Rotational Differential-Linear Distinguishers of ARX Ciphers with Arbitrary Output Linear Masks

Zhongfeng Niu [1] [2], Siwei Sun [2], Yunwen Liu [3], Chao Li [4]

[1]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China

[2]School of Cryptology, University of Chinese Academy of Sciences, China

[3]Cryptape Technology Co., Ltd. Hangzhou, China

[4]College of Liberal arts and Science, National University of Defense Technology, China

August 14, 2022

Table of Content

(Rotational) Differential-Linear Cryptanalysis

- For a vectorial boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, a rotational differential-linear distinguisher with an input difference δ and output mask λ holds with a correlation

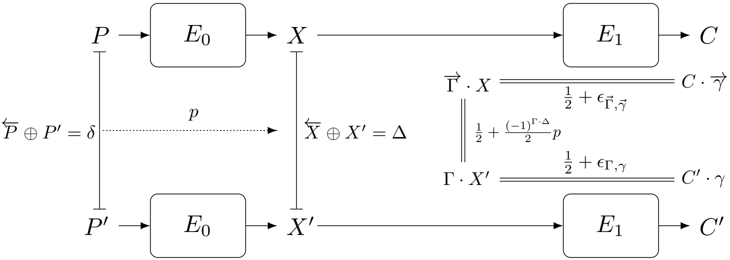
$$\mathbb{C}_{\delta,\lambda} = 2^{-n} \cdot \sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda \cdot \left(\overrightarrow{F(x)} \oplus F\left(\overrightarrow{x} \oplus \delta \right) \right)}$$

Problem: How to estimate the correlation?

Mind: When the rotational parameter is 0, then the rotational differential-linear cryptanalysis is differential-linear cryptanalysis.

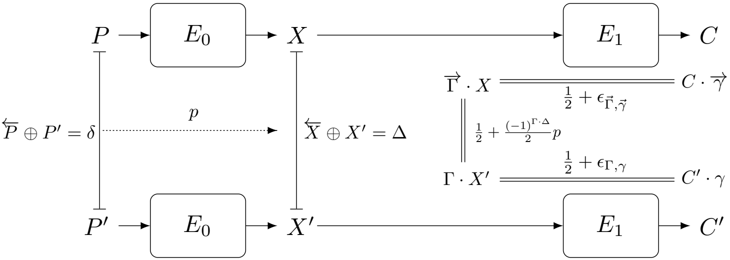
(Rotational) Differential-Linear Approximation

- (Rotational) Differential: $\delta \to \Delta$, probability *p*.
- Linear Approximation 1: $\Gamma \to \gamma$, probability $\frac{1}{2} + \epsilon_{\Gamma,\gamma}$;
- Linear Approximation 2: $\overrightarrow{\Gamma} \to \overrightarrow{\gamma}$, probability $\frac{1}{2} + \epsilon_{\vec{\Gamma},\vec{\gamma}}$.



(Rotational) Differential-Linear Approximation

- (Rotational) Differential: $\delta \to \Delta$, probability *p*.
- Linear Approximation 1: $\Gamma \to \gamma$, probability $\frac{1}{2} + \epsilon_{\Gamma,\gamma}$;
- Linear Approximation 2: $\overrightarrow{\Gamma} \to \overrightarrow{\gamma}$, probability $\frac{1}{2} + \epsilon_{\vec{\Gamma},\vec{\gamma}}$.
- (Rotational) Differential-Linear Approximation: $\delta \to \gamma$, theoretical probability: $\frac{1}{2} + 2p\, \epsilon_{\vec{\Gamma},\vec{\gamma}}\, \epsilon_{\Gamma,\gamma}$?



Estimating the (Rotational) Differential-Linear Correlation

- Differential-Linear Cryptanalysis
  - Differential-Linear Connectivity Table (DLCT, EUROCRYPT 2019)
  - Differential-Linear cryptanalysis from algebraic point (CRYPOTO 2021)

Only applicable for SPN !!

Estimating the (Rotational) Differential-Linear Correlation

- Differential-Linear Cryptanalysis
  - Differential-Linear Connectivity Table (DLCT, EUROCRYPT 2019)
  - Differential-Linear cryptanalysis from algebraic point (CRYPOTO 2021)

Only applicable for SPN !!

- Rotational Differential-Linear Cryptanalysis
  - Morawiekci's technique (EUROCRYPT 2021)

Only applicable for the output mask with Hamming weight 1 !!

Importance

- $\boxplus$ is the core component for ARX ciphers.
- Differential-Linear Cryptanalysis is one of the most powerful methods for ARX ciphers.

Motivation

- How to accurately calculate the (rotational) differential-linear correlation of $\boxplus$ for arbitrary output linear masks?
- Can we evaluate the (rotational) differential-linear correlation of Iterative ARX Primitives for arbitrary output linear masks?

(Rotational) Differential-Linear Correlation of $\boxplus$

Definition

The ordinary differential-linear correlation of $S(\mathbf{x},\mathbf{y}) = \mathbf{x} \boxplus \mathbf{y}$ with input difference $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, and output linear mask $\boldsymbol{\lambda} \in \mathbb{F}_2^n$ is defined as

$$\mathcal{C}^{\mathrm{DL}}_{(\boldsymbol{\alpha},\boldsymbol{\beta}),\boldsymbol{\lambda}}(S) = \frac{1}{2^{2n}} \sum_{(\mathbf{x},\mathbf{y}) \in \mathbb{F}_2^{2n}} (-1)^{\boldsymbol{\lambda} \cdot (S(\mathbf{x} \oplus \boldsymbol{\alpha}, \mathbf{y} \oplus \boldsymbol{\beta}) \oplus S(\mathbf{x},\mathbf{y}))}.$$

Definition

The rotational differential-dinear correlation of the modulo addition $S(x, y) = x \boxplus y$ with rotational offset t, rotational difference $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, and linear mask $\boldsymbol{\lambda}$ is defined as

$$\mathcal{C}^{\mathrm{R\text{-}DL}}_{(\boldsymbol{\alpha},\boldsymbol{\beta}),\boldsymbol{\lambda}}(S) = \frac{1}{2^{2n}} \sum_{(\mathbf{x},\mathbf{y}) \in \mathbb{F}_2^{2n}} (-1)^{\boldsymbol{\lambda} \cdot \left[(((\mathbf{x} \lll t) \oplus \boldsymbol{\alpha}) \boxplus ((\mathbf{y} \lll t) \oplus \boldsymbol{\beta})) \oplus ((\mathbf{x} \boxplus \mathbf{y}) \lll t)\right]}.$$

Motivation

- The time complexity for computing the (rotational) differential-linear correlation of $\boxplus$ is about $O(2^{2n})$.
- In practice, the modulo additions often operate on large words (e.g., 32-bit or 64-bit words). The way of enumerating the input pairs is infeasible.

How to compute the (rotational) differential-linear correlation of $\boxplus$ in polynomial time?

Related work in [LSL21] (EUROCRYPT 2021)

Some constraints:

- Liu.etc's method is only applicable for the output mask with Hamming weight 1.
- For the rotational differential-linear correlation of $\boxplus$, Liu.etc's method adopts certain statistical assumptions, which may give rise to some inaccurate result.

Related work in [LSL21] (EUROCRYPT 2021)

Some constraints:

- Liu.etc's method is only applicable for the output mask with Hamming weight 1.
- For the rotational differential-linear correlation of $\boxplus$, Liu.etc's method adopts certain statistical assumptions, which may give rise to some inaccurate result.

Improvement:

- A partition schemes of the sets $\mathbb{F}_2^n \times \mathbb{F}_2^n$.
- Give a formula a formula efficiently computes the exact correlations of arbitrary (rotational) differential-linear distinguishers of $\boxplus$.

Ordinary Differential-Linear Correlation of $\boxplus$

Theorem

The differential-linear correlation of the modulo addition $\mathcal{C}^{\mathrm{DL}}_{(\boldsymbol{\alpha},\boldsymbol{\beta}),\boldsymbol{\lambda}}$ can be computed as

$$\frac{1}{2^{2n}} \begin{pmatrix} 1, & 1, & 1, & 1 \end{pmatrix} \mathbf{M}^{(n-1)}_{\alpha_{n-1},\beta_{n-1},\lambda_{n-1}} \cdots \mathbf{M}^{(0)}_{\alpha_0,\beta_0,\lambda_0} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

where $\mathbf{M}_{a,b,c}$ for All $(a, b, c) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ is defined as:

$$\mathbf{M}_{0,0,0} = \begin{pmatrix} 3 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 3 \end{pmatrix}, \quad \mathbf{M}_{0,0,1} = \begin{pmatrix} 3 & -1 & -1 & 1 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 1 & -1 & -1 & 3 \end{pmatrix}, \quad \mathbf{M}_{0,1,0} = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix},$$

$$\mathbf{M}_{1,1,0} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 3 & 1 & 1 \\ 1 & 1 & 3 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad \mathbf{M}_{1,1,1} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & -3 & -1 & 1 \\ 1 & -1 & -3 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad \mathbf{M}_{0,1,1} = \begin{pmatrix} -2 & 1 & 1 & 0 \\ -1 & 2 & 0 & -1 \\ -1 & 0 & 2 & -1 \\ 0 & 1 & 1 & -2 \end{pmatrix},$$

$$\mathbf{M}_{1,0,0} = \mathbf{M}_{0,1,0}, \qquad \mathbf{M}_{1,0,1} = \mathbf{M}_{0,1,1}.$$

Rotational Differential-Linear Correlation of $\boxplus$

Theorem

The rotational differential-linear correlation of $\boxplus$ *with rotational offset* t*, rotational difference* $(\boldsymbol{\alpha}, \boldsymbol{\beta})$*, and linear mask* $\boldsymbol{\lambda}$ *can be computed as*

$$\frac{1}{2^{2n}}\begin{pmatrix}1, & 0, & 1, & 0\end{pmatrix}\mathbf{C}_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\lambda}}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \frac{1}{2^{2n}}\begin{pmatrix}0, & 1, & 0, & 1\end{pmatrix}\mathbf{C}_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\lambda}}\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

where

$$\mathbf{C}_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\lambda}} = \prod_{i=0}^{t-1}\mathbf{M}_{\alpha_i,\beta_i,\lambda_i}\begin{pmatrix}1 & 1 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 1 & 1\\0 & 0 & 0 & 0\end{pmatrix}\prod_{j=t}^{n-1}\mathbf{M}_{\alpha_j,\beta_j,\lambda_j}.$$

Compared with [LSL21] in EUROCRYPT 2021

Example

Consider the 32-bit modulo addition. Let $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{F}_2^{32} \times \mathbb{F}_2^{32}$ be the input difference

$$\begin{cases} \boldsymbol{\alpha} = (01100011101110001111101101010111)_2 \\ \boldsymbol{\beta} = (01010011001111111101001111100111)_2 \end{cases} .$$

Then, the rotational differential-linear correlations $\mathcal{C}^{\text{R-DL}}_{(\boldsymbol{\alpha},\boldsymbol{\beta}),\mathbf{e}_i}$ with rotation offset $t = 30$ can be computed with the formula presented in [LSL21] or theorem in our work, and the results are listed in following table.

i	0	1	2	3	4	5
[LSL21]	0	-0.5	-0.75	-0.875	-0.0625	0
This work	0.25	-0.375	-0.6875	-0.84375	-0.078125	0

- **Observation 1.** Rotational cryptanalysis et al. is a special case of rotational differential-linear cryanalysis, where the Hamming weight of the output mask is equal to 1.

$$\Pr[y_{i-t} = y_t^{'}] - \Pr[y_{i-t} \neq y_t^{'}] = \Pr[e_i \cdot (y_{i-t} \oplus y_t^{'}) = 0] - \Pr[e_i \cdot (y_{i-t} \oplus y_t^{'}) = 1]$$

- **Observation 2.** The output RD-L probability for the function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be evaluated by the distribution of input difference:

$$\Pr[y_{i-t} \neq y_t^{'}] = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \#\{x \in \mathbb{F}_2^n \mid \overrightarrow{x} \oplus x^{'} = u,\ y_{i-t} \neq y_t^{'}\} \prod_{i=0}^{n} ((1 - u_i) - (-1)^{u_i} p_i)$$

Problem: How to estimate the correlation for arbitrary output masks?

Morawiecki's technique for arbitrary output masks

Lemma

Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^n$ be a vectorial Boolean function and $0 \le t \le m-1$ be an integer. Assume that the input pair $(\mathbf{x}, \mathbf{x}') \in \mathbb{F}_2^m \times \mathbb{F}_2^m$ satisfies $\Pr[x_{i-t} \oplus x'_i = 1] = p_i$ for $0 \le i < m$, and the events $x_{i-t} \ne x'_i$ and $x_{j-t} \ne x'_j$ for different i and j are mutually independent. Then, for $\boldsymbol{\lambda} \in \mathbb{F}_2^n$ and rotation offset t, the rotational differential-linear correlation of F can be computed as

$$\mathcal{C}_{\boldsymbol{\lambda}}^{\text{R-DL}} = \Pr[\boldsymbol{\lambda} \cdot (\overleftarrow{F}(\mathbf{x}) \oplus F(\mathbf{x}')) = 0] - \Pr[\boldsymbol{\lambda} \cdot (\overleftarrow{F}(\mathbf{x}) \oplus F(\mathbf{x}')) = 1]$$

$$= \sum_{\mathbf{u} \in \mathbb{F}_2^m} \frac{1}{2^m} \sum_{\mathbf{x} \in \mathbb{F}_2^m} (-1)^{\boldsymbol{\lambda} \cdot (\overleftarrow{F}(\mathbf{x}) \oplus F(\overleftarrow{\mathbf{x}} \oplus \mathbf{u}))} \prod_{i=0}^{m-1} ((1 - u_i) - (-1)^{u_i} p_i).$$

Differential-Linear Correlation :

Theorem

Let $\mathbf{x}$, $\mathbf{x}'$, $\mathbf{y}$, *and* $\mathbf{y}'$ *be random n-bit strings such that* $\Pr[x_i \oplus x_i' = 1] = p_i$ *and* $\Pr[y_i \oplus y_i' = 1] = q_i$ *for* $0 \le i < n$*. In addition, the events* $x_i \oplus x_i' = 1$ *and* $y_j \oplus y_j' = 1$ *for* $0 \le i, j < n$ *are mutually independent. For* $\boldsymbol{\lambda} \in \mathbb{F}_2^n$*, the differential-linear correlation of* $F(\mathbf{x}, \mathbf{y}) = \mathbf{x} \boxplus \mathbf{y}$ *can be computed as*

$$\mathcal{C}_{\boldsymbol{\lambda}}^{\mathrm{DL}} = \frac{1}{2^{2n}}(1,1,1,1)\prod_{i=0}^{n-1}\mathbf{H}_{\lambda_i}^{p_i,q_i}(1,0,0,0)^T,$$

where $\mathbf{H}_{\lambda_i}^{p_i,q_i}$ *is a* 4×4 *matrix and is defined as*

$$\mathbf{H}_{\lambda_i}^{p_i,q_i} = \sum_{a,b\in\mathbb{F}_2}((1-a)-(-1)^a p_i)((1-b)-(-1)^b q_i)\mathbf{M}_{a,b,\lambda_i}.$$

Rotational Differential-Linear Correlation :

Theorem

We use $\mathbf{x}$, $\mathbf{x}'$, $\mathbf{y}$, *and* $\mathbf{y}'$ *to represent random n-bit strings such that* $\Pr[x_{i-t} \oplus x'_i = 1] = p_i$ *and* $\Pr[y_{i-t} \oplus y'_i = 1] = q_i$ *for* $0 \leq i < n$. *In addition, the events* $x_{i-t} \oplus x'_i = 1$ *and* $y_{j-t} \oplus y'_j = 1$ *for* $0 \leq i, j < n$ *are mutually statistical independent. Let* $S(\mathbf{x}, \mathbf{y}) = \mathbf{x} \boxplus \mathbf{y}$ *and* $\mathbf{W}$ *be*

$$\prod_{i=0}^{t-1} \left(\sum_{(c,d) \in \mathbb{F}_2^2} \zeta(c, d, p_i, q_i) \mathbf{M}_{c,d,\lambda_i} \right) \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \prod_{i=t}^{n-1} \left(\sum_{(a,b) \in \mathbb{F}_2^2} \zeta(a, b, p_i, q_i) \mathbf{M}_{a,b,\lambda_i} \right),$$

where $\zeta(a, b, p, q) = ((1-a) - (-1)^a p)((1-b) - (-1)^b q)$. *Then, for* $\boldsymbol{\lambda} \in \mathbb{F}_2^n$ *and rotation offset t, the rotational differential-linear correlation of* $S(\mathbf{x}, \mathbf{y})$ *can be computed as*

$$\mathcal{C}_{\boldsymbol{\lambda}}^{\text{R-DL}} = (1, 0, 1, 0)\mathbf{W}(1, 0, 0, 0)^T + (0, 1, 0, 1)\mathbf{W}(0, 1, 0, 0)^T.$$

New Morawiecki's technique for the Linear part

Lemma

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be a vectorial Boolean function mapping* $\mathbf{x} \in \mathbb{F}_2^n$ *to* $L \circ S(\mathbf{x}) \oplus \mathbf{c}$, *where* $\mathbf{c} \in \mathbb{F}_2^n$ *is a constant,* $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *is a nonlinear permutation, and* L *is an* $n \times n$ *binary matrix such that* $L(\mathbf{y} \lll t) = (L\mathbf{y}) \lll t$ *for all* $\mathbf{y} \in \mathbb{F}_2^n$ *and integer* t*. Then, the correlation of the rotational differential-linear approximation of* F *with rotation offset* t*, RX-difference* $\boldsymbol{\Delta}$*, and output linear mask* $\boldsymbol{\lambda} \in \mathbb{F}_2^n$ *can be computed as*

$$\mathcal{C}^{\text{R-DL}}_{\boldsymbol{\Delta},\boldsymbol{\lambda}}(F) = (-1)^{\boldsymbol{\lambda}\cdot(\mathbf{c}\oplus\overleftarrow{\mathbf{c}})}\mathcal{C}^{\text{R-DL}}_{\boldsymbol{\Delta},L^T\boldsymbol{\lambda}}(S).$$

Iterated evaluation of the D-L and R-L correlation

Algorithm 1: Iterated evaluation of the D-L and R-L correlation

Input: Input difference $\delta \in \mathbb{F}_2^n$; Output mask $\lambda \in \mathbb{F}_2^n$; Rotation offset t; Round m; Round function $F = L \circ S$ where L is a linear function.

Output: The D-L/R-L correlation

Initialization: generate the initial input RD-L probability distribution $\mathbb{D}_0$ according to input difference δ.

for $k = 1$ *to* $m - 1$ **do**

  for $i = 0$ *to* $n - 1$ **do**

    Under the input RD-L probability distribution $\mathbb{D}_{k-1}$, calculate the D-L/R-L correlation c_i of function S for output mask $L^T e_i$;

  According to $c_0, \cdots, c_{n-1}$, generate input RD-L probability distribution $\mathbb{D}_k$.

Under the input RD-L probability distribution $\mathbb{D}_{m-1}$, calculate the D-L/R-L correlation θ of function S for output mask $L^T\lambda$;

return θ;

Summary of Applications

Permutation/Block cipher	Type	# Round	Probability/Correlation		Ref.
			Theoretical	Experimental	
Alzette	DC	4	2^{-6}	–	[BBdS+20a]
	R-DL	4	$2^{-11.37}$	$2^{-7.35}$	[LSL21]
	DL	4	$2^{-0.27}$	$2^{-0.1}$	[LSL21]
	DC	8	$\leq 2^{-32}$	–	[BBdS+20a]
	DL	4	1	1	This talk
	R-DL	4	$2^{-5.57}$	$2^{-3.14}$	This talk
	DL	5	$-2^{-0.33}$	$-2^{-0.13}$	This talk
	DL	6	$2^{-4.95}$	$2^{-1.45}$	This talk
	DL	8	$-2^{-8.24}$	$-2^{-5.50}$	This talk
SipHash	DC	4	2^{-35}	–	[DSM14]
	DL	3	$2^{-2.19}$	$2^{-0.78}$	This talk
	DL	4	$2^{-12.45}$	$2^{-6.03}$	This talk
SPECK32	DC	8	2^{-24}	–	[ALLW14]
	LC	9	2^{-14}	–	[FWG+16]
	DC	10	$2^{-31.01}$	–	[SHY16]
	DL	8	$2^{-8.23}$	$2^{-6.87}$	This talk
	DL	9	$2^{-10.23}$	$2^{-8.93}$	This talk
	DL	10	$2^{-15.23}$	$2^{-13.90}$	This talk
ChaCha	DL	4	–	$2^{-1.19}$	[CM16]
	DL	4	$2^{-0.02}$	$2^{-0.98}$	This talk

Conclusion

- A formula efficiently computes the exact correlations of arbitrary (rotational) differential-linear distinguishers of $\boxplus$.
- A new method estimates the correlations of arbitrary (rotational) differential-linear distinguishers of ARX Ciphers.
- It works well in round-reduced `Alzette`, `SipHash`, `SPECK-32` and `ChaCha`.