Methods for rotational cryptanalysis of ARX ciphers

S. Barbero

CrypTo
Gruppo di Crittografia e Teoria dei Numeri
Politecnico di Torino - Università di Torino

ARX operations

- n-bits strings: we essentially play in $\mathbb{F}_2^n$ and use the natural correspondence with $\mathbb{Z}_{2^n}$

$$x = (x_{n-1}, x_{n-2}, \ldots, x_1, x_0) \leftrightarrow x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \cdots + x_1 2 + x_0$$

- Addition : $\boxplus$ is the modular addiction mod 2^n
- Rotation: $\lll_r$ and $\ggg_r$ respectively indicate a constant-distance left-rotation or right-rotation of r bits ($r < n$) of a n-bit word x (when will be clear from the context, we will also use the notations $\overleftarrow{x} = \lll_r$ $\overrightarrow{x} = x \ggg_r$)

$$x \lll_r = (x_{n-r-1}, x_{n-r-2}, \ldots, x_1, x_0, x_{n-1}, \ldots x_{n-r})$$

$$x \ggg_r = (x_{r-1}, \ldots, x_1, x_0, x_{n-1}, x_{n-2}, \ldots, x_r)$$

- XOR: $\oplus$ is the bitwise addition (exclusive OR)

Why ARX?

ARX ciphers are block ciphers with very interesting advantages such as

- fast performance on PCs;
- compact implementation;
- easy algorithms;
- no timing attacks: in many other ciphers analyzing the time taken to execute cryptographic algorithms gives useful informations to the attacker in order to work backwards to the input, since the time of execution can differ based on the input;
- functionally completeness (assuming constants included): every possible logic gate can be realized as a network of gates using ARX operations and constants.

Basic disavantages of ARX

On the other hand we have some disavantages

- not best trade–off in hardware, although there are some different attempts of optimizations for various ARX ciphers;
- it is still not so clear which is their security against some cryptanalytic tools such as linear and differential cryptanalysis,
- it is also still not so clear which is their security against side channel attacks, i.e. attacks based on all hardware informations detected from their implementation (power attacks, electromagnetic attacks, fault attacks...)

Rotational cryptanalysis

- **Rotational cryptanalysis** is a probabilistic chosen plaintext attack, based on the study of propagation of rotations throughout the encryption steps of an ARX scheme. [Khovratovich 1]

Rotational cryptanalysis

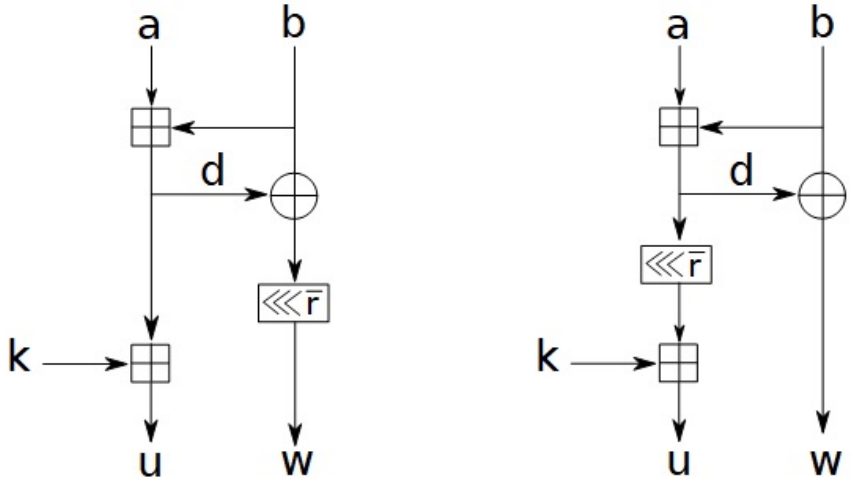
- X, Y be messages of n bits and $\mathcal{S}$ an ARX scheme with q modular additions. We have
  - $(X \oplus Y) \lll_r = X \lll_r \oplus Y \lll_r$
  - $p_r := \mathbb{P}\left[(X \boxplus Y) \lll_r = X \lll_r \boxplus Y \lll_r\right] = \frac{1}{4}(1 + 2^{-(n-r)} + 2^{-r} + 2^{-n})$ [Daum]
  - this probability is maximized to $2^{-1.415}$ when n is large and $r = 1$
  - $\mathcal{S}(X \lll_r) = \mathcal{S}(X) \lll_r$ with probability $(p_r)^q$ *if we assume that the q modular additions could be considered independent*
  - given a random function $\mathcal{P} : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, $\mathcal{P}(X \lll_r) = (\mathcal{P}(X)) \lll_r$ with probability 2^{-n}

Rotational cryptanalysis

Thus, we can detect nonrandomness in the ARX scheme $\mathcal{S}$ if $(p_r)^q > 2^{-n}$. For example, when $r = 1$, an ARX scheme implemented with less than $t/1.415$ additions is vulnerable to rotational cryptanalysis.
In general the attack procedure is

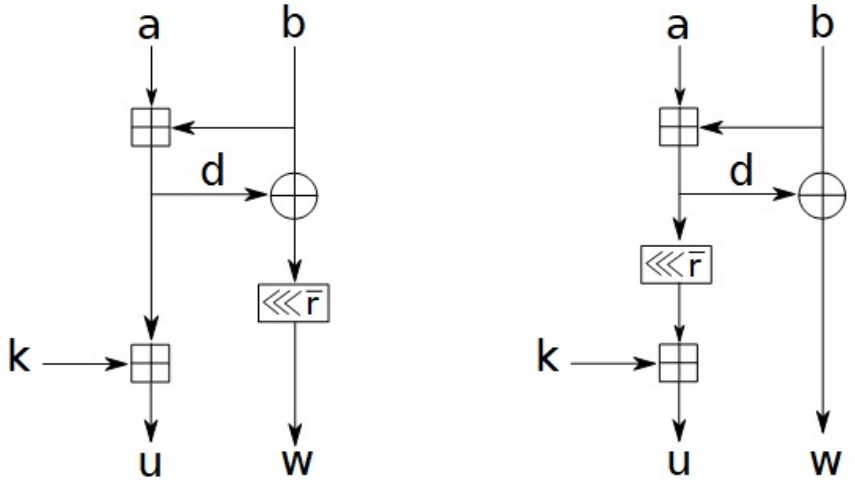
- Generate a random plaintext P and evaluate $C = \mathcal{S}_K(P)$, where K is the first secret key
- Evaluate $P' = P \lll_r \oplus d$, where d is the correction due to the presence of constants
- Evaluate $C' = \mathcal{S}_{K'}(P')$, with $K' = K \lll_r \oplus e$ the second key and e is the correction due to the presence of constants
- Check if (C, C') is a rotational pair, i. e., if $C' = C \lll_r$

Rotational cryptanalysis



In the ARX on the left, the two modular additions are chained, i.e. the output of the first is the input to the second. If $r = 1$ The most significant bit of the word $d = a \boxplus b$, when $(a \boxplus b) \lll_1 = a \lll_1 \boxplus b \lll_1$, is biased towards 1. Therefore, the second modular addition $u = k \boxplus d$ has rotational probability smaller than p_r.

Rotational cryptanalysis



In the ARX on the right, the two modular additions are separated by rotation: the most significant bit of d is still biased towards 1, but the rotation moves this bit to a different position, where the bias is negligible. The least significant bit of $d \lll_r$ becomes a completely random bit, thus $d \lll_r \boxplus k$ has probability given by p_r.

Rotational cryptanalysis

- The rotational probability of ARX cannot in general be computed simply by counting the number of modular additions.
- One has to investigate the relative positions of modular additions, i.e. if they are chained or separated by rotations.
- *The longer the chain of modular additions, the lower the rotational probability for each consecutive addition*

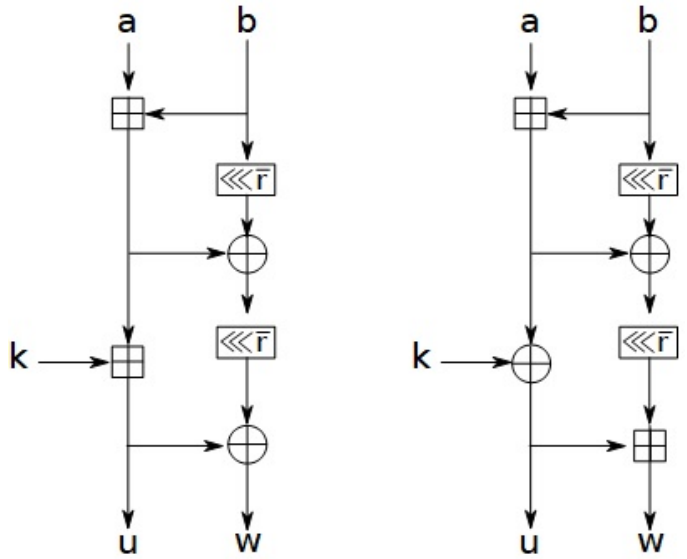
Rotational cryptanalysis

Theorem [Khovratovich] If we consider n–bits words $a_1, ..., a_k$ chosen at random, r a positive integer such that $0 < r < n$ and for $1 \leq h \leq k-1$ we consider the equalities

$$A_h := (a_1 \boxplus a_2 \boxplus \cdots \boxplus a_{h+1}) \lll_r = a_1 \lll_r \boxplus a_2 \lll_r \boxplus \cdots \boxplus a_{h+1} \lll_r$$

we have

$$\mathbb{P}[\cap_{h=1}^{k-1} A_h] = \frac{1}{2^{kn}} \binom{k + 2^{n-r} - 1}{2^{n-r} - 1} \binom{k + 2^r - 1}{2^r - 1}$$



- XORs also break such chains as long as the second term of the XOR is a random value. In practice, for ARX algorithms, the chains are broken by both XORs and rotations.
- *Rotational probability of ARX primitives highly depends on the way round keys are incorporated into the state, i.e. it is important if round keys are modularly added or XORed to the state.*

Rotational-XOR cryptanalysis with constants

Rotational-XOR difference

Combine rotational difference with XOR difference

$$(x, (x \lll \gamma) \oplus a)$$

$((a_1, a_2), \gamma)$-Rotational-XOR difference (RX-difference)

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

equivalent to

$$(\tilde{x}, (\tilde{x} \lll \gamma) \oplus (a_1 \lll \gamma) \oplus a_2)$$

Rotational-XOR cryptanalysis with constants

Rotational-XOR difference through ARX

Rotation

$$x \xrightarrow{\lll \gamma} x \lll \gamma$$

$$\overleftarrow{x} \oplus a \xrightarrow{\lll \gamma} \overleftarrow{x \lll \gamma} \oplus (a \lll \gamma)$$

$$\Rightarrow ((0, a), 1) \xrightarrow{\lll \gamma} ((0, a \lll \gamma), 1)$$

XOR

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

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

$$\Rightarrow ((0, a), 1), ((0, b), 1) \xrightarrow{\oplus} ((0, a \oplus b), 1)$$

Rotational-XOR cryptanalysis with constants

We introduce some notations

- $x = (x_{n-1}, x_{n-2}, \ldots, x_1, x_0)$ a n-bit boolean vector,
- $SHL(x)$ an arithmetic left shift of x by one bit, $(I \oplus SHL)(x) = x \oplus SHL(x)$
- $x|y$ the vector bitwise OR operation,
- $x||y$ the concatenation of x and y
- $|x|$ the Hamming weight of a boolean vector x
- $L(x)$ the γ most significant bits of x
- $L'(x)$ the $n - \gamma$ most significant bits of x
- $R(x)$ the $n - \gamma$ least significant bits of x
- $R'(x)$ the γ least significant bits of x
- $x \preceq y$ holds if and only if $x_i \leq y_i$ for all $i = 0, \cdots, n-1$

Rotational-XOR cryptanalysis with constants

Theorem (T. Ashur, Y. Liu)

Let $x, y \in \mathbb{F}_{2^n}$ be independent random variables. Let $a_1, b_1, a_2, b_2, \Delta_1, \Delta_2$ be constants in $\mathbb{F}_{2^n}$ then

$$\mathbb{P}[\overleftarrow{(x \oplus a_1) \boxplus (y \oplus b_1) \oplus \Delta_1} = (\overleftarrow{x} \oplus a_2) \boxplus (\overleftarrow{y} \oplus b_2) \oplus \Delta_2]$$

is equal to $2^{-|SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))|-3}$ if the following condition holds

$$(I \oplus SHL)(\delta_1 \oplus \delta_2 \oplus \delta_3) \oplus 1 \preceq SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3)),$$

otherwise is equal to $2^{-|SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))|-1.415}$ if the following condition holds

$$(I \oplus SHL)(\delta_1 \oplus \delta_2 \oplus \delta_3) \preceq SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))$$

where $\delta_1 = R(a_1) \oplus L'(a_2)$,$\delta_2 = R(b_1) \oplus L'(b_2)$ and $\delta_3 = R(\Delta_1) \oplus L'(\Delta_2)$.

Rotational-XOR cryptanalysis with constants

Lemma (E. Shulte–Geers)

Let $\zeta_1, \zeta_2, \zeta_3 \in \mathbb{F}_{2^n}$ be constants. Let $x, y \in \mathbb{F}_{2^n}$ be independent random variables. Then

$$\mathbb{P}[x \boxplus y = (x \oplus \zeta_1) \boxplus (y \oplus \zeta_2) \oplus \zeta_3] = 2^{-|SHL((\zeta_1 \oplus \zeta_3)|(\zeta_2 \oplus \zeta_3))|}$$

if the following condition holds

$$(I \oplus SHL)(\zeta_1 \oplus \zeta_2 \oplus \zeta_3) \preceq SHL((\zeta_1 \oplus \zeta_3)|(\zeta_2 \oplus \zeta_3))$$

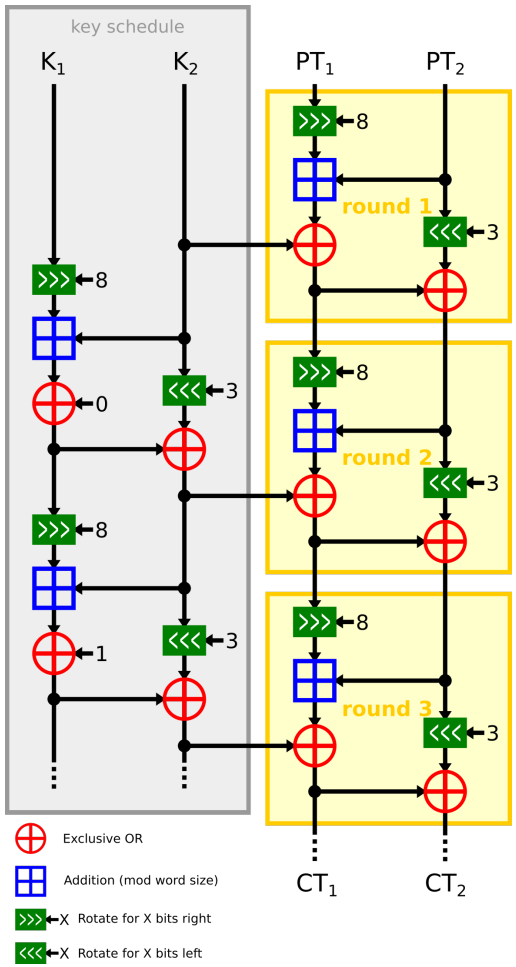
and $\mathbb{P}[x \boxplus y \boxplus 1 = (x \oplus \zeta_1) \boxplus (y \oplus \zeta_2) \oplus \zeta_3] = 2^{-|SHL((\zeta_1 \oplus \zeta_3)|(\zeta_2 \oplus \zeta_3))|}$ if the following condition holds

$$(I \oplus SHL)(\zeta_1 \oplus \zeta_2 \oplus \zeta_3) \oplus 1 \preceq SHL((\zeta_1 \oplus \zeta_3)|(\zeta_2 \oplus \zeta_3))$$

SPECK $2n/mn$

- SPECK is a family of lightweight ARX block ciphers publicly released by the National Security Agency (NSA) in June 2013
- every element of the SPECK family is indicated as SPECK $2n/mn$ where the size of every block is $2n$ with $n \in \{16, 24, 32, 48, 64\}$ and the key size is mn where $m \in \{2, 3, 4\}$ depending on the desired security
- the round function consists of two rotations, adding the right word to the left word, xoring the key into the left word, then xoring the left word into the right word.
- the number of rounds depends on the parameters selected and the key schedule uses the same round function as the main block cipher.

SPECK $2n/mn$



Three rounds of SPECK

SPECK $2n/mn$

Round function

When $i \geq 0$, (x_0, y_0) and $K = (l_{m-2}, \ldots, l_0, k_0)$ are respectively the round number, a $2n$ bits plaintext and a $2nm$ bits master key, we have the i–th round output (x_{i+1}, y_{i+1}) from the input (x_i, y_i) and the $i+1$-round key (l_{i+m-1}, k_{i+1}) from (l_{i+m-2}, k_i) as follows

$$x_{i+1} = ((x_i \ggg_\alpha) \boxplus y_i) \oplus k_i \quad y_{i+1} = (y_i \lll_\beta) \oplus x_{i+1}$$

$$l_{i+m-1} = ((l_i \ggg_\alpha) \boxplus k_i) \oplus i, \quad k_{i+1} = (k_i \lll_\beta) \oplus l_{i+m-1}$$

where $(\alpha, \beta) = (7, 2)$ for $n = 16$ and $(\alpha, \beta) = (8, 3)$ for the larger versions. The key schedule uses the same round function to generate the next round key.

Automated search for RX-Characteristics

- A possible path of RX-differences through different encryption rounds of a block cipher is called an *RX-characteristic*
- Using the notation

$$\Delta_1 x = x \oplus \overleftarrow{x}$$

the RX-differences in round i with $0 \leq i \leq r$, are

$$\Delta_1 a_i \ggg_\alpha, \Delta_1 b_i, \Delta_1 d_i$$

and for the key schedule

$$\Delta_1 l_i \ggg_\alpha, \Delta_1 k_i, \Delta_1 e_i, \Delta_1 c$$

where c depends on round number i.

Automated search for RX-Characteristics

- Search of valid r-round RX-characteristics for SPECK 32/64 with Automated Search (SAT-Solvers) finding when the boolean bits of RX-differences in round i with $0 \leq i \leq r$ satisfy one of the conditions of Theorem 1 plus the additional conditions for $0 \leq j < n$

$$\Delta_1 a_{i+1}^j = \Delta_1 d_i^j \oplus \Delta_1 k_i^j$$

$$\Delta_1 b_{i+1}^j = \Delta_1 b_i^{j-\beta} \oplus \Delta_1 a_{i+1}^j$$

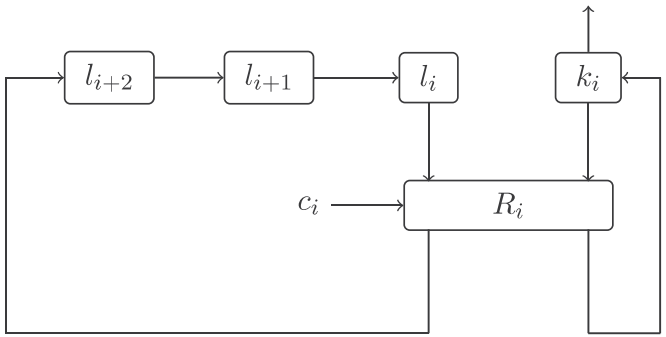
- Similar situation concerning the key schedule in order to find a valid r-round RX-characteristic, with the additional conditions for $0 \leq j < n$

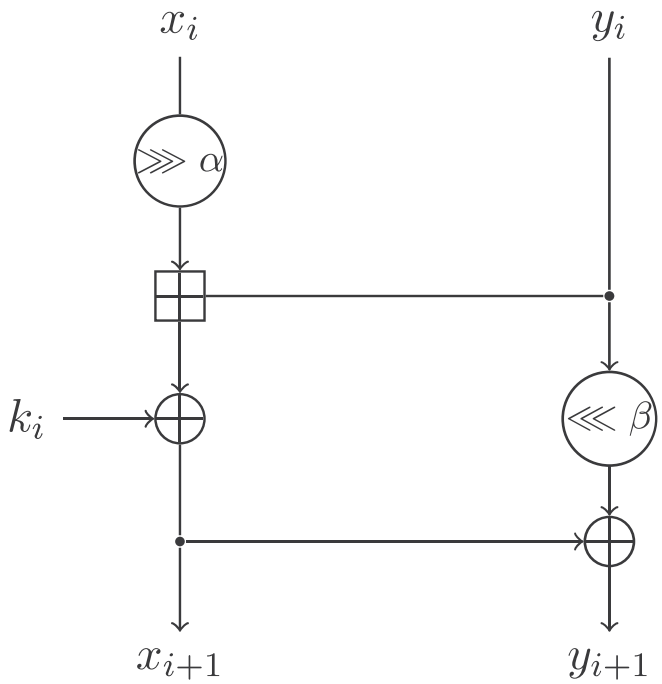
$$\Delta_1 l_{i+1}^j = \Delta_1 e_i^j \oplus \Delta_1 c$$

$$\Delta_1 k_{i+1}^j = \Delta_1 k_i^{j-\beta} \oplus \Delta_1 l_{i+1}^j$$

Automated search for RX-Characteristics-SPECK32/64

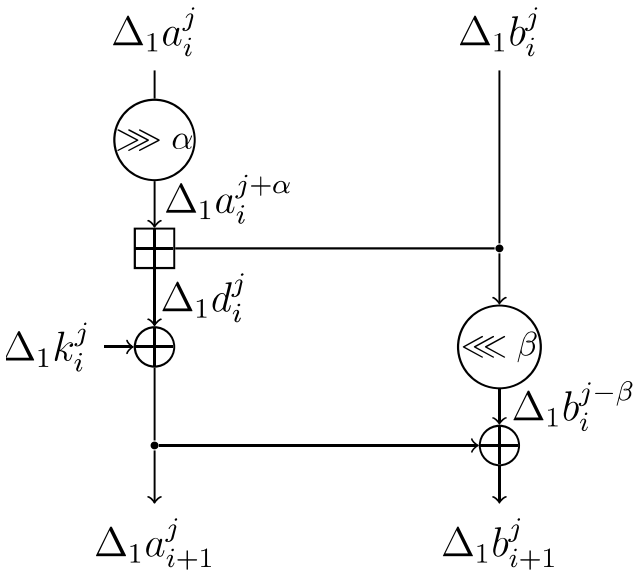
Application to SPECK32/64



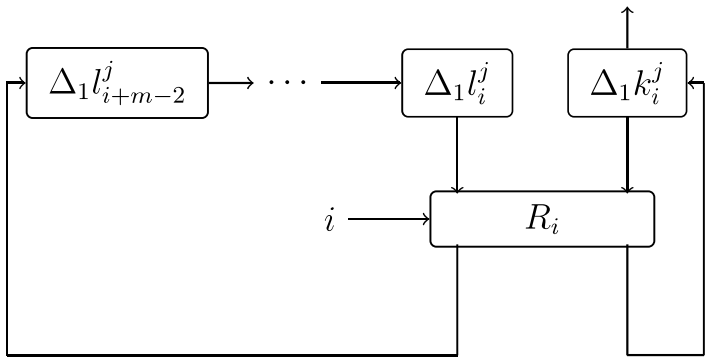


- Track RX-difference propagation in the key schedule
- Based on the good RX-trails found in the key schedule, track the propagation of RX-differences in the encryption

Automated search for RX-Characteristics-SPECK32/64



(a) Notation of the bits of RX-differences in the round function of SPECK.



(b) Notation of the bits of RX-differences in the key schedule of SPECK.

Future works

- A deep comprehension of these results, in order to consider the feasibility of a generalization to (at least a toy version of) other ARX like Chacha, a lot of work in progress!

Essential bibliography

- M. Daum *Cryptananlysis of Hash Functions of the MD4-Family* Ph.D. Thesis, Rhur Univesität Bochum,2005
- D. Khovratovich, I. Nikolic *Rotational Cryptanalysis of ARX* FSE 2010. Lecture Notes in Computer Science, vol 6147 pp 333-346,. Springer, Berlin, Heidelberg
- D. Khovratovich et al. *Rotational Cryptanalysis of ARX Revisited* https://eprint.iacr.org/2015/095.pdf
- T.Ashur, Y. Liu *Rotational Cryptanalysis in the Presence of Constants* IACR Trans. Symmetric Cryptol. 2016 (1) 57–70, 2016
- E. Schulte–Geers *On CCZ–equivalence of addition* mod2^n Designs, Codes and Cryptography 66 (1–3), 111–127, 2013