Rotational-XOR cryptanalysis

on ARX and AND-RX ciphers

Yunwen Liu

ASK 2019 at Kobe

National University of Defense Technology

Acknowledgement

This talk is based on the joint works with:

Tomer Ashur, Adrián Ranea & Glenn De Witte from KU Leuven

Chao Li, Jinyu Lu, Bing Sun & Wenqian Xin from NUDT

Cryptanalysis with Invariance

Some lightweight block ciphers are vulnerable to invariant attacks: light round function + simple key schedule

- Invariant subspace [LAA+11]
- Nonlinear invariants [TLS16]
- Rotational invariance

[LAA+11] Leander G., Abdelraheem M.A., AlKhzaimi H., Zenner E. (2011) A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. CRYPTO 2011
[TLS16] Todo Y., Leander G., Sasaki Y. (2016) Nonlinear Invariant Attack. ASIACRYPT 2016.

Rotational Invariance

For a function:

$$f(x_1, x_2, \ldots, x_m) = (y_1, y_2, \ldots, y_l) : \mathrm{F}_{2^n}^m \rightarrow \mathrm{F}_{2^n}^l$$

Given a bitwise left rotation by γ bits S^γ on the inputs, if the outputs are also rotated, then f is rotational invariant.

$$f(S^\gamma(x_1), S^\gamma(x_2), \ldots, S^\gamma(x_m)) = (S^\gamma(y_1), S^\gamma(y_2), \ldots, S^\gamma(y_l))$$

Rotational Invariance in Bitwise AND

Observation:

$$S^{\gamma}(x) \odot S^{\gamma}(y) = S^{\gamma}(x \odot y) \qquad \text{with probability } 1$$

- Bitwise AND is rotational invariant for any γ

Rotational Invariance in Modular Addition

Observation:

$$S^1(x) \boxplus S^1(y) = S^1(x \boxplus y) \qquad \text{with probability } 2^{-1.415}$$

Rotational Cryptanalysis (v1), [KN10]

A rotational distinguisher holds for an ARX structure with

$$\Pr = (2^{-1.415})^{\#\boxplus}$$

Rotational Cryptanalysis (v2), [KN15]

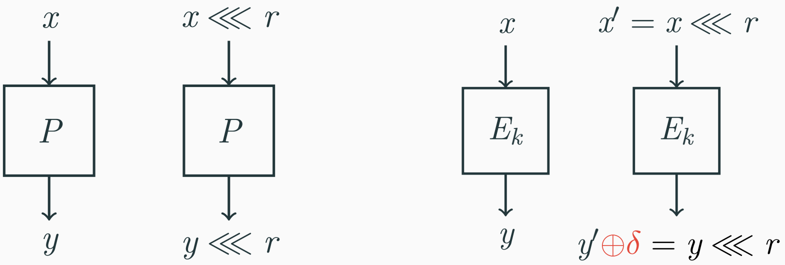
Refined probability estimation for a chain of modular additions

Rotational Invariance in the Presence of Constants

- Round keys: under related-key setting
- Rotational-invariant constants: for free in most cases
- Arbitrary constants?

Rotational-XOR Cryptanalysis

Idea in a Nutshell



By XORing some difference to the outputs, the rotational invariance is regained.

Rotational-XOR difference

Combine rotational relation with an XOR difference to obtain an RX-pair

$$(x, S^\gamma(x) \oplus \delta)$$

RX-difference   The RX-difference of a pair (x_1, x_2):

$$\Delta_\gamma(x_1, x_2) = x_2 \oplus S^\gamma(x_1)$$

Given an RX-difference δ, an RX-pair is $(x, S^\gamma(x) \oplus \delta)$

[AL17] T. Ashur and Y. Liu. Rotational cryptanalysis in the presence of constants. ToSC 2017
[LDRA18] Y. Liu, G. D. Witte, A. Ranea, and T. Ashur. Rotational-XOR Cryptanalysis of Reduced-round SPECK. ToSC 2018

Properties of RX-difference

Rotation

$$x \xrightarrow{\lll \eta} x \lll \eta$$

$$S^{\gamma}(x) \oplus a \xrightarrow{\lll \eta} S^{\gamma}(x \lll \eta) \oplus (a \lll \eta)$$

$$\text{RX-difference: } a \xrightarrow{\lll \eta} (a \lll \eta)$$

XOR

$$x, y \xrightarrow{\oplus} x \oplus y$$

$$\overleftarrow{x} \oplus a, \overleftarrow{y} \oplus b \xrightarrow{\oplus} \overleftarrow{x \oplus y} \oplus (a \oplus b)$$

$$\text{RX-difference: } (a, b) \xrightarrow{\oplus} a \oplus b$$

Rotational-XOR Cryptanalysis on ARX

Propagation of RX-difference in Modular Addition

Modular addition

$$S^{\gamma}(z) \oplus d_z = (S^{\gamma}(x) \oplus d_x) \boxplus (S^{\gamma}(y) \oplus d_y)$$

RX-differences for $\gamma = 1$: $d_x, d_y \xrightarrow{\boxplus} d_z$ with a probability

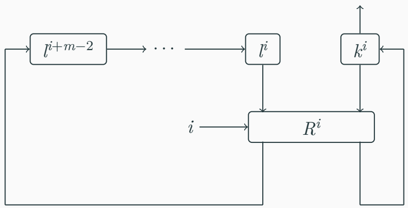
$$\begin{aligned}
&\Pr[(d_x, d_y) \to d_z] = \\
&\quad 1_{(I \oplus SHL)(\delta_x \oplus \delta_y \oplus \delta_z) \oplus 1 \preceq SHL((\delta_x \oplus \delta_z)|(\delta_y \oplus \delta_z))} \cdot 2^{-|SHL((\delta_x \oplus \delta_z)|(\delta_y \oplus \delta_z))|} \cdot 2^{-3} \\
&+ 1_{(I \oplus SHL)(\delta_x \oplus \delta_y \oplus \delta_z) \preceq SHL((\delta_x \oplus \delta_z)|(\delta_y \oplus \delta_z))} \cdot 2^{-|SHL((\delta_x \oplus \delta_z)|(\delta_y \oplus \delta_z))|} \cdot 2^{-1.415},
\end{aligned}$$

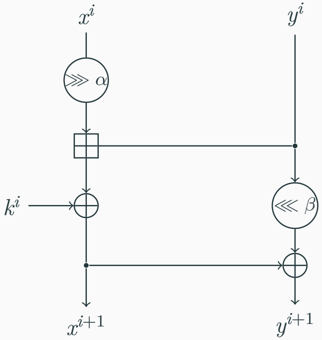
where

$$\delta_x = L'(d_x), \delta_y = L'(d_y), \delta_z = L'(d_z).$$

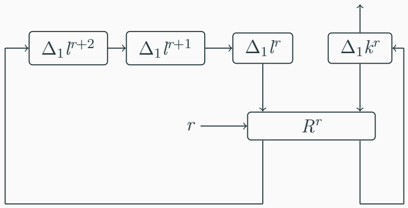
SPECK Block Ciphers

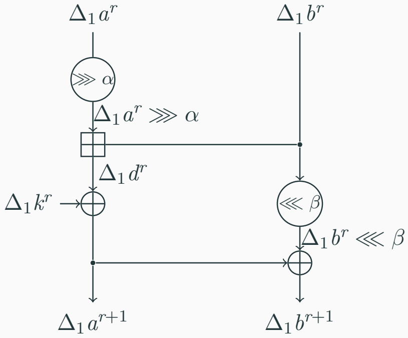
- ARX cipher designed by the NSA in 2013
- Block size $2n$ bits, $n = 16/24/32/48/64$
- Key size mn bits, $m = 2, 3, 4$





RX-differences in SPECK





Search for RX-characteristics in the key part and data part

Search Strategy

1. Aim: Find a characteristic covering more rounds
2. Find a good key characteristic with weight w_k
3. Fix the RX-characteristic in the key part and use it to find a good characteristic in the encryption part with weight w_d
4. Binary search

RX-characteristics found in SPECK32/SPECK48

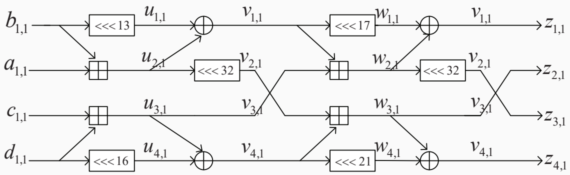
Version	Rounds	Data Prob.	Key Class Size	Ref.
32/64	9	2^{-30}	2^{64}	[Din14]
32/64	10	$2^{-19.15}$	$2^{28.10}$	Ours
32/64	11	$2^{-22.15}$	$2^{18.68}$	
32/64	12	$2^{-25.57}$	$2^{4.92}$	
48/96	11	2^{-45}	2^{96}	[FWG+16]
48/96	11	$2^{-24.15}$	$2^{25.68}$	Ours
48/96	12	$2^{-26.57}$	$2^{43.51}$	
48/96	13	$2^{-31.98}$	$2^{24.51}$	
48/96	14	$2^{-37.40}$	$2^{0.34}$	
48/96	15	$2^{-43.81}$	$2^{1.09}$	

[Din14] Dinur, I. Improved Differential Cryptanalysis on Round-reduced SPECK. FSE 2014.
[FWG+16] Fu K., Wang M., Guo Y., Sun S., and Hu L. MILP-Based Automatic Search Algorithms for Differential and Linear Trails for SPECK. FSE 2016.

Application to the pseudorandom function SipHash

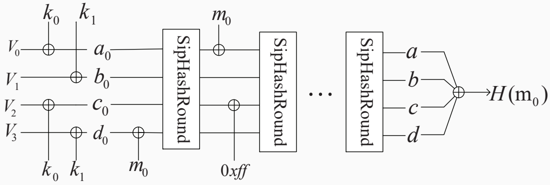
- ARX-based Pseudorandom function
- 256-bit permutation parted to 4 branches
- Four 64-bit modular additions in each SipHash round

SipHash Round



Application to the pseudorandom function SipHash

SipHash-1-x with one message block



1. Related-key setting and RX-differences injected by the messages
2. Requirements on the input and output RX-differences to get a collision
3. Initial constants

Application to the pseudorandom function SipHash

Version	Type	Blocks	Probability
SipHash-1-x	RX	2	2^{-280}
Revised SipHash-1-x	RX	1	$2^{-93.6}$
Revised SipHash-1-x	RX	2	2^{-160}

[XLL19] W. Xin, Y. Liu, C. Li. Improved cryptanalysis on SipHash. CANS 2019.

Rotational-XOR Cryptanalysis on AND-RX

Properties of RX-difference

Bitwise AND: $S^a(x) \odot S^b(x)$

$$S^a(S^\gamma(x) \oplus \alpha) \odot S^b(S^\gamma(x) \oplus \alpha) = S^\gamma(S^a(x) \odot S^b(x)) \oplus \beta$$

RX-differences: $\alpha \xrightarrow{\odot} \beta$

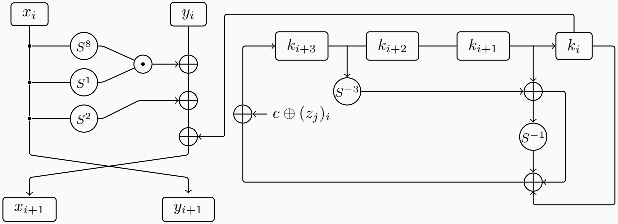
- It has a probability that is the same as the probability of the XOR-difference propagation ($\alpha \to \beta$) through the same function.
- The resistance against RX-cryptanalysis relies on the design of the constants

The block ciphers SIMON and SIMECK

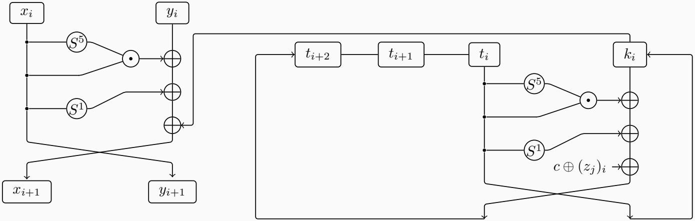
- SIMON: proposed together with SPECK
- AND-RX-based structure with a linear key schedule
- No design rationales

- SIMECK: SIMON + SPECK by Yang et al. in 2015
- SIMON-like cipher with a nonlinear key schedule
- Different rotational amounts

One round of SIMON:



One round of SIMECK:



Find RX-characteristics in SIMECK

Model for RX-difference propagations

1. Define RX-differences as bit-string variables in SMT
2. Describe the propagation rules in the round function and the key schedule by clauses
3. Set an upper bound for the cost w_d and w_k
4. Ask for a satisfiability verification

Advantage: The characteristics do not require a key characteristic found beforehand

Applications to SIMON32/64

Best RX-characteristic found in round-reduced SIMON32/64 with $\gamma = 1$

Version	Rounds	Probability	Type
32/64	10	2^{-16}	RKDC
	10	2^{-14}	RX
	11	2^{-24}	RX

However, the best found RX-characteristic in SIMON32 covers less rounds than the differential ones.

Applications to SIMECK

RX-characteristics found in SIMECK32 and SIMECK48

Cipher	Round	Data prob.	Weak keys
SIMECK32	15	2^{-16}	2^{40}
	19	2^{-30}	2^{30}
SIMECK48	16	2^{-20}	2^{70}
	18	2^{-26}	2^{64}
	19	2^{-30}	2^{64}
	25	2^{-46}	2^{48}

Observations

1. It takes much longer to find RX-characteristics in SIMON than in SIMECK
2. SIMECK seems to be more vulnerable to RX-cryptanalysis than SIMON
3. We believe that the cause lies in the key schedule
4. In our case, a nonlinear key schedule is no better than a linear one

Comparisons

1. Change the rotational amount: not much influence observed
2. Change the key schedule: relatively high contrast

SIM1: round function of SIMON and key schedule of SIMECK
SIM2: round function of SIMECK and key schedule of SIMON

Rounds	SIM-1	SIM-2	SIMON32
5	1	1	1
6	1	1	1
7	2^{-2}	2^{-4}	2^{-4}
8	2^{-4}	2^{-6}	2^{-6}
9	2^{-6}	2^{-10}	2^{-10}
10	2^{-8}	2^{-14}	2^{-14}

Conclusion

Wrap up

1. Rotational-XOR cryptanalysis generalises the rotational cryptanalysis to include the effect of constants
2. A new type of difference for tracking the rotational relation: RX-difference
3. RX-characteristics found
    - in ARX ciphers SPECK & SipHash
    - in AND-RX ciphers SIMON & SIMECK
4. Insights on the key schedules in terms of the resistance against RX-cryptanalysis

Thank you for your attention!