Cryptanalysis of Round Reduced SKINNY under Related-Tweakey Settings

Guozhen Liu[2,1], Mohona Ghosh[1,3], Ling Song[1,4]

[1]Nanyang Technological University

[2]Shanghai Jiao Tong University

[3]Indian Institute of Information Technology, Design and Manufacturing (IIITDM)

[4]State Key Laboratory of Information Security, Institute of Information Engineering, China

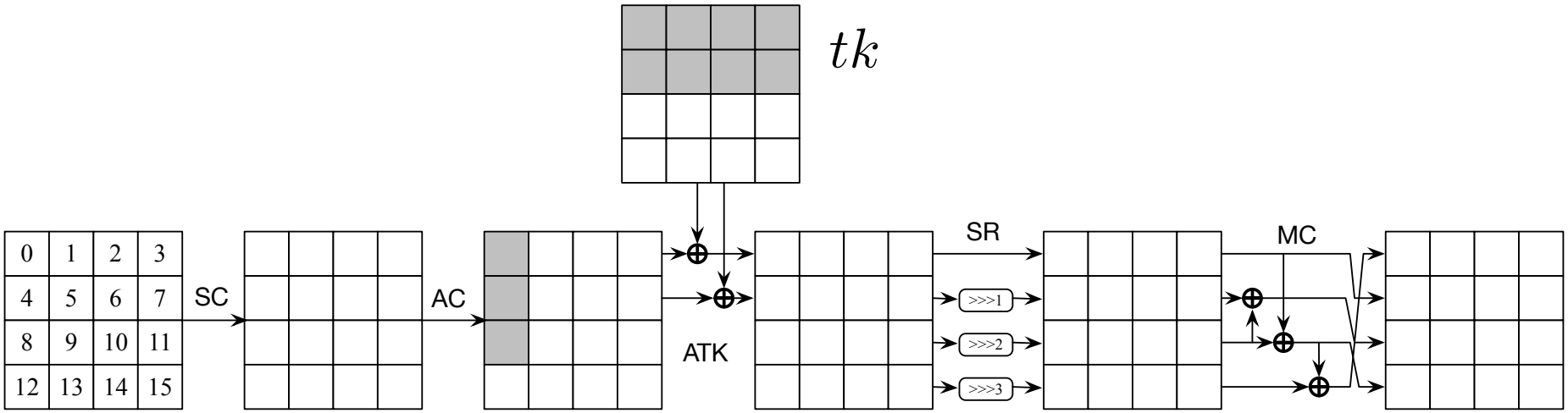
March 6, 2018

Overview

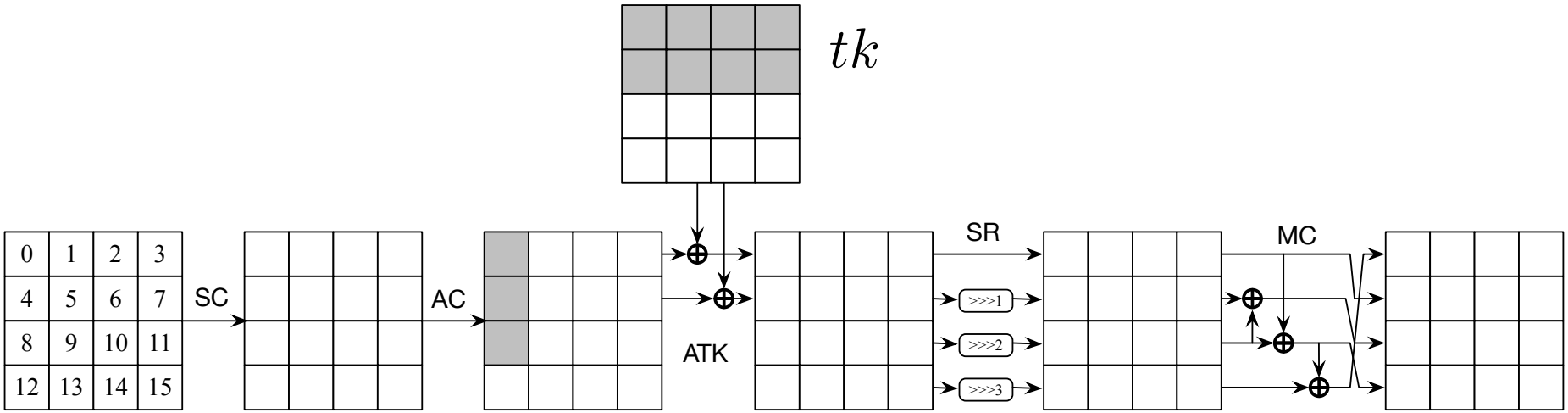
SKINNY-A Lightweight Tweakable Block Cipher

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)



Tweakey Schedule Algorithm



- There is no key whitening operation before the first round
- Tweakey State: Computed as a XORed group of z $(= \frac{t}{n})$ 4×4 arrays
  - For example, for SKINNY-n-3n, $z = 3$ and round tweakey $(tk_i) = (TK\text{-}1)_i \oplus (TK\text{-}2)_i \oplus (TK\text{-}3)_i$
- The tweakeys $(TK\text{-}1)_i$, $(TK\text{-}2)_i$ and $(TK\text{-}3)_i$ for each round i are generated by a *linear tweakey scheduling algorithm*.
  - The key is updated with a permutation and the tweak is updated with a LFSR transformation additionally

Properties of the Tweakey Schedule Algorithm

Predictability of Subtweakey Difference

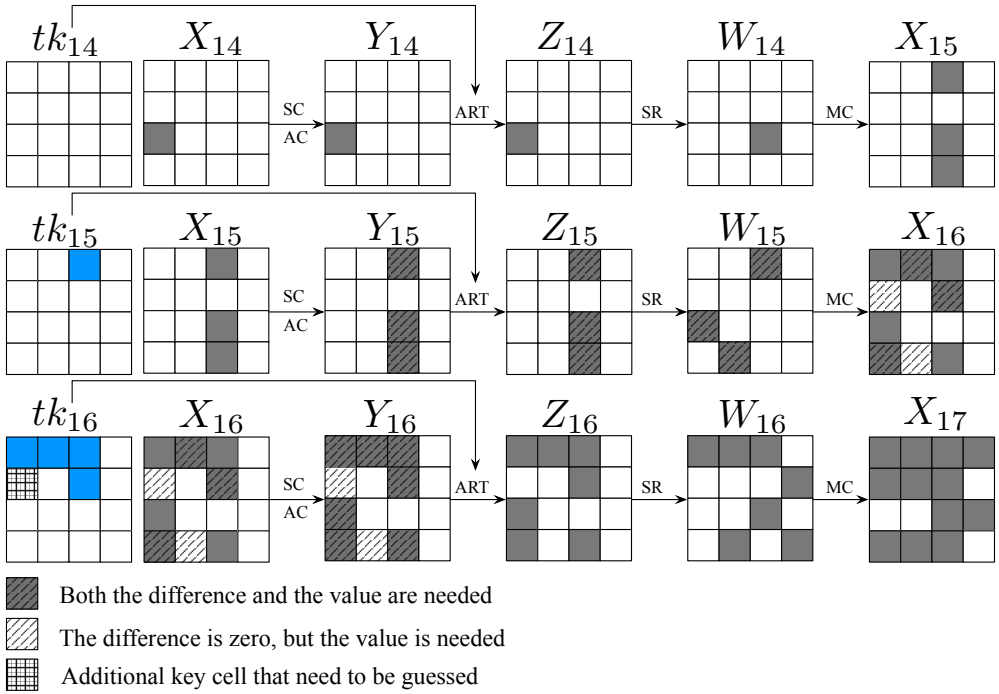
- The linear *tweakey schedule algorithm*.
- The tweakey cells involved in the i^{th} round will next appear in $(i+2)^{th}$ round and so on.

Subtweakey Difference Cancellation

- For a given active tweakey cell, only a single subtweakey difference cancellation can happen every 30 rounds for TK2, and two subtweakey difference cancellations for TK3.
- There can be *three* and *five* rounds of *fully inactive internal states for* TK2 and TK3.

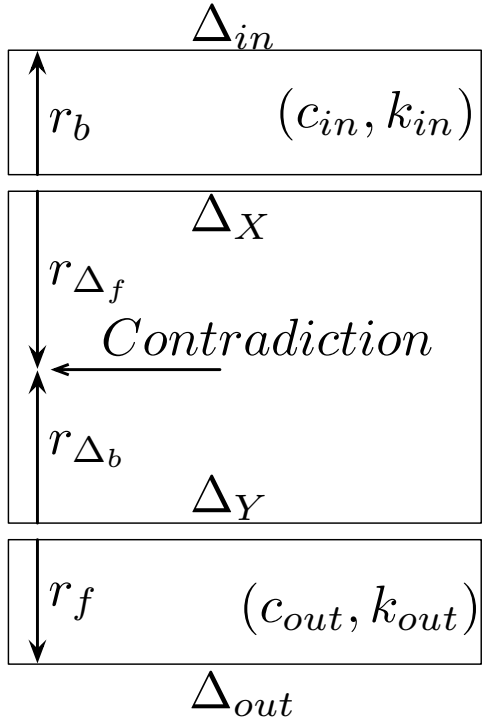
The Matrix used in MixColumns is not MDS

During the tweakey recovery phase, it is not enough to know the values of only the active cells in the output column to determine the value of the active cell in the input column. Usually more cells need to be guessed.



The Impossible Differential Attack Model

1. **Impossible Differential Distinguisher**, i.e., $Pr(\Delta_X \rightarrow \Delta_Y) = 0$, where related tweakey differences are added to cancel state differences.
2. **Key Recovery**.
   - $c_{in}(c_{out})$: bit conditions need to be verified in the $r_b(r_f)$ rounds to ensure. $\Delta_{in} \rightarrow \Delta X(\Delta_{out} \rightarrow \Delta Y)$
   - k_{in}, k_{out}: subkey bits involved in the extended rounds.
   - $Pr(\Delta_{in} \rightarrow \Delta X) = 2^{-c_{in}}$, $Pr(\Delta_{out} \rightarrow \Delta Y) = 2^{-c_{out}}$.
   - $K_{rem} = 2^{|k_{in} \bigcup k_{out}|}(1 - 2^{-(c_{in}+c_{out})})^N$: 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 $(\Delta_{in}, \Delta_{out})$.



Related-Tweakey Impossible Differential Attack

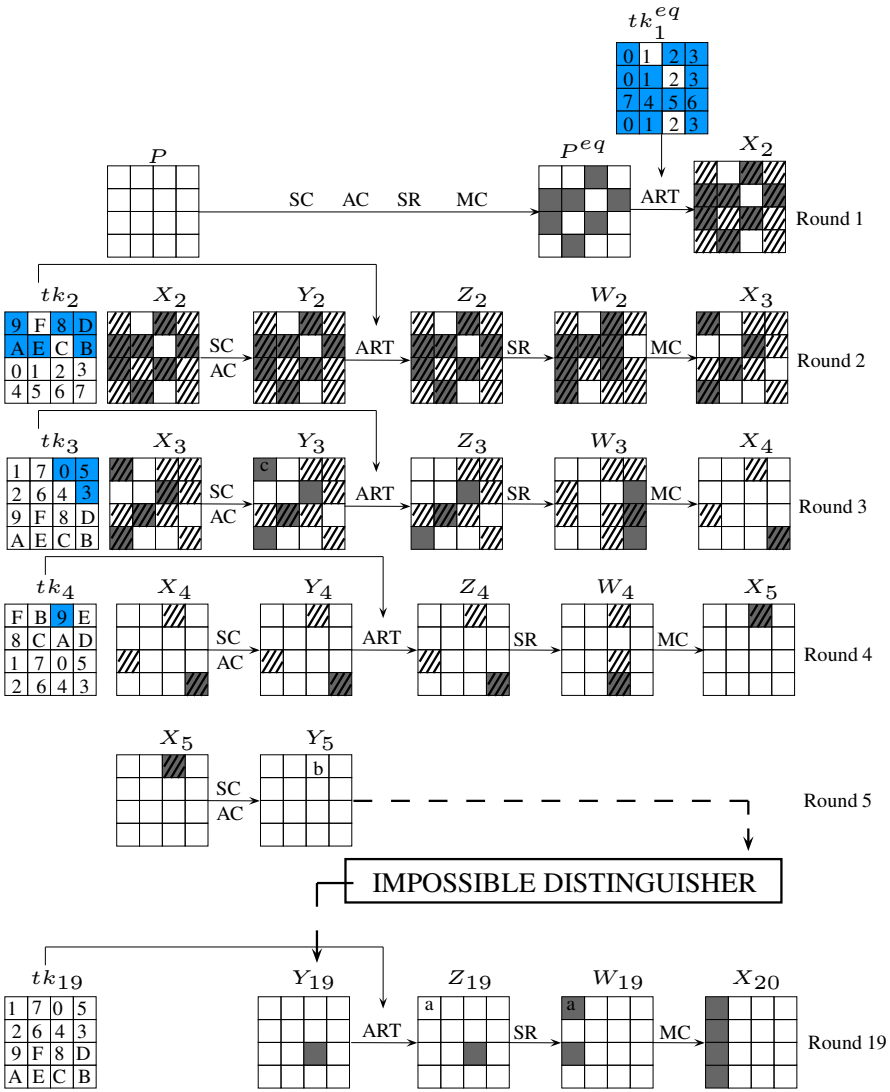
- **Impossible Truncated Differential Distinguisher**
  - A 14-round impossible distinguisher for SKINNY-n-$2n$ is constructed by the MILP tool as follows:

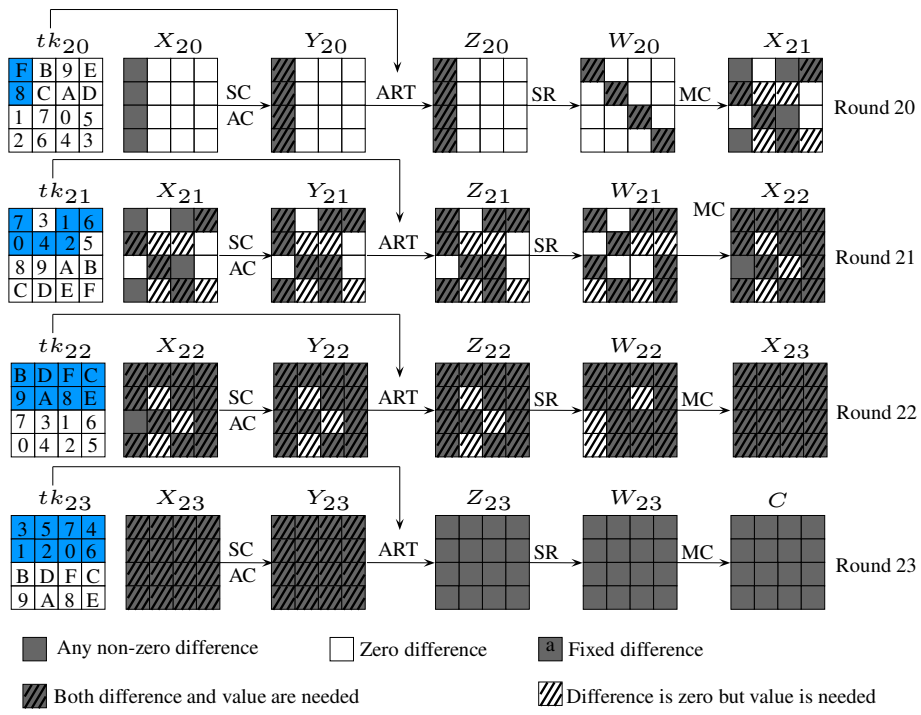
$$(00b0 \mid 0000 \mid 0000 \mid 0000) \overset{14r}{\not\longrightarrow} (0000 \mid 0000 \mid 00N0 \mid 0000).$$

  - The *subtweakey difference cancellation* property ensures 3 rounds full non-active states.
  - The position of the *active cell* at the beginning of the differential trail is chosen so that
    1. it covers more rounds at the distinguisher,
    2. and extends to more rounds in the tweakey recovery phase.
- **Tweakey Recovery**
  - The 14-round distinguisher is extended 4.5 rounds forward and 4.5 rounds backward(take SKINNY-n-2n as an example).
  - The related tweakey difference is set as

$$\Delta = (00d0 \mid 0000 \mid 0000 \mid 0000).$$

A 23-round Attack on SKINNY-n-2n





A 23-round Attack on SKINNY-n-2n

Data Collection

- Set a pair of structures S_1 and S_2 encrypted by related tweakey, and store all the pairs such that Δ_{in} and Δ_{out} are satisfied.
- Generate 2^x such structures until sufficient pairs are obtained.

Tweakey Recovery

- For each remained pair, derive the associated subtweakeys at each round according to the difference propagation.
- Delete all the derived tweakeys.

Vers	n	Rounds	Data	Time	Memory
n-n	64	**19**	$2^{61.47}$	$2^{63.03}$	2^{56}
n-$2n$	64	**23**	$2^{62.47}$	$2^{125.91}$	2^{124}

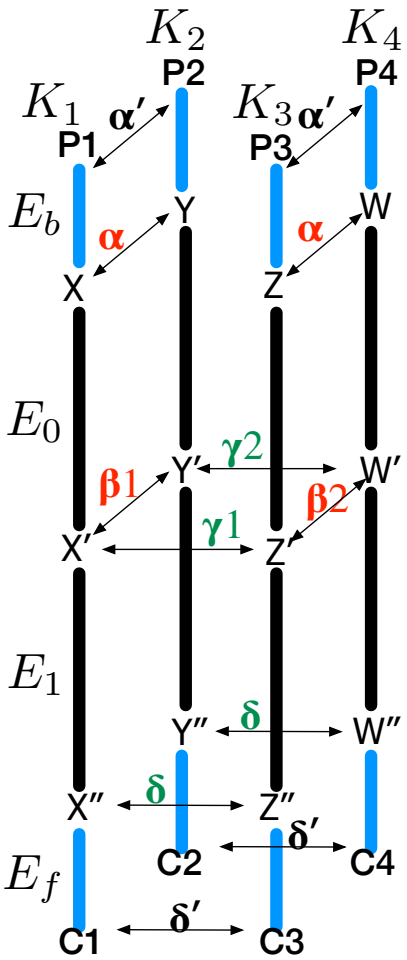
Related Tweakey Boomerang and Rectangle Attack

Boomerang attacks

- $P(\alpha \to \beta)$=**p**, $P(\delta \to \gamma)$=**q**.
- With probability $\mathbf{p^2q^2}$, $E^{-1}(Z'') \oplus E^{-1}(W'') = Z \oplus W = \alpha$.
- If, $(\mathbf{pq}) > 2^{-n/2}$, a valid distinguisher is constructed.

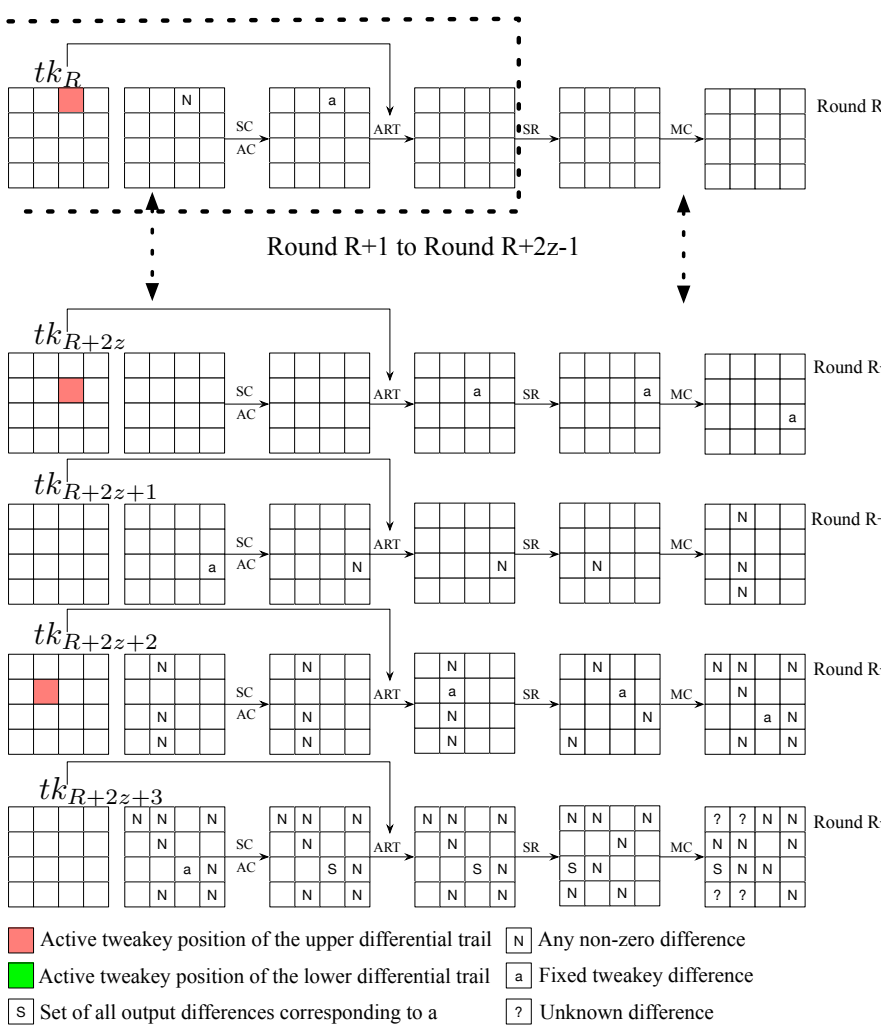
Rectangle attacks

- **Amplified boomerangs**, a right quartet is of probability $2^{-n}p^2q^2$.
- **Rectangle attacks**, the probability of the right quartet is increased to $2^{-n}\hat{p}^2\hat{q}^2$.



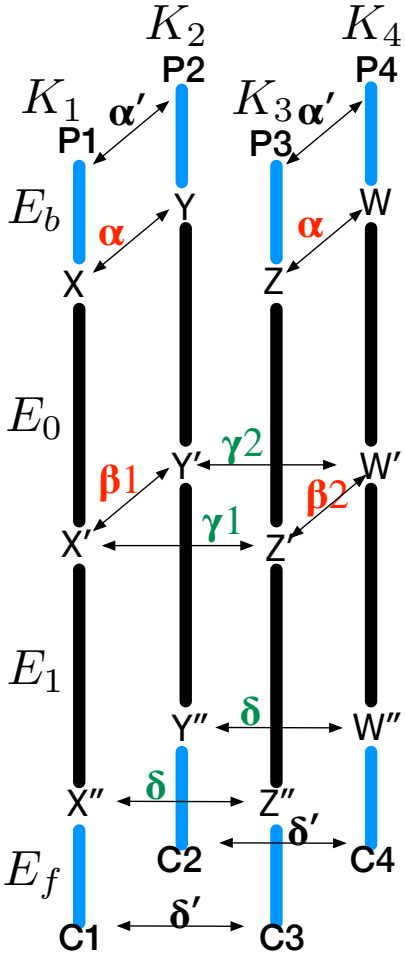
An Example Upper Trail of a SKINNY-64-128 Distinguisher

- Four related tweakeys are used to cancel state differences in upper trail and lower trail.
- The probability of the upper trail $\alpha \xrightarrow{\Delta_1} \beta$ is $\sum_{\beta_1,\beta_2} P_r(\alpha \xrightarrow{\Delta_1} \beta_1) \cdot P_r(\alpha \xrightarrow{\Delta_1} \beta_2) \cdot P_r(\beta_1 = \beta_2)$.
- The probability of the lower trail $\gamma \xleftarrow{\Delta_2} \delta$ is $\sum_{\gamma_1,\gamma_2} P_r(\gamma_1 \xleftarrow{\Delta_2} \delta) \cdot P_r(\gamma_2 \xleftarrow{\Delta_2} \delta) \cdot P_r(\gamma_1 = \gamma_2)$.
- A 15-round distinguisher of probability $2^{-57.1}$.



Related-Tweakey Recovery Algorithms

- Create y structures of 2^{r_b} plaintexts each. Encrypt these y structures with K_1, K_2 respectively. Similarly, create y structures of 2^{r_b} plaintexts each and encrypt these y structures with K_3, K_4.
- Initialize a list of $2^{m_b+m_f}$ counters.
- Generate **right quartes** by using hash tables.
- For all right quartets, increment the counters of $(m_b + m_f)$-bit subtweakeys that satisfies the differences.
- Output the subtweakeys corresponding to top hits of counters.



Attack Complexities

Data complexity

$D = 4M$ chosen plaintexts, where $M = \sqrt{s} \cdot 2^{n/2}/\hat{p}\hat{q}$ and s is the expected number of right quartets.

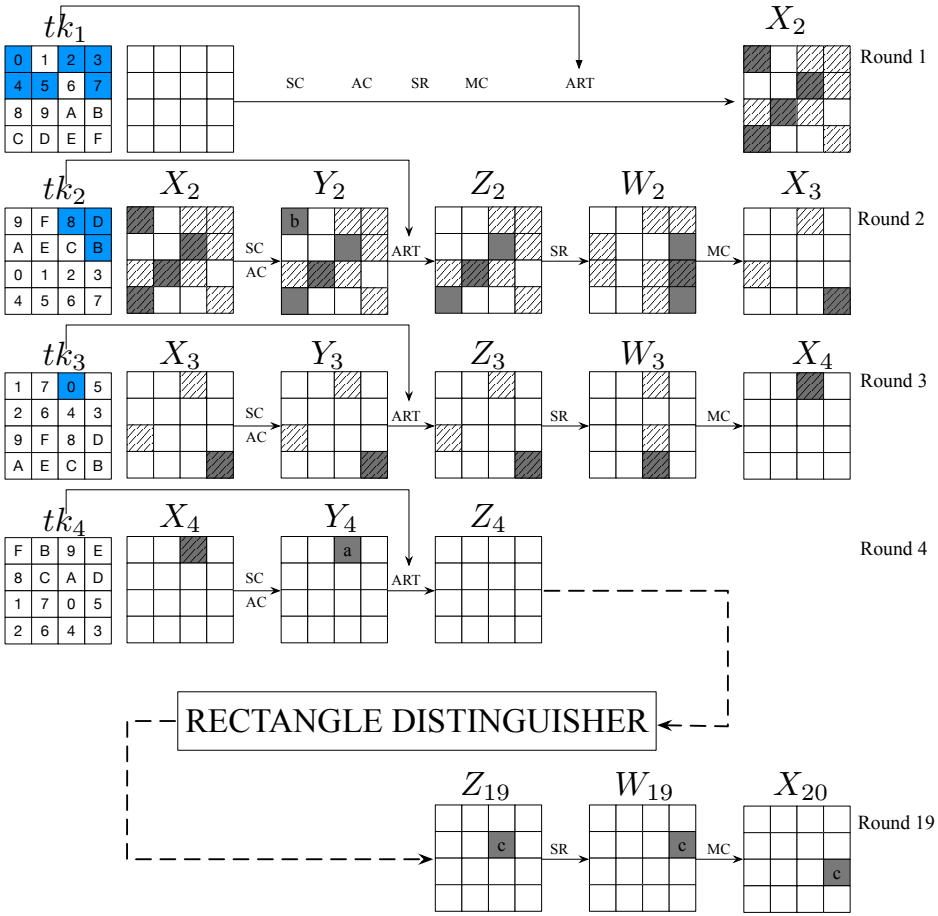
Time complexity

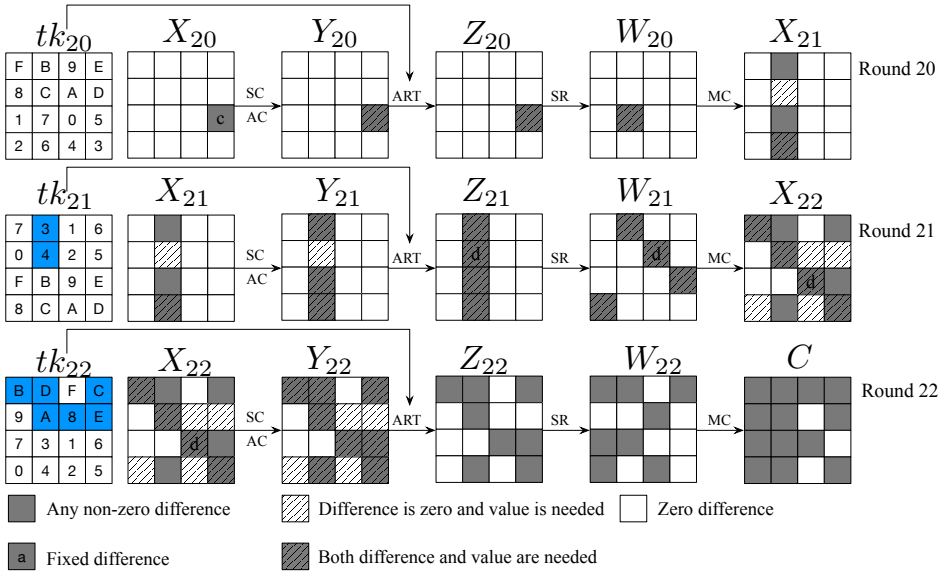
$4M + 2 \cdot M^2 \cdot 2^{r_f - n} + 2 \cdot M^2 \cdot 2^{t_f - n} + M^2 \cdot 2^{2t_f + 2r_b - 2n}(1 + 2^{t_b - r_b}) + M^2 \cdot 2^{t_b + t_f - 2n + 1}(2^{m_b + t_f} + 2^{m_f + t_b})$ memory accesses and 2^{k-h} encryptions.

Memory complexity

$4M + 2^{t_b} + 2^{t_f} + 2^{m_b + m_f}$.

A 22-Round Related-Tweakey Rectangle Attack on SKINNY-64-128





Attack Settings for SKINNY-64-128

Parameters

$r_b = log_2(15^4) = 15.6$, $t_b = log_2(15^3) + log_2 6 = 14.3$, $m_b = 10c = 40$, $r_f = log_2(15^8) = 31.3$, $t_f = log_2(15^7) + log_2 8 = 30.3$ and $m_f = 8c = 32$. As we have analyzed previously, the probability of the related-tweakey rectangle distinguisher is $\hat{p}^2\hat{q}^2 = (2^{-3.9})^7 \cdot 2^{-2.4} \cdot (2^{-3.9})^6 \cdot 2^{-4} = 2^{-57.1}$.

Complexities

The total data complexity for 22-round SKINNY64-128 is $D = 4 \cdot \sqrt{s} \cdot 2^{n/2}/\hat{p}\hat{q} = 4 \cdot \sqrt{s} \cdot 2^{32} \cdot 2^{28.5} = \sqrt{s} \cdot 2^{62.5}$, i.e. if we choose $s = 4$, the data complexity would be $2^{63.5}$. The time complexity required is $2^{110.9}$ memory access and 2^{108} encryptions, and the memory complexity is $2^{63.5}$.

Summary of Cryptanalytic Results

Table: Summary of cryptanalytic results on SKINNY

Vers.	n	Rounds	Data	Time	Memory	Attack
n-n	64	**19**	$2^{61.47}$	$2^{63.03}$	2^{56}	**Imposs.**
	128	19	$2^{122.47}$	$2^{124.60}$	2^{112}	Imposs.
n-$2n$	64	**23**	$2^{62.47}$	$2^{125.91}$	2^{124}	**Imposs.**
	128	23	$2^{124.47}$	$2^{251.47}$	2^{248}	Imposs.
n-$3n$	64	**27**	$2^{63.5}$	$2^{165.5}$	2^{80}	**Rect.**
	128	27	2^{127}	2^{351}	2^{160}	Rect.
	128	27	2^{112}	2^{331}	2^{144}	Rect.

- 19, 23 and 27 rounds of SKINNY-n-n, SKINNY-n-$2n$ and SKINNY-n-$3n$ can be attacked respectively.

Thanks for your attention!