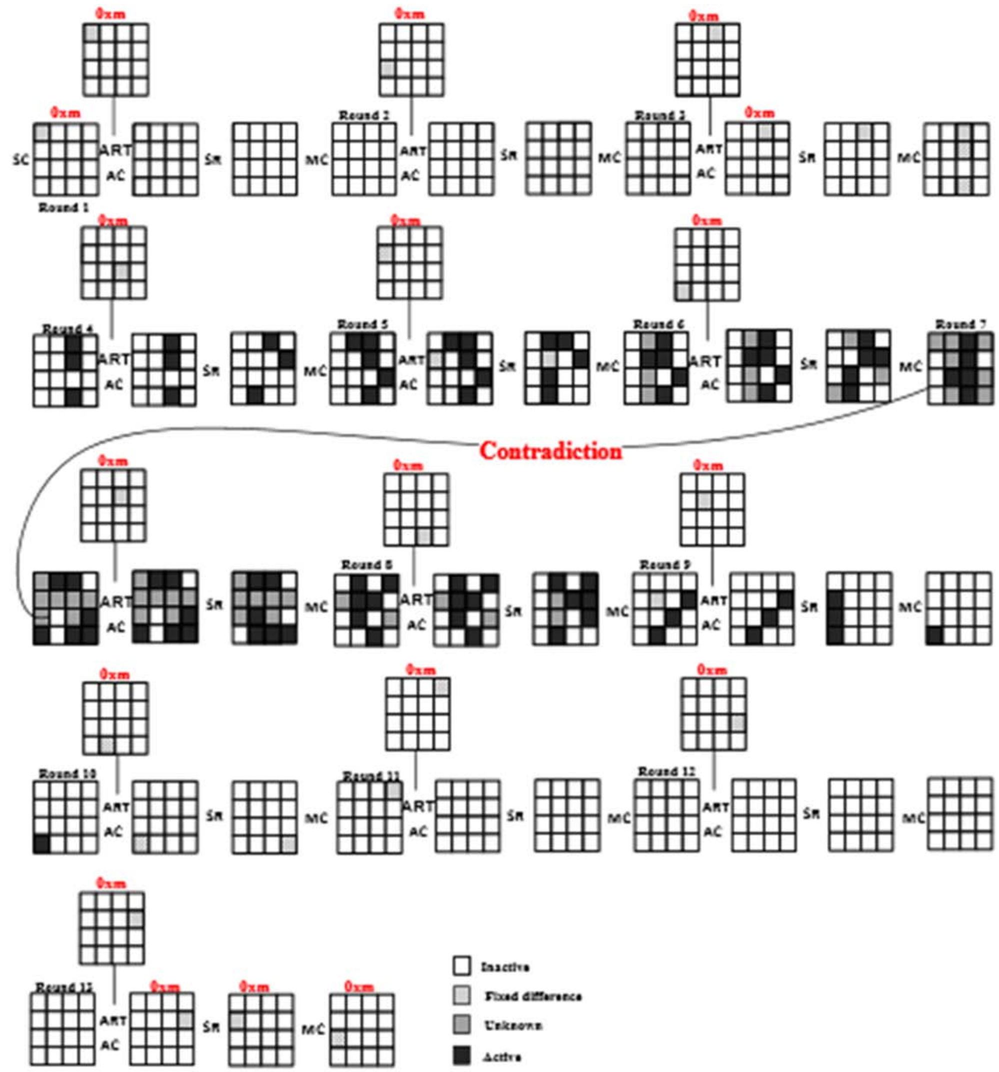
Cipher	Model Differentials	# Rounds
SKINNY (In TK-1 model)	$(\Delta(input), \Delta(tk_1^1), \Delta(output))$	12
	$(\Delta(S_1), \Delta(tk_1^1), \Delta(output))$	13
	$(\Delta(input), \Delta(tk_1^1), 0)$	11
	$(\Delta(S_1), \Delta(tk_1^1), 0)$	12
	$(0, \Delta(tk_1^1), \Delta(output))$	12
	$(0, \Delta(tk_1^1), 0)$	11
SKINNY (In TK-2 model)	$(\Delta(input), \Delta(tk_1^1), \Delta(tk_2^1)\Delta(output))$	12
	$(\Delta(S_1), \Delta(tk_1^1), \Delta(tk_2^1), \Delta(output))$	14
		15
	$(\Delta(input), \Delta(tk_1^1), \Delta(tk_2^1), 0)$	12
	$(\Delta(input), 0, \Delta(tk_2^1), \Delta(output))$	11
	$(\Delta(S_1), 0, \Delta(tk_2^1), \Delta(output))$	12
	$(\Delta(input), 0, \Delta(tk_2^1), 0)$	11
	$(0, \Delta(tk_1^1), \Delta(tk_2^1), \Delta(output))$	14
	$(0, 0, \Delta(tk_2^1), \Delta(output))$	11
	$(0, \Delta(tk_1^1), \Delta(tk_2^1), 0)$	13
	$(0, 0, \Delta(tk_2^1), 0)$	11

Based on the previous Table:

For SKINNY-n-n and SKINNY-n-2n, we construct 13 and 15-round related-tweakey ID characteristics, respectively. These improve the previous longest 12 and 14-round related-tweakey ID characteristics of SKINNY-n-n and SKINNY-n-2n, respectively.

13-round Related-tweakey ID Characteristics of SKINNY-n-n

For example, we have considered this 13-round characteristic for 19-round attack on SKINNY-n-n



Related-tweakey impossible differential characteristic $(\Delta^0_{0xm}(S_1), \Delta^0_{0xm}(tk^1_1), \Delta^8_{0xm}(output))$ for 13-round SKINNY in TK-1 model.

15-round Related-tweakey ID Characteristics of SKINNY-n-2n

The differential $\left(\Delta^{i}_{0xm}(S_1), \Delta^{i}_{0xn}(tk^{1}_{1}), \Delta^{i}_{0xp}(tk^{1}_{2}), \Delta^{l}_{0xq}(output)\right)$ is a 15-round related tweakey impossible differential characteristic for SKINNYn-2n when the following conditions are satisfied:

- Choose (i, l) from the sets $\{(1,8), (3,10), (5,11), (6,9)\}$.
- $m = n \oplus p$.
- $LFSR(p) = n$.
- $n \oplus LFSR^{7}(p) = q$.

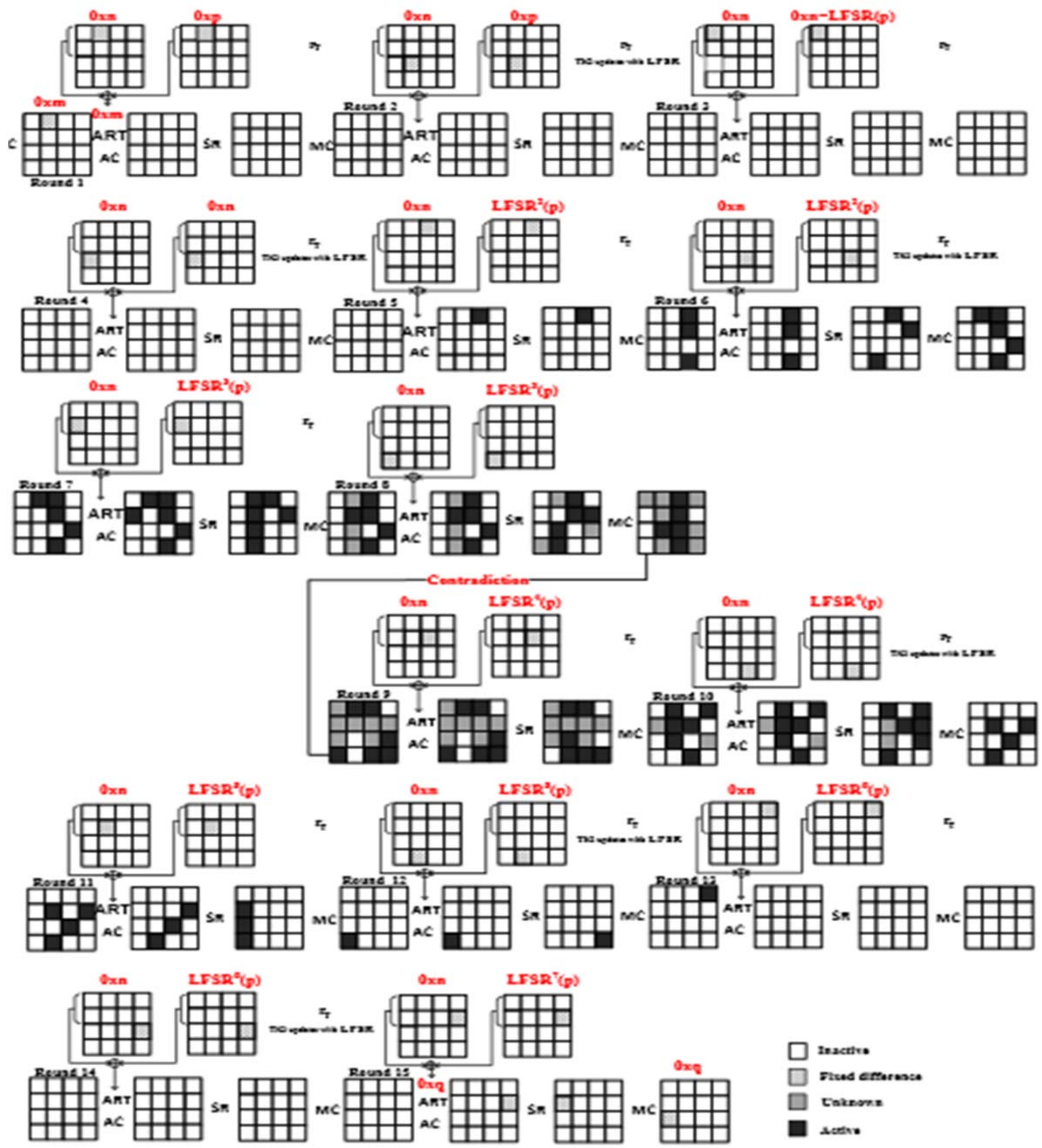
For SKINNY64-128, the possible values of m, n, p, and q that satisfy above conditions are listed in the following Table. For SKINNY128-256 the table can be derived by the same approach.

The values of m, n, p, and q for 15-round RK-ID as $\left(\Delta^{i}_{0xm}(S_1), \Delta^{i}_{0xn}(tk^{1}_{1}), \Delta^{i}_{0xp}(tk^{1}_{2}), \Delta^{l}_{0xq}(output)\right)$ in TK2 model.

	m	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	n	E	C	2	8	6	4	A	F	1	3	D	7	9	B	5
⇓	p	F	E	1	C	3	2	D	7	8	9	6	B	4	5	A
	q	7	F	8	E	9	1	6	B	C	4	3	5	2	A	D

15-round Related-tweakey ID Characteristics of SKINNY-n-2n

For example, we have considered this 15-round characteristic for 23-round attack on SKINNY-n-2n



Outline

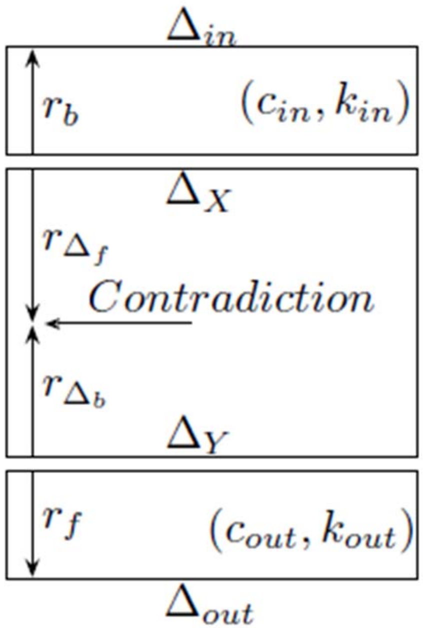
- A brief description of SKINNY
- Zero-Correlation Linear Cryptanalysis of SKINNY
- MILP model for SKINNY64 cipher
  - Using MILP in Impossible differential cryptanalysis
- Searching Related-tweakey Impossible Differential Characteristics of SKINNY
- The related-tweakey Impossible Differential attack of SKINNY
- Conclusion
  - Cryptanalytic Results

The related tweakey Impossible Differential attack of SKINNY

- **Impossible Differential Distinguisher**, i.e.,

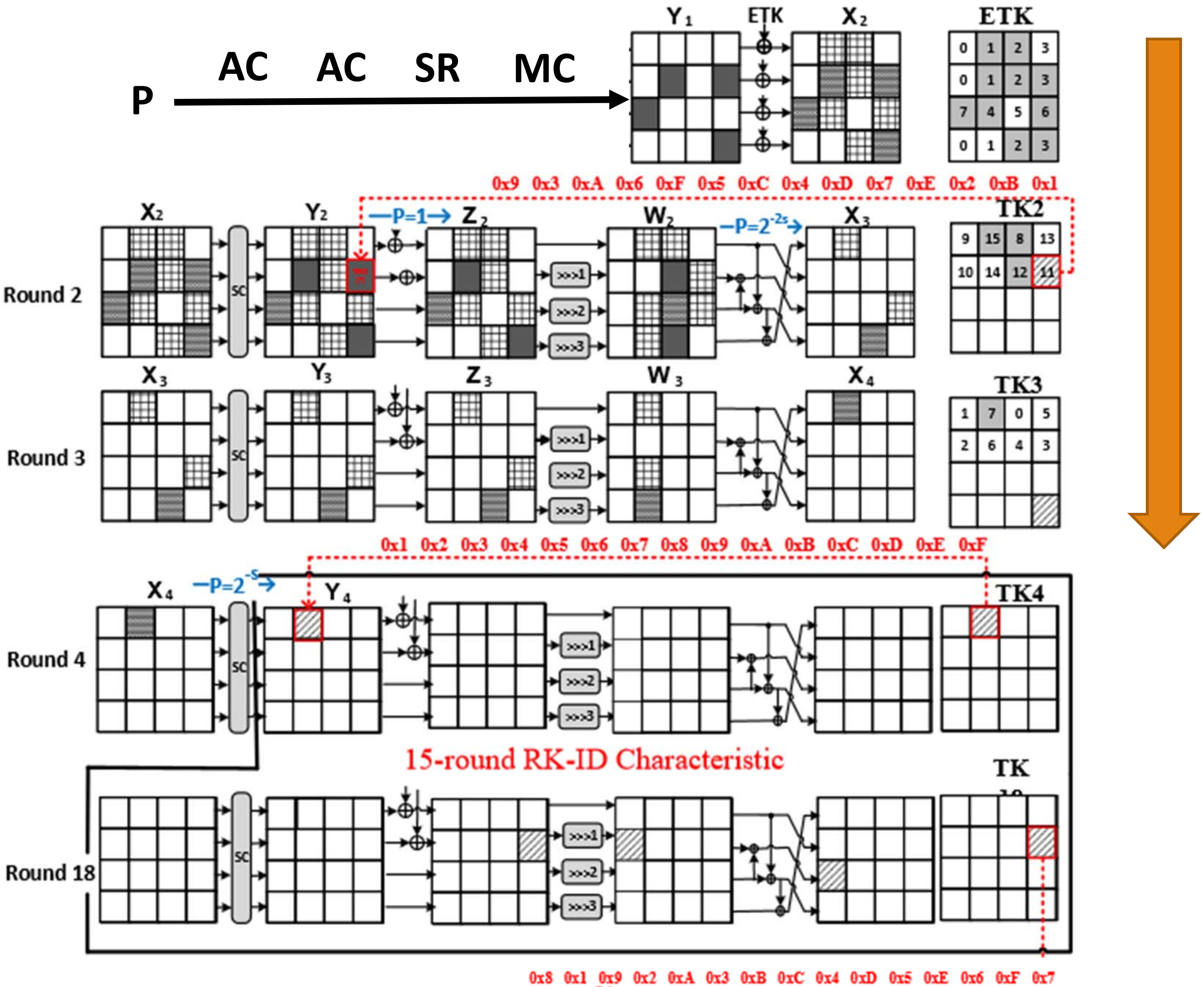
$\Pr(\Delta_X \longrightarrow \Delta_Y) = 0$, where related tweakey differences are added to cancel state differences.

- **Key Recovery.**

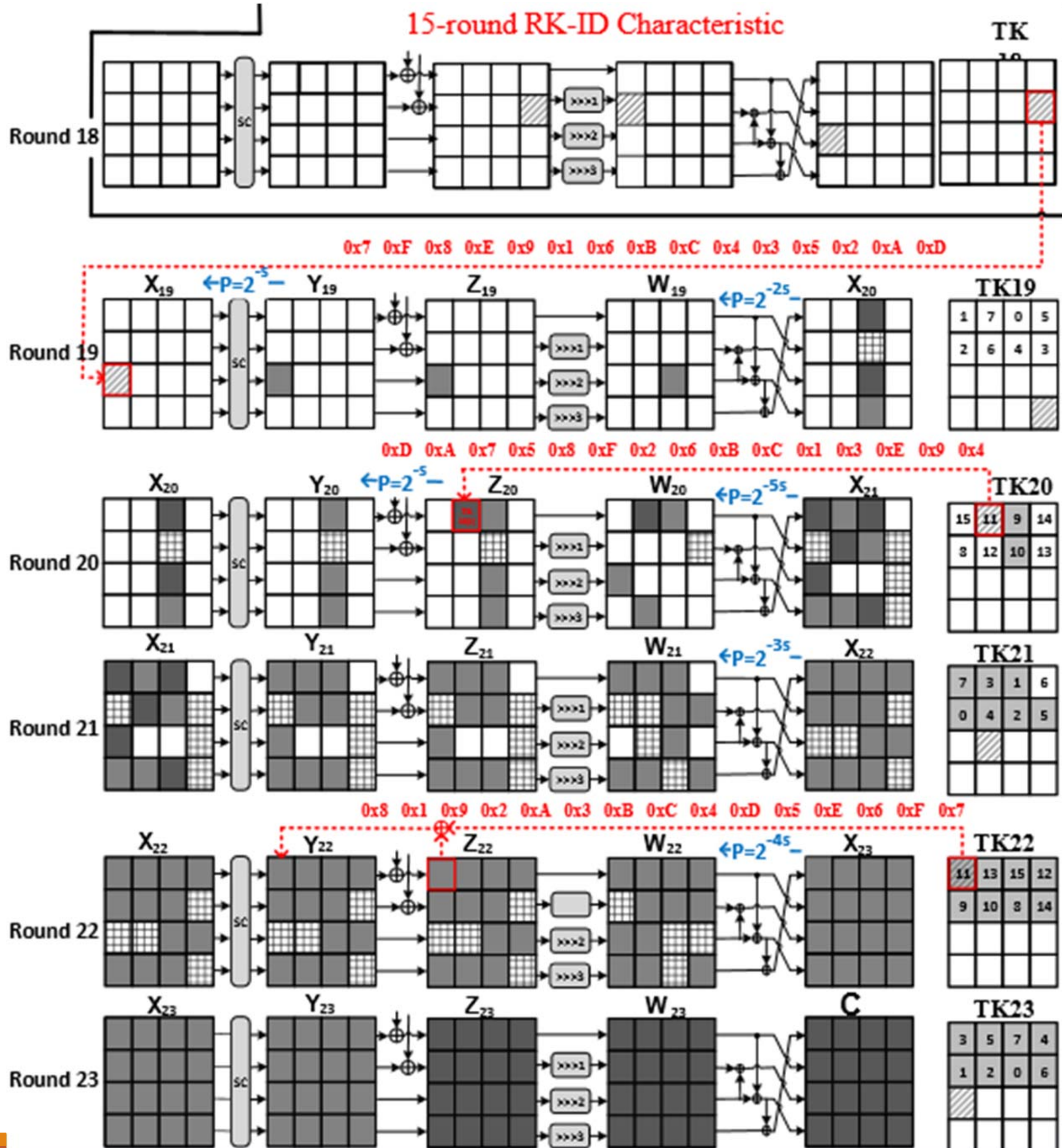


  - $\mathbf{C_{in}}(\mathbf{C_{out}})$**:** bit conditions need to be verifed in the $r_b(r_f)$ rounds to ensure $\Delta_{in} \longrightarrow \Delta_X(\Delta_{out} \longrightarrow \Delta_Y)$.
  - k_{in}, k_{out}**:** subkey bits involved in the extended rounds.
  - $\Pr(\Delta_{in} \longrightarrow \Delta_X) = 2^{-C_{in}}$
  - $\Pr(\Delta_{out} \longrightarrow \Delta_Y) = 2^{-C_{out}}$
  - $2^{|k_{in} \cup k_{out}|(1-2^{-(C_{in}+C_{out})})^N}$**:** the number of key candidates left in the key space after N trials where N is the number of message pairs of input and output difference $(\Delta_{in}, \Delta_{out})$.

23-Round Related-Tweakey Impossible Differential Attack of SKINNYn-2n



23-Round Related-Tweakey Impossible Differential Attack of SKINNYn-2n



Outline

- A brief description of SKINNY
- Zero-Correlation Linear Cryptanalysis of SKINNY
- MILP model for SKINNY64 cipher
  - Using MILP in Impossible differential cryptanalysis
- Searching Related-tweakey Impossible Differential Characteristics of SKINNY
- The related-tweakey Impossible Differential attack of SKINNY
- Conclusion
  - Cryptanalytic Results

Cryptanalytic Results

Summary of the main results of attacks on SKINNY, where ID, RK-ID, and ZC denote impossible differential, related-key(tweakey) impossible differential, and zero correlation cryptanalysis, respectively.

Vers.	n	Attack	# Rounds	$\log_2$(Time)	$\log_2$(Data)	$\log_2$(Memory)	Ref.
n-$2n$	64	ID	20	121.08	47.69	74.69	[TAY17]
		RK-ID	23	$79^\dagger$	-	-	[ABC+17]
		RK-ID	23	125.91	62.47	124	[LGS17]
		RK-ID	23	124	62.47	77.47	this paper
		ZC	18	126	62.68	64	this paper
	128	ID	20	245.72	92.1	147.1	[TAY17]
		RK-ID	23	251.47	124.47	248	[LGS17]
		RK-ID	23	243.41	124.41	155.41	this paper
n-n	64	ID	18	57.1	47.52	58.52	[TAY17]
		RK-ID	19	63.03	61.47	56	[LGS17]
		RK-ID	19	62.83	61.30	48.30	this paper
		ZC	14	62	62.58	64	this paper
	128	ID	18	116.94	92.42	115.42	[TAY17]
		RK-ID	19	124.60	122.47	112	[LGS17]
		RK-ID	19	124.43	122.47	97.47	this paper

† : In this attack, 48 bits of the tweakey are considered publicly as tweak. So the upper bound for exhaustive search is 80 bits.

Thanks for your attention !