Exploiting Non-Full Key Additions: Full-Fledged Automatic Demirci-Selçuk Meet-in-the-Middle Cryptanalysis of SKINNY

Danping Shi[1] Siwei Sun[2] Ling Song[3] Lei Hu[1] Qianqian Yang[1]

[1]Institute of Information Engineering, Chinese Academy of Sciences, China

[2]School of Cryptology, University of Chinese Academy of Sciences, Beijing, China

[3]Jinan University, Guangzhou, China

Eurocrypt 2023

Outlines

1. Introduction
2. Full-fledged Framework with New Improvement Techniques
3. Results of SKINNY Block Cipher

Outline

1 Introduction
- Brief Description of Demirci-Selçuk Meet-in-the-Middle
- Previous Models Based on CP

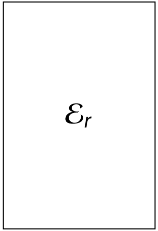
2 Full-fledged Framework with New Improvement Techniques

3 Results of SKINNY Block Cipher

DS-MITM Attack

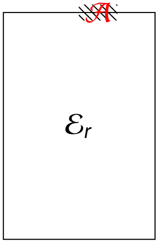
- Demirci-Selçuk MITM, FSE 2008 [DS08].
- Differential enumeration technique and key bridging technique, ASIACRYPT 2010 [DKS10].
- Improved differential enumeration technique, EUROCRYPT 2013 [DF13]
- Key dependent Sieve technique, FSE 2014 [LJW14]
- Tweak-difference cancellation technique, IET Inf. Secur 2019 [LJ19]
- Dedicated search algorithm, CRYPTO 2016 [DF16]
- Constraints programming based approach, Asiacrypt 2018 [SSD$^+$18]

DS-MITM Distinguisher



DS-MITM Distinguisher

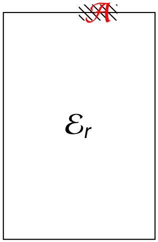
- $\mathcal{A} = [\mathbf{S}_0[j_0], \mathbf{S}_0[j_1], \ldots, \mathbf{S}_0[j_s]]$ is a sequence of positions.



DS-MITM Distinguisher

- $\mathcal{A} = [\mathbf{S}_0[j_0], \mathbf{S}_0[j_1], \dots, \mathbf{S}_0[j_s]]$ is a sequence of positions.
- $\delta(\mathcal{A})$: a set of messages that are all different in positions specified by $\mathcal{A}$ and all equal in other positions

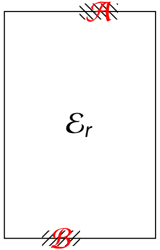
$\delta(\mathcal{A})$-set: $\{P^0, P^1, \dots, P^{N-1}\}$



DS-MITM Distinguisher

- $\mathcal{A} = [\mathbf{S}_0[j_0], \mathbf{S}_0[j_1], \ldots, \mathbf{S}_0[j_s]]$ is a sequence of positions.
- $\delta(\mathcal{A})$: a set of messages that are all different in positions specified by $\mathcal{A}$ and all equal in other positions
- $\mathcal{B} = [\mathbf{S}_r[i_0], \ldots, \mathbf{S}_r[i_t]]$ is a sequence of positions.

$\delta(\mathcal{A})$-set: $\{P^0, P^1, \ldots, P^{N-1}\}$

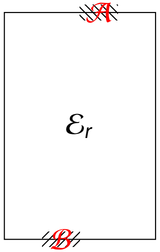


$\{C^0, C^1, \ldots, C^{N-1}\}$

DS-MITM Distinguisher

- $\mathcal{A} = [\mathbf{S}_0[j_0], \mathbf{S}_0[j_1], \ldots, \mathbf{S}_0[j_s]]$ is a sequence of positions.
- $\delta(\mathcal{A})$: a set of messages that are all different in positions specified by $\mathcal{A}$ and all equal in other positions
- $\mathcal{B} = [\mathbf{S}_r[i_0], \ldots, \mathbf{S}_r[i_t]]$ is a sequence of positions.
- $\Delta\mathcal{E}_r(\delta(\mathcal{A}))[\mathcal{B}]$-sequence: an ordered sequence in positions specified by $\mathcal{B}$ of the associated $\delta(\mathcal{A})$-set

$\delta(\mathcal{A})$-set: $\{P^0, P^1, \ldots, P^{N-1}\}$



$\{C^0, C^1, \ldots, C^{N-1}\}$

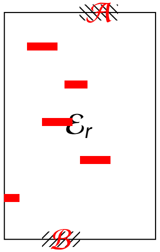
$C^0[\mathcal{B}] \oplus C^1[\mathcal{B}] || \ldots || C^0[B] \oplus C^{N-1}[B]$

$(\Delta\mathcal{E}_r(\delta(\mathcal{A}))[\mathcal{B}]$-sequence)

DS-MITM Distinguisher

- $\mathcal{A} = [\mathbf{S}_0[j_0], \mathbf{S}_0[j_1], \ldots, \mathbf{S}_0[j_s]]$ is a sequence of positions.
- $\delta(\mathcal{A})$: a set of messages that are all different in positions specified by $\mathcal{A}$ and all equal in other positions
- $\mathcal{B} = [\mathbf{S}_r[i_0], \ldots, \mathbf{S}_r[i_t]]$ is a sequence of positions.
- $\Delta\mathcal{E}_r(\delta(\mathcal{A}))[\mathcal{B}]$-sequence: an ordered sequence in positions specified by $\mathcal{B}$ of the associated $\delta(\mathcal{A})$-set
- $\Delta\mathcal{E}_{r_1}(\delta(\mathcal{A}))[\mathcal{B}]$ sequence is uniquely determined by several internal parameters.

$\delta(\mathcal{A})$-set: $\{P^0, P^1, \ldots, P^{N-1}\}$



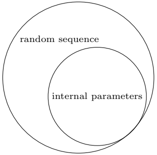
$\{C^0, C^1, \ldots, C^{N-1}\}$

$C^0[\mathcal{B}] \oplus C^1[\mathcal{B}] || \ldots || C^0[B] \oplus C^{N-1}[B]$

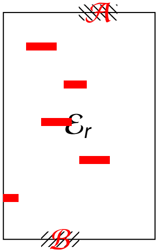
$(\Delta\mathcal{E}_r(\delta(\mathcal{A}))[\mathcal{B}]$-sequence$)$

DS-MITM Distinguisher

- $\mathcal{A} = [\mathbf{S}_0[j_0], \mathbf{S}_0[j_1], \ldots, \mathbf{S}_0[j_s]]$ is a sequence of positions.
- $\delta(\mathcal{A})$: a set of messages that are all different in positions specified by $\mathcal{A}$ and all equal in other positions
- $\mathcal{B} = [\mathbf{S}_r[i_0], \ldots, \mathbf{S}_r[i_t]]$ is a sequence of positions.
- $\Delta\mathcal{E}_r(\delta(\mathcal{A}))[\mathcal{B}]$-sequence: an ordered sequence in positions specified by $\mathcal{B}$ of the associated $\delta(\mathcal{A})$-set
- $\Delta\mathcal{E}_{r_1}(\delta(\mathcal{A}))[\mathcal{B}]$ sequence is uniquely determined by several internal parameters.
- condition:



$\delta(\mathcal{A})$-set: $\{P^0, P^1, \ldots, P^{N-1}\}$



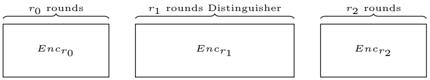
$\{C^0, C^1, \ldots, C^{N-1}\}$

$C^0[\mathcal{B}] \oplus C^1[\mathcal{B}] || \ldots || C^0[B] \oplus C^{N-1}[B]$

$(\Delta\mathcal{E}_r(\delta(\mathcal{A}))[\mathcal{B}]$-sequence)

Attack Process

- **Precomputation phase.**
  - A lookup table is built to save all possible values of $\Delta\mathcal{E}_3(\delta(\mathcal{A}))[\mathcal{B}]$.
- **Online phase**
  - Guess round-keys involved in r_0 rounds to identify a $\delta(A)$-set for the distinguisher.
  - Guess round-keys involved in r_2 rounds to compute the output difference $\Delta\mathcal{E}_{r_1}(\delta(\mathcal{A}))[\mathcal{B}]$.
  - Check whether the sequence in the lookup table, obtain the candidate of guessed round-keys involved in r_0, r_2 rounds that pass the test.



Basic Distinguisher on Toy Cipher

- $\mathbb{L} = [[0, 1, 1, 1], [1, 0, 1, 1], [1, 1, 0, 1]]$
- $\mathcal{A} = [\mathbf{S}_0[3]], \mathcal{B} = [\mathbf{S}_3[1]]$
- $\Delta\mathcal{E}_3(\delta(\mathcal{A}))[\mathcal{B}] = P^0 \oplus P^1[\mathbf{S}_3[1]] \| \ldots \| P^0 \oplus P^{255}[\mathbf{S}_3[1]]$ can be uniquely determined:

$$P^0[\mathbf{S}_0[3]], \{P^0[\mathbf{S}_1[j]] : j \in [0, 1, 2]\}, \{P^0[\mathbf{S}_2[j]] : j \in [0, 2, 3]\}.$$

- $\Delta\mathcal{E}_3(\delta(\mathcal{A}))[\mathcal{B}]$ can take at most $2^{7\times 8}$ possible values ($2^{255\times 8} = 2^{2040}$ possibilities for a random 255-byte sequence)

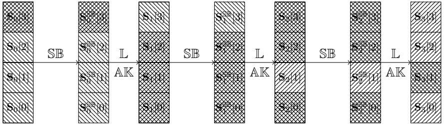


Figure: A 3-round toy SPN block cipher

Improvement Techniques-Differential Enumeration Technique

Differential property of S-box

Given an input and output difference pair of $(\Delta_{in}, \Delta_{out})$ of an Sbox, the equation $\mathrm{Sbox}(x) \oplus \mathrm{Sbox}(x \oplus \Delta_{in}) = \Delta_{out}$ has one solution on average.

- Assume (P^0, P') conforms to a truncated differential trail, $P^0 \in \delta(\mathcal{A})$, many values of the internal parameters are not reached.
- $P^0[\mathbf{S}_0[3]], \{P^0[\mathbf{S}_1[j]] : j \in [0,1,2]\}, \{P^0[\mathbf{S}_2[j]] : j \in [0,2,3]\}$ can be determined by $P^0[\mathbf{S}_0[3]], \{P^0[\mathbf{S}_1[j]], j \in [0,1,2]\}, \{P^0 \oplus P'[\mathbf{S}_0^{\mathbb{SB}}[3]]\}, \{P^0 \oplus P'[\mathbf{S}_3[1]]\}$.

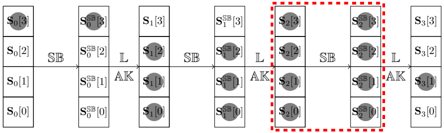


Figure: A truncated differential trail on toy cipher

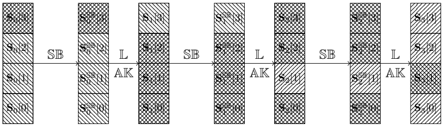


Figure: A valid typeZ trail on toy cipher

Improvement Techniques

- **Key-Dependent-Sieve Technique.** Utilize the relations on round keys deduced from these internal parameters.
- **Tweak-Difference Cancellation Technique.** Utilize the tweak difference to cancel a difference in the state.
- **Key-Bridging Technique.** Utilize the dependent relations on keys involved in the key-recovery phase.

Modelling the Basic DS-MITM Distinguisher based on CP

Three types (typeX, typeY, typeZ) of 0-1 variables for each cell are introduced. $\mathbb{L} = [[0, 1, 1, 1], [1, 0, 1, 1], [1, 1, 0, 1]]$

- typeX variables (▨) form a forward differential trail.
- Define $\overline{\mathcal{A}_i} = [\mathbf{S}_i[j] : \text{typeX-}\mathbf{S}_i[j] = 0]$. For each pair of (P, P') satisfying $P \oplus P'[j] = 0, \forall j \in \overline{\mathcal{A}_i}$, obtain $P \oplus P'[j] = 0, \forall j \in \overline{\mathcal{A}_{i+1}}$.
- Constraints over typeX variables follow the differential propagation rule with probability 1.

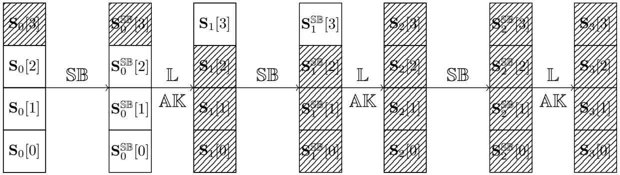


Figure: A valid forward differential trail on toy cipher

Modelling the Basic DS-MITM Distinguisher Based on CP

Three types (typeX, typeY, typeZ) of 0-1 variables for each cell are introduced. $\mathbb{L} = [[0,1,1,1],[1,0,1,1],[1,1,0,1]]$

- typeY variables (▧) form a backward determination trail.
- Define $\mathcal{B}_i = \{\mathbf{S}_i[j] : \text{typeY-}\mathbf{S}_i[j] = 1\}$. For any pair of (P, P'), each difference among $\{P \oplus P'[j] : j \in \mathcal{B}_{i+1}\}$ can be uniquely determined by $\{P \oplus P'[j], P[j] : j \in \mathcal{B}_i\}$.
- typeY-$\mathbf{S}_i[j] = 0$ indicates that difference in each cell in $\mathcal{B}_{i+1}$ is independent of the knowledge of $\mathbf{S}_i[j]$.

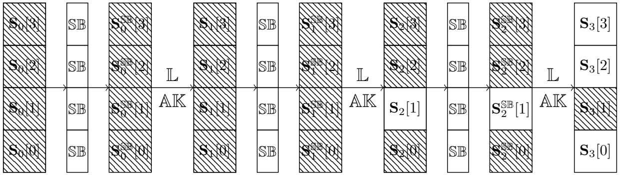


Figure: A valid backward determination on toy cipher

Modelling the Basic DS-MITM Distinguisher based on CP

Three types (typeX, typeY, typeZ) of 0-1 variables for each cell are introduced. $\mathbb{L} = [[0,1,1,1],[1,0,1,1],[1,1,0,1]]$

- typeZ-$*$ (⊠) equals 1 if and only if typeX-* = 1 (▨) and typeY-* = 1 (▧)
- $\Delta\mathcal{E}_{r_1}(\delta(\mathcal{A}))[\mathcal{B}]$ can be uniquely determined by the following internal parameters:

$$\{P^0[\mathbf{S}_i[j]] : \text{typeZ-}\mathbf{S}_i[j] = 1, r_0 \leq i \leq r_0 + r_1 - 1, j \in [0, \dots, n]\}.$$

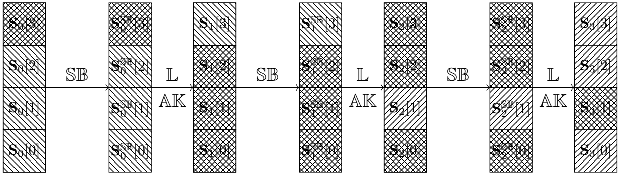


Figure: A valid typeZ trail on toy cipher

Outline

1. Introduction
2. Full-fledged Framework with New Improvement Techniques
   - A High Level Overview
   - Differential Enumeration Technique
   - Key-Dependent-Sieve Technique
   - Tweak-Difference Cancellation Technique
3. Results of SKINNY Block Cipher

A High Level Overview

- **Basic DS-MITM distinguisher.** three types (typeX, typeY, typeZ) of 0-1 variables
- **Differential enumeration.** typeT variables describe the traditional truncated differential trail. typeGT variables describe the internal parameters whose values will be bounded by truncated differential trail. typeGZ variables describe the remaining internal parameters.
- **Key-dependent sieve.** typeGT and typeGZ variables are unified by typeV variables. typeK variables are introduced to describe the round-keys deduced from these internal parameters.
- **Tweak-difference cancellation.** typeX variables for each tweak cell and describe forward differential trail propagation for both tweak addition and tweak schedule.
- **Key-recovery phase** model the phase of obtaining a pair conforming to the truncated differential trail of the distinguisher. Impose variables to form *a backward differential trail* through the first r_0 rounds and *a forward differential trail* through the last r_2 rounds.

Modelling the Differential Enumeration Technique

Three types (typeT (▣), typeGT (■), typeGZ (■)) of 0-1 variables for each cell are introduced.

- typeT variables (▣): truncated differential propagation

typeT-based backward determination trail ■

Define $\mathcal{G}_i = [\mathbf{S}_i[j] : \text{typeGT-}\mathbf{S}_i[j] = 1, j \in [0, \ldots, n-1]]$. (P, P') conforms to the truncated differential trail, obtain each difference in $\{P \oplus P'[j] : j \in \mathcal{G}_{i+1}\}$ can be uniquely determined by $\{P \oplus P'[j], P[j] : j \in \mathcal{G}_i\}$.

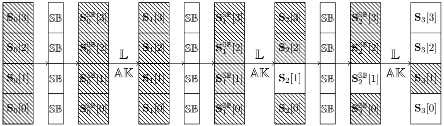


Figure: A valid backward determination on toy cipher

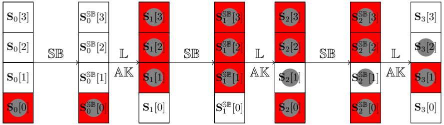


Figure: A typeT-based backward determination trail on toy cipher

Modelling the Differential Enumeration Technique

Three types (typeT, typeGT, typeGZ) of 0-1 variables for each cell are introduced.

- typeT-based forward determination trail
- Each difference in $\{P \oplus P'[j] : j \in \mathcal{G}_i\}$ can be uniquely determined by

$$\{P \oplus P'[j] : j \in \mathcal{G}_{i+1}\}, \{P[j] : j \in \mathcal{G}_i\}.$$

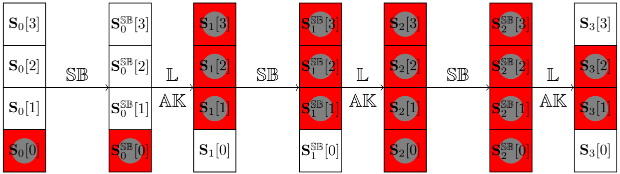


Figure: A typeT-based forward determination trail on toy cipher

Modelling the Differential Enumeration Technique

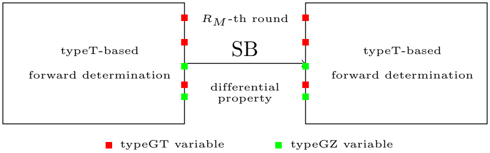
Three types (typeT, typeGT, typeGZ) of 0-1 variables for each cell are introduced.

Differential property of S-box

Given an input and output difference pair of $(\Delta_{in}, \Delta_{out})$ of an Sbox, the equation $\text{Sbox}(x) \oplus \text{Sbox}(x \oplus \Delta_{in}) = \Delta_{out}$ has one solution on average.

- Initialize typeGT variables in R_M-th round.

$$\text{typeGT-}\mathbf{S}_{R_M}[j] = \begin{cases} 1, & \text{if typeT-}\mathbf{S}_{R_M}[j] = 1 \text{ and typeZ-}\mathbf{S}_{R_M}[j] = 1, \\ 0, & \text{otherwise.} \end{cases}$$



Modelling the Differential Enumeration Technique

Three types (typeT, typeGT, typeGZ) of 0-1 variables for each cell are introduced.

- typeGZ variables are utilized to consider the remaining internal parameters except those covered by typeGT variables (typeGT-* = 1)

$$\text{typeGZ-}* = \begin{cases} 1(\blacksquare) : \text{if typeZ-}* = 1 \text{ and typeGT-}* = 0, \\ 0(\square) : \text{otherwise.} \end{cases}$$

Objective Function

$\Delta\mathcal{E}_{r_1}(\delta(\mathcal{A}))[\mathcal{B}]$-sequence can be uniquely determined by the following internal parameters:

$$\{P^0 \oplus P'[\mathbf{S}_r[j]] : \text{typeGT-}\mathbf{S}_r[j] = 1, r \in \{r_0, r_0 + r_1\}, j \in [0, \dots, n-1]\},$$
$$\{P^0[\mathbf{S}_i[j]] : \text{typeGT-}\mathbf{S}_i[j] = 1, r_0 \le i \le r_0 + r_1 - 1, i \ne R_M, j \in [0, \dots, n-1]\},$$
$$\{P^0[\mathbf{S}_i[j]] : \text{typeGZ-}\mathbf{S}_i[j] = 1, r_0 \le i \le r_0 + r_1 - 1, j \in [0, \dots, n-1]\}.$$

Modelling Key-Dependent-Sieve Technique

- Some round keys can be deduced from these internal parameters.

$$\text{typeV-}* = \begin{cases} 1 : \text{if typeGZ-}* = 1 \text{ or typeGT-}* = 1, \\ 0 : \text{otherwise.} \end{cases}$$

- Assume $\mathbf{S}_{r+1} = \mathbb{L}(\mathbf{S}_r^{\mathbb{SB}}) \oplus RK_r$.

$$\text{typeK-}RK_r[j] = \begin{cases} 1(\blacksquare) : \text{if typeV-}\mathbf{S}_{r+1}[j] = 1, \text{typeV-}\mathbf{S}_r^{\mathbb{SB}}[j_i] = 1, \forall i, \\ 0(\square) : \text{otherwise.} \end{cases}$$

- The various relations for specified cipher can be included in the model dynamically.

Modelling the Tweak-Difference Cancellation Technique

- $\delta(\mathcal{A})$-set: $\{(P^0, TW^0), \ldots, (P^N, TW^N)\}$.
- Tweak differences: cancel the state difference in one round.
- Constraints over typeX variables follows the forward differential propagation except for the round with tweak-difference cancellation.
- Assume tweak addition operation is expressed by $y = x \oplus rT$.

$$\text{typeX-}y = \begin{cases} 0 : \text{typeX-}x = \text{typeX-}rT = 0, \\ 1 : \text{typeX-}x \oplus \text{typeX-}rT = 1, \\ 0 \text{ or } 1 : \text{typeX-}x = \text{typeX-}rT = 1. \end{cases}$$

$$\text{typeX-}y = \begin{cases} 0 : \text{typeX-}x = \text{typeX-}rT = 0, \\ 1 : \text{others}. \end{cases}$$

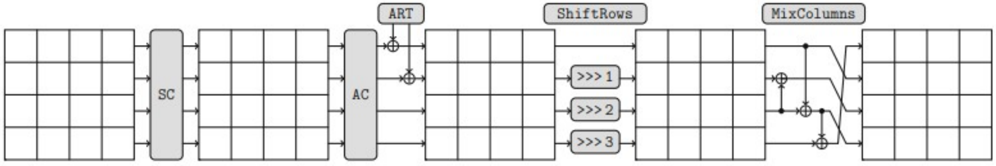
Outline

1 Introduction

2 Full-fledged Framework with New Improvement Techniques

3 Results of SKINNY Block Cipher

Brief Description of SKINNY Block Cipher



- SubCells: Apply a non-linear substitution-box operation to each cell.
- AddConstants: update the state by XORing constants.
- AddRoundTweakey: update the state by XORing the first two rows with tweakey arrays.
- ShiftRows(SR): rotate *i*-th row to the right by *i* cells.
- MixColums: multiply each column by a binary matrix.

Non-full Key-addition Technique

- States between two consecutive rounds are not totally independent.
- Dependencies between the variables can be described by the rank of a matrix derived from the linear transformation.
- $(x_4, x_5, x_6, x_7) = \mathbb{L}(x_0 \oplus rk_0, x_1 \oplus rk_1, x_2, x_3)$.
- For each subset $\{x_i : \text{typeV-}x_i = 1, i \in \{2, 3, \ldots, 7\}\}$, the degree of freedom β can be computed from the linear transformation.
- The reduced bytes are $\sum_{i=2}^{7} \text{typeV-}x_i - \beta$.

A Summary of the Results

Version	Approach	R_{attack}	Time	Data	Memory	CT	Ref.
SKINNY-128-128	ID	17	$2^{120.8}$	$2^{118.5}$	$2^{97.5}$	✗	[23]
	ID	17	$2^{116.51}$	$2^{116.37}$	2^{80}		[15]
	DS-MITM	17	$2^{122.06}$	2^{96}	$2^{118.91}$		Sect. L, Fig. 35
SKINNY-128-256	ID	19	$2^{119.8}$	2^{62}	2^{110}	✗	[23]
	ID	19	$2^{219.23}$	$2^{117.86}$	2^{208}		[15]
	DS-MITM	19	$2^{238.26}$	2^{96}	$2^{210.99}$		[14]
	DS-MITM	19	$2^{235.05}$	2^{96}	$2^{207.7}$		Sect. I, Fig. 29
	DS-MITM	20	$2^{254.28}$	2^{96}	$2^{250.99}$		Sect. H, Fig. 27
	DS-MITM	21	$2^{234.84}$	2^{96}	$2^{183.52}$	✓	Sect. A, Fig. 13(8-bit tweak)
	DS-MITM	21	$2^{234.99}$	2^{64}	$2^{231.86}$		Sect. C, Fig. 17(8-bit tweak)
	Int	22	2^{216}	$2^{113.58}$	2^{216}		[15]
SKINNY-128-384	ID	22	$2^{373.48}$	$2^{92.22}$	$2^{147.22}$	✗	[22]
	ID	21	$2^{347.35}$	$2^{122.89}$	2^{336}		[15]
	MITM	23	2^{368}	2^{120}	2^{16}		[2]
	DS-MITM	22	$2^{366.28}$	2^{96}	$2^{370.99}$		[4]
	DS-MITM	23	2^{372}	2^{96}	$2^{352.46}$		Sect. G, Fig. 25
	DS-MITM	25	$2^{363.83}$	2^{96}	$2^{336.39}$	✓	Sect. 5.2, Fig. 11(8-bit tweak)
	Int	26	2^{344}	2^{121}	2^{340}		[15]
SKINNY-64-128	ID	18	2^{116}	2^{60}	2^{112}	✗	[12]
	ID	19	$2^{119.8}$	2^{60}	2^{112}		[23]
	ID	19	$2^{110.34}$	$2^{60.86}$	2^{104}		[15]
	DS-MITM	18	$2^{126.32}$	2^{32}	$2^{61.91}$		[14]
	DS-MITM	19	$2^{123.43}$	2^{52}	$2^{126.95}$		Sect. N, Fig. 39
	DS-MITM	21	$2^{119.32}$	2^{60}	$2^{114.81}$	✓	Sect. D, Fig. 19(8-bit tweak)
	ZC/Integral	20	$2^{97.5}$	$2^{68.4}$	2^{82}		[1]
	Int	22	2^{110}	$2^{57.58}$	2^{108}		[15]
SKINNY-64-192	ID	22	$2^{183.97}$	$2^{47.84}$	$2^{74.84}$	✗	[22]
	ID	21	$2^{174.42}$	$2^{62.43}$	2^{168}		[15]
	MITM	23	2^{188}	2^{52}	2^{4}		[11]
	MITM	23	2^{188}	2^{28}	2^{4}		[2]
	MITM	23	2^{184}	2^{60}	2^{8}		[2]
	DS-MITM	21	$2^{186.63}$	2^{60}	$2^{133.99}$		[14]
	DS-MITM	21	$2^{180.01}$	2^{44}	$2^{191.55}$		Sect. K, Fig. 33
	DS-MITM	23	$2^{179.9}$	2^{32}	$2^{183.49}$	✓	Sect. F, Fig. 23(8-bit tweak)
	DS-MITM	23	$2^{174.9}$	2^{56}	$2^{179.46}$		Sect. E, Fig. 21(16-bit tweak)
	ZC/Integral	23	$2^{155.6}$	$2^{73.2}$	2^{138}		[1]
	Int	26	2^{172}	2^{61}	2^{172}		[15]

Thanks for your attention.

Reference I

Patrick Derbez and Pierre-Alain Fouque.
Exhausting demirci-selçuk meet-in-the-middle attacks against reduced-round AES.
In *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, pages 541–560, 2013.

Patrick Derbez and Pierre-Alain Fouque.
Automatic search of meet-in-the-middle and impossible differential attacks.
In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, pages 157–184, 2016.

Orr Dunkelman, Nathan Keller, and Adi Shamir.
Improved single-key attacks on 8-round AES-192 and AES-256.
In *Advances in Cryptology - ASIACRYPT 2010. Proceedings*, pages 158–176, 2010.

Hüseyin Demirci and Ali Aydin Selçuk.
A meet-in-the-middle attack on 8-round AES.
In *Fast Software Encryption, 15th International Workshop, FSE 2008*, pages 116–126, 2008.

Rongjia Li and Chenhui Jin.
Meet-in-the-middle attacks on round-reduced tweakable block cipher deoxys-bc.
IET Inf. Secur., 13(1):70–75, 2019.

Reference II

Leibo Li, Keting Jia, and Xiaoyun Wang.
Improved single-key attacks on 9-round AES-192/256.
In *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, pages 127–146, 2014.

Danping Shi, Siwei Sun, Derbez, Yosuke Todo, Bing Sun, and Lei Hu.
Programming the demirci-selçuk meet-in-the-middle attack with constraints.
In *Advances in Cryptology - ASIACRYPT 2018, Proceedings, Part II*, volume 11273 of *Lecture Notes in Computer Science*, pages 3–34. Springer, 2018.