Zero-Correlation Attacks on Tweakable Block Ciphers with Linear Tweakey Expansion

Ralph Ankele[1,4], Christoph Dobraunig[2,3], Jian Guo[4],
Eran Lambooij[5], Gregor Leander[6], Yosuke Todo[7]

[1]Royal Holloway University of London, United Kingdom
[2]Graz University of Technology, Austria
[3]Radboud University Nijmegen, The Netherlands
[4]Nanyang Technological University, Singapore
[5]University of Haifa, Israel
[6]Ruhr-Universitaet Bochum, Germany
[7]NTT Secure Platform Laboratories, Japan

March 26, 2019
FSE 2019, Paris, France

Ralph Ankele has received funding from the European Unions Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 643161

Tweakable Block Ciphers

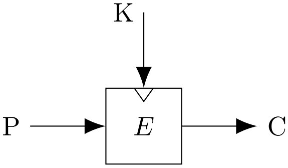


Figure: Regular Block Cipher

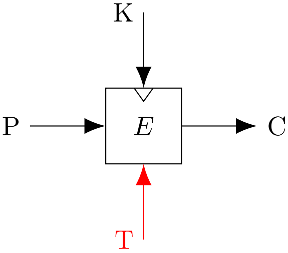


Figure: Tweakable Block Cipher

- Tweak does not have to be secure → public
- Move randomisation from protocol to block cipher level

Tweakable Block Ciphers

- Tweakable block ciphers from modes (i.e. AES-GCM, ...)
- Dedicated Tweakable block ciphers (i.e. Skinny, Mantis, Qarma, Deoxys, ...)
- Tweakey framework [JNP14]

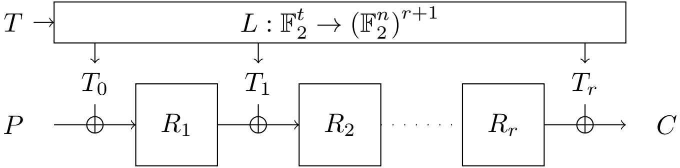


Figure: Key-alternating tweakable block cipher with linear tweak schedule.

Contributions

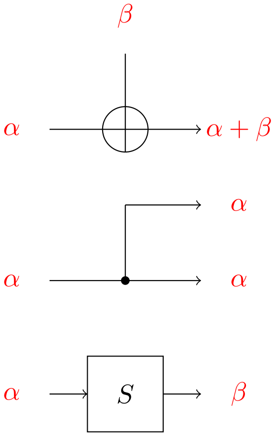
Cipher	Rounds	Attack type	Time	Data	Memory	Ref.
Qarma-64	$4/4^*$	MITM	2^{90}	2^{16}	2^{90}	[LJ18]
Qarma-64	$4/5^*$	MITM	2^{89}	2^{16}	2^{89}	[LJ18]
Qarma-64	$4/6^*$	MITM	$2^{70.1}$	2^{53}	2^{116}	[ZD16]
Qarma-64	$4/6^*$	RT SS	2^{59}	2^{59}	$2^{29.6}$	[LHW19]
Qarma-64	$3/8^*$	ID	$2^{64.4}$	2^{61}	-	[ZDW18]
Qarma-64	$4/7^*$	ID	$2^{120.4}$	2^{61}	2^{116}	[YQC18]
Qarma-64	$4/8^*$	ZC/Integral	$2^{66.2}$	$2^{48.4}$	$2^{53.64}$	This Work
Mantis	$5/5^*$	Diff.	2^{56}	$2^{9.3}$	-	[Bey18]
Mantis	$6/6^*$	Diff.	2^{38}	2^{28}	-	[DEKM16]
Mantis	$4/8^*$	ZC/Integral	$2^{66.2}$	$2^{48.4}$	$2^{53.64}$	This Work
Mantis	$7/7^*$	Diff.	$2^{53.94}$	$2^{53.94}$	-	[EK17]
Skinny-64/128	18	ZC	2^{126}	$2^{62.68}$	2^{64}	[SMB18]
Skinny-64/128	19	ID	$2^{119.8}$	2^{62}	2^{110}	[YQC17]
Skinny-64/128	20	ID	$2^{121.08}$	$2^{47.69}$	$2^{47.69}$	[TAY17]
Skinny-64/128	20	ZC/Integral	$2^{97.5}$	$2^{68.4\dagger}$	2^{82}	This Work
Skinny-64/128	23	ID	2^{124}	$2^{62.47}$	$2^{77.47}$	[SMB18]
Skinny-64/128	23	ID	$2^{125.9}$	$2^{62.5}$	$2^{124.0}$	[LGS17]
Skinny-64/128	23	ID	2^{79}	$2^{71.4\dagger}$	$2^{64.0}$	[ABC+17]
Skinny-64/192	21	ID	$2^{180.5}$	2^{62}	2^{170}	[YQC17]
Skinny-64/192	22	ID	$2^{183.97}$	$2^{47.84}$	$2^{74.84}$	[TAY17]
Skinny-64/192	23	ZC/Integral	$2^{155.6}$	$2^{73.2\dagger}$	2^{138}	This Work
Skinny-64/192	27	Rectangle	$2^{165.5}$	$2^{63.5}$	2^{80}	[LGS17]

Overview

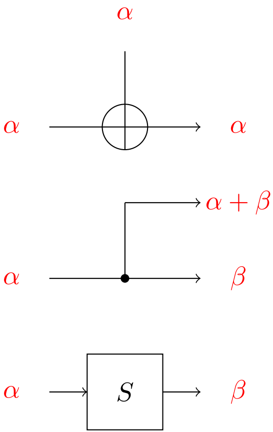
1. Preliminaries
2. Zero-Correlation Attacks on TBC
3. Application to Qarma
4. Application to Mantis
5. Application to Skinny

Propagation of Differences/Linear Masks

Differences:



Linear Masks:



Security Evaluation of Tweakable BC

Differential Cryptanalysis

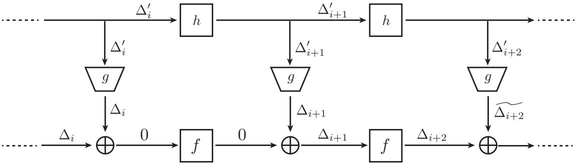


Figure: Differential model.

Linear Cryptanalysis

- Tweak does not introduce new linear characteristics [KLW17]
- Tweak adds additional restrictions in zero-correlation attacks

Zero-Correlation Linear Cryptanalysis

- Introduced by Bogdanov and Rijmen [BR11]
- For given masks α, β it exploits a correlation of exactly zero
- Requires huge data complexity

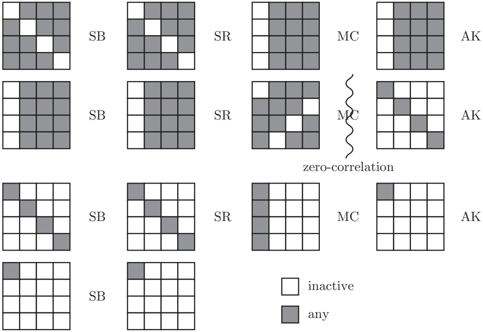


Figure: Zero-correlation linear hull on 4-round AES.

Overview

1. Preliminaries

2. Zero-Correlation Attacks on TBC

3. Application to Qarma

4. Application to Mantis

5. Application to Skinny

Zero-Correlation Attacks on TBC

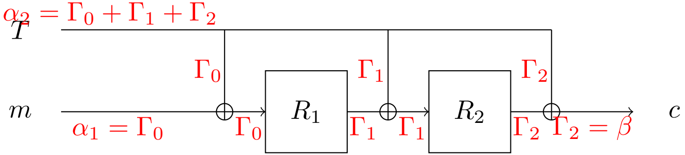
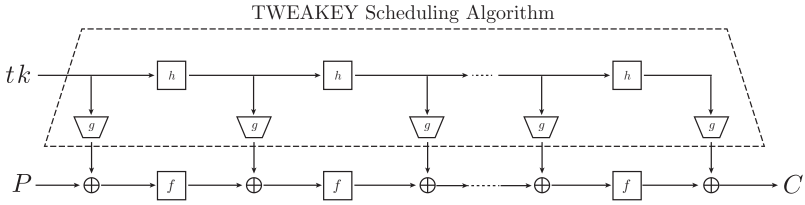


Figure: Propagation of masks in a simple two round tweakable block cipher.

- Tweak adds additional restrictions in zero-correlation attacks
- Link zero-correlation attacks to integral attacks to reduce data complexity [SLR+15].

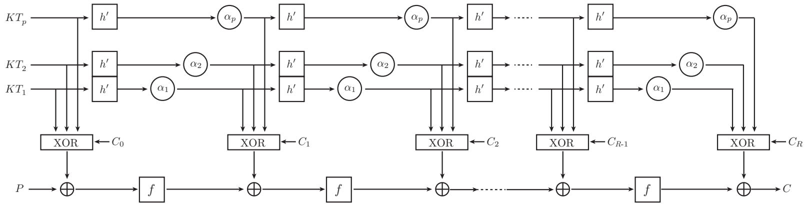
Tweakey Framework [JNP14]

Rationale: tweak and key should be treated the same way → **tweakey**



- Generalizes the class of key-alternating ciphers
- Framework for designing tweakable block ciphers

STK Construction (Superposition-Tweakey)

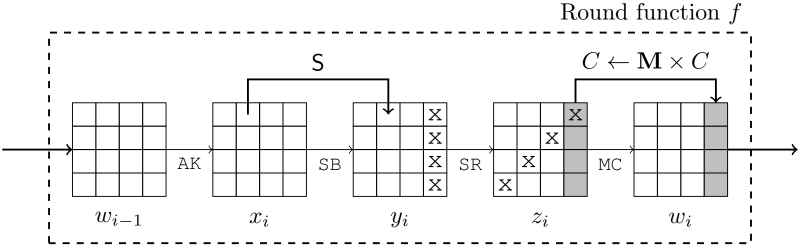


From Tweakey to the STK construction:

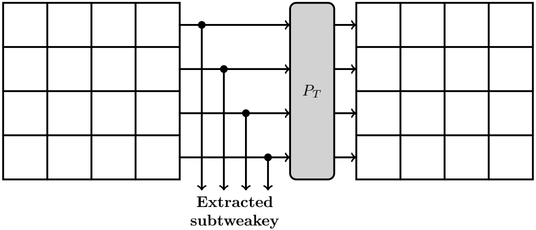
- State-update function h is a permutation that is applied to each tweakey word
- Subtweakey extraction function g XORs all tweakey words together
    - Adds round-dependent constants against slide attacks
    - Reduces many tweakey words to one
- Reduces implementation overhead
- Simplifies security analysis

Toy Cipher

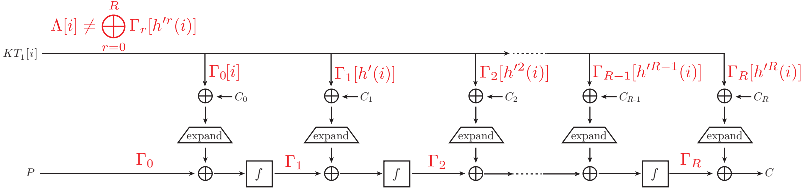
Round function: Same as AES



Tweak schedule: Permutation of SKINNY



Zero-Corr. Attacks on STK with TK-1



- ▶ For a fixed Γ_0, Γ_R

$$\Lambda[i] = \bigoplus_{r=0}^{R} \Gamma_r[h'^r(i)] \;|\; \forall\; (\Gamma_0[i], \Gamma_1[h'(i)], \ldots, \Gamma_R[h'^R(i)])$$

- ▶ Γ sequence: Forward and backward propagation with probability 1 of Γ_0, Γ_r
- ▶ Zero-correlation when $\Lambda[i] \neq \Gamma$ sequence, where Γ sequence has at most 1 linearly active value

ZC Linear Hull on STK with TK-1

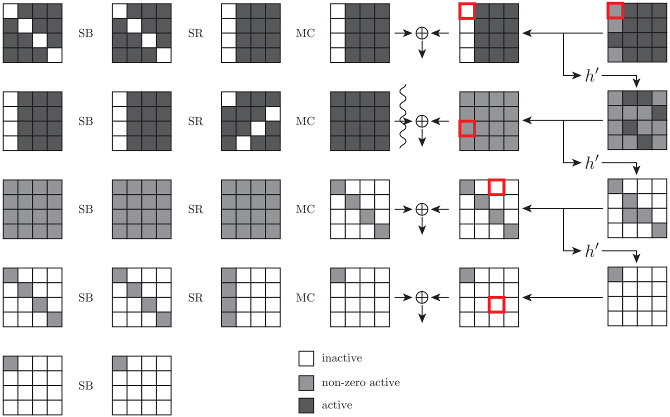
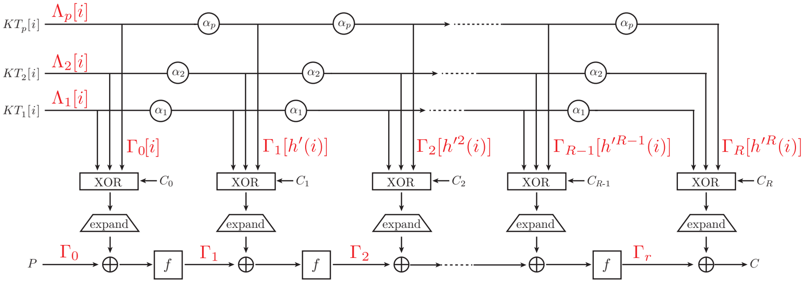


Figure: 5-round zero-correlation linear hull on Toy-TBC.

Zero-Corr. Attacks on STK with TK-p



- For a fixed Γ_0, Γ_R

$$\begin{pmatrix} \Lambda_1[i] \\ \Lambda_2[i] \\ \vdots \\ \Lambda_p[i] \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1^T & (\alpha_1^T)^2 & \cdots & (\alpha_1^T)^R \\ 1 & \alpha_2^T & (\alpha_2^T)^2 & \cdots & (\alpha_2^T)^R \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_p^T & (\alpha_p^T)^2 & \cdots & (\alpha_p^T)^R \end{pmatrix} \times \begin{pmatrix} \Gamma_0[i] \\ \Gamma_1[h'(i)] \\ \Gamma_2[h'^2(i)] \\ \vdots \\ \Gamma_R[h'^R(i)] \end{pmatrix}$$

- Zero-correlation when $\Lambda[i] \neq \Gamma$ sequence, where Γ sequence has at most p linearly active value

ZC Linear Hull on STK with TK-2

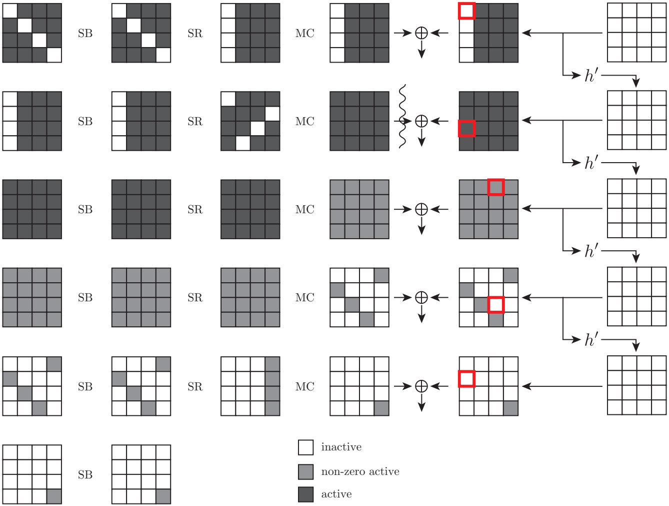
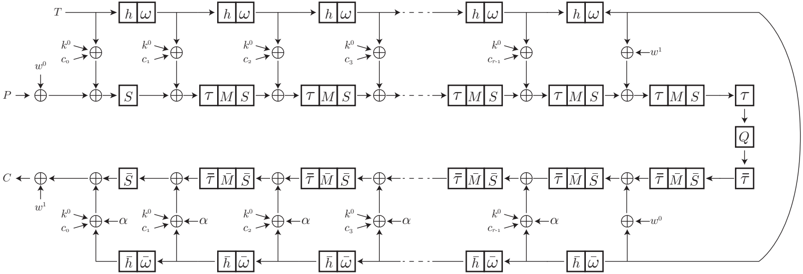


Figure: 6-round zero-correlation linear hull on Toy-TBC.

Overview

1. Preliminaries
2. Zero-Correlation Attacks on TBC
3. Application to Qarma
4. Application to Mantis
5. Application to Skinny

QARMA [Ava17]



- Tweakable block cipher based on the TWEAKEY framework
- Reflection-like cipher

QARMA

Round function:

- Lightweight involutory 4-bit S-box σ_1:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\sigma_1(x)$	a	d	e	6	f	7	3	5	9	8	0	c	b	1	2	4

- Cell permutation of MIDORI τ:

$$\tau = [0, 11, 6, 13, 10, 1, 12, 7, 5, 14, 3, 8, 15, 4, 9, 2]$$

- MixColumns

$$M = circ(0, \rho, \rho^2, \rho) = \begin{pmatrix} 0 & \rho & \rho^2 & \rho \\ \rho & 0 & \rho & \rho^2 \\ \rho^2 & \rho & 0 & \rho \\ \rho & \rho^2 & \rho & 0 \end{pmatrix}$$

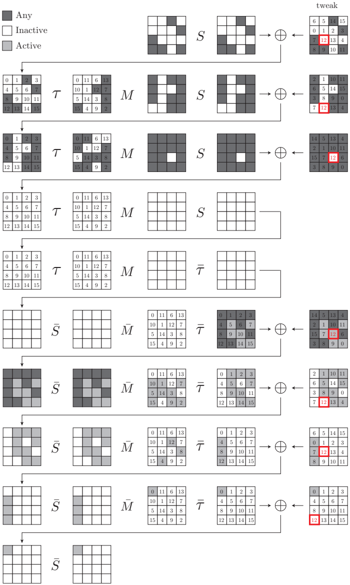
Tweak schedule:

- Permutation h:

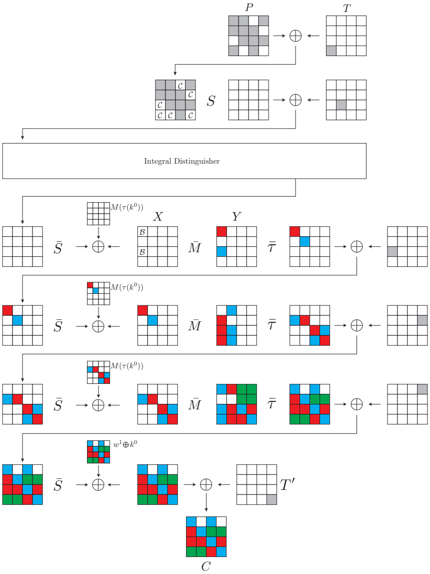
$$h = [6, 5, 14, 15, 0, 1, 2, 3, 7, 12, 13, 4, 8, 9, 10, 11]$$

- Bit-based LFSR ω

Distinguishers



KEY-RECOVERY



12-round Key-recovery attack

- Prepend 1 round to distinguisher and append three rounds
- X_0 and X_8 are balanced at the same time

$$\begin{aligned}\bigoplus(X_0 + X_8) &= \bigoplus(\rho Y_4 + \rho^2 Y_8 + \rho Y_{12}) \oplus (\rho^2 Y_0 + \rho Y_4 + \rho Y_{12}) \\ &= \bigoplus(\rho^2 Y_0 + \rho^2 Y_8) = 0.\end{aligned}$$

- Use Meet-in-the-middle technique for integral attacks [SW13] to evaluate Y_0 and Y_8 independently
- Use FFT key-recovery technique [TA14]
    - Time complexity: Recover 56-bit of $w^1 \oplus k^0$, and 28-bit of $M(\tau(k^0)) \approx 2^{66.2}$
    - Data complexity: 21 structures $\times\ 2^{44} \approx 2^{48.4}$
    - Memory complexity: $2^{53.7}$

Overview

1. Preliminaries

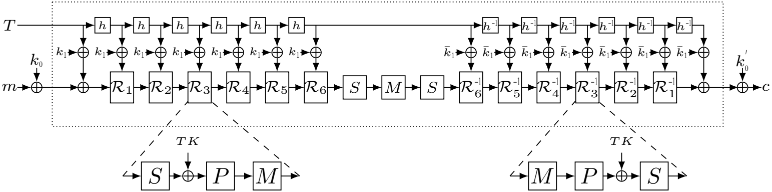
2. Zero-Correlation Attacks on TBC

3. Application to Qarma

4. Application to Mantis

5. Application to Skinny

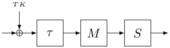
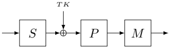
Mantis [BJK$^+$16]



- Tweakable block cipher based on the Tweakey framework
- Reflection cipher

Mantis [BJK$^+$16]

Table: Comparison between Mantis and Qarma.

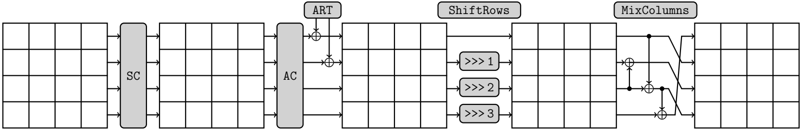
	Qarma	Mantis
Round function		
S-box	$\sigma_1 = [a, d, e, 6, f, 7, 3, 5, 9, 8, 0, c, b, 1, 2, 4]$	$\mathrm{Sb}_0 = [c, a, d, 3, e, b, f, 7, 8, 9, 1, 5, 0, 2, 4, 6]$
	$\tau = [0, b, 6, d, a, 1, c, 7, 5, e, 3, 8, f, 4, 9, 2]$	$P = [0, b, 6, d, a, 1, c, 7, 5, e, 3, 8, f, 4, 9, 2]$
Linear Layer	$M = \begin{pmatrix} 0 & \rho & \rho^2 & \rho \\ \rho & 0 & \rho & \rho^2 \\ \rho^2 & \rho & 0 & \rho \\ \rho & \rho^2 & \rho & 0 \end{pmatrix}$	$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

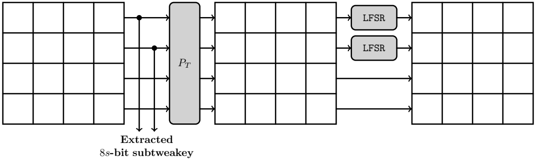
- Same attack as for Qarma is also valid of Mantis

Overview

1. Preliminaries
2. Zero-Correlation Attacks on TBC
3. Application to Qarma
4. Application to Mantis
5. Application to Skinny

Skinny [BJK$^+$16]





- Tweakable block cipher based on the Tweakey framework

SKINNY

Round function:

- Lightweight 4-bit S-box:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	c	6	9	0	1	a	2	b	3	8	5	d	4	e	7	f

- AES-like ShiftRows (to the right, instead of left)
- MixColumns (binary matrix)

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Tweakey schedule:

- Permutation h:

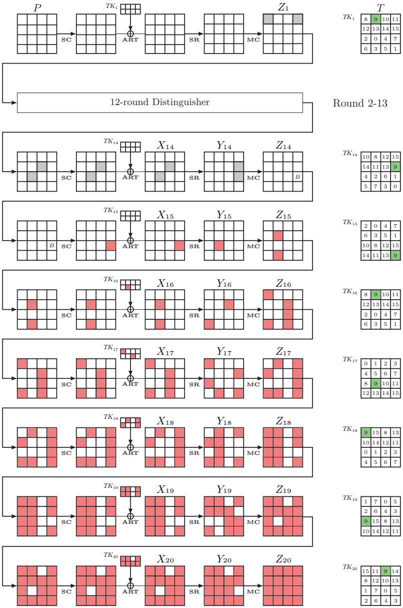
$$P_T = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$$

- Bit-based LFSR (topmost 2 rows, only for TK2, TK3)

Distinguishers

- We can attack 20 rounds of Skinny-64/128 in the TK2 setting
  - Skinny-64/128 uses a 13-round distinguisher with a complexity of 2^{56} plaintexts and 2^{8} related tweakeys
- We can attack 23 rounds of Skinny-64/192 in the TK3 setting
  - Skinny-64/192 uses a 15-round distinguisher with a complexity of 2^{56} plaintexts and 2^{12} related tweakeys

Key-recovery Skinny-64/128



T

TK_1

8	9	10	11
12	13	14	15
2	0	4	7
6	3	5	1

TK_{14}

10	8	12	15
14	11	13	9
4	2	6	1
5	7	3	0

TK_{15}

2	0	4	7
6	3	5	1
10	8	12	15
14	11	13	9

TK_{16}

8	9	10	11
12	13	14	15
2	0	4	7
6	3	5	1

TK_{17}

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

TK_{18}

9	15	8	13
10	14	12	11
0	1	2	3
4	5	6	7

TK_{19}

1	7	0	5
2	6	4	3
9	15	8	13
10	14	12	11

TK_{20}

15	11	9	14
8	12	10	13
1	7	0	5
2	6	4	3

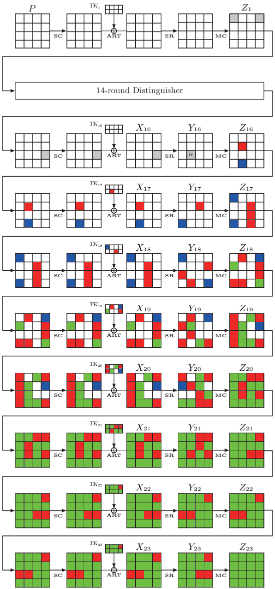
20-round Key-recovery attack

- Prepend 1 round to distinguisher and append six rounds
- $Z_{14}[11]$ is balanced

$$\bigoplus Z_{14}[11] = \bigoplus (Y_{14}[7] \oplus Y_{14}[11]) = 0$$

- Use Partial-Sum technique [FKL$^+$01] as just the two topmost rows of the tweakey are added to the state, which makes the FFT key-recovery technique less efficient [TA14]
  - Time complexity: $\approx 2^{97.5}$
  - Data complexity: 20 structures $\times\ 2^{64} \approx 2^{68.4}$
  - Memory complexity: 2^{82}

Key-recovery Skinny-64/192



T

TK_1

8	9	10	11
12	13	14	15
2	0	4	7
6	3	5	1

Round 2-15

TK_{16}

2	0	4	7
6	3	5	1
10	8	12	15
14	11	13	9

TK_{17}

8	9	10	11
12	13	14	15
2	0	4	7
6	3	5	1

TK_{18}

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

TK_{19}

9	15	8	13
10	14	12	11
0	1	2	3
4	5	6	7

TK_{20}

1	7	0	5
2	6	4	3
9	15	8	13
10	14	12	11

TK_{21}

15	11	9	14
8	12	10	13
1	7	0	5
2	6	4	3

TK_{22}

7	3	1	6
0	4	2	5
15	11	9	14
8	12	10	13

TK_{23}

11	13	15	12
9	10	8	14
7	3	1	6
0	4	2	5

23-round Key-recovery attack

- Prepend 1 round to distinguisher and append eight rounds
- $Z_{16}[5]$ and $Z_{16}[13]$ are balanced at the same time

$$\bigoplus Z_{16}[5] + Z_{16}[13] = \bigoplus Y_{16}[9] = 0$$

- Use Meet-in-the-middle technique for integral attacks [SW13] to evaluate $Z_{16}[5]$ and $Z_{16}[13]$ independently
- Use Partial-Sum technique [FKL$^+$01] as just the two topmost rows of the tweakey are added to the state, which makes the FFT key-recovery technique less efficient [TA14]
  - Time complexity: $\approx 2^{155.6}$
  - Data complexity: 37 structures $\times\, 2^{68} \approx 2^{73.2}$
  - Memory complexity: 2^{138}

Conclusions

- New attack technique to analyse tweakable block ciphers
- Currently best attacks on Qarma
- Independent of keyed middle rounds
- Further insights into Mantis and Skinny

Questions?

Thank you for your attention!

References I

[ABC$^+$17] Ralph Ankele, Subhadeep Banik, Avik Chakraborti, Eik List, Florian Mendel, Siang Meng Sim, and Gaoli Wang. Related-key impossible-differential attack on reduced-round skinny. In Dieter Gollmann, Atsuko Miyaji, and Hiroaki Kikuchi, editors, *ACNS 17*, volume 10355 of *LNCS*, pages 208–228. Springer, Heidelberg, July 2017.

[Ava17] Roberto Avanzi. The qarma block cipher family. almost mds matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency s-boxes. *IACR Transactions on Symmetric Cryptology*, 2017(1):4–44, Mar. 2017.

[Bey18] Tim Beyne. Block cipher invariants as eigenvectors of correlation matrices. Cryptology ePrint Archive, Report 2018/763, 2018. `https://eprint.iacr.org/2018/763`.

[BJK$^+$16] 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 Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 123–153. Springer, Heidelberg, August 2016.

References II

[BR11] Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Cryptology ePrint Archive, Report 2011/123, 2011. `http://eprint.iacr.org/2011/123`.

[DEKM16] Christoph Dobraunig, Maria Eichlseder, Daniel Kales, and Florian Mendel. Practical key-recovery attack on MANTIS5. *IACR Trans. Symm. Cryptol.*, 2016(2):248–260, 2016. `http://tosc.iacr.org/index.php/ToSC/article/view/573`.

[EK17] Maria Eichlseder and Daniel Kales. Clustering related-tweak characteristics: Application to mantis-6. Cryptology ePrint Archive, Report 2017/1136, 2017. `https://eprint.iacr.org/2017/1136`.

[FKL$^+$01] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 213–230. Springer, Heidelberg, April 2001.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 274–288. Springer, Heidelberg, December 2014.

References III

[KLW17] Thorsten Kranz, Gregor Leander, and Friedrich Wiemer. Linear cryptanalysis: Key schedules and tweakable block ciphers. *IACR Trans. Symm. Cryptol.*, 2017(1):474–505, 2017.

[LGS17] Guozhen Liu, Mohona Ghosh, and Ling Song. Security analysis of SKINNY under related-tweakey settings (long paper). *IACR Trans. Symm. Cryptol.*, 2017(3):37–72, 2017.

[LHW19] Muzhou Li, Kai Hu, and Meiqin Wang. Related-tweak statistical saturation cryptanalysis and its application on qarma. *IACR Transactions on Symmetric Cryptology*, 2019(1):236–263, Mar. 2019.

[LJ18] Rongjia Li and Chenhui Jin. Meet-in-the-middle attacks on reduced-round QARMA-64/128. *Comput. J.*, 61(8):1158–1165, 2018.

[SLR$^+$15] Bing Sun, Zhiqiang Liu, Vincent Rijmen, Ruilin Li, Lei Cheng, Qingju Wang, Hoda AlKhzaimi, and Chao Li. Links among impossible differential, integral and zero correlation linear cryptanalysis. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 95–115. Springer, Heidelberg, August 2015.

[SMB18] Sadegh Sadeghi, Tahereh Mohammadi, and Nasour Bagheri. Cryptanalysis of reduced round SKINNY block cipher. *IACR Trans. Symm. Cryptol.*, 2018(3):124–162, 2018.

References IV

[SW13] Yu Sasaki and Lei Wang. Meet-in-the-middle technique for integral attacks against Feistel ciphers. In Lars R. Knudsen and Huapeng Wu, editors, *SAC 2012*, volume 7707 of *LNCS*, pages 234–251. Springer, Heidelberg, August 2013.

[TA14] Yosuke Todo and Kazumaro Aoki. FFT key recovery for integral attack. In Dimitris Gritzalis, Aggelos Kiayias, and Ioannis G. Askoxylakis, editors, *CANS 14*, volume 8813 of *LNCS*, pages 64–81. Springer, Heidelberg, October 2014.

[TAY17] Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef. Impossible differential cryptanalysis of reduced-round SKINNY. In Marc Joye and Abderrahmane Nitaj, editors, *AFRICACRYPT 17*, volume 10239 of *LNCS*, pages 117–134. Springer, Heidelberg, May 2017.

[YQC17] Dong Yang, Wen-Feng Qi, and Hua-Jin Chen. Impossible differential attacks on the SKINNY family of block ciphers. *IET Information Security*, 11(6):377–385, 2017.

[YQC18] Dong Yang, Wen-Feng Qi, and Hua-Jin Chen. Impossible differential attack on qarma family of block ciphers. Cryptology ePrint Archive, Report 2018/334, 2018. https://eprint.iacr.org/2018/334.

References V

[ZD16] Rui Zong and Xiaoyang Dong. Meet-in-the-middle attack on QARMA block cipher. Cryptology ePrint Archive, Report 2016/1160, 2016. http://eprint.iacr.org/2016/1160.

[ZDW18] Rui Zong, Xiaoyang Dong, and Xiaoyun Wang. Milp-aided related-tweak/key impossible differential attack and its applications to qarma, joltik-bc. Cryptology ePrint Archive, Report 2018/142, 2018. https://eprint.iacr.org/2018/142.