A Note on the Bias of Rotational Differential-Linear Distinguishers

Yunwen Liu[1,2,3], Zhongfeng Niu[2,3], Siwei Sun[2,3⋆],Chao Li[1], Lei Hu[2,3]

[1] College of Liberal arts and Science, National University of Defense Technology, China univerlyw@hotmail.com

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

[3] University of Chinese Academy of Sciences, China

niuzhongfeng@iie.ac.cn, siweisun.isaac@gmail.com

Abstract. This note solves the open problem of finding a closed formula for the bias of a rotational differential-linear distinguisher proposed in IACR ePrint 2021/189 (EUROCRYPT 2021), completely generalizing the results on ordinary differential-linear distinguishers due to Blondeau, Leander, and Nyberg (JoC 2017) to the case of rotational differential-linear distinguishers.

Keywords: Rotational Differential-linear, · Differential-linear Attacks · Rotational Cryptanalysis · Multidimensional Differential-linear Attacks

1 Introduction

In [LSL21], the framework of rotational differential-linear cryptanalysis was established by replacing the differential part of the differential-linear framework [LH94,LGZL09,Lu15,BLN17,BDKW19,BLT20] with rotational-xor differentials [KN10,KNR10,KNP+15,KAR20,AJN14,MPS13,AL16,LWRA17,LLA+20]. This work left it as an open problem to derive a closed formula for the bias of a rotational differential-linear distinguisher. In this note, we solve this open problem and investigate the so-called *multidimensional* rotational differential-linear distinguishers, which completely generalizes the results on ordinary differential-linear distinguishers due to Blondeau, Leander, and Nyberg [BLN17] to the case of rotational differential-linear distinguishers.

2 Notations and Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the field with two elements. We denote by x_i the i-th bit of a bit string $x \in \mathbb{F}_2^n$. For a vectorial Boolean function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ with $y = F(x) \in \mathbb{F}_2^m$, its i-th output bit y_i is denoted by $(F(x))_i$. The XOR-difference and rotational-xor difference with offset t of two bit strings x and x' in $\mathbb{F}_2^n$ are

⋆ Corresponding author

defined as $x \oplus x'$ and $(x \lll t) \oplus x'$, respectively. For the rotational-xor difference $\delta = (x \lll t) \oplus x'$, we may omit the rotation offset and write $\delta = \overleftarrow{x} \oplus x'$ or $\delta = \mathtt{rot}(x) \oplus x'$ to make the notation more compact when it is clear from the context. Correspondingly, $\overrightarrow{x}$ and $\mathtt{rot}^{-1}(x)$ rotate x or its substrings to the right. Similar to differential cryptanalysis with XOR-difference, we can define the probability of an RX-differential as follows.

Definition 1 (RX-differential probability). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial boolean function. Let α and β be n-bit words. Then, the RX-differential probability of the RX-differential $\alpha \to \beta$ for f is defined as*

$$\Pr[\alpha \xrightarrow{\text{RX}} \beta] = 2^{-n} \#\{x \in \mathbb{F}_2^n : \mathtt{rot}(f(x)) \oplus f(\mathtt{rot}(x) \oplus \alpha) = \beta\}$$

Finally, the definitions of correlation, bias, and some lemmas concerning Boolean functions together with the piling-up lemma are needed.

Definition 2 ([Car06,Can16]). *The correlation of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as $\mathrm{cor}(f) = 2^{-n}(\#\{x \in \mathbb{F}_2^n : f(x) = 0\} - \#\{x \in \mathbb{F}_2^n : f(x) = 1\})$.*

Definition 3 ([Car06,Can16]). *The bias $\epsilon(f)$ of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as $2^{-n}\#\{x \in \mathbb{F}_2^n : f(x) = 0\} - \frac{1}{2}$.*

From Definition 2 and Definition 3 we can see that $\mathrm{cor}(f) = 2\epsilon(f)$.

Definition 4. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The Walsh-Hadamard transformation takes in f and produces a real-valued function $\hat{f} : \mathbb{F}_2^n \to \mathbb{R}$ such that*

$$\forall w \in \mathbb{F}_2^n, \quad \hat{f}(w) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{x \cdot w}.$$

Definition 5. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be two Boolean functions. The convolutional product of f and g is a Boolean function defined as*

$$\forall y \in \mathbb{F}_2^n, \quad (f \star g)(y) = \sum_{x \in \mathbb{F}_2^n} g(x) f(x \oplus y).$$

Lemma 1 ([Car06], Corollary 2). *Let $\hat{f}$ be the Walsh-Hadamard transformation of f. Then the Walsh-Hadamard transformation of $\hat{f}$ is $2^n f$.*

Lemma 2 ([Car06], Proposition 6). *$\widehat{(f \star g)}(z) = \hat{f}(z)\hat{g}(z)$ and thus $\widehat{(f \star f)} = (\hat{f})^2$.*

Lemma 3 (Piling-up Lemma [Mat93]). *Let $Z_0, \cdots, Z_{m-1}$ be m independent binary random variables with $\Pr[Z_i = 0] = p_i$. Then we have that*

$$\Pr[Z_0 \oplus \cdots \oplus Z_{m-1} = 0] = \frac{1}{2} + 2^{m-1} \prod_{i=0}^{m-1} (p_i - \frac{1}{2}),$$

or alternatively, $2\Pr[Z_0 \oplus \cdots \oplus Z_{m-1} = 0] - 1 = \prod_{i=0}^{m-1}(2p_i - 1)$.

3 Rotational Differential-linear cryptanalysis

A natural extension of the differential-linear cryptanalysis is to replace the differential part of the attack by rotational-xor (RX) differentials. Let $E = E_1 \circ E_0$ be an encryption function. Assume that we have an RX-differential $\delta \to \Delta$ covering E_0 with $\Pr[\mathtt{rot}(E_0(x)) \oplus E_0(\mathtt{rot}(x) \oplus \delta) = \Delta] = p$ and a linear approximation $\Gamma \to \gamma$ of E_1 such that

$$\begin{cases} \epsilon_{\Gamma,\gamma} = \Pr[\Gamma \cdot y \oplus \gamma \cdot E_1(y) = 0] - \frac{1}{2}, \\ \epsilon_{\mathtt{rot}^{-1}(\Gamma),\mathtt{rot}^{-1}(\gamma)} = \Pr[\mathtt{rot}^{-1}(\Gamma) \cdot y \oplus \mathtt{rot}^{-1}(\gamma) \cdot E_1(y) = 0] - \frac{1}{2}. \end{cases}$$

Let $x' = \mathtt{rot}(x) \oplus \delta$. If the assumption

$$\Pr[\Gamma \cdot (\mathtt{rot}(E_0(x)) \oplus E_0(x')) = 0 \mid \mathtt{rot}(E_0(x)) \oplus E_0(x') \neq \Delta] = \frac{1}{2} \tag{1}$$

holds. We have

$$\Pr[\Gamma \cdot (\mathtt{rot}(E_0(x)) \oplus E_0(x')) = 0] = \frac{1}{2} + \frac{(-1)^{\Gamma \cdot \Delta}}{2} p.$$

Since

$$\begin{aligned} \gamma \cdot (\mathtt{rot}(E(x)) \oplus E(x')) &= \gamma \cdot \mathtt{rot}(E(x)) \oplus \Gamma \cdot \mathtt{rot}(E_0(x)) \\ &\oplus \Gamma \cdot (\mathtt{rot}(E_0(x)) \oplus E_0(x')) \\ &\oplus \Gamma \cdot E_0(x') \oplus \gamma \cdot E(x') \\ &= \mathtt{rot}(\mathtt{rot}^{-1}(\gamma) \cdot E(x) \oplus \mathtt{rot}^{-1}(\Gamma) \cdot E_0(x)) \\ &\oplus \Gamma \cdot (\mathtt{rot}(E_0(x)) \oplus E_0(x')) \\ &\oplus \Gamma \cdot E_0(x') \oplus \gamma \cdot E(x'), \end{aligned}$$

the bias of the rotational differential-linear distinguisher can be estimated by piling-up lemma as

$$\mathcal{E}^{\text{R-DL}}_{\delta,\gamma} = \Pr[\gamma \cdot (\overleftarrow{E}(x) \oplus E(x')) = 0] - \frac{1}{2} = (-1)^{\Gamma \cdot \Delta} \cdot 2p\epsilon_{\Gamma,\gamma}\epsilon_{\mathtt{rot}^{-1}(\Gamma),\mathtt{rot}^{-1}(\gamma)},$$

and the corresponding correlation of the distinguisher is

$$\mathcal{C}^{\text{R-DL}}_{\delta,\gamma} = 2\mathcal{E}^{\text{R-DL}}_{\delta,\gamma} = (-1)^{\Gamma \cdot \Delta} \cdot 4p\epsilon_{\Gamma,\gamma}\epsilon_{\mathtt{rot}^{-1}(\Gamma),\mathtt{rot}^{-1}(\gamma)}.$$

We can distinguish E from random permutations if the absolute value of $\mathcal{E}^{\text{R}-\text{DL}}_{\delta,\gamma}$ or $\mathcal{C}^{\text{R-DL}}_{\delta,\gamma}$ is sufficiently high. Note that if we set the rotation offset to zero, the rotational differential-linear attack is exactly the ordinary differential-linear cryptanalysis. Therefore, the rotational differential-linear attack is a strict generalization of the ordinary differential-linear cryptanalysis. However, as in ordinary differential-linear attacks, the assumption described by Equation (1) may not hold in practice, and we prefer a closed formula for the bias $\mathcal{E}^{\text{R-DL}}_{\delta,\gamma}$ without this assumption for much the same reasons leading to Blondeau, Leander, and Nyberg's work [BLN17].

4 The Bias of A Rotational Differential-Linear Distinguisher

In [BLN17], Blondeau, Leander, and Nyberg proved the following theorem based on the general link between differential and linear cryptanalysis [CV94].

Theorem 1 **([BLN17]).** *If E_0 and E_1 are independent, the bias of a differential-linear distinguisher with input difference δ and output linear mask γ can be computed as*

$$\mathcal{E}_{\delta,\gamma} = \sum_{v\in\mathbb{F}_2^n} \epsilon_{\delta,v} c_{v,\gamma}^2, \tag{2}$$

for all $\delta \neq 0$ and $\gamma \neq 0$, where

$$\begin{cases} \epsilon_{\delta,v} = \Pr[v\cdot(E_0(x)\oplus E_0(x\oplus\delta)) = 0] - \frac{1}{2} \\ c_{v,\gamma} = \mathrm{cor}(v\cdot y \oplus \gamma\cdot E_1(y)) \end{cases}.$$

To replay Blondeau, Leander, and Nyberg's technique in an attempt to derive the rotational differential-linear counterpart of Equation (2), we have to first establish the relationship between rotational differential-linear cryptanalysis and linear cryptanalysis.

4.1 The Link between RX and Linear Cryptanalysis

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. The cardinality of the set

$$\{x \in \mathbb{F}_2^n : \overleftarrow{F}(x) \oplus F(\overleftarrow{x}\oplus a) = b\}$$

is denoted by $\xi_F(a,b)$, and the correlation of $u\cdot x\oplus v\cdot F(x)$ is $\mathrm{cor}(u\cdot x\oplus v\cdot F(x))$. Let $\overleftarrow{\underrightarrow{F}} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the vectorial Boolean function mapping x to $\overleftarrow{F}(\overrightarrow{x})$. It is easy to show that $\mathrm{cor}(u\cdot x\oplus v\cdot \overleftarrow{\underrightarrow{F}}(x)) = \mathrm{cor}(\overrightarrow{u}\cdot x \oplus \overrightarrow{v}\cdot F(x))$. In what follows, we are going to establish the relationship between

$$\xi_F(a,b), \quad \mathrm{cor}(u\cdot x\oplus v\cdot F(x)), \quad \text{and} \quad \mathrm{cor}(\overrightarrow{u}\cdot x\oplus\overrightarrow{v}\cdot F(x)).$$

Definition 6. *Given a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the Boolean function $\theta_F : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ is defined as*

$$\theta_F(x,y) = \begin{cases} 1 & \text{if } \; y = F(x), \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 4. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. Then for any $(a,b)\in\mathbb{F}_2^{2n}$, we have $\xi_F(a,b) = (\theta_{\overleftarrow{\underrightarrow{F}}} \star \theta_F)(a,b)$.*

Proof. According to Definition 5, we have

$$\begin{aligned}
(\theta_{\overleftarrow{\underrightarrow{F}}} \star \theta_F)(a,b) &= \sum_{x||y \in \mathbb{F}_2^{2n}} \theta_{\overleftarrow{\underrightarrow{F}}}(x,y)\theta_F(a \oplus x, b \oplus y) \\
&= \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^n} \theta_{\overleftarrow{\underrightarrow{F}}}(x,y)\theta_F(a \oplus x, b \oplus y) \\
&= \sum_{x \in \mathbb{F}_2^n} \theta_{\overleftarrow{\underrightarrow{F}}}(x, \overleftarrow{\underrightarrow{F}}(x))\theta_F(a \oplus x, b \oplus \overleftarrow{\underrightarrow{F}}(x)) = \sum_{x \in \mathbb{F}_2^n} \theta_F(a \oplus x, b \oplus \overleftarrow{\underrightarrow{F}}(x)) \\
&= \#\{x \in \mathbb{F}_2^n : b \oplus \overleftarrow{\underrightarrow{F}}(x) = F(a \oplus x)\} = \xi_F(a,b).
\end{aligned}$$

□

Lemma 5. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. Then for any $(a,b) \in \mathbb{F}_2^{2n}$, we have $\mathrm{cor}(a \cdot x \oplus b \cdot F(x)) = 2^{-n}\hat{\theta}_F(a,b)$.*

Proof. According to Definition 4, we have

$$\begin{aligned}
\hat{\theta}_F(a,b) &= \sum_{x||y \in \mathbb{F}_2^{2n}} \theta_F(x,y)(-1)^{(x||y)\cdot(a||b)} \\
&= \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^n} \theta_F(x,y)(-1)^{a\cdot x \oplus b \cdot y} \\
&= \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot F(x)} = 2^n \mathrm{cor}(a \cdot x \oplus b \cdot F(x)).
\end{aligned}$$

□

In addition, applying Lemma 5 to $\overleftarrow{\underrightarrow{F}}$ gives $\mathrm{cor}(a \cdot x \oplus b \cdot \overleftarrow{\underrightarrow{F}}(x)) = \frac{1}{2^n}\hat{\theta}_{\overleftarrow{\underrightarrow{F}}}(a,b)$.

Theorem 2. *The link between RX-differentials and linear approximations can be summarized as*

$$\xi_F(a,b) = \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^n} (-1)^{u \cdot a \oplus v \cdot b} \mathrm{cor}(\overrightarrow{u} \cdot x \oplus \overrightarrow{v} \cdot F(x))\mathrm{cor}(u \cdot x \oplus v \cdot F(x)).$$

Proof. According to Lemma 4 and Lemma 2, we have

$$2^{2n}\xi_F(a,b) = (\widehat{\widehat{\theta_{\overleftarrow{\underrightarrow{F}}} \star \theta_F}})(a,b) = \widehat{\hat{\theta}_{\overleftarrow{\underrightarrow{F}}}\hat{\theta}_F}(a,b).$$

Since $\hat{\theta}_{\overleftarrow{\underrightarrow{F}}}\hat{\theta}_F = 2^{2n}\mathrm{cor}(u \cdot x \oplus v \cdot \overleftarrow{\underrightarrow{F}}(x))\mathrm{cor}(u \cdot x \oplus v \cdot F(x))$ due to Lemma 5,

$$\begin{aligned}
\widehat{\hat{\theta}_{\overleftarrow{\underrightarrow{F}}}\hat{\theta}_F}(a,b) &= 2^{2n} \sum_{u||v \in \mathbb{F}_2^{2n}} (-1)^{(u||v)\cdot(a||b)} \mathrm{cor}(u \cdot x \oplus v \cdot \overleftarrow{\underrightarrow{F}}(x))\mathrm{cor}(u \cdot x \oplus v \cdot F(x)) \\
&= 2^{2n} \sum_{u,v \in \mathbb{F}_2^n} (-1)^{u \cdot a \oplus v \cdot b} \mathrm{cor}(u \cdot x \oplus v \cdot \overleftarrow{\underrightarrow{F}}(x))\mathrm{cor}(u \cdot x \oplus v \cdot F(x)) \\
&= 2^{2n} \sum_{u,v \in \mathbb{F}_2^n} (-1)^{u \cdot a \oplus v \cdot b} \mathrm{cor}(\overrightarrow{u} \cdot x \oplus \overrightarrow{v} \cdot F(x))\mathrm{cor}(u \cdot x \oplus v \cdot F(x))
\end{aligned}$$

□

If the function F is rotation invariant, i.e., $\overleftarrow{F(x)} = F(\overleftarrow{x})$, then we have $\mathrm{cor}(\overrightarrow{u} \cdot x \oplus \overrightarrow{v} \cdot F(x)) = \mathrm{cor}(u \cdot x \oplus v \cdot F(x))$. As a result, the theoretical link between rotational-xor and linear cryptanalysis degenerates to the link between ordinary differential cryptanalysis and linear cryptanalysis. Moreover, based on the link between differential and linear cryptanalysis, Blondeau, Leander, and Nyberg derived a closed formula for the bias of an ordinary differential-linear distinguisher as shown in Equation (2). We now try to mimic Blondeau, Leander, and Nyberg's approach to obtain a closed formula for the bias of rotational differential-linear distinguishers.

Note that this attempt was failed in [LSL21] and it was noted that this was due to a fundamental difference between rotational-xor differentials and ordinary differentials: the output RX-difference is not necessarily zero when the input RX-difference $\mathtt{rot}(x) \oplus x'$ is zero. In this work, we show that the difficulty brought by the difference is only technical.

4.2 A Closed Formula

Hereafter, we will denote $\mathrm{cor}(\overrightarrow{u} \cdot x \oplus \overrightarrow{v} \cdot F(x))\mathrm{cor}(u \cdot x \oplus v \cdot F(x))$ by $\lambda_F(u, v)$.

Definition 7. *Let $V \subseteq \mathbb{F}_2^n$ be a linear space and $\delta \in \mathbb{F}_2^n$ be a given vector. The probability of an RX-differential from δ to V is defined as*

$$\Pr[\delta \xrightarrow[F]{\mathrm{RX}} V] = \sum_{b \in V} \Pr[\delta \xrightarrow[F]{\mathrm{RX}} b].$$

Definition 8. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. The probability of the RX-differential from a linear space $U \subseteq \mathbb{F}_2^n$ to a linear space $V \subseteq \mathbb{F}_2^n$ for F is defined as*

$$\begin{aligned}
\Pr[U \xrightarrow[F]{\mathrm{RX}} V] &= \frac{1}{2^n \cdot |U|} \#\{(x, a) \in \mathbb{F}_2^n \times U : \overleftarrow{F}(x) \oplus F(\overleftarrow{x} \oplus a) \in V\} \\
&= \frac{1}{2^n \cdot |U|} \#\{(x, a, b) \in \mathbb{F}_2^n \times U \times V : \overleftarrow{F}(x) \oplus F(\overleftarrow{x} \oplus a) = b\} \\
&= \frac{1}{|U|} \sum_{a \in U} \sum_{b \in V} \Pr[a \xrightarrow[F]{\mathrm{RX}} b] = \frac{1}{|U|} \sum_{a \in U} \Pr[a \xrightarrow[F]{\mathrm{RX}} V].
\end{aligned}$$

Denote by $\mathrm{sp}(\delta)$ the linear space spanned by δ. According to Definition 8 and Definition 7, we have

$$\Pr[\mathrm{sp}(\delta) \xrightarrow[F]{\mathrm{RX}} V] = \frac{1}{2} \Pr[\delta \xrightarrow[F]{\mathrm{RX}} V] + \frac{1}{2} \Pr[0 \xrightarrow[F]{\mathrm{RX}} V],$$

which implies that

$$\Pr[\delta \xrightarrow[F]{\mathrm{RX}} V] = 2 \Pr[\mathrm{sp}(\delta) \xrightarrow[F]{\mathrm{RX}} V] - \Pr[0 \xrightarrow[F]{\mathrm{RX}} V]. \tag{3}$$

Lemma 6 ([Bon20]). *Let $\mathcal{H}$ be an additive subgroup of $\mathbb{F}_2^n$ and $f : \mathbb{F}_2^n \to \mathbb{R}$ be a function. Then*

$$f(x) = \sum_{h\in\mathcal{H}} (-1)^{x\cdot h} = \begin{cases} |\mathcal{H}|, & x \in \mathcal{H}^\perp \\ 0, & x \notin \mathcal{H}^\perp \end{cases}.$$

Proof. Let $\{h_1, \cdots, h_c\}$ be a basis of $\mathcal{H}$, and thus $\mathcal{H} = \{\tau_1 h_1 + \cdots + \tau_c h_c : (\tau_1, \cdots, \tau_c) \in \mathbb{F}_2^c\}$ has totally 2^c elements. Consequently, we have

$$\begin{aligned}\sum_{h\in\mathcal{H}} (-1)^{x\cdot h} &= \sum_{(\tau_1,\cdots,\tau_c)\in\mathbb{F}_2^c} (-1)^{x\cdot(\tau_1 h_1+\cdots+\tau_c h_c)} \\ &= \sum_{(\tau_1,\cdots,\tau_c)\in\mathbb{F}_2^c} (-1)^{x\cdot\tau_1 h_1} \cdots (-1)^{x\cdot\tau_c h_c} \\ &= \sum_{\tau_1\in\mathbb{F}_2} (-1)^{x\cdot\tau_1 h_1} \cdots \sum_{\tau_c\in\mathbb{F}_2} (-1)^{x\cdot\tau_c h_c} \\ &= (1 + (-1)^{x\cdot h_1}) \cdots (1 + (-1)^{x\cdot h_c}),\end{aligned}$$

which equals to $\mathcal{H} = 2^c$ if and only if $x \cdot h_1 = \cdots = x \cdot h_c = 0$. ◻

Theorem 3. *Let U and V be linear spaces in $\mathbb{F}_2^n$, then we have*

$$\Pr[U^\perp \xrightarrow[F]{\text{RX}} V^\perp] = \frac{1}{|V|} \sum_{\substack{u\in U\\ v\in V}} \operatorname{cor}(\overrightarrow{u} \cdot x \oplus \overrightarrow{v} \cdot F(x)) \operatorname{cor}(u \cdot x \oplus v \cdot F(x)).$$

Proof. Let $\lambda(u, v) = \operatorname{cor}(\overrightarrow{u} \cdot x \oplus \overrightarrow{v} \cdot F(x)) \operatorname{cor}(u \cdot x \oplus v \cdot F(x))$. According to Definition 8 and Theorem 2, we have

$$\begin{aligned}\Pr[U^\perp \xrightarrow[F]{\text{RX}} V^\perp] &= \frac{1}{|U^\perp|} \sum_{\substack{a\in U^\perp\\ b\in V^\perp}} \frac{1}{2^n} \sum_{\substack{u\in\mathbb{F}_2^n\\ v\in\mathbb{F}_2^n}} (-1)^{u\cdot a\oplus v\cdot b} \lambda(u, v) \\ &= \frac{1}{2^n} \cdot \frac{1}{|U^\perp|} \sum_{\substack{u\in\mathbb{F}_2^n\\ v\in\mathbb{F}_2^n}} \lambda(u, v) \sum_{a\in U^\perp} (-1)^{u\cdot a} \sum_{b\in V^\perp} (-1)^{v\cdot b}.\end{aligned}$$

Applying Lemma 6 gives

$$\begin{aligned}\Pr[U^\perp \xrightarrow[F]{\text{RX}} V^\perp] &= \frac{1}{2^n} \cdot \frac{1}{|U^\perp|} \cdot |U^\perp| \cdot |V^\perp| \sum_{\substack{u\in U\\ v\in V}} \lambda(u, v) \\ &= \frac{1}{|V|} \sum_{\substack{u\in U\\ v\in V}} \lambda(u, v).\end{aligned}$$

◻

Lemma 7. *Let* $\lambda(u,v) = \mathrm{cor}(\overrightarrow{u} \cdot x \oplus \overrightarrow{v} \cdot F(x))\mathrm{cor}(u \cdot x \oplus v \cdot F(x))$. *For* Δ, $w \in \mathbb{F}_2^n$, *we have*

$$\Pr[\Delta \xrightarrow[F]{\mathrm{RX}} \mathrm{sp}(w)^\perp] = \frac{1}{2} \sum_{u \in \mathrm{sp}(\Delta)^\perp} \lambda(u,w) - \frac{1}{2} \sum_{u \in \mathbb{F}_2^n \setminus \mathrm{sp}(\Delta)^\perp} \lambda(u,w) + \frac{1}{2}. \tag{4}$$

Proof. According to Equation (3), we have

$$\begin{aligned}
\Pr[\Delta \xrightarrow[F]{\mathrm{RX}} \mathrm{sp}(w)^\perp] &= 2\Pr[\mathrm{sp}(\Delta) \xrightarrow[F]{\mathrm{RX}} \mathrm{sp}(w)^\perp] - \Pr[0 \xrightarrow[F]{\mathrm{RX}} \mathrm{sp}(w)^\perp] \\
&= 2 \cdot \frac{1}{2} \sum_{\substack{u \in \mathrm{sp}(\Delta)^\perp \\ v \in \mathrm{sp}(w)}} \lambda(u,v) - \frac{1}{2} \sum_{\substack{u \in \mathbb{F}_2^n \\ v \in \mathrm{sp}(w)}} \lambda(u,v) \qquad \text{(Theorem 3)} \\
&= \frac{1}{2} \sum_{\substack{u \in \mathrm{sp}(\Delta)^\perp \\ v \in \mathrm{sp}(w)}} \lambda(u,v) - \frac{1}{2} \left(\sum_{\substack{u \in \mathbb{F}_2^n \\ v \in \mathrm{sp}(w)}} \lambda(u,v) - \sum_{\substack{u \in \mathrm{sp}(\Delta)^\perp \\ v \in \mathrm{sp}(w)}} \lambda(u,v) \right) \\
&= \frac{1}{2} \sum_{\substack{u \in \mathrm{sp}(\Delta)^\perp \\ v \in \mathrm{sp}(w)}} \lambda(u,v) - \frac{1}{2} \sum_{\substack{u \in \mathbb{F}_2^n \setminus \mathrm{sp}(\Delta)^\perp \\ v \in \mathrm{sp}(w)}} \lambda(u,v)
\end{aligned}$$

$\square$

Since $\lambda(u,0) = 0$ for $u \neq 0$ and $\lambda(u,0) = 1$ for $u = 0$,

$$\Pr[\Delta \xrightarrow[F]{\mathrm{RX}} \mathrm{sp}(w)^\perp] = \frac{1}{2} \sum_{u \in \mathrm{sp}(\Delta)^\perp} \lambda(u,w) - \frac{1}{2} \sum_{u \in \mathbb{F}_2^n \setminus \mathrm{sp}(\Delta)^\perp} \lambda(u,w) + \frac{1}{2}.$$

Theorem 4. *If two parts* E_0 *and* E_1 *of an* n*-bit block cipher* $E = E_1 \circ E_0$ *are RX-differentially independent, that is, for all* $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$,

$$\Pr[a \xrightarrow[E]{\mathrm{RX}} b] = \sum_{\Delta \in \mathbb{F}_2^n} \Pr[a \xrightarrow[E_0]{\mathrm{RX}} \Delta] \cdot \Pr[\Delta \xrightarrow[E_1]{\mathrm{RX}} b],$$

then we have

$$\Pr[\delta \xrightarrow[E]{\mathrm{RX}} \mathrm{sp}(w)^\perp] - \frac{1}{2} = \sum_{u \in \mathbb{F}_2^n} \left(\Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(u)^\perp] - \frac{1}{2} \right) \cdot \lambda_{E_1}(u,w).$$

Proof. Substituting Equation (4) into the right-hand side of

$$\Pr[\delta \xrightarrow[E]{\mathrm{RX}} \mathrm{sp}(w)^\perp] - \frac{1}{2} = \sum_{\Delta \in \mathbb{F}_2^n} \Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \Delta] \Pr[\Delta \xrightarrow[E_1]{\mathrm{RX}} \mathrm{sp}(w)^\perp] - \frac{1}{2}$$

gives

$$\frac{1}{2} \left(\sum_{\substack{\Delta \in \mathbb{F}_2^n \\ u \in \mathrm{sp}(\Delta)^\perp}} \Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \Delta] \lambda(u,w) - \sum_{\substack{\Delta \in \mathbb{F}_2^n \\ u \in \mathbb{F}_2^n \setminus \mathrm{sp}(\Delta)^\perp}} \Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \Delta] \lambda(u,w) \right). \tag{5}$$

Since $\mathbb{S} = \{(u, \Delta) : \Delta \in \mathbb{F}_2^n, u \in \mathrm{sp}(\Delta)^\perp\} = \{(u, \Delta) : u \in \mathbb{F}_2^n, \Delta \in \mathrm{sp}(u)^\perp\}$ and thus $(\mathbb{F}_2^n, \mathbb{F}_2^n)\backslash\mathbb{S} = \{(u, \Delta) : \Delta \in \mathbb{F}_2^n, u \in \mathbb{F}_2^n\backslash\mathrm{sp}(\Delta)^\perp\} = \{(u, \Delta) : u \in \mathbb{F}_2^n, \Delta \in \mathbb{F}_2^n\backslash\mathrm{sp}(u)^\perp\}$, Equation (5) can be written as

$$
\begin{aligned}
&\frac{1}{2}\left(\sum_{\substack{u\in\mathbb{F}_2^n\\ \Delta\in\mathrm{sp}(u)^\perp}} \Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \Delta]\lambda(u,w) - \sum_{\substack{u\in\mathbb{F}_2^n\\ \Delta\in\mathbb{F}_2^n\backslash\mathrm{sp}(u)^\perp}} \Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \Delta]\lambda(u,w)\right)\\
=&\frac{1}{2}\left(\sum_{u\in\mathbb{F}_2^n} \Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(u)^\perp]\lambda(u,w) - \sum_{u\in\mathbb{F}_2^n} \Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \mathbb{F}_2^n\backslash\mathrm{sp}(u)^\perp]\lambda(u,w)\right)\\
=&\sum_{u\in\mathbb{F}_2^n}\left(\Pr[\delta \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(u)^\perp] - \frac{1}{2}\right)\lambda(u,w).
\end{aligned}
$$

□

4.3 The Multidimensional Case

Let U and W be subspaces of $\mathbb{F}_2^n$, we define the bias of the rotational differential-linear distinguisher in the multidimensional case by

$$\mathcal{E}_{U,W}^{\text{R-DL}} = \Pr[U^\perp\backslash\{0\} \xrightarrow[E]{\mathrm{RX}} W^\perp] - \frac{1}{|W|}.$$

The following lemma can be regarded as the dual of Theorem 2.

Lemma 8. *For any permutation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, we have*

$$\lambda_F(u,v) = \frac{1}{2^n}\sum_{a,b\in\mathbb{F}_2^n} (-1)^{u\cdot a\oplus v\cdot b} \Pr[a \xrightarrow[F]{\mathrm{RX}} b].$$

Proof. According to Lemma 4 and Lemma 2, we have

$$\hat{\xi}_F(u,v) = (\widehat{\theta_{\overleftarrow{\underrightarrow{F}}} \star \theta_F})(u,v) = \hat{\theta}_{\overleftarrow{\underrightarrow{F}}}\hat{\theta}_F(u,v).$$

Applying Definition 4 and Lemma 5 gives

$$2^n \sum_{a,b\in\mathbb{F}_2^n} (-1)^{u\cdot a\oplus v\cdot b} \Pr[a \xrightarrow[F]{\mathrm{RX}} b] = 2^{2n}\lambda_F(u,v),$$

which completes the proof. □

Lemma 9. *If two parts E_0 and E_1 of an n-bit block cipher $E = E_1 \circ E_0$ are RX-differentially independent, that is, for all $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$,*

$$\Pr[a \xrightarrow[E]{\mathrm{RX}} b] = \sum_{\Delta\in\mathbb{F}_2^n} \Pr[a \xrightarrow[E_0]{\mathrm{RX}} \Delta]\cdot\Pr[\Delta \xrightarrow[E_1]{\mathrm{RX}} b],$$

then for all u, $w \in \mathbb{F}_2^n$, we have $\lambda_E(u,w) = \sum_{v\in\mathbb{F}_2^n} \lambda_{E_0}(u,v)\lambda_{E_1}(v,w)$.

Proof. According to Lemma 8, we have

$$\lambda_E(u,w) = \frac{1}{2^n} \sum_{a,b\in\mathbb{F}_2^n} (-1)^{u\cdot a\oplus v\cdot b} \Pr[a \xrightarrow[F]{\text{RX}} b].$$

Since E_0 and E_1 are RX-differentially independent,

$$\lambda_E(u,w) = \frac{1}{2^n} \sum_{a,b\in\mathbb{F}_2^n} (-1)^{u\cdot a\oplus v\cdot b} \sum_{c\in\mathbb{F}_2^n} \Pr[a \xrightarrow[E_0]{\text{RX}} c] \cdot \Pr[c \xrightarrow[E_1]{\text{RX}} b].$$

Applying Theorem 2 gives

$$\begin{aligned}
\lambda_E(u,w) =& \frac{1}{2^{2n}} \sum_{c\in\mathbb{F}_2^n} \sum_{m,v\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} (-1)^{(u\oplus m)\cdot a\oplus c\cdot v} \lambda_{E_0}(m,v) \sum_{b\in\mathbb{F}_2^n} \Pr[c \xrightarrow[E_1]{\text{RX}} b] \\
=& \frac{1}{2^{3n}} \sum_{m,v\in\mathbb{F}_2^n} \sum_{s,p\in\mathbb{F}_2^n} \lambda_{E_0}(m,v)\lambda_{E_1}(p,s) \sum_{a\in\mathbb{F}_2^n} (-1)^{(u\oplus m)\cdot a} \sum_{b\in\mathbb{F}_2^n} (-1)^{(w\oplus s)\cdot b} \sum_{c\in\mathbb{F}_2^n} (-1)^{(v\oplus p)\cdot c} \\
=& \sum_{v\in\mathbb{F}_2^n} \lambda_{E_0}(u,v)\lambda_{E_1}(v,w)
\end{aligned}$$

□

Theorem 5. *If two parts E_0 and E_1 of an n-bit block cipher $E = E_1 \circ E_0$ are RX-differentially independent, that is, for all $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$,*

$$\Pr[a \xrightarrow[E]{\text{RX}} b] = \sum_{\Delta\in\mathbb{F}_2^n} \Pr[a \xrightarrow[E_0]{\text{RX}} \Delta] \cdot \Pr[\Delta \xrightarrow[E_1]{\text{RX}} b],$$

then we have

$$\mathcal{E}_{U,W}^{\text{R-DL}} = \frac{2}{|W|} \sum_{v\in\mathbb{F}_2^n} \epsilon_{U,v}^{\text{R-DL}} C_{v,W}^{\text{R-DL}}$$

where $\epsilon_{U,v}^{\text{R-DL}} = \Pr[U^\perp\backslash\{0\} \xrightarrow[E_0]{\text{RX}} \text{sp}(v)^\perp]$ *and* $C_{v,W}^{\text{R-DL}} = \sum_{w\in W\backslash\{0\}} \lambda_{E_1}(v,w)$.

Proof. According to the Theorem 2, we have

$$\begin{aligned}
\Pr[U^\perp \xrightarrow[E_0]{\text{RX}} \text{sp}(w)^\perp] =& \frac{1}{2} \sum_{\substack{u\in U\\ v\in\text{sp}(w)}} \lambda_{E_0}(u,v) \\
=& \frac{1}{2} \sum_{u\in U} \lambda_{E_0}(u,v) + \frac{1}{2} \sum_{u\in U} \lambda_{E_0}(u,0) \\
=& \frac{1}{2} \sum_{u\in U} \lambda_{E_0}(u,v) + \frac{1}{2}
\end{aligned}$$

Thus,

$$2\Pr[U^\perp \xrightarrow[E_0]{\text{RX}} \text{sp}(w)^\perp] - 1 = \sum_{u\in U} \lambda_{E_0}(u,v) \tag{6}$$

For any subspaces U and $W \subseteq \mathbb{F}_2^n$, we have

$$
\begin{aligned}
&\Pr[U^\perp \xrightarrow[E]{\mathrm{RX}} W^\perp] \\
=&\frac{1}{|W|} \sum_{\substack{u\in U\\ w\in W}} \lambda_E(u,w) \\
=&\frac{1}{|W|} \sum_{\substack{u\in U\\ w\in W\\ v\in\mathbb{F}_2^n}} \lambda_{E_0}(u,v)\lambda_{E_1}(v,w) && \text{(Lemma 9)} \\
=&\frac{1}{|W|} \sum_{v\in\mathbb{F}_2^n} \sum_{u\in U} \lambda_{E_0}(u,v) \sum_{w\in W} \lambda_{E_1}(v,w) && \text{(Equation (6))} \\
=&\sum_{v\in\mathbb{F}_2^n} \frac{1}{|W|}(2\Pr[U^\perp \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^\perp] - 1) \sum_{w\in W} \lambda_{E_1}(v,w).
\end{aligned}
$$

Thus, when $U = \{0\} = (\mathbb{F}_2^n)^\perp$,

$$
\Pr[U^\perp \xrightarrow[E]{\mathrm{RX}} W^\perp] = \sum_{v\in\mathbb{F}_2^n} \frac{1}{|W|}(2\Pr[0 \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^\perp] - 1) \sum_{w\in W} \lambda_{E_1}(v,w).
$$

According to Definition 8, for any F, the following relation holds

$$
(|U^\perp| - 1)\Pr[U^\perp\backslash\{0\} \xrightarrow[F]{\mathrm{RX}} W^\perp] = |U^\perp|\Pr[U^\perp \xrightarrow[F]{\mathrm{RX}} W^\perp] - \Pr[0 \xrightarrow[F]{\mathrm{RX}} W^\perp]
$$

Then, we have

$$
\begin{aligned}
&(|U^\perp| - 1)\Pr[U^\perp\backslash\{0\} \xrightarrow[F]{\mathrm{RX}} W^\perp] \\
=&\sum_{v\in\mathbb{F}_2^n} \frac{1}{|W|}|U^\perp|(2\Pr[U^\perp \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^\perp] - 1) \sum_{w\in W} \lambda_{E_1}(v,w) \\
-&\sum_{v\in\mathbb{F}_2^n} \frac{1}{|W|}(2\Pr[0 \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^\perp] - 1) \sum_{w\in W} \lambda_{E_1}(v,w) \\
=&\frac{1}{|W|} \sum_{v\in\mathbb{F}_2^n} 2(|U^\perp|\Pr[U^\perp \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^\perp] - \Pr[0 \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^\perp]) - (|U^\perp| - 1) \sum_{w\in W} \lambda_{E_1}(v,w) \\
=&\frac{1}{|W|} \sum_{v\in\mathbb{F}_2^n} 2(|U^\perp| - 1)\Pr[U^\perp\backslash\{0\} \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^\perp] - (|U^\perp| - 1) \sum_{w\in W} \lambda_{E_1}(v,w)
\end{aligned}
$$

Dividing both sides by $|U^\perp| - 1$ gives

$$
\Pr[U^\perp\backslash\{0\} \xrightarrow[F]{\mathrm{RX}} W^\perp] = \frac{2}{|W|} \sum_{v\in\mathbb{F}_2^n} (\Pr[U^\perp\backslash\{0\} \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^\perp] - \frac{1}{2}) \sum_{w\in W} \lambda_{E_1}(v,w).
$$

Since $\Pr[U^{\perp}\backslash\{0\} \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(0)^{\perp}] = 1$, $\lambda(u,0) = 0$ for $u \neq 0$ and $\lambda(u,0) = 1$ for $u = 0$, $\Pr[U^{\perp}\backslash\{0\} \xrightarrow[F]{\mathrm{RX}} W^{\perp}]$ can be computed as

$$\frac{2}{|W|} \sum_{v \in \mathbb{F}_2^n} (\Pr[U^{\perp}\backslash\{0\} \xrightarrow[E_0]{\mathrm{RX}} \mathrm{sp}(v)^{\perp}] - \frac{1}{2}) \sum_{\substack{w \in W \\ w \neq 0}} \lambda_{E_1}(v,w) + \frac{1}{|W|}.$$

□

References

AJN14. Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. Analysis of NORX: investigating differential and rotational properties. In *Progress in Cryptology - LATINCRYPT 2014 - Third International Conference on Cryptology and Information Security in Latin America, Florianópolis, Brazil, September 17-19, 2014, Revised Selected Papers*, pages 306–324, 2014.

AL16. Tomer Ashur and Yunwen Liu. Rotational cryptanalysis in the presence of constants. *IACR Trans. Symmetric Cryptol.*, 2016(1):57–70, 2016.

BDKW19. Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman. DLCT: A new tool for differential-linear cryptanalysis. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I*, pages 313–342, 2019.

BLN17. Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-linear cryptanalysis revisited. *J. Cryptology*, 30(3):859–888, 2017.

BLT20. Christof Beierle, Gregor Leander, and Yosuke Todo. Improved differential-linear attacks with applications to ARX ciphers. In *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*, pages 329–358, 2020.

Bon20. Xavier Bonnetain. Tight Bounds for Simon's Algorithm. *IACR Cryptol. ePrint Arch.*, 2020:919, 2020. `https://eprint.iacr.org/2020/919`.

Can16. Anne Canteaut. Lecture notes on cryptographic boolean functions, 2016. `https://www.rocq.inria.fr/secret/Anne.Canteaut/`.

Car06. Claude Carlet. Boolean functions for cryptography and error correcting codes, 2006. `https://www.rocq.inria.fr/secret/Anne.Canteaut/`.

CV94. Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pages 356–365, 1994.

KAR20. Liliya Kraleva, Tomer Ashur, and Vincent Rijmen. Rotational cryptanalysis on MAC algorithm Chaskey. In *Applied Cryptography and Network Security - 18th International Conference, ACNS 2020, Rome, Italy, October 19-22, 2020, Proceedings, Part I*, pages 153–168, 2020.

KN10. Dmitry Khovratovich and Ivica Nikolic. Rotational cryptanalysis of ARX. In *Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers*, pages 333–346, 2010.

KNP$^+$15. Dmitry Khovratovich, Ivica Nikolic, Josef Pieprzyk, Przemyslaw Sokolowski, and Ron Steinfeld. Rotational cryptanalysis of ARX revisited. In *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, pages 519–536, 2015.

KNR10. Dmitry Khovratovich, Ivica Nikolic, and Christian Rechberger. Rotational rebound attacks on reduced Skein. In *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, pages 1–19, 2010.

LGZL09. Zhiqiang Liu, Dawu Gu, Jing Zhang, and Wei Li. Differential-multiple linear cryptanalysis. In *Information Security and Cryptology - 5th International Conference, Inscrypt 2009, Beijing, China, December 12-15, 2009. Revised Selected Papers*, pages 35–49, 2009.

LH94. Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. In *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, pages 17–25, 1994.

LLA$^+$20. Jinyu Lu, Yunwen Liu, Tomer Ashur, Bing Sun, and Chao Li. Rotational-XOR cryptanalysis of Simon-like block ciphers. In *Information Security and Privacy - 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30 - December 2, 2020, Proceedings*, pages 105–124, 2020.

LSL21. Yunwen Liu, Siwei Sun, and Chao Li. Rotational Cryptanalysis From a Differential-linear Perspective – Practical Distinguishers for Round-reduced FRIET, Xoodoo, and Alzette. *IACR Cryptol. ePrint Arch.*, 2021:189, 2021. `https://eprint.iacr.org/2021/189`.

Lu15. Jiqiang Lu. A methodology for differential-linear cryptanalysis and its applications. *Des. Codes Cryptogr.*, 77(1):11–48, 2015.

LWRA17. Yunwen Liu, Glenn De Witte, Adrián Ranea, and Tomer Ashur. Rotational-xor cryptanalysis of reduced-round SPECK. *IACR Trans. Symmetric Cryptol.*, 2017(3):24–36, 2017.

Mat93. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 386–397, 1993.

MPS13. Pawel Morawiecki, Josef Pieprzyk, and Marian Srebrny. Rotational cryptanalysis of round-reduced Keccak. In Shiho Moriai, editor, *Fast Software Encryption 2013*, volume 8424 of *Lecture Notes in Computer Science*, pages 241–262. Springer, 2013.