Finding the Impossible: Automated Search for Full Impossible-Differential, Zero-Correlation, and Integral Attacks

Hosein Hadipour Sadegh Sadeghi Maria Eichlseder

EUROCRYPT 2023 - Lyon, France

› hossein.hadipour@iaik.tugraz.at

TU Graz
SCIENCE PASSION TECHNOLOGY

Research Gap and Our Contributions

Research gap

- Lack of automatic tool to find full ID/ZC, and integral attacks

Contributions

- Introduced a new CP-based method to find ID/ZC, and integral distinguishers
- Our CP model can be extended to an efficient unified model for key recovery
- Found improved attacks for SKINNY, CRAFT, SKINNYee, and SKINNYe-v2

Research Gap and Our Contributions

Research gap

- Lack of automatic tool to find full ID/ZC, and integral attacks

Contributions

- Introduced a new CP-based method to find ID/ZC, and integral distinguishers
- Our CP model can be extended to an efficient unified model for key recovery
- Found improved attacks for SKINNY, CRAFT, SKINNYee, and SKINNYe-v2

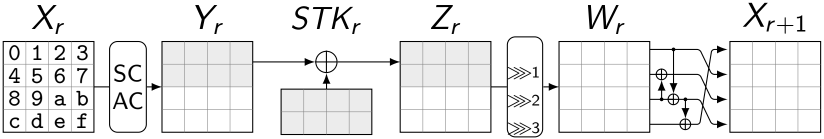
Part of Our Result

Cipher	#R	Time	Data	Mem.	Attack	Setting / Model	Ref.
SKINNY-64-192	23	$2^{155.60}$	$2^{73.20}$	2^{138}	Int	180,SK / CP,CT	[Ank+19]
	26	2^{172}	2^{61}	2^{172}	Int	180,SK / CP,CT	This paper
SKINNY-64-128	18	2^{126}	$2^{62.68}$	2^{64}	ZC	STK / KP	[SMB18]
	19	$2^{119.12}$	$2^{62.89}$	2^{49}	ZC	STK / KP	This paper
	20	$2^{97.50}$	$2^{68.40}$	2^{82}	Int	120,SK / CP,CT	[Ank+19]
	22	2^{110}	$2^{57.58}$	2^{108}	Int	120,SK / CP,CT	This paper
SKINNY-128-256	19	$2^{241.80}$	2^{123}	2^{221}	ID	STK / CP	[YQC17]
	19	$2^{219.23}$	$2^{117.86}$	2^{208}	ID	STK / CP	This paper
SKINNY-64-64	14	2^{62}	$2^{62.58}$	2^{64}	ZC	STK / KP	[SMB18]
	16	$2^{62.71}$	$2^{61.35}$	$2^{37.80}$	ZC	STK / KP	This paper
CRAFT	**20**	$2^{120.43}$	$2^{62.89}$	2^{49}	ZC	STK / KP	This paper
	21	$2^{106.53}$	$2^{60.99}$	2^{100}	ID	STK / CP	This paper

Outline

Background and the Research Gap

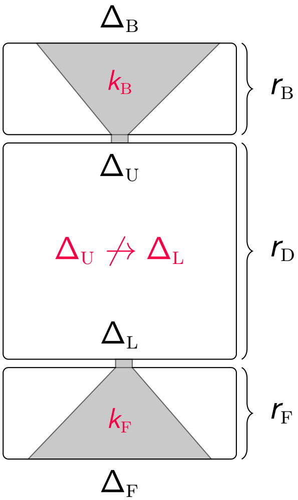
SKINNY Family of Tweakable Block Ciphers [Bei+16]



- Introduced in CRYPTO 2016 [Bei+16]
- It has 6 main variants: SKINNY-n-$z \cdot n$, where $n \in \{64, 128\}$, and $z \in \{1, 2, 3\}$
- ISO/IEC 18033-7: SKINNY-64-192, SKINNY-128-256, SKINNY-128-384

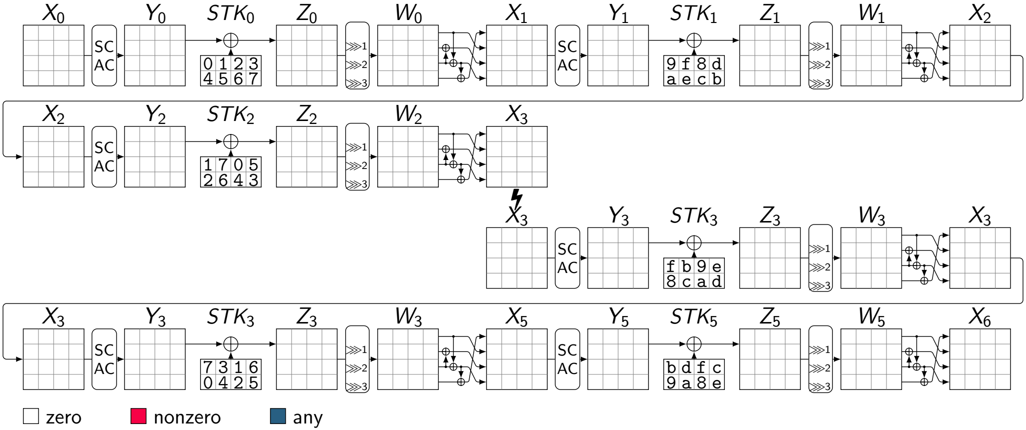
Impossible Differential Attack [BBS99; Knu98]

- Find an impossible-differential $\Delta_U \not\rightarrow \Delta_L$
- Build a key-recovery attack
  - Create a pool of pairs satisfying (Δ_B, Δ_F)
  - For all $k \in k_B \cup k_F$:
    - If a pair suggests (Δ_U, Δ_L), discard k
  - Brute force the remaining key candidates

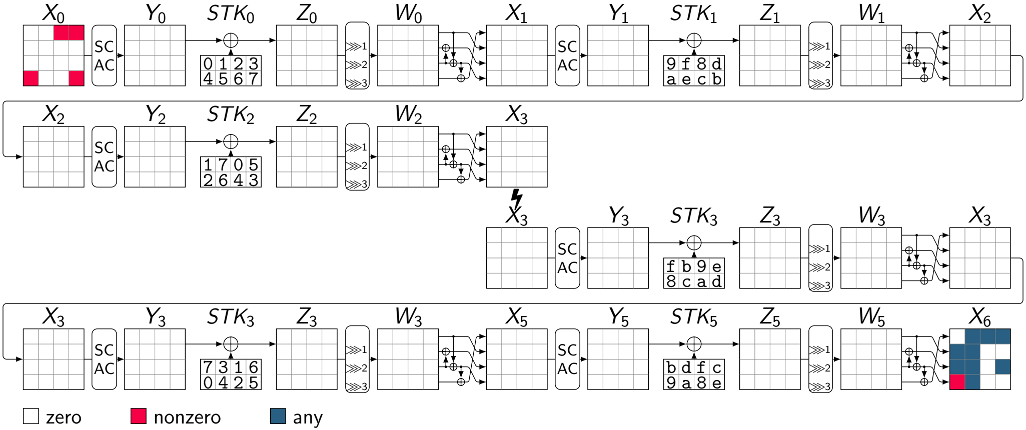


Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

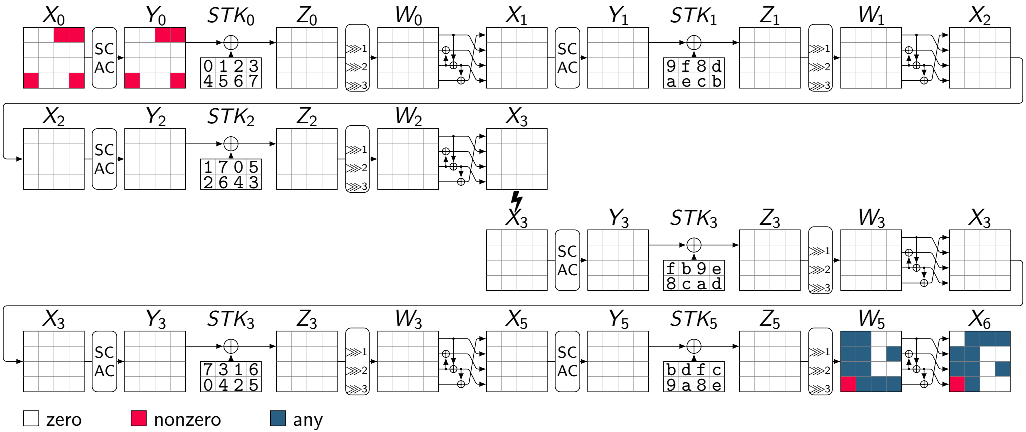
Miss-in-the-Middle Technique [BBS99]



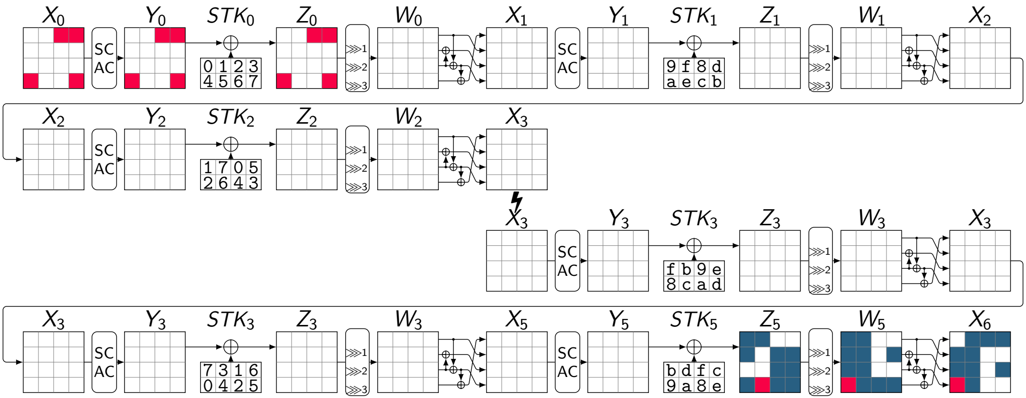
Miss-in-the-Middle Technique [BBS99]



Miss-in-the-Middle Technique [BBS99]

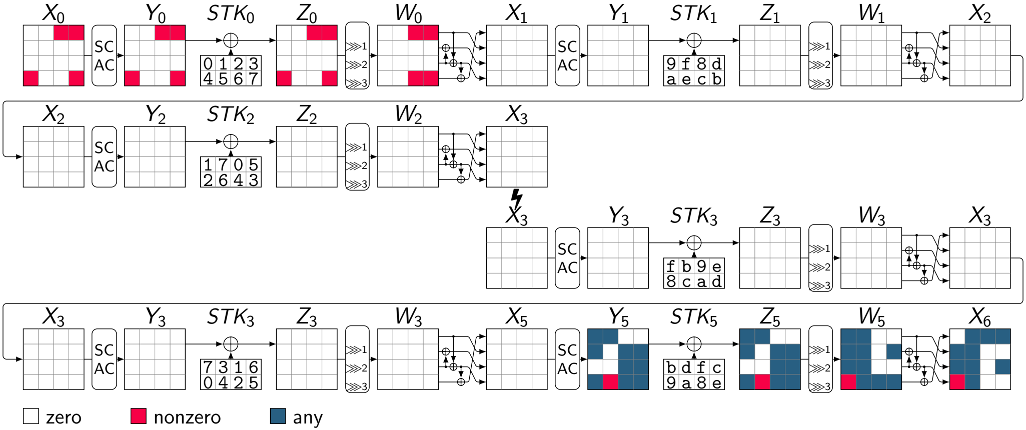


Miss-in-the-Middle Technique [BBS99]

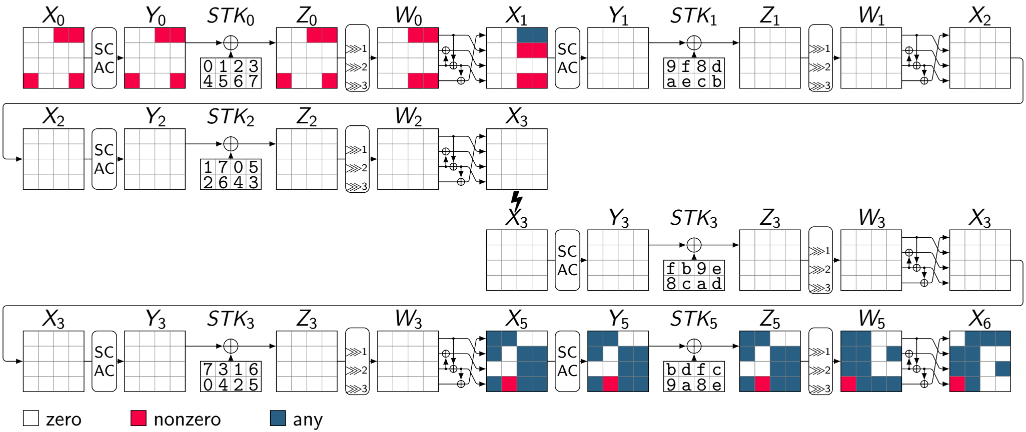


zero nonzero any

Miss-in-the-Middle Technique [BBS99]

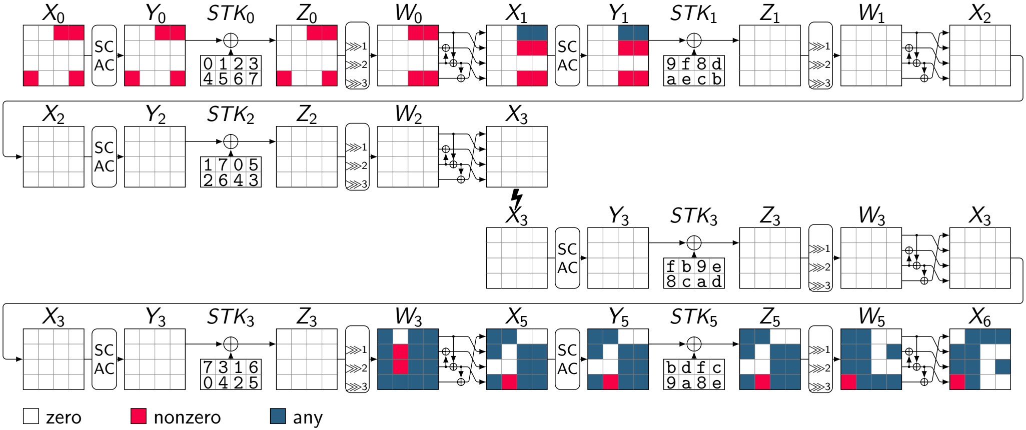


Miss-in-the-Middle Technique [BBS99]

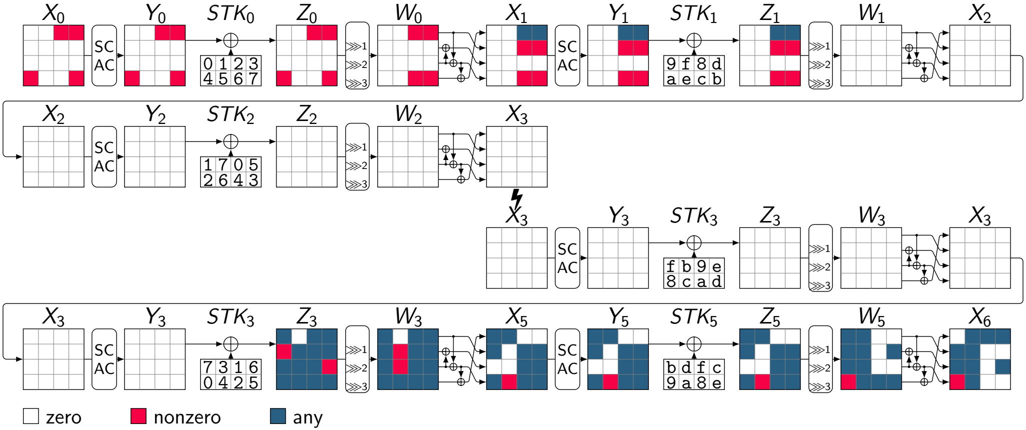


Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

Miss-in-the-Middle Technique [BBS99]

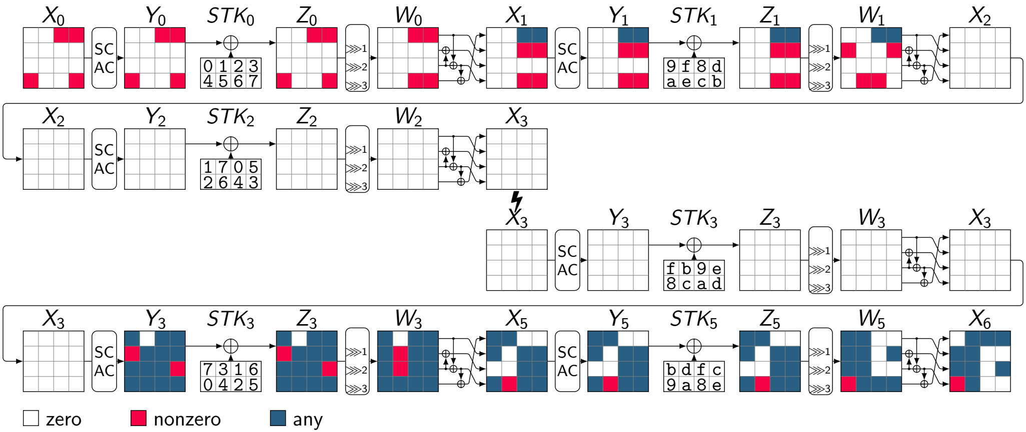


Miss-in-the-Middle Technique [BBS99]



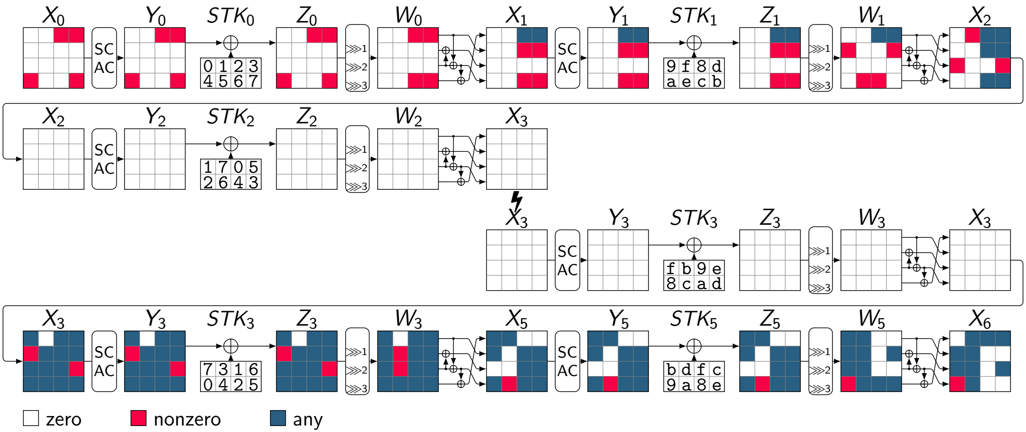
Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

Miss-in-the-Middle Technique [BBS99]



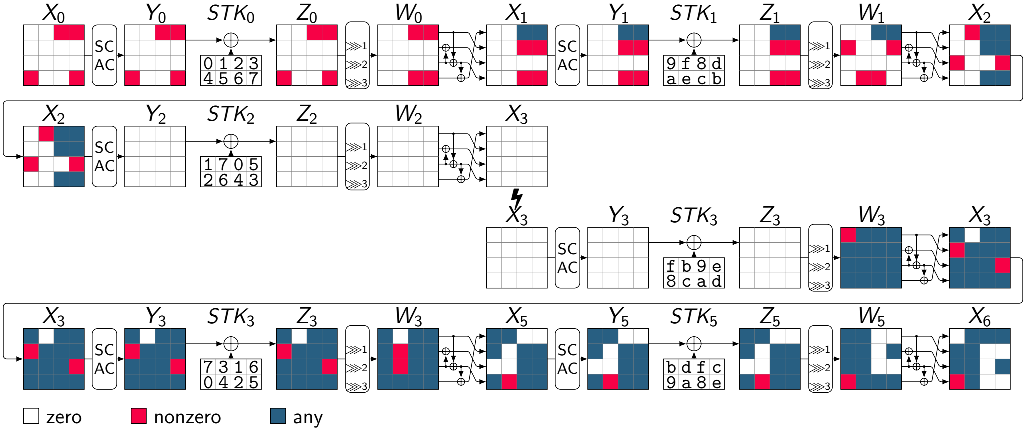
Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

Miss-in-the-Middle Technique [BBS99]

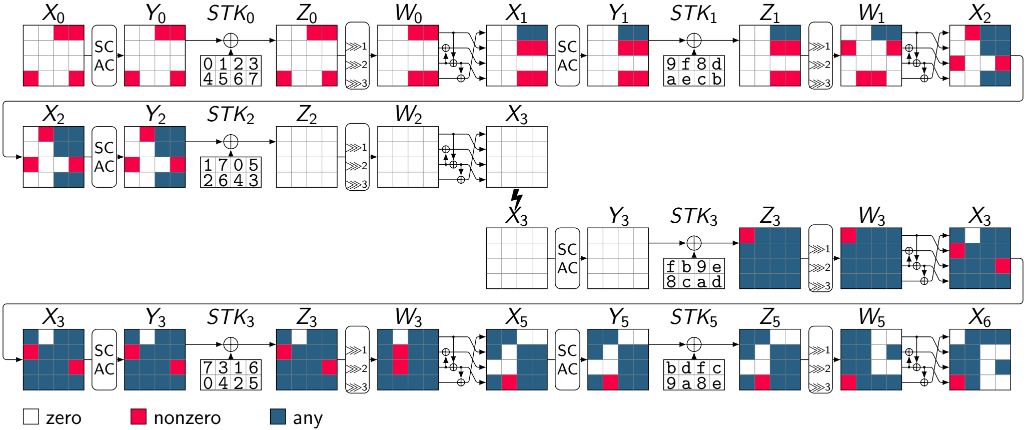


Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

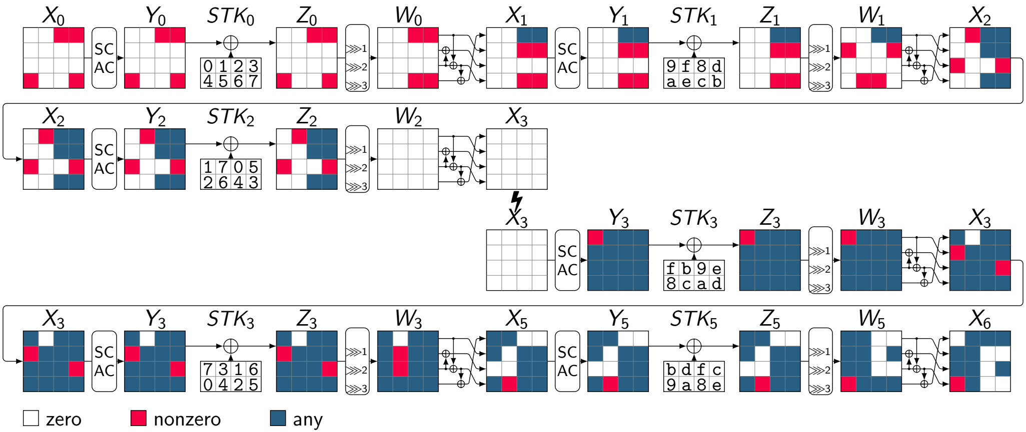
Miss-in-the-Middle Technique [BBS99]



Miss-in-the-Middle Technique [BBS99]

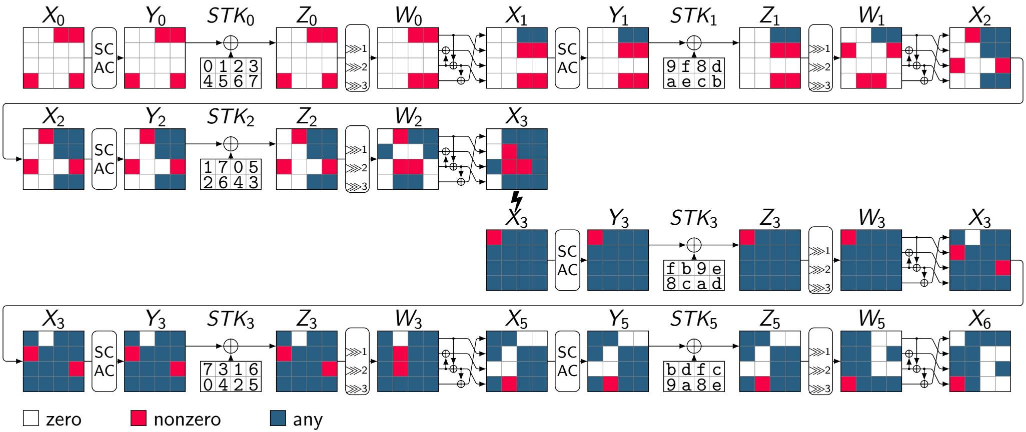


Miss-in-the-Middle Technique [BBS99]



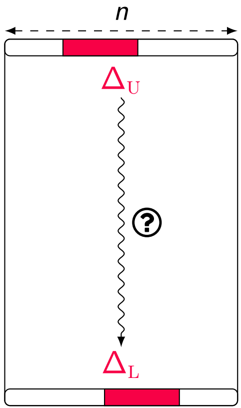
Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder
EUROCRYPT 2023 - Lyon, France

Miss-in-the-Middle Technique [BBS99]



Previous Tools for ID/ZC, and Integral Attacks

- Tools based on dedicated algorithms:
  - CRYPTO 2016 ($\mathcal{DC}$-MITM, ID) [DF16]
- Tools based on general purpose solvers:
  - Eprint 2016 (ID) [Cui+16]
  - ASIACRYPT 2016 (Integral) [Xia+16]
  - EUROCRYPT 2017 (ID, ZC) [ST17]
  - ToSC 2017 (ID, ZC) [Sun+17]
  - ToSC 2020 (ID, ZC) [Sun+20]



Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

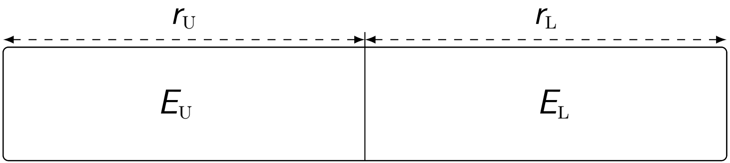
Our Method to Search for Distinguishers

Our Method to Search for ID/ZC and Integral Distinguishers

$$E$$

- $CSP_{\mathrm{U}}(\Delta_{\mathrm{U}}, \Delta'_{\mathrm{U}})$
- $CSP_{\mathrm{L}}(\Delta_{\mathrm{L}}, \Delta'_{\mathrm{L}})$
- $CSP_{\mathrm{M}}(\Delta'_{\mathrm{U}}, \Delta'_{\mathrm{L}})$

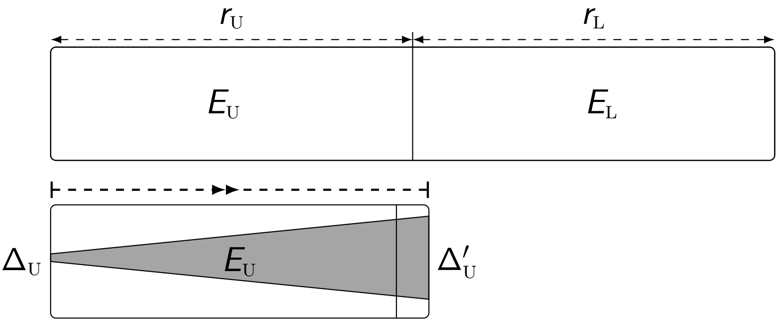
Our Method to Search for ID/ZC and Integral Distinguishers



- $CSP_U(\Delta_U, \Delta'_U)$
- $CSP_L(\Delta_L, \Delta'_L)$
- $CSP_M(\Delta'_U, \Delta'_L)$

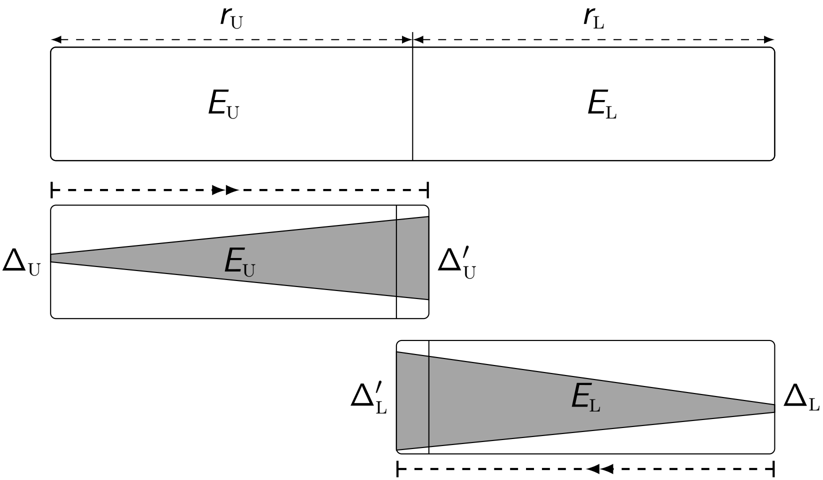
Our Method to Search for ID/ZC and Integral Distinguishers

- $CSP_{\mathrm{U}}(\Delta_{\mathrm{U}}, \Delta'_{\mathrm{U}})$
- $CSP_{\mathrm{L}}(\Delta_{\mathrm{L}}, \Delta'_{\mathrm{L}})$
- $CSP_{\mathrm{M}}(\Delta'_{\mathrm{U}}, \Delta'_{\mathrm{L}})$



Our Method to Search for ID/ZC and Integral Distinguishers

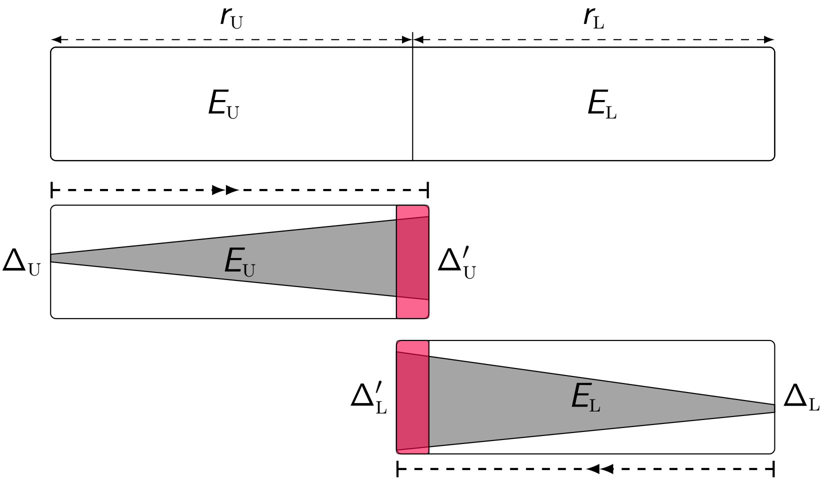
- $CSP_{\mathrm{U}}(\Delta_{\mathrm{U}}, \Delta'_{\mathrm{U}})$
- $CSP_{\mathrm{L}}(\Delta_{\mathrm{L}}, \Delta'_{\mathrm{L}})$
- $CSP_{\mathrm{M}}(\Delta'_{\mathrm{U}}, \Delta'_{\mathrm{L}})$



Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

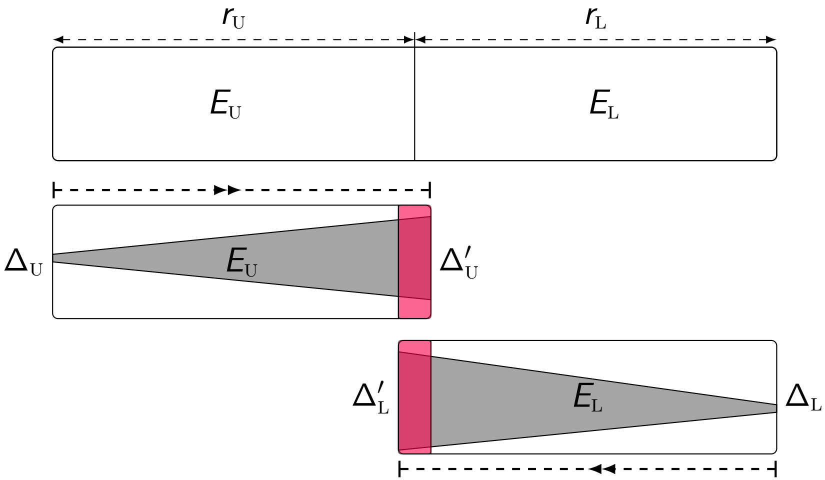
Our Method to Search for ID/ZC and Integral Distinguishers

- $CSP_{\mathrm{U}}(\Delta_{\mathrm{U}}, \Delta'_{\mathrm{U}})$
- $CSP_{\mathrm{L}}(\Delta_{\mathrm{L}}, \Delta'_{\mathrm{L}})$
- $CSP_{\mathtt{M}}(\Delta'_{\mathrm{U}}, \Delta'_{\mathrm{L}})$



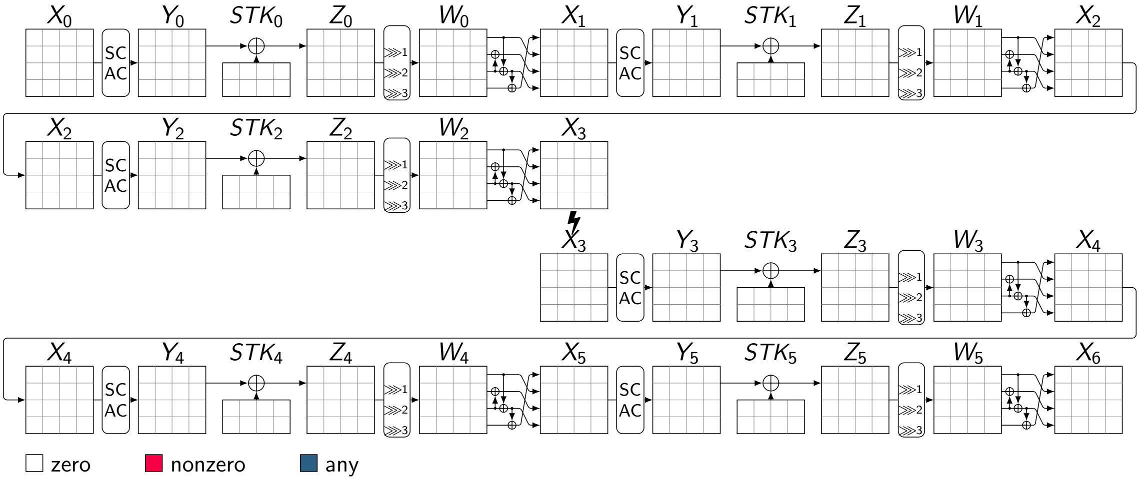
Our Method to Search for ID/ZC and Integral Distinguishers

- $CSP_{\mathrm{U}}(\Delta_{\mathrm{U}}, \Delta'_{\mathrm{U}})$
- $CSP_{\mathrm{L}}(\Delta_{\mathrm{L}}, \Delta'_{\mathrm{L}})$
- $CSP_{\mathtt{M}}(\Delta'_{\mathrm{U}}, \Delta'_{\mathrm{L}})$



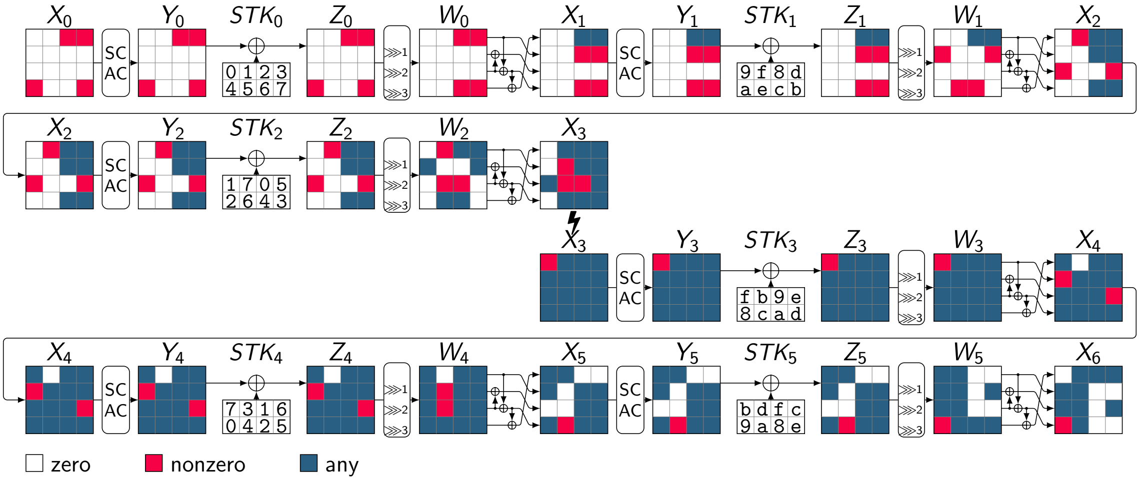
Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

A Basic Example



Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

A Basic Example



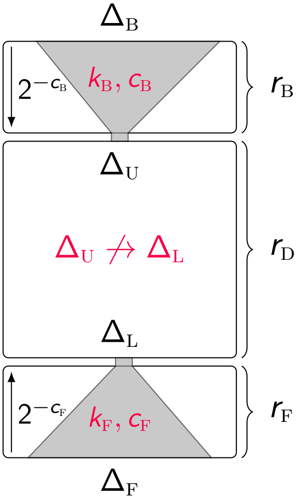
The Advantages of Our Method to Search for Distinguishers

- Based on satisfiability of the CP model
- Any feasible solutions of our CP model is a distinguisher
- We do not fix the input/output of distinguisher
- Extendable to a unified model for key-recovery
  - Find a distinguisher optimized for key-recovery
  - Taking some key-recovery techniques into account, e.g., MitM, and key bridging

Our Unified CP Model for Key-Recovery

Complexity Analysis of ID Attack [Bou+18; BNS14]

- Number of required pairs: N
- Pair generation: $T_0 = N 2^{n+1-|\Delta_{\mathrm{B}}|-|\Delta_{\mathrm{F}}|}$
- Guess-and-filter:
  - $T_1 + T_2 = N + 2^{|k_{\mathrm{B}} \cup k_{\mathrm{F}}|} \frac{N}{2^{c_{\mathrm{B}}+c_{\mathrm{F}}}}$
  - $P = \left(1 - 2^{-(c_{\mathrm{B}}+c_{\mathrm{F}})}\right)^N$
- Exhaustive search: $T_3 = P 2^k$
- $T_{tot} = (T_0 + (T_1 + T_2) C_{E'} + T_3) C_E$



Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

Overall View of Our CP Model for Key-Recovery

- Model the distinguisher for E_{D} $(\Delta_{\mathrm{U}}, \Delta_{\mathrm{F}})$
- Model the filters in E_{B}, and E_{F} $(c_{\mathrm{B}}, c_{\mathrm{F}}, \Delta_{\mathrm{B}}, \Delta_{\mathrm{F}})$
- Model the guess-and-determine in E_{B}, and E_{F}
- Model the key bridging
  - Encode $|k_{\mathrm{B}} \cup k_{\mathrm{F}}|$
- Model the complexity formulas

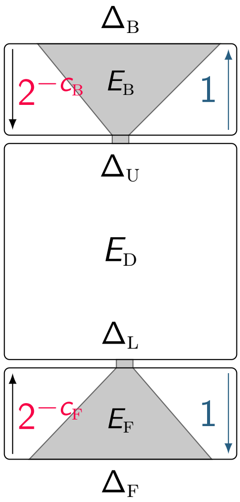
Δ_{U}

E_{D}

Δ_{L}

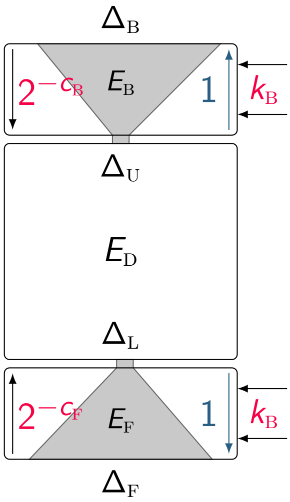
Overall View of Our CP Model for Key-Recovery

- Model the distinguisher for E_{D} $(\Delta_{\mathrm{U}}, \Delta_{\mathrm{F}})$
- Model the filters in E_{B}, and E_{F} $(c_{\mathrm{B}}, c_{\mathrm{F}}, \Delta_{\mathrm{B}}, \Delta_{\mathrm{F}})$
- Model the guess-and-determine in E_{B}, and E_{F}
- Model the key bridging
  - Encode $|k_{\mathrm{B}} \cup k_{\mathrm{F}}|$
- Model the complexity formulas



Overall View of Our CP Model for Key-Recovery

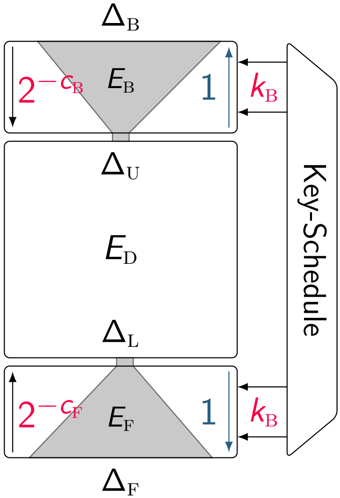
- Model the distinguisher for E_{D} $(\Delta_{\mathrm{U}}, \Delta_{\mathrm{F}})$
- Model the filters in E_{B}, and E_{F} $(c_{\mathrm{B}}, c_{\mathrm{F}}, \Delta_{\mathrm{B}}, \Delta_{\mathrm{F}})$
- Model the guess-and-determine in E_{B}, and E_{F}
- Model the key bridging
  - Encode $|k_{\mathrm{B}} \cup k_{\mathrm{F}}|$
- Model the complexity formulas



Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

Overall View of Our CP Model for Key-Recovery

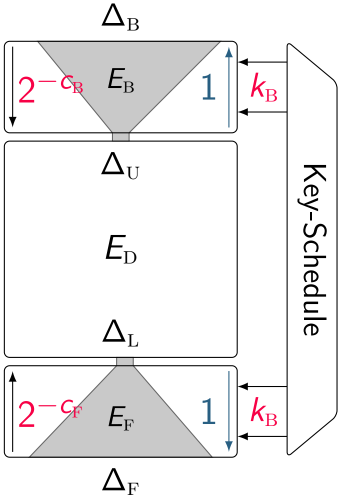
- Model the distinguisher for E_{D} $(\Delta_{\mathrm{U}}, \Delta_{\mathrm{F}})$
- Model the filters in E_{B}, and E_{F} $(c_{\mathrm{B}}, c_{\mathrm{F}}, \Delta_{\mathrm{B}}, \Delta_{\mathrm{F}})$
- Model the guess-and-determine in E_{B}, and E_{F}
- Model the key bridging
  - Encode $|k_{\mathrm{B}} \cup k_{\mathrm{F}}|$
- Model the complexity formulas



Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

Overall View of Our CP Model for Key-Recovery

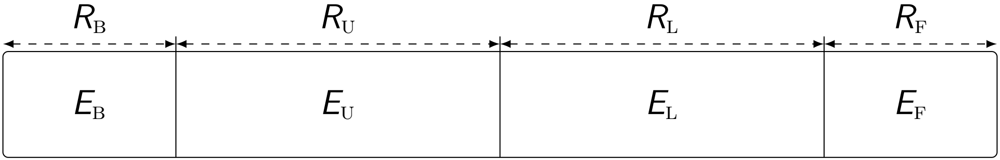
- Model the distinguisher for E_{D} $(\Delta_{\mathrm{U}}, \Delta_{\mathrm{F}})$
- Model the filters in E_{B}, and E_{F} $(c_{\mathrm{B}}, c_{\mathrm{F}}, \Delta_{\mathrm{B}}, \Delta_{\mathrm{F}})$
- Model the guess-and-determine in E_{B}, and E_{F}
- Model the key bridging
  - Encode $|k_{\mathrm{B}} \cup k_{\mathrm{F}}|$
- Model the complexity formulas



Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

Usage of Our Tool

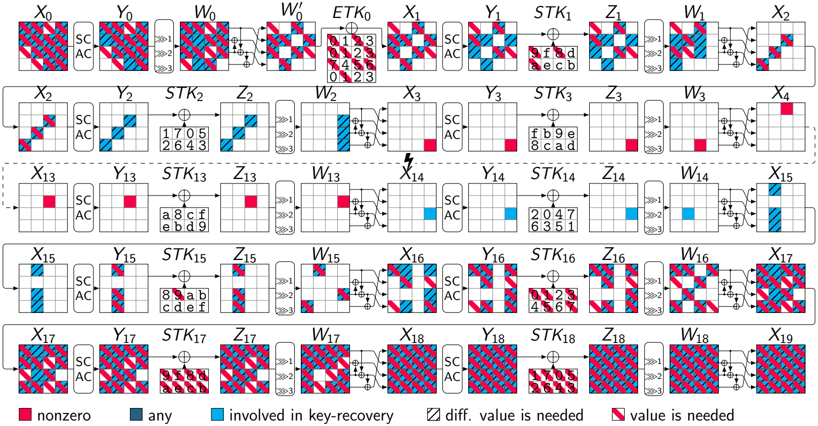
```
python3 attack.py -RB 4 -RU 10 -RL 6 -RF 7
```



- We use MiniZinc [Net+07] to create our CP models
- We use Gurobi [Gur22] and OrTools [PF] as the CP solvers
- Our tool can find the results in a few seconds running on a regular laptop

Example: 19-round ID Attack on SKINNY-n-$2n$

- $|k_{\mathrm{B}} \cup k_{\mathrm{F}}| = 26 \cdot c$
- $c_{\mathrm{B}} = 6 \cdot c$
- $c_{\mathrm{F}} = 15 \cdot c$
- $\Delta_{\mathrm{B}} = 7 \cdot c$
- $\Delta_{\mathrm{F}} = 16 \cdot c$
- $c \in \{4, 8\}$



Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder

Part of Our Improved Results for SKINNY

Cipher	#R	Time	Data	Mem.	Attack	Setting / Model	Ref.
SKINNY-64-192	23	$2^{155.60}$	$2^{73.20}$	2^{138}	Int	180,SK / CP,CT	[Ank+19]
	26	2^{172}	2^{61}	2^{172}	Int	180,SK / CP,CT	This paper
SKINNY-128-384	27	2^{378}	$2^{126.03}$	2^{368}	ID	RTK / CP	[LGS17]
	27	$2^{362.61}$	$2^{124.99}$	2^{344}	ID	RTK / CP	This paper
SKINNY-64-128	18	2^{126}	$2^{62.68}$	2^{64}	ZC	STK / KP	[SMB18]
	19	$2^{119.12}$	$2^{62.89}$	2^{49}	ZC	STK / KP	This paper
	20	$2^{97.50}$	$2^{68.40}$	2^{82}	Int	120,SK / CP,CT	[Ank+19]
	22	2^{110}	$2^{57.58}$	2^{108}	Int	120,SK / CP,CT	This paper
SKINNY-128-256	19	$2^{241.80}$	2^{123}	2^{221}	ID	STK / CP	[YQC17]
	19	$2^{219.23}$	$2^{117.86}$	2^{208}	ID	STK / CP	This paper
SKINNY-64-64	14	2^{62}	$2^{62.58}$	2^{64}	ZC	STK / KP	[SMB18]
	16	$2^{62.71}$	$2^{61.35}$	$2^{37.80}$	ZC	STK / KP	This paper

Detecting Flaws in The Previous Attacks Using our Automatic Tools

Invalid Attacks on SKINNY

Cipher	Attack	#R	Setting / Model	Ref.	Flaw
SKINNY-n-n	ID	18	STK / CP	[TAY17]	KR
SKINNY-n-$2n$	ID	20	STK / CP	[TAY17]	KR
	ZC/Int †	22	SK / CP, CT	[ZCW22]	Dist
SKINNY-n-$3n$	ID	22	STK / CP	[TAY17]	KR
	ZC/Int †	26	SK / CP, CT	[ZCW22]	Dist

Conclusion

Contributions and Future Works

- Contributions
  - Introduced efficient unified model for finding full ID/ZC/integral attacks
  - Found improved attacks for SKINNY, CRAFT, SKINNYee, and SKINNYe-v2
- Future works
  - Applying our method to other ciphers, e.g., AES, MANTIS, QARMA, etc
  - Creating the bit-oriented version of our method
  - Applying our approach in other CP models, e.g., division property
  - Improving the key-recovery part of our CP models for ZC and integral attacks

: https://github.com/hadipourh/zero

: https://ia.cr/2022/1147

Bibliography I

[Ank+19] Ralph Ankele et al. **Zero-Correlation Attacks on Tweakable Block Ciphers with Linear Tweakey Expansion**. *IACR Transactions on Symmetric Cryptology* 2019.1 (Mar. 2019), pp. 192–235. DOI: 10.13154/tosc.v2019.i1.192-235.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. **Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials**. EUROCRYPT 1999. Vol. 1592. LNCS. Springer, 1999, pp. 12–23. DOI: 10.1007/3-540-48910-X_2.

[Bei+16] Christof Beierle et al. **The SKINNY family of block ciphers and its low-latency variant MANTIS**. CRYPTO 2016. Springer. 2016, pp. 123–153. DOI: 10.1007/978-3-662-53008-5_5.

Bibliography II

[BNS14] Christina Boura, Maria Naya-Plasencia, and Valentin Suder. **Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon**. International Conference on the Theory and Application of Cryptology and Information Security. Springer. 2014, pp. 179–199. DOI: 10.1007/978-3-662-45611-8_10.

[Bog+12] Andrey Bogdanov et al. **Integral and Multidimensional Linear Distinguishers with Correlation Zero**. ASIACRYPT 2012. Vol. 7658. LNCS. Springer, 2012, pp. 244–261. DOI: 10.1007/978-3-642-34961-4_16.

[Bou+18] Christina Boura et al. **Making the impossible possible**. *Journal of Cryptology* 31.1 (2018), pp. 101–133. DOI: 10.1007/s00145-016-9251-7.

Bibliography III

[BR14] Andrey Bogdanov and Vincent Rijmen. **Linear hulls with correlation zero and linear cryptanalysis of block ciphers**. *Des. Codes Cryptogr.* 70.3 (2014), pp. 369–383. DOI: 10.1007/s10623-012-9697-z.

[Cui+16] Tingting Cui et al. **New Automatic Search Tool for Impossible Differentials and Zero-Correlation Linear Approximations**. IACR Cryptology ePrint Archive, Report 2016/689. 2016. URL: https://eprint.iacr.org/2016/689.

[DF16] Patrick Derbez and Pierre-Alain Fouque. **Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks**. CRYPTO 2016. Vol. 9815. LNCS. Springer, 2016, pp. 157–184.

[Gur22] Gurobi Optimization, LLC. **Gurobi Optimizer Reference Manual**. 2022. URL: https://www.gurobi.com.

Bibliography IV

[Knu98] Lars Knudsen. **DEAL-a 128-bit block cipher**. *complexity* 258.2 (1998), p. 216.

[LGS17] Guozhen Liu, Mohona Ghosh, and Ling Song. **Security Analysis of SKINNY under Related-Tweakey Settings**. *IACR Trans. Symmetric Cryptol.* 2017.3 (2017), pp. 37–72. DOI: 10.13154/tosc.v2017.i3.37-72.

[Net+07] Nicholas Nethercote et al. **MiniZinc: Towards a Standard CP Modelling Language**. CP 2007. Vol. 4741. LNCS. Springer, 2007, pp. 529–543.

[PF] Laurent Perron and Vincent Furnon. **OR-Tools**. Version 9.3. Google. URL: https://developers.google.com/optimization/.

[SMB18] Sadegh Sadeghi, Tahereh Mohammadi, and Nasour Bagheri. **Cryptanalysis of Reduced round SKINNY Block Cipher**. *IACR Trans. Symmetric Cryptol.* 2018.3 (2018), pp. 124–162. DOI: 10.13154/tosc.v2018.i3.124-162.

Bibliography V

[ST17] Yu Sasaki and Yosuke Todo. **New Impossible Differential Search Tool from Design and Cryptanalysis Aspects**. EUROCRYPT 2017. Cham: Springer International Publishing, 2017, pp. 185–215. DOI: 10.1007/978-3-319-56617-7_7.

[Sun+15] Bing Sun et al. **Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis**. CRYPTO 2015. Vol. 9215. LNCS. Springer, 2015, pp. 95–115. DOI: 10.1007/978-3-662-47989-6_5.

[Sun+17] Siwei Sun et al. **Analysis of AES, SKINNY, and Others with Constraint Programming**. *IACR Transactions on Symmetric Cryptology* 2017.1 (Mar. 2017), pp. 281–306. DOI: 10.13154/tosc.v2017.i1.281-306.

Bibliography VI

[Sun+20] Ling Sun et al. **On the Usage of Deterministic (Related-Key) Truncated Differentials and Multidimensional Linear Approximations for SPN Ciphers**. *IACR Transactions on Symmetric Cryptology* 2020.3 (Sept. 2020), pp. 262–287. DOI: 10.13154/tosc.v2020.i3.262-287.

[TAY17] Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef. **Impossible Differential Cryptanalysis of Reduced-Round SKINNY**. AFRICACRYPT 2017. Vol. 10239. LNCS. 2017, pp. 117–134. DOI: 10.1007/978-3-319-57339-7_7.

[Xia+16] Zejun Xiang et al. **Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers**. ASIACRYPT 2016. Vol. 10031. LNCS. 2016, pp. 648–678. DOI: 10.1007/978-3-662-53887-6_24.

Bibliography VII

[YQC17] Dong Yang, Wen-Feng Qi, and Hua-Jin Chen. **Impossible differential attacks on the SKINNY family of block ciphers**. *IET Inf. Secur.* 11.6 (2017), pp. 377–385. DOI: 10.1049/iet-ifs.2016.0488.

[ZCW22] Yi Zhang, Ting Cui, and Congjun Wang. **Zero-correlation linear attack on reduced-round SKINNY**. *Frontiers of Computer Science* 17.174808 (2023) (2022), pp. 377–385. DOI: 10.1007/s11704-022-2206-2.

Zero-Correlation Attack and Its Relation to Integral Attack

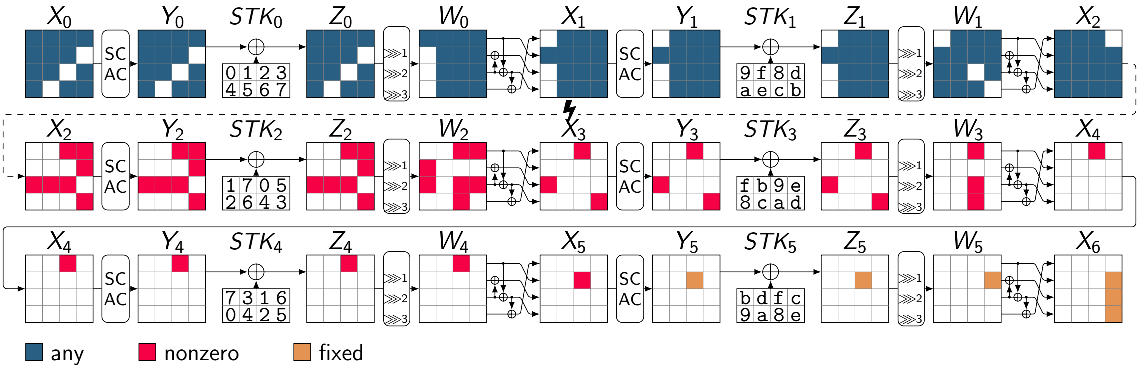
- ZC is the dual of ID in the context of linear cryptanalysis [BR14]
- Multidimensional ZC attack (ASIACRYPT 2012 [Bog+12])

Link Between ZC and Integral Attack [Sun+15]

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. Assume A is a subspace of $\mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^n \setminus \{0\}$ such that (α, β) is a ZC approximation for any $\alpha \in A$. Then, for any $\lambda \in \mathbb{F}_2^n$, $\langle \beta, F(x + \lambda) \rangle$ is balanced over the set

$$A^{\perp} = \{x \in \mathbb{F}_2^n \mid \forall\, \alpha \in A : \langle \alpha, x \rangle = 0\}.$$

Example: Conversion of ZC Distinguisher to Integral Distinguisher



- $X_0[7, 10, 13]$ takes all possible values and the remaining cells take a fixed value
- $X_6[7] \oplus X_6[11] \oplus X_6[15]$ is balanced

Hosein Hadipour, Sadegh Sadeghi, Maria Eichlseder