Comprehensive Security Analysis of CRAFT

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

[1]University of Tehran, Iran

[2]Kharazmi University, Iran

[4]Shahid Rajaee Teacher Training University, Iran

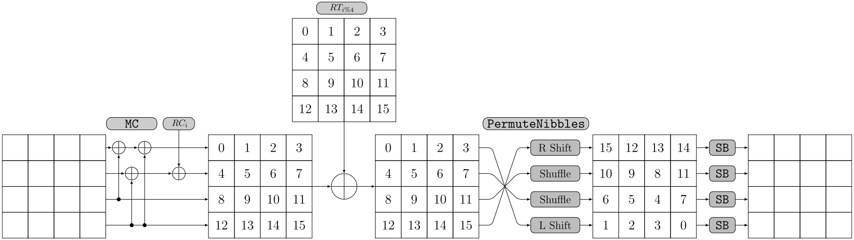
Feb 2, 2020

Outline

Outline

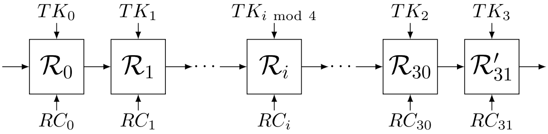
CRAFT[2]

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



[1] Differential Fault Attack

CRAFT



- Structure: 32 rounds consisting of 31 identical round, plus one linear round (without `PN`, and `SB` layers)

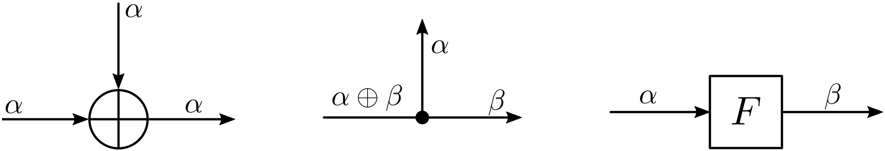
$$TK_0 = K_0 \oplus T, \qquad TK_1 = K_1 \oplus T,$$
$$TK_2 = K_0 \oplus Q(T), \qquad TK_3 = K_1 \oplus Q(T),$$

where $K = K_0 \| K_1 \in \mathbb{F}_2^{64} \times \mathbb{F}_2^{64}$ is the secret key, and $T \in \mathbb{F}_2^{64}$ is the master tweak.

- Q is a permutation on the position of tweak nibbles

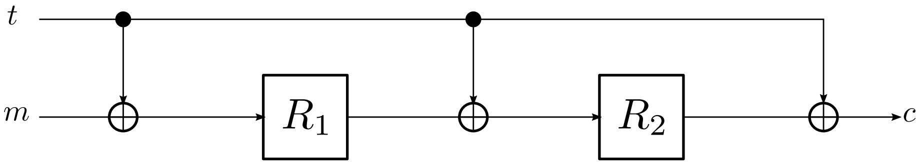
Outline

Reviewing Some Rules About Linear Masks Propagation



Impact of Considering Tweakey Schedule on ZC Distinguisher

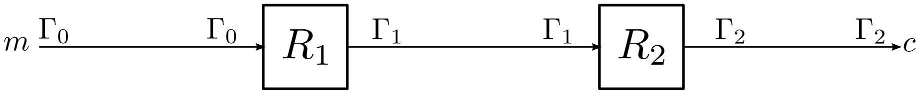
- Consider a toy tweakable block cipher like this:



- Suppose that the same tweak is used for each round

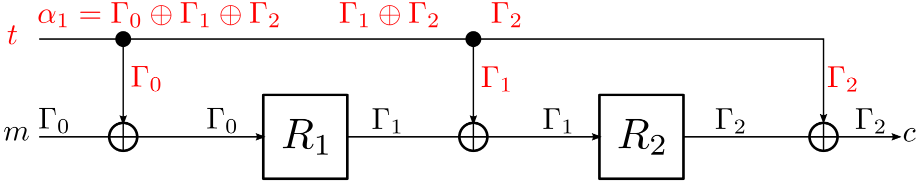
Impact of Considering Tweakey Schedule on ZC Distinguisher

- Remove the tweakey schedule, and propagate the linear masks through the data path

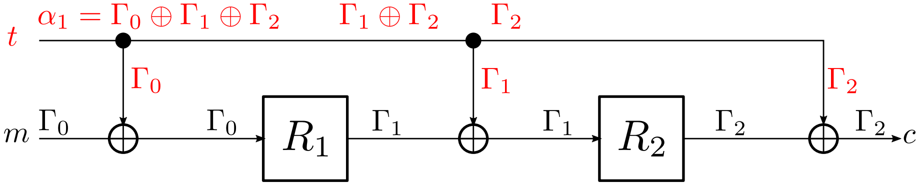


Impact of Considering Tweakey Schedule on ZC Distinguisher

- Now, Consider the tweakey schedule in the analysis. What will be happened for the previous propagation?



Impact of Considering Tweakey Schedule on ZC Distinguisher



- No extra linear trail will be crated
- The following extra restriction is induced by the tweakey schedule:

$$\alpha_1 = \Gamma_0 \oplus \Gamma_1 \oplus \Gamma_2$$

- The extra constraint, increases the probability of existing a zero-correlation linear hull [1]

Our Strategy to Find New ZC Distinguisher for CRAFT

Fact

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

Tasks Performed by Computer

zero correlation linear hulls are obtained automatically via MILP based method

Task Performed by Human

The obtained zero-correlation linear hulls, are mathematically proven

New ZC Distinguishers Covering 14 rounds of `CRAFT`

RT0

$$0000\ \ \gamma000\ \ 0000\ \ \gamma000 \xrightarrow{\text{14-round-}RT_0} 0000\ \ \delta000\ \ 0000\ \ 0000,$$

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

RT2, and RT3

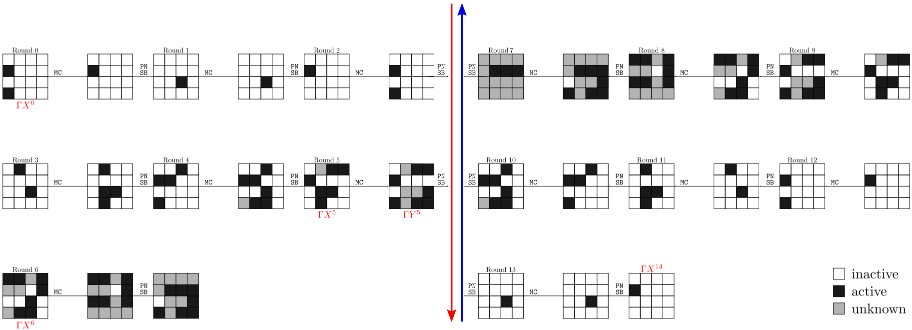
$$0000\ \ \gamma000\ \ 0000\ \ 0000 \xrightarrow{\text{14-round-}RT_2} 0000\ \ 0\delta00\ \ 0000\ \ 0000,$$

$$0000\ \ 0\gamma00\ \ 0000\ \ 0000 \xrightarrow{\text{14-round-}RT_3} 0000\ \ \delta000\ \ 0000\ \ 0000,$$

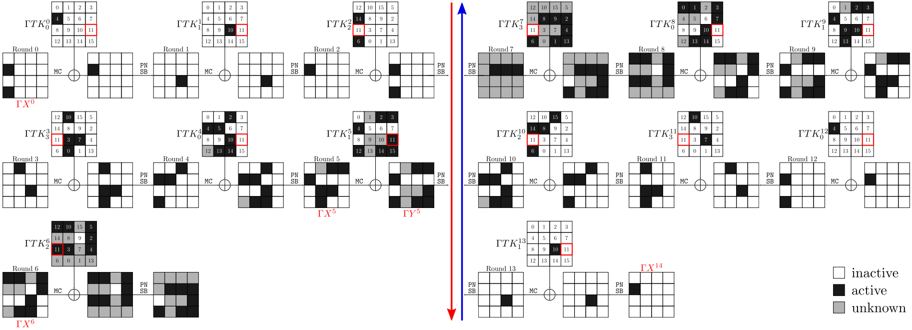
$$\Gamma T = {*}{*}{*}{*}\ \ {*}{*}{*}{*}\ \ {*}{*}{*}0\ \ {*}{*}{*}{*}$$

- $*$ depicts an arbitrary value in $\mathbb{F}_2^4$, and $\gamma, \delta \in \mathbb{F}_2^4 \setminus \{0\}$
- We have not found a ZC distinguisher covering 14 rounds, in case RT_1

Proof of 14-round ZC disntinguisher in case $RT0$

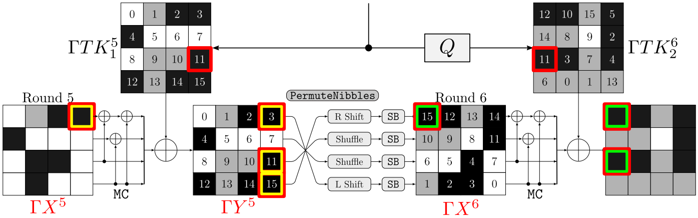


What if we consider the tweakey schedule?



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

Proof of 14-round ZC disntinguisher in case $RT0$



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

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

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

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

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

Outline

Link Between Zero-Correlation and Integral Distinguishers

Theorem

[8] 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

[8] 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
- Attacker can choose an arbitrary fixed value for those tweak nibbles 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 eqauls 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

1. CRAFT Specifiction
2. Zero-Correlation Cryptanalysis of CRAFT
   - Improving Zero-Correlation Distinguisher of CRAFT
3. Integral Cryptanalysis of CRAFT
   - Improving Integral Distinguishers of CRAFT
4. Differential Cryptanalysis of CRAFT
   - Making the CryptoSMT Faster
   - Divide and Conquer Strategy
   - Improving Differential Distinguishers of CRAFT

Our Strategy to Evaluate the Differential Effect

We use `CryptoSMT`[7] to estimate the differential effect, and it uses the following strategy to enumerate the differential trails in a differential effect [5, 4]:

1. Build the `CNF` modeling the problem, ask the solver to give one solution x if it exists
2. Add a new condition to the current `CNF` model in order to remove x
3. Ask the solver to give a solution, repeat step 2 until solver returns unsatisfiable

Improving the Sbox-Encoding in `CryptoSMT`

In order to make the `CryptoSMT` faster, the following method is used:

- Let $x, y \in \mathbb{F}_2^4$ are the input/output differences of the Sbox, and $p = (p_0, p_1, p_2)$ is used to encode $\Pr\{x \to y\} = 2^{-wt(p)}$
- The truth table of the following 11-bit Boolean function [9], is generated at first:

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

- The minimized product-of-sum (CNF) representation of the above Boolean function, is used to model the differential behaviour of Sbox

A Light of Hope and A New Issue!

First Success:

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

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{10-round;} \quad \Pr \geq 2^{-50.2554}} \texttt{0A00 0000 0000 00AA}$$

- The input/output differences were fixed, and the optimized `CryptoSMT` was used to evaluate the differential effect
- 3513898 optimal trails were counted in 4 days, before interrupting the run!
- We could improve the designers' claim ($2^{-62.61}$) at this stage

A new issue:

- The evaluation of differential effect was still very time consuming! Especially for more number of rounds

Some Inspiring Observations

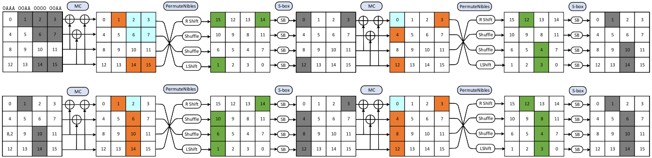
- We observed that there are optimum trails for even (strating from 8), and odd (starting from 9) number of roudns, with the same input/output differences:

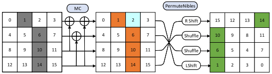
$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{r-round; even,}\quad \Pr_c^{o,r} = 2^{-(56+8(r-8))}} \texttt{0A00 0000 0000 00AA},$$

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

- The above observations, lead us to divide and conquer strategy

Building Blocks of Even Number of Rounds





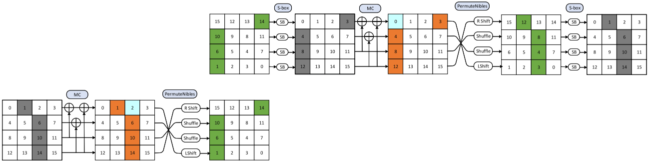
X^4 Y^4

Intermedaite values are taken from $\{5, 7, A, D, F\}$

$X^4[14] = X^4[10] \neq X^4[6] \Longrightarrow$ There are $5 \times 5 \times 4 = 100$ possible values for Y^4

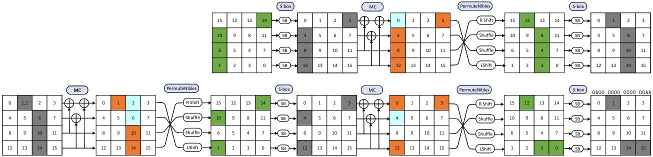
$E^{even}_{in,4}$

$$p^{in} = \begin{pmatrix} p^{in}_1 & \dots & p^{in}_{100} \end{pmatrix}$$



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

$$p^m = \begin{pmatrix} p^m_{1,1} & \dots & p^m_{1,100} \\ \vdots & \ddots & \vdots \\ p^m_{100,1} & \dots & p^m_{100,100} \end{pmatrix}$$



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

$$p^{out} = \begin{pmatrix} p^{out}_1 \\ \vdots \\ p^{out}_{100} \end{pmatrix}$$

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

Improving Differential Distinguishers of CRAFT

We could improve the differential distinguishers of `CRAFT` by four rounds in the single tweak model:

♯ 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	$2^{-62.61}$	[2]
	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}	[6]
ST-LH	14	$2^{-62.12}$	[2]
RT_0-D	15	$2^{-55.14}$	[2]
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}	[3]

Thank You for Listening!

all the codes are publicly available via the following link:
https://github.com/hadipourh/craftanalysis

Bibliography 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.

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.

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

Bibliography II

Stefan Kölbl, Gregor Leander, and Tyge Tiessen.
Observations on the simon block cipher family.
In *Annual Cryptology Conference*, pages 161–185. Springer, 2015.

Yunwen Liu, Qingju Wang, and Vincent Rijmen.
Automatic search of linear trails in arx with applications to speck and chaskey.
In *International Conference on Applied Cryptography and Network Security*, pages 485–499. Springer, 2016.

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.

Bibliography III

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

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 *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 95–115, 2015.

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