Comprehensive Security Analysis of CRAFT

Hosein Hadipour[1] Sadegh Sadeghi[2] Majid M. Niknam[2]
Ling Song[3] Nasour Bagheri[4]

[1]University of Tehran, Iran

[2]Kharazmi University, Iran

[3]Chinese Academy of Sciences, China

[4]Shahid Rajaee Teacher Training University, Iran

Nov 13, 2020

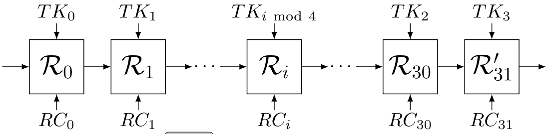
Outline

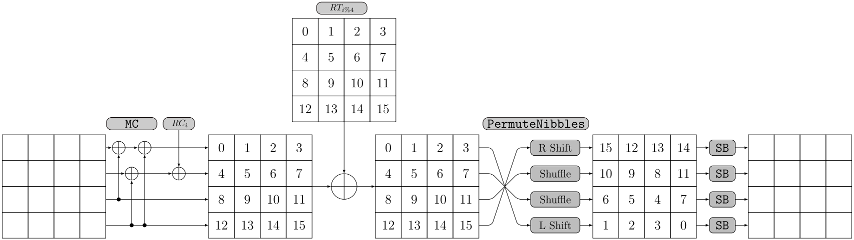
1. CRAFT's Specification
2. Improved Zero-Correlation Distinguishers of CRAFT
3. Improved Integral Distinguishers of CRAFT
4. Improved Single Tweak Differential Distinguishers of CRAFT

Outline

CRAFT

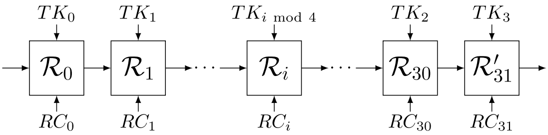
- CRAFT: A light-weight tweakable block cipher, taking efficient protection against DFA[1] in consideration, from design phase [BLMR19]
- Main Parameters: 64-bit block, 128-bit key, 64-bit tweak, 32 rounds





[1]Differential Fault Attack

CRAFT's Tweakey Schedule



Tweakey Schedule

Let $K_0 \| K_1 \in \mathbb{F}_2^{64} \times \mathbb{F}_2^{64}$ are two halves of secret key K, and $T \in \mathbb{F}_2^{64}$ is the master tweak. Then

$$TK_0 = K_0 \oplus T, \qquad TK_1 = K_1 \oplus T,$$
$$TK_2 = K_0 \oplus Q(T), \qquad TK_3 = K_1 \oplus Q(T),$$

where Q is a circular permutation on the position of tweak nibbles

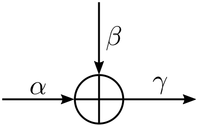
$$Q = [12, 10, 15, 5, 14, 8, 9, 2, 11, 3, 7, 4, 6, 0, 1, 13]$$

Outline

1. CRAFT's Specification
2. Improved Zero-Correlation Distinguishers of CRAFT
3. Improved Integral Distinguishers of CRAFT
4. Improved Single Tweak Differential Distinguishers of CRAFT

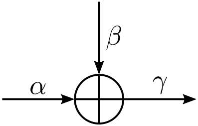
Propagation of Linear Masks

Propagation of Linear Masks

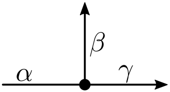


$$\alpha = \beta = \gamma$$

Propagation of Linear Masks

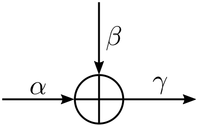


$$\alpha = \beta = \gamma$$

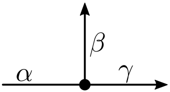


$$\alpha = \beta \oplus \gamma$$

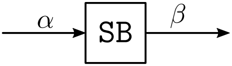
Propagation of Linear Masks



$$\alpha = \beta = \gamma$$



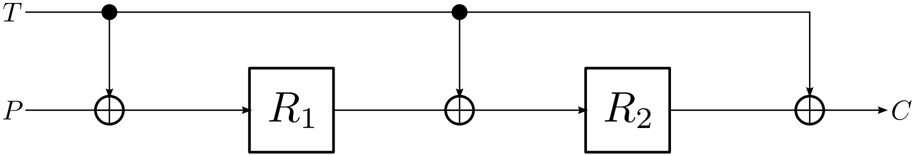
$$\alpha = \beta \oplus \gamma$$



$$\mathtt{LAT}[\alpha][\beta] \neq 0$$

Impact of Tweakey Schedule on ZC Distinguisher

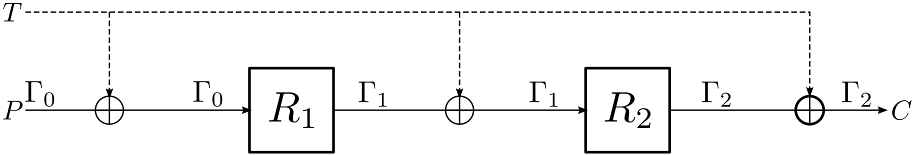
- Consider a toy tweakable block cipher like this[2]:



[2] Has been taken from [ADG+19]

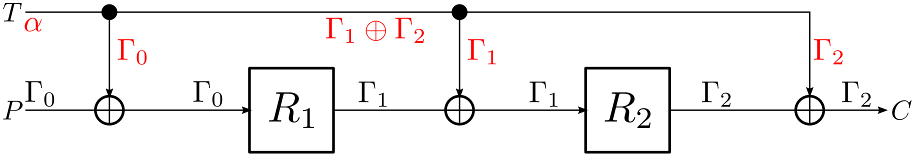
Impact of Tweakey Schedule on ZC Distinguisher

- Propagation of linear masks through the data path:



Impact of Tweakey Schedule on ZC Distinguisher

- Extra (linear) constraint is induced: $\alpha = \Gamma_0 \oplus \Gamma_1 \oplus \Gamma_2$
- Possibility of existing a ZC distinguisher is increased [ADG+19]



Our Strategy to Search for ZC Distinguishers

Tasks Performed by Computer

1. Generate a bit-oriented MILP model describing the propagation of linear masks
2. Solve the generated model for all possible input/output masks with hamming weight of one
3. The correlation of a linear hull with input/output masks for which the MILP model is infeasible, will be zero

Tasks Performed by Human

Using manual approaches, the contradiction inside the discovered ZC distinguishers, is extracted

New ZC Distinguishers for 14 Rounds of CRAFT

Fact

*Linear behavior of **CRAFT** depends on the starting round (RT_0, RT_1, RT_2, RT_3)*

New ZC Distinguishers for 14 Rounds of CRAFT

Fact

Linear behavior of **CRAFT** *depends on the starting round* (RT_0, RT_1, RT_2, RT_3)

New ZC Distinguishers

$$\Gamma T = \texttt{****}\ \texttt{****}\ \texttt{***8}\ \texttt{****}$$

$$\texttt{0000}\ \gamma\texttt{000}\ \texttt{0000}\ \gamma\texttt{000} \xrightarrow{\text{14-round-}RT_0} \texttt{0000}\ \delta\texttt{000}\ \texttt{0000}\ \texttt{0000},$$

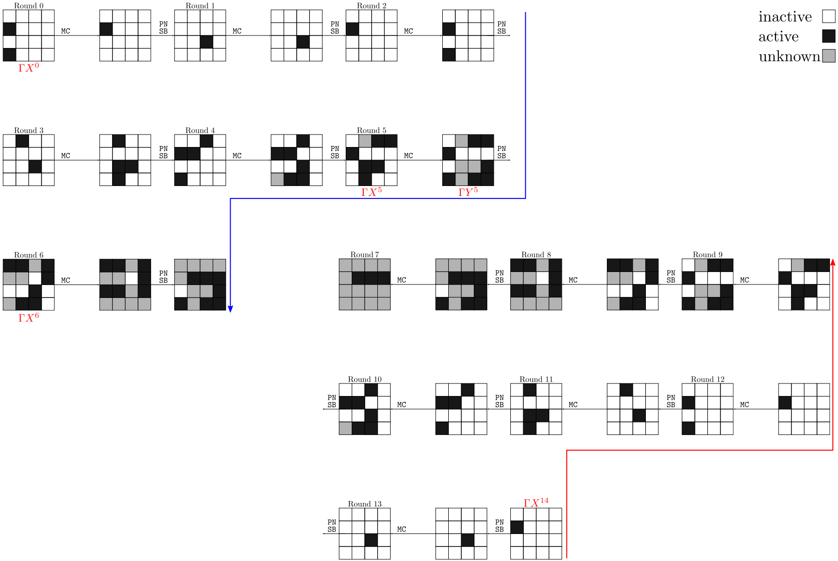
$$\Gamma T = \texttt{****}\ \texttt{****}\ \texttt{***0}\ \texttt{****}$$

$$\texttt{0000}\ \gamma\texttt{000}\ \texttt{0000}\ \texttt{0000} \xrightarrow{\text{14-round-}RT_2} \texttt{0000}\ \texttt{0}\delta\texttt{00}\ \texttt{0000}\ \texttt{0000},$$

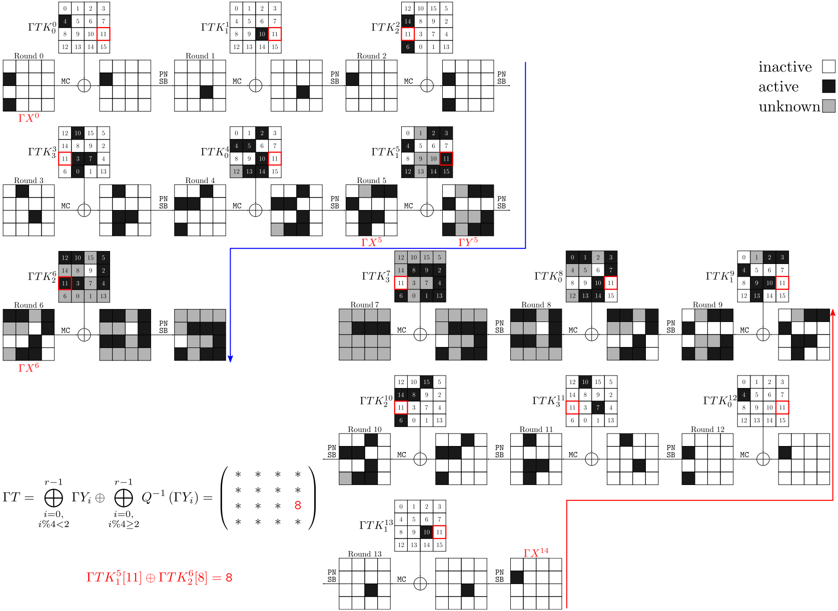
$$\texttt{0000}\ \texttt{0}\gamma\texttt{00}\ \texttt{0000}\ \texttt{0000} \xrightarrow{\text{14-round-}RT_3} \texttt{0000}\ \delta\texttt{000}\ \texttt{0000}\ \texttt{0000},$$

where $*$ depicts an arbitrary value in $\mathbb{F}_2^4$, and $\gamma, \delta \in \mathbb{F}_2^4 \setminus \{0\}$.

Proof of 14-round ZC disntinguisher in case RT_0



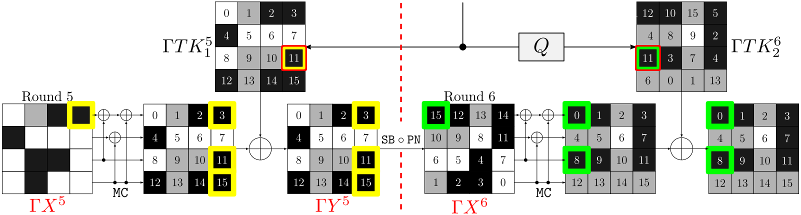
Proof of 14-round ZC disntinguisher in case RT_0



$$\Gamma T = \bigoplus_{\substack{i=0,\\ i\%4<2}}^{r-1} \Gamma Y_i \oplus \bigoplus_{\substack{i=0,\\ i\%4\geq 2}}^{r-1} Q^{-1}(\Gamma Y_i) = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & 8 \\ * & * & * & * \end{pmatrix}$$

$\Gamma TK_1^5[11] \oplus \Gamma TK_2^6[8] = 8$

Proof of 14-round ZC disntinguisher in case RT_0



According to the tweakey schedule, and MC in rounds 5, and 6

$$\Gamma TK_1^5[11] \oplus \Gamma TK_2^6[8] = 8 \xRightarrow[\Gamma Y^5[11]=\Gamma TK_1^5[11]]{\Gamma X^6[0]=\Gamma TK_2^6[8]} \Gamma Y^5[11] \oplus \Gamma X^6[0] = 8$$

According to the MC, PN, and SB in round 5

$$\Gamma Y^5[11] = \Gamma Y^5[15] \Rightarrow \Gamma X^6[0] \in \mathtt{LAT}[\Gamma Y^5[11]]$$

Contradiction: $\exists\ (x, y) \in \mathbb{F}_2^4 \times \mathbb{F}_2^4\ s.t.\ (\mathtt{LAT}[x][y] \neq 0) \wedge (x \oplus y = 8)$

Outline

Link Between ZC and Integral Distinguishers

Theorem

[BLNW12] Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be a function, and* A *be a subspace of* $\mathbb{F}_2^n$ *and* $\beta \in \mathbb{F}_2^n \setminus \{0\}$. *Suppose that* (α, β) *is a zero-correlation linear approximation for any* $\alpha \in A$, *then for any* $\lambda \in \mathbb{F}_2^n$, $\langle \beta, F(x + \lambda) \rangle$ *is balanced on the following set*

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

Theorem

[BLNW12] A nontrivial zero-correlation linear hull of a block cipher always implies the existence of an integral distinguisher.

New Integral Distinguishers for CRAFT

- Only one nibble of tweak is involved in our ZC distnguishers

New Integral Distinguishers for CRAFT

- Only one nibble of tweak is involved in our ZC distnguishers
- Attacker can choose an arbitrary fixed value for those tweak nibbles that are not involved in the distinguisher

New Integral Distinguishers for CRAFT

- Only one nibble of tweak is involved in our ZC distnguishers
- Attacker can choose an arbitrary fixed value for those tweak nibbles that are not involved in the distinguisher
- The domain space of the corresponding integral distinguishers is 68, instead of 128

New Integral Distinguishers for CRAFT

- Only one nibble of tweak is involved in our ZC distnguishers
- Attacker can choose an arbitrary fixed value for those tweak nibbles that are not involved in the distinguisher
- The domain space of the corresponding integral distinguishers is 68, instead of 128
- The required data for the corresponding integral distinguishers must be taken form $A^{\perp}$

New Integral Distinguishers for CRAFT

- Only one nibble of tweak is involved in our ZC distnguishers
- Attacker can choose an arbitrary fixed value for those tweak nibbles that are not involved in the distinguisher
- The domain space of the corresponding integral distinguishers is 68, instead of 128
- The required data for the corresponding integral distinguishers must be taken form $A^{\perp}$
- The data complexity of the corresponding integral distinguisher equals to $2^{\dim(A^{\perp})} = 2^{68-\dim(A)}$

Case	$\dim(A)$	$\dim(A^{\perp})$	data complexity	$\sharp$ rounds
RT_0	1	67	$2^{67} = 2^4 \times 2^{63}$	14
RT_2	4	64	$2^{64} = 2^4 \times 2^{60}$	14
RT_3	4	64	$2^{64} = 2^4 \times 2^{60}$	14

Outline

Our Strategy to Find The Best Differential Trails

1. Using a word-oriented MILP/SAT model, find an optimum truncated differential characteristic

Our Strategy to Find The Best Differential Trails

1. Using a word-oriented MILP/SAT model, find an optimum truncated differential characteristic

2. Using a bit-oriented MILP/SAT model, find an actual differential characteristic satisfying the discovered active cell pattern if it exists

Our Strategy to Find The Best Differential Trails

1. Using a word-oriented MILP/SAT model, find an optimum truncated differential characteristic

2. Using a bit-oriented MILP/SAT model, find an actual differential characteristic satisfying the discovered active cell pattern if it exists

3. If there is not an actual differential characteristic, repeat the process with another truncated differential characteristic

Evaluating the Differential Effect

We use CryptoSMT [Ste]:

1. Encode the problem into a SAT problem in CNF form
2. Fix the input and output differences
3. Ask a SAT solver[2] to find differential trail x if it exists
4. Add a new condition to exclude x
5. Ask the solver to find a new differential trail x if it exists
6. Repeat steps 4 and 5 until the solver returns UNSAT
7. Add the probability of all differential trails together

[2] CryptoMiniSat

Optimizing Sbox-Encoding in CryptoSMT

From DDT to CNF

DDT of Sbox is encoded using the minimized CNF representation of the following Boolean function:

$$
\begin{aligned}
f(x,y,p) &= 0 && if \;\; \Pr\{x \to y\} = 0,\\
f(x,y,p) &= \begin{cases} 1 & p = (1,1,1) \\ 0 & o.w \end{cases} && if \;\; \Pr\{x \to y\} = 2^{-3},\\
f(x,y,p) &= \begin{cases} 1 & p = (0,1,1) \\ 0 & o.w \end{cases} && if \;\; \Pr\{x \to y\} = 2^{-2},\\
f(x,y,p) &= \begin{cases} 1 & p = (0,0,0) \\ 0 & o.w \end{cases} && if \;\; \Pr\{x \to y\} = 1
\end{aligned},
$$

where $x, y \in \mathbb{F}_2^4$ are the input/output differences of the Sbox, and $p = (p_0, p_1, p_2)$, such that $\sum_{i=0}^{2} p_i = -\log_2(\Pr\{x \to y\})$ [SWW18].

The minimized CNF can be obtained via QM [Qui52] and Espresso [BHMSV84]

Achievements By Our Simple Strategy

- We found an optimum differential trail covering 10 rounds of `CRAFT` with the following input/output differences

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{10-round;} \quad \Pr \geq 2^{-50.25}} \texttt{0A00 0000 0000 00AA}$$

Achievements By Our Simple Strategy

- We found an optimum differential trail covering 10 rounds of `CRAFT` with the following input/output differences

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{10-round;} \quad \Pr \geq 2^{-50.25}} \texttt{0A00 0000 0000 00AA}$$

- The best ST differential distinguisher provided by designers:

$$\texttt{A0AA 00AA 0000 00AA} \xrightarrow{\text{10-round;} \quad \Pr \geq 2^{-62.61}} \texttt{A000 0000 0000 00AA}$$

Achievements By Our Simple Strategy

- We found an optimum differential trail covering 10 rounds of `CRAFT` with the following input/output differences

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{10-round;} \quad \Pr \geq 2^{-50.25}} \texttt{0A00 0000 0000 00AA}$$

- The best ST differential distinguisher provided by designers:

$$\texttt{A0AA 00AA 0000 00AA} \xrightarrow{\text{10-round;} \quad \Pr \geq 2^{-62.61}} \texttt{A000 0000 0000 00AA}$$

- Computing differential effect using MILP/SAT based methods is generally a very time consuming task!

Achievements By Our Simple Strategy

- We found an optimum differential trail covering 10 rounds of `CRAFT` with the following input/output differences

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{10-round;} \quad \Pr \geq 2^{-50.25}} \texttt{0A00 0000 0000 00AA}$$

- The best ST differential distinguisher provided by designers:

$$\texttt{A0AA 00AA 0000 00AA} \xrightarrow{\text{10-round;} \quad \Pr \geq 2^{-62.61}} \texttt{A000 0000 0000 00AA}$$

- Computing differential effect using MILP/SAT based methods is generally a very time consuming task!
- $3513898 = 2^{21.74}$ optimal trails were counted on a desktop in 4 days, before interrupting the run!

Some Inspiring Observations

Observation I

There is always an optimum distinguishers for any even (starting from 8) or odd (starting from 9) number of rounds, with the following input/output differences:

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{r-round; even,}\quad \Pr_c^{o,r} = 2^{-(56+8(r-8))}} \texttt{0A00 0000 0000 00AA},$$

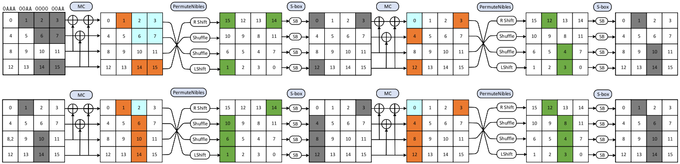
$$\texttt{AA0A AA00 0000 AA00} \xrightarrow{\text{r-round; odd,}\quad \Pr_c^{o,r} = 2^{-(64+8(r-9))}} \texttt{0A00 0000 0000 00AA}.$$

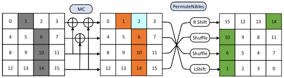
Observation II

The above differential distinguishers can be divided into three parts in which the middle part is a repeatable one.

The above observations, lead us to the partitioning technique

Partitioning Technique I





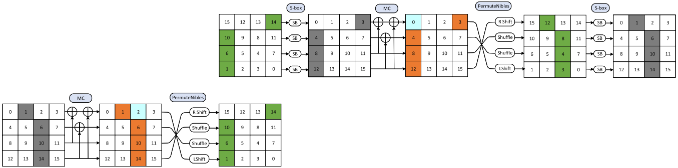
X^4 Y^4

$X^4[14] = X^4[10] \neq X^4[6]$

There are $n = 15 \times 15 \times 14 = 3150 \approx 2^{11.62}$ possible values for Y^4

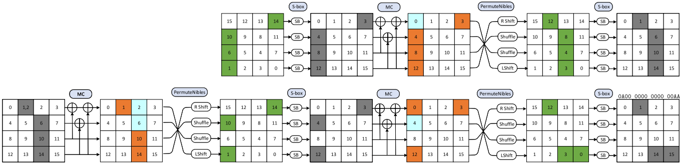
$E^{even}_{in,4}$

$p^{in} = \left(p^{in}_1 \quad \dots \quad p^{in}_n\right)$



$E^{even}_{m,2}$

$$p^m = \begin{pmatrix} p^m_{1,1} & \cdots & p^m_{1,n} \\ \vdots & \ddots & \vdots \\ p^m_{n,1} & \cdots & p^m_{n,n} \end{pmatrix}$$



$E^{even}_{out,4}$

$$p^{out} = \begin{pmatrix} p^{out}_1 \\ \vdots \\ p^{out}_n \end{pmatrix}$$

$$p^{tot} = p^{in} \times p^m \times p^{out}$$

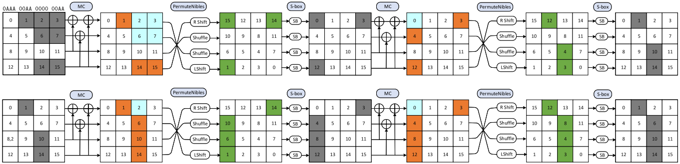
Another Observation - DDT of CRAFT'Sbox

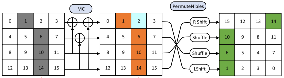
x/y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	4	0	2	2	2	0	2	0	0	0	0	0	2	0
2	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0	0
3	0	0	0	0	2	0	4	2	2	2	0	0	0	2	0	2
4	0	2	4	2	2	2	0	0	2	0	0	2	0	0	0	0
5	0	2	0	0	2	0	0	4	0	2	4	0	2	0	0	0
6	0	2	0	4	0	0	0	2	2	0	0	0	2	2	0	2
7	0	0	0	2	0	4	2	0	0	0	0	2	0	4	2	0
8	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
9	0	0	4	2	0	2	0	0	2	2	0	2	2	0	0	0
A	0	0	0	0	0	4	0	0	0	0	4	0	0	4	0	4
B	0	0	0	0	2	0	0	2	2	2	0	4	0	2	0	2
C	0	0	4	0	0	2	2	0	2	2	0	0	2	0	2	0
D	0	0	0	2	0	0	2	4	0	0	4	2	0	0	2	0
E	0	2	0	0	0	0	0	2	2	0	0	0	2	2	4	2
F	0	0	0	2	0	0	2	0	0	0	4	2	0	0	2	4

$$\forall\, x \in \{5, 7, \mathtt{A}, \mathtt{D}, \mathtt{F}\}\ \exists\, y \in \{5, 7, \mathtt{A}, \mathtt{D}, \mathtt{F}\}\ s.t.\, \Pr\{x \to y\} = 2^{-2}$$

$$\forall\, x \in \{5, 7, \mathtt{A}, \mathtt{D}, \mathtt{F}\}\ \forall\, z \notin \{5, 7, \mathtt{A}, \mathtt{D}, \mathtt{F}\}\ :\ \Pr\{x \to z\} \leq 2^{-3}$$

Partitioning Technique II





X^4 Y^4

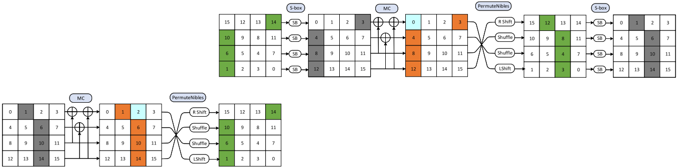
Intermediate active cells are limited to be in $\{5, 7, A, D, F\}$

$$X^4[14] = X^4[10] \neq X^4[6]$$

There are $n = 5 \times 5 \times 4 = 100$ possible values for Y^4

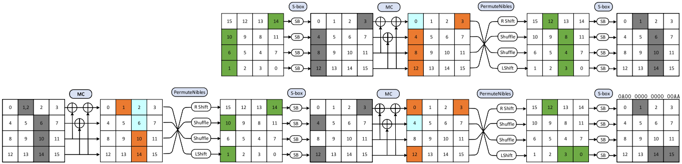
$E^{even}_{in,4}$

$$p^{in} = \begin{pmatrix} p^{in}_1 & \dots & p^{in}_n \end{pmatrix}$$



$E^{even}_{m,2}$

$$p^m = \begin{pmatrix} p^m_{1,1} & \cdots & p^m_{1,n} \\ \vdots & \ddots & \vdots \\ p^m_{n,1} & \cdots & p^m_{n,n} \end{pmatrix}$$



$E^{even}_{out,4}$

$$p^{out} = \begin{pmatrix} p^{out}_1 \\ \vdots \\ p^{out}_n \end{pmatrix}$$

$$p^{tot} = p^{in} \times p^m \times p^{out}$$

Improved Differential Distinguishers of CRAFT

Results achieved by combining SAT based method and partitioning technique:

♯ Rounds	r_{in}	r_m	r_{out}	Pr	♯ optimum trails
9	4	-	5	$2^{-40.20}$	$2^{23.32}$
10	4	-	6	$2^{-44.89}$	$2^{26.49}$
11	4	2	5	$2^{-49.79}$	$2^{29.66}$
12	4	2	6	$2^{-54.48}$	$2^{32.83}$
13	4	4	5	$2^{-59.13}$	$2^{36.00}$
14	4	4	6	$2^{-63.80}$	$2^{39.18}$

Contributions

Attack	♯ Rounds	Probability	Reference
ST-D	10	$2^{-62.61}$	[BLMR19]
	10	$2^{-44.89}$	this paper
	11	$2^{-49.79}$	
	12	$2^{-54.48}$	
	13	$2^{-59.13}$	
	14	$2^{-63.80}$	
ST-TD	12	2^{-36}	[MA19]
ST-LH	14	$2^{-62.12}$	[BLMR19]
RT_0-D	15	$2^{-55.14}$	[BLMR19]
RT_1-D	16	$2^{-57.18}$	
RT_2-D	17	$2^{-60.14}$	
RT_3-D	16	$2^{-55.14}$	
ST-ID	13	-	
ST-INT	13	-	
ST-ZC	13	-	
RT-ZC	14	-	this paper
RT-INT	14	-	this paper
RK-D	32	2^{-32}	[EY19]

Thank You for Listening!

All of our codes are publicly available via the following link:

`https://github.com/hadipourh/craftanalysis`

References I

Ralph Ankele, Christoph Dobraunig, Jian Guo, Eran Lambooij, Gregor Leander, and Yosuke Todo.
Zero-correlation attacks on tweakable block ciphers with linear tweakey expansion.
IACR Trans. Symmetric Cryptol., 2019(1):192–235, 2019.

Robert K Brayton, Gary D Hachtel, Curt McMullen, and Alberto Sangiovanni-Vincentelli.
Logic minimization algorithms for VLSI synthesis, volume 2.
Springer Science & Business Media, 1984.

Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh.
CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks.
IACR Trans. Symmetric Cryptol., 2019(1):5–45, 2019.

- Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang.
  Integral and multidimensional linear distinguishers with correlation zero.
  In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 244–261. Springer, 2012.

- Muhammad ElSheikh and Amr M. Youssef.
  Related-key differential cryptanalysis of full round CRAFT.
  IACR Cryptology ePrint Archive, 2019:932, 2019.

- Thorsten Kranz, Gregor Leander, and Friedrich Wiemer.
  Linear cryptanalysis: Key schedules and tweakable block ciphers.
  IACR Transactions on Symmetric Cryptology, pages 474–505, 2017.

References III

AmirHossein E. Moghaddam and Zahra Ahmadian.
New automatic search method for truncated-differential characteristics: Application to midori, skinny and craft.
Cryptology ePrint Archive, Report 2019/126, 2019.
`https://eprint.iacr.org/2019/126`.

Edward J McCluskey Jr.
Minimization of boolean functions.
Bell system technical Journal, 35(6):1417–1444, 1956.

Willard V Quine.
The problem of simplifying truth functions.
The American mathematical monthly, 59(8):521–531, 1952.

Willard V Quine.
A way to simplify truth functions.
The American Mathematical Monthly, 62(9):627–631, 1955.

References IV

Stefan Kölbl.
CryptoSMT: An easy to use tool for cryptanalysis of symmetric primitives.
https://github.com/kste/cryptosmt.

Ling Sun, Wei Wang, and Meiqin Wang.
More accurate differential properties of led64 and midori64.
IACR Transactions on Symmetric Cryptology, pages 93–123, 2018.