Rotational-XOR Differential Rectangle Cryptanalysis on Simon-like Ciphers

Siwei Chen[1], Mingming Zhu[1], Zejun Xiang[1](✉), Runqing Xu[1], Xiangyong Zeng[2], and Shasha Zhang[1]

[1] School of Cyber Science and Technology, Hubei University, Wuhan, 430062, China
{chensiwei_hubu,amushasha}@163.com, xiangzejun@hubu.edu.cn,
1942742852@qq.com, xu_runqing@foxmail.com,

[2] Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan, 430062, China xzeng@hubu.edu.cn

Abstract. In this paper, we propose a rectangle-like method called *rotational-XOR differential rectangle* attack to search for better distinguishers. It is a combination of the rotational-XOR cryptanalysis and differential cryptanalysis in the rectangle-based way. In particular, we put a rotational-XOR characteristic before a differential characteristic to construct a rectangle structure. By choosing some appropriate rotational-XOR and differential characteristics as well as considering multiple differentials, some longer distinguishers that have the probability greater than 2^{-2n} can be constructed effectively where n is the block size of a block cipher. We apply this new method to some versions of Simon and Simeck block ciphers. As a result, we obtain rotational-XOR differential rectangle distinguishers up to 16, 16, 17, 16 and 21 rounds for Simon32/64, Simon48/72, Simon48/96, Simeck32 and Simeck48, respectively. Our distinguishers for Simon32/64 is longer than the best differential and rotational-XOR distinguishers. As for Simon48/96, the distinguisher is longer than the rotational-XOR distinguisher and as long as the best differential distinguisher. Also, our distinguisher for Simeck32 is longer than the best differential distinguisher (14 rounds) and has the full weak key space (i.e., 2^{64}) whereas the 16-round rotational-XOR distinguisher has a weak key class of 2^{36}. In addition, our distinguisher for Simeck48 has a better weak key class (2^{72} weak keys) than the 21-round rotational-XOR distinguisher (2^{60} weak keys). To the best of our knowledge, this is the first time to consider the combinational cryptanalysis based on rotational-XOR and differential cryptanalysis using the rectangle structure.

Keywords: Rotational-XOR cryptanalysis · Differential cryptanalysis · Rectangle · Simon · Simeck · Distinguisher

1 Introduction

The security of a symmetric-key cryptographic primitive is determined by evaluating its resistance to a list of known cryptanalysis. Thus, it is important to come up with some new attacks and extend the known ones which contribute to the development of analysis and design of cryptography. In the past few decades, a series of cryptanalysis methods have been proposed, such as differential cryptanalysis [6], linear cryptanalysis [22], integral cryptanalysis [12], rotational cryptanalysis [10] and some derivative methods like differential-linear cryptanalysis [16], rectangle cryptanalysis [5] and rotational-XOR cryptanalysis [1], etc. The derivants of some conventional cryptanalysis methods have been proved to be more effective in some circumstances. For example, Liu et al. [18] utilized the differential-linear cryptanalysis, which is a combination of differential and linear cryptanalysis, to achieve the best key-recovery attack on the AES finalist Serpent [4]. Lu et al. [20] investigated the security of Simon-like ciphers against the rotational-XOR attack, which is a combination of differential and rotational cryptanalysis, and obtained the longest distinguishers for Simeck [28]. In addition, rectangle cryptanalyis is also an adaption of differential cryptanalysis and aims to construct longer distinguishers by exploiting two shorter differential characteristics. These methods have been more and more widely applied to block ciphers, hash functions, etc.

In 2013, the National Security Agency (NSA) designed two families of lightweight block ciphers, Simon and Speck [3]. In order to obtain a more compact and efficient implementation in hardware, Yang et al. [28] combined the good components of Simon and Speck ciphers, and proposed a new lightweight block cipher named Simeck at CHES 2015. Both Simeck and Simon ciphers are based on Feistel structure and their round functions are similarly designed by bitwise AND, rotation and XOR (AND-RX) operations but using different rotation parameters. Therefore, they are collectively called Simon-like ciphers. In the past decade, Simon-like ciphers have attracted a lot of attention from cryptographers, and various cryptanalyses have been carried out including but not limited to [7,13,14,27,19,26,24,20,15,17,21]. Among them, Rohit and Gong [24] proposed a correlated sequence attack and presented the best key-recovery attacks on round-reduced Simon32 and Simeck32. At ASIACRYPT 2021, Leurent et al. [17] investigated the clustering effect on the differential and linear characteristics of Simon-like ciphers. By considering the lowest w active bits of each branch, it is practical to generate a tighter bound on the probability of the differential or linear approximation. Therefore they explored some better differential and linear distinguishers and presented the best key-recovery attacks for Simeck48, Simeck64, Simon96 and Simon128.

Besides, under the related-key scenario, Lu et al. [20] presented the best distinguishers for some versions of Simeck by rotational-XOR cryptanalysis. Nevertheless, Simeck has the nonlinear key schedule, which brings a probability to the rotational-XOR transition. In other words, those distinguishers in [20] only exist in the corresponding weak key spaces. Later in [15], Koo et al. proposed the rotational-XOR rectangle (abbreviated as RXR) cryptanalysis, which replaces the differential characteristics by rotational-XOR characteristics in conventional rectangle attack, and then obtained several longer related-key distinguishers for Simon. For instance, they constructed a 16-round RXR distinguisher by exploiting two 8-round rotational-XOR characteristics and utilized this distinguisher to present a 22-round key-recovery attack for Simon32/64. However, the probability of RXR distinguisher might deviate from the theoretical estimations due to some reasons like dependency, key injection, etc. Thus it is significant to provide the experimental verification. But the distinguishers proposed in [15] lack such a verification. In addition, RXR method utilizes two rotational-XOR characteristics, so it is unfriendly to the ciphers with nonlinear key schedules since the final distinguishers have a quite low key probability, which means the distinguishers can only survive in a very small weak key space. It is natural to ask whether there is an alternative approach to utilize rotational-XOR characteristics in the rectangle structure such that the derived distinguishers not only can be verified experimentally but also have a larger, or even full weak key space. This question motivates us to study what will happen if we consider the rotational-XOR and differential characteristics respectively as the upper and lower parts in a rectangle structure.

1.1 Our Contributions

Inspired by the rotational-XOR rectangle cryptanalysis, we propose a novel method in this paper, called *rotational-XOR differential rectangle* (RXDR) cryptanalysis, to construct longer distinguishers for block ciphers. It is an adaption of the rotational-XOR and differential cryptanalysis methods, which is applied in the related-key attacking scenario. To be more specific, we split a cipher E into two parts as $E = E_1 \circ E_0$ and then search rotational-XOR and differential characteristics for E_0 and E_1, respectively. Naturally, linking them in a rectangle-based way can construct a distinguisher. This procedure is similar to the construction of classical rectangle distinguisher, but the distinction is that we replace the differential characteristic by a rotational-XOR characteristic in the upper part (i.e., E_0) of the distinguisher. For the sake of universal understanding, we next call E_0 the rotational-XOR part and E_1 the differential part in a rectangle structure. In our rectangle structure, we can ensure that the difference on keys will be eliminated in the beginning of the differential part, so we only need to consider the single-key differential transition with E_1. Under the random and independent assumptions, the construction and theory of the RXDR cryptanalysis are fully analyzed.

As an illustration, we apply the RXDR method to Simon-like ciphers. First, we discuss the rotational-invariant property on differential characteristics, based on which it becomes easier to evaluate the probability of the differential part. Thus we next exploit the existing best rotational-XOR and differential characteristics to straightforwardly build RXDR characteristics. This is a straightforward and simple way but the obtained RXDR distinguishers are not very long. Apparently, if we consider the differential clustering effect and multiple differentials in the differential part of rectangle structure, better distinguishers can be explored. Based on this idea, we give an improved evaluation on the probability of RXDR distinguishers by exploiting differential clustering effect and multiple differentials. Moreover, for a given output difference, we propose an algorithm based on the method in [17] to calculate the probability of the differential part of rectangle structure. As a consequence, we found RXDR distinguishers covering 16, 16, 17, 16 and 21 rounds with probabilities of $2^{-63.98}$, $2^{-89.78}$, $2^{-89.78}$, $2^{-63.76}$ and $2^{-94.52}$ for Simon32/64, Simon48/72, Simon48/96, Simeck32 and Simeck48, respectively. These concrete RXDR distinguishers are listed in Section 4. Meanwhile, we verified the distinguishers of Simon32/64 and Simeck32 experimentally. The source code is available at `https://github.com/chensivvei/simon-like_RXDR_cryptanalysis.git`.

We list our main results and compare with some published works including rotational-XOR, differential and RXR distinguishers in Table 1. It is worth noting that our distinguisher for Simon32/64 is longer than the differential [19] and rotational-XOR [21] distinguishers. Our RXDR distinguisher for Simon48/72 cannot reach the length of the best differential distinguisher [13] but is longer than the longest rotational-XOR distinguisher [21]. As for Simon48/96, the distinguisher is longer than rotational-XOR [21] distinguisher and is as long as differential distinguisher [13]. It seems that our results cannot reach or surpass the RXR disinguishers [15]. But whether those RXR distinguishers are valid or not needs to be verified experimentally, which was not discussed in [15]. Therefore, our results are indeed more convincing than [15]. For Simeck32, our RXDR distinguisher is longer than the differential distinguisher [9]. Also, it has a full weak key space i.e., 2^{64} weak keys whereas the 16-round rotational-XOR distinguisher presented by Lu et al. [20] has the weak key space of size 2^{36}. As for Simeck48, we cannot find longer RXDR distinguisher than the differential distinguisher [17] or the rotational-XOR distinguisher [20], but our 21-round distinguisher has a better weak key class (2^{72} weak keys) than the 21-round rotational-XOR distinguisher (2^{60} weak keys) presented in [20].

1.2 Organization of This Paper

In Section 2, we give a brief description on Simon-like ciphers and revisit the rotational-XOR and classical rectangle cryptanalysis. In Section 3, we will introduce the basic idea of RXDR cryptanalysis and give an argument on the construction and probability of RXDR characteristics. Later we will apply RXDR method to construct disinguishers for some versions of Simon and Simeck ciphers in Section 4. Finally, we conclude our paper and give a discussion on our results in Section 5.

2 Preliminaries

We first give some notations throughout this paper in Table 2.

2.1 Description of Simon-like Ciphers

Simon [3] is a family of lightweight block ciphers published by the NSA in 2013. A member of the family is denoted by Simon$2n/mn$, where the block size is $2n$

Table 1. Summary on our results (RK = Related-key, SK = Single-key).

Cipher	Round	Method	Scenario	Weak key⋆	Ref.
Simon32/64	13	Rotational-XOR	RK	Full	[21]
	14	Differential	SK	Full	[19]
	16†	RXR	RK	Full	[15]
	16	**RXDR**	RK	Full	**Sect. 4.3**
Simon48/72	13	Rotational-XOR	RK	Full	[21]
	16†	RXR	RK	Full	[15]
	16	**RXDR**	RK	Full	**Sect. 4.3**
	17	Differential	SK	Full	[13]
Simon48/96	15	Rotational-XOR	RK	Full	[21]
	17	Differential	SK	Full	[13]
	17	**RXDR**	RK	Full	**Sect. 4.3**
	18†	RXR	RK	Full	[15]
Simeck32	14	Differential	SK	Full	[9]
	16	Rotational-XOR	RK	2^{36}	[21]
	16	**RXDR**	RK	**Full**	**Sect. 4.3**
	20	Rotational-XOR	RK	2^{30}	[21]
Simeck48	21	Differential	SK	Full	[9]
	21	Rotational-XOR	RK	2^{60}	[21]
	21	**RXDR**	RK	$\mathbf{2^{72}}$	**Sect. 4.3**
	22‡	Differential	SK	Full	[17]
	27	Rotational-XOR	RK	2^{46}	[21]

⋆ If the distinguisher is valid in a key, then we say this key is a weak key. The word "Full" means the weak key space is the full key space, i.e., there are 2^n weak keys if the key is n bits.

† These RXR distinguishers of Simon ciphers had not been verified in [15] whether they are valid or not, even for the 32-bit block version.

‡ In [17], the authors did not give any details on this 22-round differential and only mentioned it in the summary table (Table 7 in [17]) that the 30-round key-recovery attacks could be built using this distinguisher.

for $n \in \{16, 24, 32, 48, 64\}$, and the key size is mn for $m \in \{2, 3, 4\}$. Simon adopts a quite simple round function which includes three bitwise operations: AND($\wedge$), XOR($\oplus$) and cyclic rotation by λ bits (S^{λ}). The round function is defined as

$$f(x) = (S^8(x) \wedge S^1(x)) \oplus S^2(x),$$

where $x \in \mathbb{F}_2^n$ denotes the left branch of the state.

Simon-like ciphers have the same round function as Simon, but the cyclic rotation parameters are different. For arbitrary rotation offsets (a, b, c), the definition of round function is

$$f_{(a,b,c)}(x) = (S^a(x) \wedge S^b(x)) \oplus S^c(x).$$

Table 2. Some notations of this paper.

Notation	Description
$\mathbb{F}_2$	A finite field only contains two elements, i.e. $\{0,1\}$
$\mathbb{F}_2^n$	An n-dimensional vectorial space defined over $\mathbb{F}_2$
$\vee$	Bitwise OR
$\wedge$	Bitwise AND
$\oplus$	Bitwise XOR
$x = (x_{n-1}, \ldots, x_1, x_0)$	Binary vector of n bits where $x_i \in \mathbb{F}_2$
$x \lll \lambda, S^{\lambda}(x)$	Circular left shift of x by λ bits
$x \ggg \lambda, S^{-\lambda}(x)$	Circular right shift of x by λ bits
$\overleftarrow{x}$	Circular left shift of x by 1 bit
$(I \oplus S^{\lambda})(x)$	$x \oplus S^{\lambda}(x)$
$\overline{x}$	Bitwise negation
$wt(x)$	Hamming weight of x
$0^n, 1^n$	The vectors of $\mathbb{F}_2^n$ with all 0s and all 1s
$x \| y$	Concatenation of x and y $(x, y \in \mathbb{F}_2^n)$

In 2015, Yang et al. [28] proposed a family of lightweight block ciphers Simeck. They chose the different rotation offsets in round function, and reuse the round function as its key schedule which leads to better implementation in hareware than Simon. Simeck has three variants: Simeck32/64, Simeck48/96 and Simeck64/128. We represent various versions of Simeck by Simeck$2n$ for $n \in \{16, 24, 32\}$. The rotation offsets for all Simeck versions are (5,0,1). The round function of Simon-like ciphers is depicted in Figure 1.

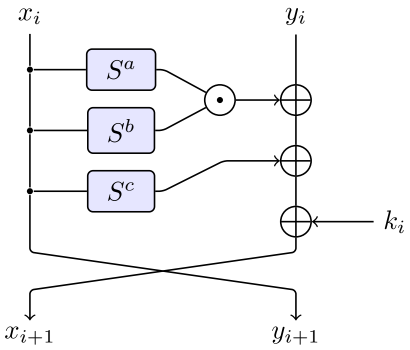


Fig. 1. Round function of Simon-like ciphers.

Simon utilizes a linear key schedule to generate round keys. Let $K = (k^{m-1}, ..., k^1, k^0)$ be a master key and T be the full rounds for Simon$2n/mn$.

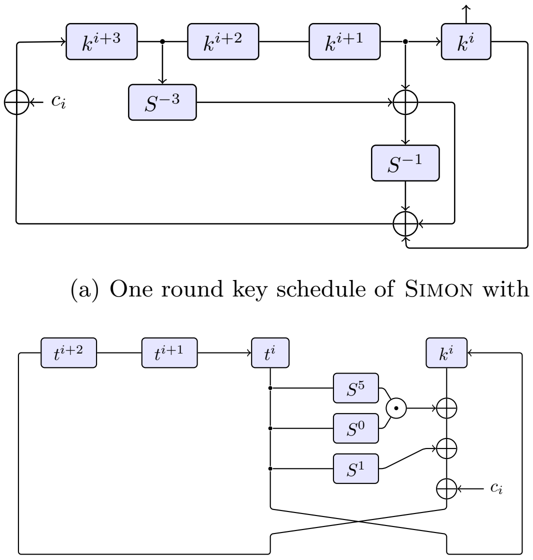
The i-round key k^i is generated by

$$k^{i+m} = \begin{cases} c^i \oplus k^i \oplus (I \oplus S^{-1}) S^{-3} k^{i+1}, & \text{if} \quad m = 2 \\ c^i \oplus k^i \oplus (I \oplus S^{-1}) S^{-3} k^{i+2}, & \text{if} \quad m = 3 \\ c^i \oplus k^i \oplus (I \oplus S^{-1}) (S^{-3} k^{i+3} \oplus k^{i+1}), & \text{if} \quad m = 4 \end{cases}$$

where $c^i \in \{\texttt{0xfffc}, \texttt{0xfffd}\}$ and $0 \leq i < T - m$. The key schedule of Simeck reuses its round function. Let $K = (t^2, t^1, t^0, k^0)$ be the master key of Simeck$2n$. The master key is loaded in the key registers and the round key is updated by

$$\begin{cases} k^{i+1} = t^i \\ t^{i+3} = k^i \oplus f_{(5,0,1)}(t^i) \oplus c^i \end{cases}$$

where $c^i \in \{\texttt{0xfffc}, \texttt{0xfffd}\}$. The key schedules of Simon and Simeck are shown in Figure 2.



(a) One round key schedule of Simon with $m = 4$

(b) One round key schedule of Simeck

Fig. 2. The key schedules of Simon and Simeck.

2.2 Rotational-XOR Cryptanalysis

Rotational cryptanalysis [10,11] is a common attack studying the propagation of rotational pairs. This attack will lose efficacy in the presence of constants since XORing with a constant is not rotational-invariant. Ashur and Liu [1] solved this problem by considering the propagation of rotation and difference for Addition-RX ciphers, which is the so-called rotational-XOR cryptanalysis. Then, Lu et al. [20] extended rotational-XOR cryptanalysis to AND-RX ciphers, especially for the Simon-like ciphers.

An RX-pair is defined as a rotational pair with rotational offset λ under the XOR-difference α as $(x, (x \lll \lambda) \oplus \alpha)$.

Definition 1 (RX-difference [20]). *The RX-difference of x and $x' = (x \lll \lambda) \oplus \alpha$ is denoted by*

$$\Delta_\lambda(x, x') = (x \lll \lambda) \oplus x' = \alpha,$$

where $\alpha \in \mathbb{F}_2^n$ is a constant and λ is a rotational offset with $0 < \lambda < n$.

The propagation of an RX-difference through linear operations of AND-RX ciphers follows three rules [20].

- XOR. The XOR of two input RX-pairs $(x, (x \lll \lambda) \oplus \alpha_1)$ and $(y, (y \lll \lambda) \oplus \alpha_2)$ is also an RX-pair $(x \oplus y, ((x \oplus y) \lll \lambda) \oplus \alpha_1 \oplus \alpha_2)$.
- Cyclic rotation by λ' bits. The cyclic rotation λ' bits of RX-pair $(x, (x \lll \lambda) \oplus \alpha)$ is also an RX-pair $(x \lll \lambda', ((x \lll \lambda) \oplus \alpha) \lll \lambda')$
- XOR with a constant c. The XOR with a constant c of RX-pair $(x, (x \lll \lambda) \oplus \alpha)$ is also an RX-pair $(x \oplus c, (x \lll \lambda) \oplus \alpha \oplus c)$, the corresponding RX-difference is presented by $\Delta_\lambda = c \oplus (c \lll \lambda)$.

From the above rules we know that an RX-difference after performing linear operations is a new RX-difference with a probability of 1. As for the nonlinear operation AND, the RX-difference propagation is given by following proposition:

Proposition 1 ([20]). *For $f(x) = S^a(x) \wedge S^b(x)$ where $gcd(n, a-b) = 1$, n is even, $a > b$ and $x = (x_{n-1}, ..., x_1, x_0) \in \mathbb{F}_2^n$, the probability distribution that α goes to β through f is*

$$\Pr(\alpha \xrightarrow{f} \beta) = \begin{cases} 2^{-n+1} & \textit{if } \alpha = 1^n \textit{ and } wt(\beta) \equiv 0 \mod 2, \\ 2^{-w} & \textit{if } \alpha \neq 1^n \textit{ and } \beta \wedge (\overline{S^a(\alpha) \vee S^b(\alpha)}) = 0^n \textit{ and} \\ & (\beta \oplus S^{a-b}(\beta)) \wedge (\overline{S^a(\alpha)} \wedge S^{2a-b}(\alpha) \wedge S^b(\alpha)) = 0^n, \\ 0 & \textit{otherwise}, \end{cases}$$

where $w = wt((\overline{S^a(\alpha) \vee S^b(\alpha)} \oplus (\overline{S^a(\alpha)} \wedge S^{2a-b}(\alpha) \wedge S^b(\alpha)))$.

2.3 Rectangle Cryptanalysis

The rectangle attack [5] is a differential-based attack that uses two short differential characteristics instead of one long differential characteristic. This attack is originally based on boomerang attacks [25], which is an adaptive chosen plaintext and ciphertext attack. The rectangle attack has a similar structure to the boomerang attack, but it is a chosen plaintext attack by a slight change of boomerang. This technique is very useful when we have good short differential characteristics but bad long ones.

Let a cipher $E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ consist of two independent sub-encryptions E_0 and E_1 as $E = E_1 \circ E_0$. Assume that we have a differential characteristic $\alpha \rightarrow \beta$ with probability p for E_0 and a differential characteristic $\gamma \rightarrow \delta$ with probability q for E_1. For a given plaintext tuple (P_1, P_2, P_3, P_4) where P_1 is independent to P_3, the intermediate states encrypted by E_0 and the ciphertexts encrypted by E are denoted by (P'_1, P'_2, P'_3, P'_4) and (C_1, C_2, C_3, C_4). The specified attack is to construct a plaintext quartet (P_1, P_2, P_3, P_4) that satisfies the conditions that $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$, $P'_1 \oplus P'_2 = P'_3 \oplus P'_4 = \beta$ and $P'_1 \oplus P'_3 = \gamma$ with probability $p^2 \cdot 2^{-n}$. Under these conditions, it is easy to conclude $P'_2 \oplus P'_4 = \gamma$. When encrypting (P'_1, P'_2, P'_3, P'_4) by E_1, the difference γ goes to δ with probability q. Then $C_1 \oplus C_3 = \delta$ and $C_2 \oplus C_4 = \delta$ hold with probability q^2. We call a quartet (P_1, P_2, P_3, P_4) whose ciphertexts meet the condition $C_1 \oplus C_3 = \delta$ and $C_2 \oplus C_4 = \delta$ a right quartet, and the probability of a quartet being right is $p^2 \cdot q^2 \cdot 2^{-n}$.

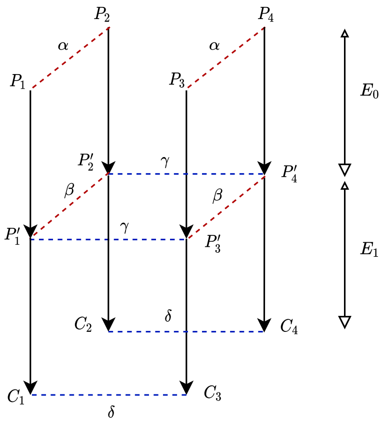


Fig. 3. Right quartet for rectangle attack.

If E is a random permutation, then the probability of having a specific difference in the output is 2^{-2n} for a random tuple (P_1, P_2, P_3, P_4). When $p^2 \cdot q^2 \cdot 2^{-n} > 2^{-2n}$, namely, $p \cdot q > 2^{-n/2}$, we can obtain a valid rectangle distinguisher.

3 Rotational-XOR Differential Rectangle Cryptanalysis

In this section, we introduce the rotational-XOR differential rectangle (RXDR) cryptanalysis, which is composed of rotational-XOR, differential and rectangle cryptanalysis. For a given block cipher $E : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$, we split it into two independent parts as $E = E_1 \circ E_0$. The classical rectangle cryptanalysis considers two short differential characteristics with higher probability covering E_0 and E_1. The basic idea of RXDR is similar to the classical rectangle cryptanalyis, but we consider the rotational-XOR and differential characteristics respectively for the upper and lower parts in our RXDR structure (see Figure 4). In other words, E_1 still utilizes a traditional differential characteristic but E_0 adopts a rotational-XOR characteristic with high probability and large weak key space.

Because rotational-XOR cryptanalysis is a kind of related-key attack, RX-difference propagation also exists in the key schedule and will cause probability when the key schedule is nonlinear. Assuming that we have a rotational-XOR characteristic $\alpha \xrightarrow{E_0} \beta$ with a probability of p, and the corresponding rotational-XOR characteristic w.r.t. the key is $\Delta_I \xrightarrow{E_0} \Delta_O$, which has a probability of p_k. Note that Δ_I and Δ_O are not necessarily related to α and β. In addition, we have a differential characteristic $\gamma \xrightarrow{E_1} \delta$ with probability q for the encryption E_1. For the given plaintext tuple (P_1, P_2, P_3, P_4) and master key tuple (K_1, K_2, K_3, K_4), we denote the tuples (P'_1, P'_2, P'_3, P'_4) and (C_1, C_2, C_3, C_4) the intermediate states and the ciphertexts encrypted by E_0 and E, respectively, i.e. $P'_i = E_0(P_i, K_i)$, $C_i = E_1(P'_i, K_i)$ for $i \in \{1, 2, 3, 4\}$. In addition, we denote K'_i the round key XORed with P'_i, which is derived from K_i by the key schedule.

The rotational-XOR part. Let us first focus on the propagation of RX-difference through the encryption E_0. We suppose (P_1, P_2) and (P_3, P_4) are RX-pairs with a rotation offset λ and an RX-difference α. Namely, $(P_1 \lll \lambda) \oplus P_2 = \alpha$, $(P_3 \lll \lambda) \oplus P_4 = \alpha$. Assume that there exists a rotational-XOR characteristic $\alpha \xrightarrow{E_0} \beta$ with probability p. Under the condition that (K_1, K_2, K_3, K_4) and (K'_1, K'_2, K'_3, K'_4) respectively satisfy the key RX-difference Δ_I and Δ_O, i.e.

$$(K_1 \lll \lambda) \oplus K_2 = \Delta_I,\ (K_3 \lll \lambda) \oplus K_4 = \Delta_I$$

and

$$(K'_1 \lll \lambda) \oplus K'_2 = \Delta_O,\ (K'_3 \lll \lambda) \oplus K'_4 = \Delta_O,$$

thus the probability that the RX-difference α can propagate to β on the both sides by E_0 is p^2. That is to say, the probability that $(P'_1 \lll \lambda) \oplus P'_2 = \beta$ and $(P'_3 \lll \lambda) \oplus P'_4 = \beta$ hold simultaneously is p^2 under the weak key space of size $2^{2k} \cdot p_k^2$.

The differential part. Now we consider the differential propagation through the encryption E_1. Denote γ' and γ'' the input differences of E_1, i.e. $\gamma' = (P'_1 \oplus K'_1) \oplus (P'_3 \oplus K'_3)$ and $\gamma'' = (P'_2 \oplus K'_2) \oplus (P'_4 \oplus K'_4)$. Before giving further illustrations, we need to introduce the following proposition.

Proposition 2. *If (P'_1, P'_2) and (P'_3, P'_4) are RX pairs with the rotation offset λ and the RX-difference β, meanwhile (K'_1, K'_2) and (K'_3, K'_4) satisfy the corresponding key RX-difference Δ_O, then we have $\gamma'' = \gamma' \lll \lambda$.*

Proof. From the structure, we know $\gamma'' = (P_2' \oplus P_4') \oplus (K_2' \oplus K_4')$. Due to the fact that (P_1', P_2') and (P_3', P_4') are RX pairs, and (K_1', K_2') and (K_3', K_4') satisfy the corresponding key RX-difference, thus we have

$$(P_1' \lll \lambda) \oplus P_2' = \beta,\ (P_3' \lll \lambda) \oplus P_4' = \beta$$

and

$$(K_1' \lll \lambda) \oplus K_2' = \Delta_O,\ (K_3' \lll \lambda) \oplus K_4' = \Delta_O.$$

The above relations imply that

$$P_2' \oplus P_4' = ((P_1' \lll \lambda) \oplus \beta) \oplus ((P_3' \lll \lambda) \oplus \beta) = (P_1' \oplus P_3') \lll \lambda$$

and

$$K_2' \oplus K_4' = ((K_1' \lll \lambda) \oplus \Delta_O) \oplus ((K_3' \lll \lambda) \oplus \Delta_O) = (K_1' \oplus K_3') \lll \lambda.$$

Therefore, γ'' can be represented as

$$\begin{aligned}\gamma'' &= ((P_1' \oplus P_3') \lll \lambda) \oplus ((K_1' \oplus K_3') \lll \lambda) \\ &= ((P_1' \oplus P_3') \oplus (K_1' \oplus K_3')) \lll \lambda \\ &= \gamma' \lll \lambda.\end{aligned}$$

□

If (P_1', P_2', P_3', P_4') and (K_1', K_2', K_3', K_4') satisfy the output pattern of the aforementioned rotational-XOR characteristic, Proposition 2 indicates that the input differences γ' and γ'' of E_1 are equivalent under the rotation. Note that γ' and γ'' are related to the round keys. In other words, we have to study the difference not only on the data but also on the round key, which will cause some trouble constructing a good RXDR distinguisher especially for the nonlinear key schedules. In order to eliminate the influence of the round key, we let $K_3 = K_1$ and $K_4 = K_2$. In this case, $K_3' = K_1'$ and $K_4' = K_2'$ hold naturally, thus γ' and γ'' become the single-key differences and the number of weak keys can be estimated as $2^k \cdot p_k$. In this way, we only need to study the single-key differential of E_1. What we expect is that γ' or γ'' is equal to the predetermined γ, which can propagate to δ through E_1 with a high probability of q. Without loss of generality, we devote our attention to γ'. Since P_1 and P_3 can be chosen randomly and independently, the corresponding P_1' and P_3' also stay independent from each other and $\gamma' = P_1' \oplus P_3' = \gamma$ will hold with probability 2^{-n} under the assumption of randomness and independency. Besides, Proposition 2 tells us $\gamma'' = \gamma' \lll \lambda = \gamma \lll \lambda$. Hence, we can use the state-of-the-art method to search an optimal differential characteristic $(\gamma \lll \lambda) \xrightarrow{E_1} \delta^*$ with probability q^*. In this case, the differences on ciphertext pairs (C_1, C_3) and (C_2, C_4) are equal to δ and δ^* with probability $2^{-n} \cdot q \cdot q^*$.

The RXDR characteristic. As a consequence, if the chosen plaintext tuple (P_1, P_2, P_3, P_4) and the master key tuple (K_1, K_2, K_3, K_4) satisfy the input patterns of the rotational-XOR characteristic $\alpha \xrightarrow{E_0} \beta$ and $\Delta_I \xrightarrow{E_0} \Delta_O$, i.e.,

$$(P_i \lll \lambda) \oplus P_{i+1} = \alpha,\ (K_i \lll \lambda) \oplus K_{i+1} = \Delta_I,\ i = 1, 3$$

and $K_3 = K_1$, $K_4 = K_2$, then the probability that the corresponding ciphertexts satisfy $C_1 \oplus C_3 = \delta$ and $C_2 \oplus C_4 = \delta^*$ is

$$Pr = p^2 \cdot 2^{-n} \cdot q \cdot q^* \tag{1}$$

under the weak key space of $2^k \cdot p_k$. Naturally, if the above probability is larger than 2^{-2n}, i.e. $p^2 \cdot q \cdot q^* > 2^{-n}$, we can utilize the aforementioned rotational-XOR and differential characteristics to form a right quartet. We call this quartet an RXDR characteristic as depicted in Figure 4.

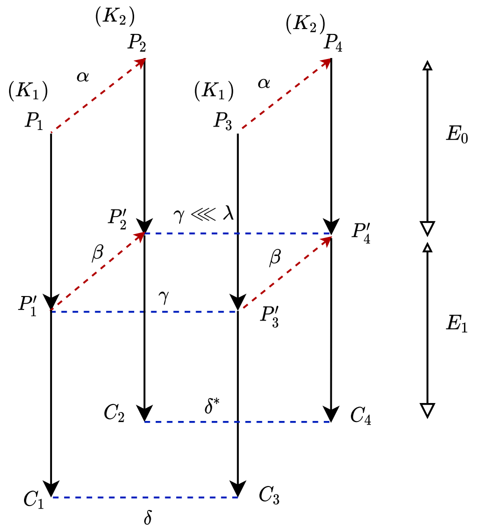


Fig. 4. RXDR characteristic.

Equation (1) gives us two directions to construct RXDR characteristics with longer rounds or higher probability. The first one is to find better rotational-XOR characteristics to improve the value of p^2. Another one is to find a difference γ such that $q \cdot q^*$ is the best, where q (q^*) is the optimal probability that the difference γ $(\gamma \lll \lambda)$ goes through E_1.

4 RXDR Distinguishers of Simon-like Ciphers

In this section, we will construct RXDR distinguishers for Simon-like ciphers. We first introduce the rotational-invariant property on differential characteristics of Simon-like ciphers. Then we find some RXDR characteristics by searching optimal rotational-XOR characteristics and using the existing optimal differential characteristics. Moreover, we exploit the differential clustering effect of Simon-like ciphers as well as multiple differentials to successfully extend RXDR distinguishers.

4.1 The Rotational-invariant Property on Differential Characteristics

Note that the round function of a Simon-like cipher is composed of bitwise AND, XOR and rotation operations. Thus, it is of great significance to study the propagation of a rotated difference through the round function and the encryption E_1. We present the relationship between the propagations of a difference and its rotated difference for Simon-like ciphers as the following proposition.

Proposition 3. *For Simon-like ciphers, let f denote the core function applied to the left branch. If $\mu \xrightarrow{f} \nu$ is a non-trivial differential characteristic with probability q, then $\overleftarrow{\mu} \xrightarrow{f} \overleftarrow{\nu}$ is also a non-trivial differential characteristic with probability q.*

Before proving this conclusion, we first give Kölbl et al.'s theory as follows.

Theorem 1 ([13]). *Let $f(x) = S^a(x) \wedge S^b(x) \oplus S^c(x)$, where $gcd(n, a-b) = 1$, n is even, and $a > b$. Let μ and ν be the input and output difference of $f(x)$. Let*

$$varibits = S^a(\mu) \vee S^b(\mu)$$

and

$$doublebits = S^b(\mu) \wedge \overline{S^a(\mu)} \wedge S^{2a-b}(\mu)$$

and

$$\eta = \nu \oplus S^c(\mu).$$

We have that the probability that difference μ goes to difference ν is

$$\Pr(\mu \xrightarrow{f} \nu) = \begin{cases} 2^{-n+1} & \textit{if } \mu = 1^n \textit{ and } wt(\eta) \equiv 0 \mod 2, \\ 2^{-wt(varibits \oplus doublebits)} & \textit{if } \mu \neq 1^n \textit{ and } \eta \wedge (\overline{varibits}) = 0^n \\ & \textit{and } (\eta \oplus S^{a-b}(\eta)) \wedge doublebits = 0^n, \\ 0 & \textit{otherwise.} \end{cases}$$

We reuse some notations defined in Theorem 1 and now proceed to prove Proposition 3.

Proof. We assume that $\Pr(\mu \xrightarrow{f} \nu) = q$ and now need to prove $\Pr(\overleftarrow{\mu} \xrightarrow{f} \overleftarrow{\nu}) = q$. Because $\mu \xrightarrow{f} \nu$ is non-trivial, we only need to consider the two former cases in Theorem 1 as follows:

- Assuming that $\mu = 1^n$ and $wt(\nu \oplus S^c(\mu)) \equiv 0 \mod 2$, then we have $q = 2^{-n+1}$. It is obvious that $\overleftarrow{\mu} = 1^n$ holds due to $\mu = 1^n$. The Hamming weight of a vector will not be changed when it is rotated, thus
$$wt(\overleftarrow{\nu} \oplus S^c(\overleftarrow{\mu})) = wt(\overleftarrow{\nu \oplus S^c(\mu)}) = wt(\nu \oplus S^c(\mu)) \equiv 0 \mod 2,$$
which implies that $\Pr(\overleftarrow{\mu} \xrightarrow{f} \overleftarrow{\nu}) = 2^{-n+1} = q$.
- Assuming that $\mu \neq 1^n$ and $\eta \wedge (\overline{varibits}) = 0^n$ and $(\eta \oplus S^{a-b}(\eta)) \wedge doublebits = 0^n$, then we have $q = 2^{-wt(varibits \oplus doublebits)}$. In this case, $\overleftarrow{\mu} \neq 1^n$ holds due to $\mu \neq 1^n$. Note that η, *varibits* and *doublebits* are calculated by a series of bitwise rotation, AND, OR and NOT operations on μ and ν, thus if $\eta \wedge (\overline{varibits})$ and $(\eta \oplus S^{a-b}(\eta)) \wedge doublebits$ both are equal to 0^n then any rotation on μ and ν will not change the values of $\eta \wedge (\overline{varibits})$ and $(\eta \oplus S^{a-b}(\eta)) \wedge doublebits$. Moreover, the Hamming weight of $varibits \oplus doublebits$ is also unchanged. Therefore, $\Pr(\overleftarrow{\mu} \xrightarrow{f} \overleftarrow{\nu}) = q$.

On summary, $\Pr(\overleftarrow{\mu} \xrightarrow{f} \overleftarrow{\nu}) = \Pr(\mu \xrightarrow{f} \nu) = q$. □

Based on Proposition 3, the following conclusion can be easily deduced.

Proposition 4. *Let $\mathcal{E}$ denote the one-round encryption of a Simon-like cipher and $\mathcal{E}^i (i > 0)$ denote i-round iterative encryption. If $(\gamma_L, \gamma_R) \xrightarrow{\mathcal{E}^r} (\delta_L, \delta_R)$ is an r-round differential characteristic with a probability of q where γ_L and γ_R respectively denote the input differences on the left and right branches, then there must exist an r-round differential characteristic $(\overleftarrow{\gamma_L}, \overleftarrow{\gamma_L}) \xrightarrow{\mathcal{E}^r} (\overleftarrow{\delta_L}, \overleftarrow{\delta_R})$ with the probability q.*

Proof. Let $(\delta_L^0, \delta_R^0) \xrightarrow{\mathcal{E}} (\delta_L^1, \delta_R^1) \xrightarrow{\mathcal{E}} \cdots \xrightarrow{\mathcal{E}} (\delta_L^r, \delta_R^r)$ be one of the differential propagation trails of $(\gamma_L, \gamma_R) \xrightarrow{\mathcal{E}^r} (\delta_L, \delta_R)$, where $(\gamma_L, \gamma_R) = (\delta_L^0, \delta_R^0)$ and $(\delta_L, \delta_R) = (\delta_L^r, \delta_R^r)$. Assuming that the ith round differential propagation $(\delta_L^{i-1}, \delta_R^{i-1}) \xrightarrow{\mathcal{E}} (\delta_L^i, \delta_R^i)$ holds with a probability of q_i for $i \in \{1, 2, ..., r\}$, thus $q = \prod_{i=1}^r q_i$. Moreover, we can deduce from Proposition 3 that $(\overleftarrow{\delta_L^{i-1}}, \overleftarrow{\delta_R^{i-1}}) \xrightarrow{\mathcal{E}} (\overleftarrow{\delta_R^i}, \overleftarrow{\delta_R^i})$ also holds with the probability q_i. Therefore, we can concatenate the r rotated differential propagations into a differential characteristic as $(\overleftarrow{\delta_L^0}, \overleftarrow{\delta_R^0}) \xrightarrow{\mathcal{E}} (\overleftarrow{\delta_L^1}, \overleftarrow{\delta_R^1}) \xrightarrow{\mathcal{E}} \cdots \xrightarrow{\mathcal{E}} (\overleftarrow{\delta_L^r}, \overleftarrow{\delta_R^r})$ with a probability of $\prod_{i=1}^r q_i$. Namely, $(\overleftarrow{\gamma_L}, \overleftarrow{\gamma_L}) \xrightarrow{\mathcal{E}^r} (\overleftarrow{\delta_L}, \overleftarrow{\delta_R})$ is an r-round differential characteristic with the probability q. □

The above proposition illustrates the *rotational-invariant* property on differential characteristics of Simon-like ciphers. This will facilitate the construction of the differential part in our RXDR structure.

4.2 RXDR Characteristics of Simon-like ciphers

As we discussed in Section 3, we first need to prepare a good rotational-XOR characteristic for E_0. Some previous works [1,20,21] indicate that the rotational-XOR characteristic is optimal when the rotation offset of an RX-difference is fixed to 1 (i.e., $\lambda = 1$). Thus we consider $\lambda = 1$ by default in the following content. Additionally, if we find an optimal differential characteristic $(\gamma_L, \gamma_R) \to (\delta_L, \delta_R)$ for E_1 with probability q, then according to Proposition 4, the differential characteristic $(\overleftarrow{\gamma_L}, \overleftarrow{\gamma_R}) \to (\overleftarrow{\delta_L}, \overleftarrow{\delta_R})$ is indeed optimal and the corresponding probability is equal to q. As a result, the RXDR characteristic has a probability of

$$Pr = p^2 \cdot 2^{-n} \cdot q^2 \tag{2}$$

due to Equation (1), where p is the probability of the optimal rotational-XOR characteristic of E_0.

According to the above analysis, we can simply construct some RXDR characteristics using the rotational-XOR characteristics in [21] and the optimal differential characteristics in [13,14,19].

RXDR characteristics of Simon32 and Simon48. In order to construct RXDR characteristics, we first need to prepare some good rotational-XOR and differential characteristics. The rotational-XOR characteristics for Simon are given in [21]. We list them in the top sub-table of Table 3. Note that the key schedules of Simon family are linear, thus the RX-difference through key schedules will not bring probability. That is to say, the key probability is always equal to 1, i.e. $p_k = 1$. In addition, we list several published optimal differential characteristics of Simon32 and Simon48 from [13] in the bottom sub-table of Table 3.

Table 3. The optimal rotational-XOR and optimal differential characteristics of Simon32 and Simon48. The corresponding optimal probabilities are given as $\log_2(p)$ and $\log_2(q)$.

(a) The optimal rotational-XOR characteristics of Simon32 and Simon48.

Round	6	7	8	9	10	11	12	13	14	15	16
Simon32/64	0	-4	-6	-10	-14	-20	-24	-30	-32	-	-
Simon48/72	-2	-4	-8	-12	-16	-26	-36	-40	-48	-	-
Simon48/96	0	-4	-4	-10	-14	-24	-32	-32	-38	-46	-

(b) The optimal differential characteristics of Simon32 and Simon48.

Round	1	2	3	4	5	6	7	8	9	10	11
Simon32	0	-2	-4	-6	-8	-12	-14	-18	-20	-25	-30
Simon48	0	-2	-4	-6	-8	-12	-14	-18	-20	-26	-30

By appropriately combining rotational-XOR and differential characteristics from Table 3, we can easily construct some RXDR characteristics. The corresponding probabilities are calculated using Equation (2). We only list the optimal

RXDR characteristics of Simon32 and Simon48 in Table 4. An RXDR characteristic is a significant distinguisher when its probability follows $p^2 \cdot 2^{-n} \cdot q^2 > 2^{-2n}$, i.e., $p^2 \cdot q^2 > 2^{-n}$. From Table 4, the longest RXDR characteristics for Simon32/64, Simon48/72 and Simon48/96 are 13 (6+7), 15 (6+9) and 16 (8+8) rounds with probabilities of 2^{-60}, 2^{-92} and 2^{-92}, respectively. The details of these optimal RXDR characteristics are listed in Appendix A.

Table 4. The optimal RXDR characteristics of Simon32 and Simon48. The probabilities are given as $\log_2(p^2 \cdot q^2)$, where p and q are probabilities of the rotational-XOR and differential characteristics, respectively.

Round	7	8	9	10	11	12	**13**	14	**15**	**16**	17
Combination[†]	6+1	6+2	6+3	6+4	6+5	6+6	**6+7**	6+8	6+9	7+9	8+9
Simon32/64	0	-4	-8	-12	-16	-24	**-28**	-36	-40	-48	-52
Combination	6+1	6+2	6+3	6+4	6+5	7+5	6+7	7+7	**6+9**	7+9	8+9
Simon48/72	-4	-8	-12	-16	-20	-24	-32	-36	**-44**	-48	-56
Combination	6+1	6+2	6+3	6+4	6+5	8+4	8+5	8+6	8+7	**8+8**	8+9
Simon48/96	0	-4	-8	-12	-16	-20	-24	-32	-36	**-44**	-48

[†] The combination $a+b$ means this optimal RXDR characteristic is constructed using a-round rotational-XOR characteristic and b-round differential characteristic. Some optimal RXDR characteristics have more than one combinations, here we only list one of them.

RXDR characteristics of Simeck32 and Simeck48. The rotational-XOR characteristics for short rounds are not given in [21], which have the potential to form a better RXDR characteristic. Thus here we use the SAT/SMT method [21] to search 6 to 9 rounds characteristics for Simeck32 and 6 to 14 rounds for Simeck48. Note that the key schedules of Simeck family are nonlinear, thus a rotational characteristic is composed of the data and key probabilities. We list our short rotational-XOR characteristics and some results from [20] in the top sub-table of Table 5. Besides, the optimal differential characteristics provided by [19] are listed in the bottom sub-table of Table 5.

By combining rotational-XOR and differential characteristics of Table 5, we obtain the optimal RXDR characteristics as illustrated in Table 6. Under the condition of $p^2q^2 > 2^{-n}$, the longest characteristics of Simeck32 and Simeck48, which can be used as significant distinguishers, are 15 and 20 rounds with probabilities of 2^{-60} and 2^{-92}. The details of the longest characteristics can be found in Appendix A.

4.3 Exploiting the Differential Clustering Effect and Multiple Differentials to Construct Better RXDR Distinguishers

The previous work [13,14,19,17] indicates that there exists a very strong differential clustering effect on Simon-like ciphers. Differential distinguishers can

Table 5. The rotational-XOR and optimal differential characteristics of Simeck32 and Simeck48. The data and key probabilities of the rotational-XOR characteristic are denoted by p and p_k, and the probability of the differential characteristic is given as $\log_2(q)$.

Round	6	7	8	9	10	11	12	13	14	15	16	17	18
Simeck32													
$\log_2(p)$	0	-2	-4	-4	-6	-10	-12	-12	-16	-18	-18	-18	-22
$\log_2(p_k)$	0	0	-2	-6	-8	-12	-12	-18	-18	-20	-28	-32	-30
Simeck48													
$\log_2(p)$	0	-2	-4	-4	-6	-8	-10	-12	-12	-18	-18	-18	-22
$\log_2(p_k)$	0	0	-2	-6	-8	-16	-20	-18	-24	-20	-28	-32	-30
Round	1	2	3	4	5	6	7	8	9	10	11	12	13
Simeck32	0	-2	-4	-6	-8	-12	-14	-18	-20	-24	-26	-30	-32
Simeck48	0	-2	-4	-6	-8	-12	-14	-18	-20	-24	-26	-30	-32

Table 6. The optimal RXDR characteristics of Simeck32 and Simeck48. The data and key probabilities are given as $\log_2(p^2q^2)$ and $\log_2(p_k)$.

(a) The optimal RXDR characteristics of Simeck32.

Round	7	8	9	10	11	12	13	14	**15**	16
Combination	6+1	6+2	6+3	9+1	9+2	9+3	9+4	9+5	**10+5**	13+3
$\log_2(p^2q^2)$	0	-4	-8	-8	-12	-16	-20	-24	**-28**	-32
$\log_2(p_k)$	0	0	0	-6	-6	-6	-6	-6	**-8**	-18

(b) The optimal RXDR characteristics of Simeck48.

Round	12	13	14	15	16	17	18	19	**20**	21
Combination	9+3	9+4	9+5	14+1	14+2	13+4	17+1	17+2	**17+3**	17+4
$\log_2(p^2q^2)$	-16	-20	-24	-24	-28	-32	-36	-40	**-44**	-48
$\log_2(p_k)$	-6	-6	-6	-24	-24	-24	-24	-24	**-32**	-32

be greatly improved by summing over partial or all differential paths that start from and end up with the same input and output differences. Similarly, we can exploit the clustering effect on the differential part in our RXDR structure to improve the probability or extend the round number of RXDR distinguishers.

Differential clustering effect. For a Simon-like cipher, we prepare a rotational-XOR characteristic for the r_0-round encryption with data and key probabilities of p and p_k, respectively. Assume that we find N differential characteristics for the r_1-round encryption that start from the difference γ and end up with the difference δ. Moreover, the i-th differential characteristic has a probability of q_i $(i \in \{1, 2, ..., N\})$. Then according to Equation 2, an $(r_0 + r_1)$-round

RXDR characteristic can be derived using the i-th differential characteristic with probability

$$p^2 \cdot 2^{-n} \cdot q_i^2.$$

By summing over N differential characteristics, we can obtain an r_1-round differential $\gamma \to \delta$ with probability $\hat{q}$ where $\hat{q} = \sum_{i=1}^{N} q_i$. Note that the rotational-invariant property is also applicable to differentials of Simon-like ciphers. Therefore we can utilize the differential to construct an $(r_0 + r_1)$-round RXDR distinguisher with a higher probability, that is

$$Pr = p^2 \cdot 2^{-n} \cdot \hat{q}^2. \tag{3}$$

Multiple differentials. An RXDR distinguisher only focuses on the differences of the ciphertext pairs (C_1, C_3) and (C_2, C_4) as shown in Figure 4. In other words, we can take multiple differentials into account as long as these differentials share the same output difference. This can further improve the probability of RXDR distinguishers. Note that there are 2^n possible input differences of the differential part in our RXDR structure since the plaintext P_1 is independent to P_3. For a fixed output difference δ, if we consider its 2^n multiple differentials and the i-th differential is $\gamma_i \to \delta$ $(i \in \{1, 2, ..., 2^n\})$ with a probability of $\hat{q}_i$, then we can use the prepared rotational-XOR characteristic and these 2^n multiple differentials to construct an RXDR distinguisher with a greatly improved probability, which is calculated as

$$Pr = \sum_{i=1}^{2^n} (p^2 \cdot 2^{-n} \cdot \hat{q}_i^2) = p^2 \cdot 2^{-n} \cdot \tilde{q} \tag{4}$$

due to Equation (3), where $\tilde{q} = \sum_{i=1}^{2^n} \hat{q}_i^2$.

Calculation of $\tilde{q}$. According to the above analysis, we need to find an output difference δ such that the corresponding probability $\tilde{q}$ is as large as possible. Note that the encryption is indeed identical to the decryption for Simon-like ciphers, which tells us that the differentials $(\gamma_L, \gamma_R) \to (\delta_L, \delta_R)$ and $(\delta_R, \delta_L) \to (\gamma_R, \gamma_L)$ have the same probability. Therefore for a given output difference (δ_L, δ_R), we can regard (δ_R, δ_L) as the input difference to calculate its multiple differentials. In [17], the authors investigated the clustering effect on Simon-like ciphers and proposed an efficient method to calculate the probability of differentials by calculating the differential transition matrix (DTM). The core idea of their method is to only consider the lowest w $(w \leq 2/n)$ active bits of the difference in each branch. The parameter w is the so-called *window*. Thus the scale of the DTM is decreased from $2^n \times 2^n$ to $2^{2w} \times 2^{2w}$. Based on their method we can calculate 2^{2w} differentials and the corresponding probability $\tilde{q}$ when the output difference (δ_L, δ_R) is given. We illustrate the brief procedure in Algorithm 2 of Appendix C.

Better RXDR distinguishers for Simon32 and Simon48. We choose $(\texttt{0x2022}, \texttt{0x8})$ and $(\texttt{0x222}, \texttt{0x80})$ as the output difference (δ_L, δ_R) for Simon32 and Simon48, which are derived using the SAT/SMT method [13]. In addition, we fix the window $w = 16$ for Simon32 and $w = 17$ for Simon48 due to the limitation of our computation power. By Algorithm 2, we obtain the probability of the best differential ($\hat{q}_B$) and the sum on squared probabilities of multiple differentials ($\tilde{q}$) as shown in Table 7. The probability produced by differential part increases significantly compared with only considering the single differential characteristic. For example, the optimal single differential characteristic of 8-round Simon32/64 has a probability of 2^{-18} (in Table 3), which means it will produce 2^{-36} to the probability of RXDR structure. Nevertheless, Table 7 shows this probability is $2^{-27.92}$.

Table 7. The probabilities $\hat{q}_B$ and $\tilde{q}$ for Simon32 (left) and Simon48 (right).

Round	$\log_2(\hat{q}_B)$	$\log_2(\tilde{q})$	$\log_2(\hat{q}_B)$	$\log_2(\tilde{q})$
1	-2	-2	-2	-2
2	-6	-6.8300	-6	-7.4150
3	-8	-12.1784	-8	-12.6784
4	-9.2996	-15.3273	-9.2996	-15.8947
5	-9.2996	-17.7060	-9.2996	-18.0040
6	-11.2996	-20.3584	-11.2996	-20.5348
7	-13.2995	-23.7946	-13.2996	-24.0664
8	-16.5986	-27.9198	-16.5991	-28.5694
9	-18.5968	-31.3192	-18.5991	-33.7847
10	-23.3970	31.9834	-23.6518	-41.0640
11	-26.8462	-31.9996	-27.0840	-48.9414

Combining with the rotational-XOR characteristics in Table 3, several longer RXDR distinguishers can be constructed. We list them in Table 8. Our results show that the longest significant RXDR distinguishers are extended from 13, 15 and 15 rounds to 16, 16, 17 rounds for Simon32/64, Simon48/72 and Simon48/96 respectively after taking the differential clustering effect and multiple differentials into consideration. The details of the longest distinguishers are listed in Appendix B.

Better RXDR distinguishers for Simeck32 and Simeck48. We use the SAT/SMT method [13] to search several optimal differential characteristics, from which we choose the output difference (δ_L, δ_R) for our RXDR structure. As a result, we choose $(\texttt{0x15}, \texttt{0x8})$ and $(\texttt{0x28}, \texttt{0x10})$ for Simeck32 and Simeck48. Moreover, similarly to Simon, we fix $w = 16$ and $w = 17$ respectively for the two versions of Simeck to calculate the probabilities $\hat{q}_B$ and $\tilde{q}$ by Algorithm 2. The results are listed in Table 9.

By combining the rotational-XOR characteristics in Table 5, we construct better RXDR distinguishers as listed in Table 10. Compared with the optimal RXDR characteristics in Table 6, we can improve the weak key classes of RXDR distinguishers for 14- and 15-round Simeck32 and extend the longest RXDR

Table 8. Some RXDR distinguishers of Simon32 and Simon48.

Version	Round[†]	Input RX-diff.	Output diff.	Prob.($> 2^{-2n}$)
Simon32/64	14 $(6+8)$	(0x0, 0x6)	(0x2022, 0x8)	$2^{-59.92}$
Simon32/64	15 $(6+9)$	(0x0, 0x6)	(0x2022, 0x8)	$2^{-63.32}$
Simon32/64	16 $(6+10)$	(0x0, 0x6)	(0x2022, 0x8)	$2^{-63.98}$
Simon48/72	15 $(7+8)$	(0x0, 0x3e)	(0x222, 0x80)	$2^{-84.57}$
Simon48/72	16 $(7+9)$	(0x0, 0x3e)	(0x222, 0x80)	$2^{-89.78}$
Simon48/96	15 $(6+9)$	(0x0, 0x6)	(0x222, 0x80)	$2^{-81.78}$
Simon48/96	16 $(8+8)$	(0x0, 0x180016)	(0x222, 0x80)	$2^{-84.57}$
Simon48/96	17 $(8+9)$	(0x0, 0x180016)	(0x222, 0x80)	$2^{-89.78}$

[†] This number r (r_0+r_1) means that the r-round RXDR distinguisher is formed by the r_0- and r_1-round rotational-XOR and differential structures.

Table 9. The probabilities $\hat{q}_B$ and $\tilde{q}$ for Simeck32 (left) and Simeck48 (right).

Round	$\log_2(\hat{q}_B)$	$\log_2(\tilde{q})$	$\log_2(\hat{q}_B)$	$\log_2(\tilde{q})$
1	-2	-2	-2	-2
2	-6	-7	-4	-5.2996
3	-8	-12.1466	-4	-7.2270
4	-9.2996	-15.3131	-6	-9.7971
5	-9.2996	-17.6736	-8	-13.2161
6	-11.2996	-20.3091	-11.2996	-17.5076
7	-13.2980	-23.7652	-13.2986	-22.5177
8	-16.5960	-27.8889	-18.2765	-28.4986
9	-18.5931	-31.3817	-19.8362	-33.6676
10	-23.5341	-31.9843	-22.2135	-37.9695
11	-24.9184	-31.9993	-22.6593	-42.0173

distinguisher from 15 to 16 rounds. For Simeck48, we also improve the probability and weak key class for the 20-round RXDR distinguisher, and extend the longest RXDR distinguisher for one round (from 20 to 21). The details of the longest distinguishers can be found in Appendix B.

4.4 Experimental Verification on Some RXDR Distinguishers

As we repeatedly mentioned, the precondition that concatenating an rotational-XOR characteristic with a differential characteristic into a rectangle structure then deriving the corresponding RXDR characteristic is the two sub-ciphers E_0 and E_1 are independent. Namely, our theoretical analysis may be inconsistent with the practical one if E_0 and E_1 are dependent. There are many re-

Table 10. Some RXDR distinguishers of Simeck32 and Simeck48.

Version	Round	Input RX-diff.	Output diff.	Data prob. ($> 2^{-2n}$)	Key prob.
Simeck32	14 $(7+7)$	(0x0, 0x4)	(0x15, 0x8)	$2^{-59.77}$	1
Simeck32	15 $(9+6)$	(0x0, 0x4)	(0x15, 0x8)	$2^{-60.31}$	2^{-6}
Simeck32	16 $(9+7)$	(0x0, 0x4)	(0x15, 0x8)	$2^{-63.76}$	2^{-6}
Simeck32	16 $(6+10)$	(0x0, 0x6)	(0x15, 0x8)	$2^{-63.98}$	1
Simeck48	19 $(9+10)$	(0x0, 0x4)	(0x28, 0x10)	$2^{-93.97}$	2^{-6}
Simeck48	20 $(14+6)$	(0x0, 0x110)	(0x28, 0x10)	$2^{-89.51}$	2^{-24}
Simeck48	21 $(14+7)$	(0x0, 0x110)	(0x28, 0x10)	$2^{-94.52}$	2^{-24}

searches about the influence of independency on distinguishers in the composite attacks [23,8,2].

In this paper, we perform some practical experiments to verify our results. Limited to the computation and memory resources, we can only experimentally verify the RXDR distinguishers of the small-block Simon and Simeck, i.e., Simon32/64 and Simeck32. In general, we need to exhaust all the 2^{64} plaintext tuples (P_1, P_2, P_3, P_4), where P_1 is independent to P_3 and P_2 (P_4) is derived from P_1 (P_3), to count the number of tuples that satisfy the RXDR distinguisher for a fixed key. But exhausting all the 2^{64} tuples (P_1, P_2, P_3, P_4) is computationally infeasible. Here we provide an efficient way to achieve the experiment as illustrated in Algorithm 1. The basic idea is that if a plaintext tuple (P_1, P_2, P_3, P_4) can satisfy the RXDR distinguisher, then the corresponding ciphertext pair (C_1, C_3) or (C_2, C_4) must satisfy the differential pattern of RXDR distinguisher. Therefore, we can choose a ciphertext pair (C_1, C_3) satisfying the given differential pattern and then obtain (P_1, P_3) by decrypting (C_1, C_3). Next we use (P_1, P_3) to get (P_2, P_4) by the rotational-XOR difference and further obtain the ciphertext pair (C_2, C_4) by encrypting (P_2, P_4). Finally, we need to verify whether the ciphertext pair (C_2, C_4) satisfies the rotated differential pattern. As a consequence, we only need to choose 2^{32} ciphertext pairs (C_1, C_3) instead of 2^{64} plaintext tuples (P_1, P_2, P_3, P_4) to count the number of right plaintexts. In other words, the computational complexity is decreased from 2^{64} to 2^{32}.

For Simon32/64, we repeat the experiment 2^{10} times by randomly choosing 2^{10} keys. The average numbers of tuples satisfying the 14-, 15- and 16-round RXDR distinguishers in Table 8 are 79.93, 3.52 and 1.08, suggesting the corresponding probabilities of $2^{-57.68}$, $2^{-62.18}$ and $2^{-63.89}$, respectively. All of these experimental probabilities are higher than the predicted ones. The comparison is listed in Table 11.

As for Simeck32, when the round is larger than 7, the optimal rotational-XOR characteristic will bring a probability to the key (see in Table 5) because of its nonlinear key schedule. Therefore, we only test the 14-, 15- and 16-round

Algorithm 1: Practically verify RXRD distinguishers of Simon-like ciphers

```
Input: The input RX-difference $\alpha$, key RX-difference $\Delta_I$ and the output
       difference $\delta$ of an RXDR distinguisher.
Output: The experimental probability of the given RXDR disitnguisher.
Initialize $cnt = 0$;
Randomly choose a master key $K_1$;
$K_3 \leftarrow K_1$, $K_2 \leftarrow \overleftarrow{K_1} \oplus \Delta_I$, $K_4 \leftarrow K_2$;
for $C_1$ in $\mathbb{F}_2^{32}$ do
    $C_3 \leftarrow C_1 \oplus \delta$;
    Decrypt $(C_1, C_3)$ under $(K_1, K_3)$ to obtain $(P_1, P_3)$;
    $(P_2, P_4) \leftarrow (\overleftarrow{P_1} \oplus \alpha, \overleftarrow{P_3} \oplus \alpha)$;
    Encrypt $(P_2, P_4)$ under $(K_2, K_4)$ to obtain $(C_2, C_4)$;
    if $C_2 \oplus C_4 == \overleftarrow{\delta}$ then
        $cnt++$;
    end
end
return $cnt \cdot 2^{-64}$.
```

RXDR distinguishers, which are composed of the 6- or 7-round rotational-XOR characteristic, to eliminate the influence of key on the experimental probability. Namely, the weak key class is 2^{64}. By repeating the experiment 2^{10} times, we obtain that the average numbers of tuples satisfying the 14-, 15- and 16-round RXDR distinguishers of Simeck32 in Table 11 are 107.75, 9.63 and 2.09. The corresponding probabilities listed in Table 11 are also higher than the predicted ones.

5 Conclusion

In this paper, we propose a new method called the rotational-XOR differential rectangle (RXDR) cryptanalysis that combines rotational-XOR, rectangle and differential cryptanalysis. We first illustrate how to build an RXDR structure and evaluate its probability in a generalized situation. Then we further discussed the probability of RXDR structure based on the rotational-invariant property for Simon-like ciphers. In order to construct better RXDR distinguishers, we further consider the differential clustering effect and multiple differentials in the differential part of an RXDR structure. As a consequence, we obtained 16-, 16-, 17-, 16- and 21-round RXDR distinguishers for Simon32/64, Simon48/72, Simon48/96, Simeck32 and Simeck48. Also, we verified the validity of some RXDR distinguishers of Simon32/64 and Simeck32 by experimentally computing their probabilities. As we expected, all of the experimental probabilities are higher than the predicted ones, which indicates that our RXDR distinguishers are indeed valid.

Table 11. The predicted and experimental probabilities of some RXDR distinguishers of Simon32/64 and Simeck32.

Cipher	Round	Input RX-diff.	Key[†] RX-diff.	Output diff.	Predicted prob.	Experimental prob.
Simon32/64	14 $(6+8)$	$(\mathtt{0x0}, \mathtt{0x6})$	0x6	$(\mathtt{0x2022}, \mathtt{0x8})$	$2^{-59.92}$	$\mathbf{2^{-57.68}}$
Simon32/64	15 $(6+9)$	$(\mathtt{0x0}, \mathtt{0x6})$	0x6	$(\mathtt{0x2022}, \mathtt{0x8})$	$2^{-63.32}$	$\mathbf{2^{-62.18}}$
Simon32/64	16 $(6+10)$	$(\mathtt{0x0}, \mathtt{0x6})$	0x6	$(\mathtt{0x2022}, \mathtt{0x8})$	$2^{-63.98}$	$\mathbf{2^{-63.89}}$
Simeck32	14 $(7+7)$	$(\mathtt{0x0}, \mathtt{0x4})$	0x4	$(\mathtt{0x15}, \mathtt{0x8})$	$2^{-59.77}$	$\mathbf{2^{-57.25}}$
Simeck32	15 $(7+8)$	$(\mathtt{0x0}, \mathtt{0x4})$	0x4	$(\mathtt{0x15}, \mathtt{0x8})$	$2^{-63.89}$	$\mathbf{2^{-60.73}}$
Simeck32	16 $(6+10)$	$(\mathtt{0x0}, \mathtt{0x6})$	0x6	$(\mathtt{0x15}, \mathtt{0x8})$	$2^{-63.98}$	$\mathbf{2^{-62.94}}$

[†] The key RX-difference is 64 bits, thus the above information indicates that there only exists non-trivial RX-difference on the first round subkey. For instance, give a master key $K = K[0]||K[1]||K[2]||K[3]$ and the key RX-difference 0x4, another key K^* can be obtained by $K^* = \overleftarrow{K}[3]||\overleftarrow{K}[2]||\overleftarrow{K}[1]||\overleftarrow{K}[0] \oplus \mathtt{0x4}$.

In addition, we did not list any results on Simon and Simeck versions with a block size larger than 48 bits, since the obtained RXDR distinguishers are much shorter than the best differential distinguishers. For example, we built an 18-round RXDR characteristic with a probability of 2^{-124} for Simon64/128 by combing a 9-round rotational-XOR characteristic and a 9-round optimal differential characteristic. The best RXDR distinguisher we could find reached 19 rounds (9 + 10) with a probability of $2^{-125.26}$ when we considered the differential clustering effect and multiple differentials. Note that the length of the best differential characteristic and the best differential are 18 and 23 rounds, respectively. It follows that there exists a gap between the best RXDR and differential distinguishers after considering the differential clustering effect for both of them, even if the best RXDR characteristic has a same round number as the best differential characteristic. Thus, it can be inferred that RXDR structures with high probability mainly benefits from their short but high-probability rotational-XOR characteristics. Therefore, once the number of rounds increases, the probability of RXDR structures will decrease rapidly.

Finally, what we would like to state is that this paper mainly devotes attention to the construction of RXDR distinguishers for the small-block versions of Simon-like ciphers. We do not present any attacks based on the proposed RXDR distinguishers, which can be further explored. Nevertheless, our results provide a new insight on the security of block ciphers (especially for AND-RX ciphers) against combined attacks derivated from classical ones.

Acknowledgement. We would like to thank Maria Eichlseder and all the anonymous reviewers from CT-RSA 2023 for their valuable comments. This work was supported by the National Natural Science Foundation of China (No. 62272147), the Science and Technology on Communication Security Laboratory

Foundation (No. 6142103012207), the Research Foundation of Department of Education of Hubei Province (No. D2020104) and the Wuhan Science and Technology Bureau (NO. 2022010801020328).

References

1. Ashur, T., Liu, Y.: Rotational cryptanalysis in the presence of constants. IACR Trans. Symmetric Cryptol. **2016**(1), 57–70 (2016), https://doi.org/10.13154/tosc.v2016.i1.57-70
2. Bar-On, A., Dunkelman, O., Keller, N., Weizman, A.: DLCT: A new tool for differential-linear cryptanalysis. In: EUROCRYPT 2019, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I. pp. 313–342 (2019), https://doi.org/10.1007/978-3-030-17653-2_11
3. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The Simon and Speck families of lightweight block ciphers. IACR Cryptol. ePrint Arch. p. 404 (2013), http://eprint.iacr.org/2013/404
4. Biham, E., Anderson, R.J., Knudsen, L.R.: Serpent: A new block cipher proposal. In: Vaudenay, S. (ed.) FSE '98, Paris, France, March 23-25, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1372, pp. 222–238. Springer (1998), https://doi.org/10.1007/3-540-69710-1_15
5. Biham, E., Dunkelman, O., Keller, N.: The rectangle attack - rectangling the Serpent. In: Pfitzmann, B. (ed.) EUROCRYPT 2001, Innsbruck, Austria, May 6-10, 2001, Proceeding. Lecture Notes in Computer Science, vol. 2045, pp. 340–357. Springer (2001), https://doi.org/10.1007/3-540-44987-6_21
6. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO '90, Santa Barbara, California, USA, August 11-15, 1990, Proceedings. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1990), https://doi.org/10.1007/3-540-38424-3_1
7. Biryukov, A., Roy, A., Velichkov, V.: Differential analysis of block ciphers Simon and Speck. In: Cid, C., Rechberger, C. (eds.) FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers. Lecture Notes in Computer Science, vol. 8540, pp. 546–570. Springer (2014), https://doi.org/10.1007/978-3-662-46706-0_28
8. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: A new cryptanalysis tool. In: EUROCRYPT 2018, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II. pp. 683–714 (2018), https://doi.org/10.1007/978-3-319-78375-8_22
9. Huang, M., Wang, L., Zhang, Y.: Improved automatic search algorithm for differential and linear cryptanalysis on Simeck and the applications. In: ICICS 2018, Lille, France, October 29-31, 2018, Proceedings. pp. 664–681 (2018), https://doi.org/10.1007/978-3-030-01950-1_39
10. Khovratovich, D., Nikolic, I.: Rotational cryptanalysis of ARX. In: Hong, S., Iwata, T. (eds.) FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers. Lecture Notes in Computer Science, vol. 6147, pp. 333–346. Springer (2010), https://doi.org/10.1007/978-3-642-13858-4_19
11. Khovratovich, D., Nikolic, I., Pieprzyk, J., Sokolowski, P., Steinfeld, R.: Rotational cryptanalysis of ARX revisited. In: Leander, G. (ed.) FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9054, pp. 519–536. Springer (2015), https://doi.org/10.1007/978-3-662-48116-5_25

12. Knudsen, L.R., Wagner, D.A.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers. Lecture Notes in Computer Science, vol. 2365, pp. 112–127. Springer (2002), https://doi.org/10.1007/3-540-45661-9_9
13. Kölbl, S., Leander, G., Tiessen, T.: Observations on the Simon block cipher family. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9215, pp. 161–185. Springer (2015), https://doi.org/10.1007/978-3-662-47989-6_8
14. Kölbl, S., Roy, A.: A brief comparison of Simon and Simeck. In: Bogdanov, A. (ed.) LightSec 2016, Aksaray, Turkey, September 21-22, 2016, Revised Selected Papers. Lecture Notes in Computer Science, vol. 10098, pp. 69–88. Springer (2016), https://doi.org/10.1007/978-3-319-55714-4_6
15. Koo, B., Jung, Y., Kim, W.: Rotational-XOR rectangle cryptanalysis on round-reduced Simon. Secur. Commun. Networks **2020**, 5968584:1–5968584:12 (2020), https://doi.org/10.1155/2020/5968584
16. Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis. In: Desmedt, Y. (ed.) CRYPTO '94, Santa Barbara, California, USA, August 21-25, 1994, Proceedings. Lecture Notes in Computer Science, vol. 839, pp. 17–25. Springer (1994), https://doi.org/10.1007/3-540-48658-5_3
17. Leurent, G., Pernot, C., Schrottenloher, A.: Clustering effect in Simon and Simeck. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Singapore, December 6-10, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13090, pp. 272–302. Springer (2021), https://doi.org/10.1007/978-3-030-92062-3_10
18. Liu, M., Lu, X., Lin, D.: Differential-linear cryptanalysis from an algebraic perspective. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III. Lecture Notes in Computer Science, vol. 12827, pp. 247–277. Springer (2021), https://doi.org/10.1007/978-3-030-84252-9_9
19. Liu, Z., Li, Y., Wang, M.: Optimal differential trails in Simon-like ciphers. IACR Trans. Symmetric Cryptol. **2017**(1), 358–379 (2017), https://doi.org/10.13154/tosc.v2017.i1.358-379
20. Lu, J., Liu, Y., Ashur, T., Sun, B., Li, C.: Rotational-XOR cryptanalysis of Simon-like block ciphers. In: Liu, J.K., Cui, H. (eds.) ACISP 2020, Perth, WA, Australia, November 30 - December 2, 2020, Proceedings. Lecture Notes in Computer Science, vol. 12248, pp. 105–124. Springer (2020), https://doi.org/10.1007/978-3-030-55304-3_6
21. Lu, J., Liu, Y., Ashur, T., Sun, B., Li, C.: Improved rotational-XOR cryptanalysis of Simon-like block ciphers. IET Inf. Secur. **16**(4), 282–300 (2022), https://doi.org/10.1049/ise2.12061
22. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT '93, Lofthus, Norway, May 23-27, 1993, Proceedings. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer (1993), https://doi.org/10.1007/3-540-48285-7_33
23. Murphy, S.: The return of the cryptographic boomerang. IEEE Trans. Inf. Theory **57**(4), 2517–2521 (2011), https://doi.org/10.1109/TIT.2011.2111091
24. Rohit, R., Gong, G.: Correlated sequence attack on reduced-round Simon-32/64 and Simeck-32/64. IACR Cryptol. ePrint Arch. p. 699 (2018), https://eprint.iacr.org/2018/699
25. Wagner, D.A.: The boomerang attack. In: Knudsen, L.R. (ed.) FSE '99, Rome, Italy, March 24-26, 1999, Proceedings. Lecture Notes in Computer

Science, vol. 1636, pp. 156–170. Springer (1999), https://doi.org/10.1007/3-540-48519-8_12

26. Wang, X., Wu, B., Hou, L., Lin, D.: Automatic search for related-key differential trails in Simon-like block ciphers based on MILP. In: Chen, L., Manulis, M., Schneider, S.A. (eds.) ISC 2018, Guildford, UK, September 9-12, 2018, Proceedings. Lecture Notes in Computer Science, vol. 11060, pp. 116–131. Springer (2018), https://doi.org/10.1007/978-3-319-99136-8_7
27. Xiang, Z., Zhang, W., Bao, Z., Lin, D.: Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In: ASIACRYPT 2016, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I. pp. 648–678 (2016), https://doi.org/10.1007/978-3-662-53887-6_24
28. Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.: The Simeck family of lightweight block ciphers. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015, Saint-Malo, France, September 13-16, 2015, Proceedings. Lecture Notes in Computer Science, vol. 9293, pp. 307–329. Springer (2015), https://doi.org/10.1007/978-3-662-48324-4_16

A Detail on RXDR characteristics of Simon and Simeck

In section 4.2, we show the optimal RXDR characteristics of small-block versions of Simon and Simeck. The detailed structures and probabilities of the longest RXDR characteristics are shown in Table 12. Moreover, the specific rotational-XOR and differential characteristics utilized in these longest optimal RXDR characteristics are listed in Tables 13,14,15,16 and 17.

Table 12. Some optimal RXDR characteristics of Simon and Simeck.

Version	Round	Data prob. ($> 2^{-2n}$)	Key Prob.
Simon32/64	13 $(6+7)$	2^{-60}	1
Simon48/72	15 $(6+9)$	2^{-92}	1
Simon48/96	16 $(8+8)$	2^{-92}	1
Simeck32	15 $(10+5)$	2^{-60}	2^{-8}
Simeck48	20 $(17+3)$	2^{-92}	2^{-32}

Table 13. The specific 6-round rotational-XOR (left) and 7-round differential (right) characteristics of Simon32/64, which form the optimal 13-round RXDR characteristic.

Round	Key RX-diff.	Data RX-diff.	Data diff.
0	0006	(0000||0006)	0008||0015
1	0000	(0000||0000)	0005||0008
2	0000	(0000||0000)	0002||0005
3	0000	(0000||0000)	0001||0002
4	0000	(0000||0000)	0000||0001
5	0006	(0000||0000)	0001||0000
6		(0006||0000)	0002||0001
7			0005||0002
Prob.	1	1	2^{-14}

Table 14. The specific 6-round rotational-XOR (left) and 9-round differential (right) characteristics of Simon48/72, which form the optimal 15-round RXDR characteristic.

Round	Key RX-diff.	Data RX-diff.	Data diff.
0	300006	(000000||300007)	001000||004440
1	000006	(000001||000000)	000440||001000
2	000001	(000000||000001)	000100||000440
3	000000	(000000||000000)	000040||000100
4	000000	(000000||000000)	000000||000040
5	00ae82	(000000||000000)	000040||000000
6		(00ae82||000000)	000100||000040
7			000440||000100
8			001000||000440
9			004440||001000
Prob.	1	2^{-2}	2^{-20}

Table 15. The specific 8-round rotational-XOR (left) and 8-round differential (right) characteristics of Simon48/96, which form the optimal 16-round RXDR characteristic.

Round	Key RX-diff.	Data RX-diff.	Data diff.
0	180016	(000000||180016)	000200||000888
1	800000	(000000||000000)	000088||000200
2	000003	(800000||000000)	000020||000088
3	800004	(000000||800000)	000008||000020
4	000010	(000004||000000)	000000||000008
5	000004	(000000||000004)	000008||000000
6	000000	(000000||000000)	000020||000008
7	800019	(000000||000000)	000088||000020
8		(800019||000000)	000200||000088
Prob.	1	2^{-4}	2^{-18}

Table 16. The specific 10-round rotational-XOR (left) and 5-round differential characteristics (right) of Simeck32, which form the optimal 15-round RXDR characteristic.

Round	Key RX-diff.	Data RX-diff.	Data diff.
0	008e	(0004||0006)	0800||1400
1	0004	(0000||0004)	0400||0800
2	0000	(0000||0000)	0000||0400
3	0000	(0000||0000)	0400||0000
4	0000	(0000||0000)	0800||0400
5	0002	(0000||0000)	1400||0800
6	0006	(0002||0000)	
7	0006	(0002||0002)	
8	0002	(0000||0002)	
9	008d	(0000||0000)	
10		(008d||0000)	
Prob.	2^{-8}	2^{-6}	2^{-8}

Table 17. The specific 17-round rotational-XOR (left) and 3-round differential characteristics (right) of Simeck48, which form the optimal 20-round RXDR characteristic.

Round	Key RX-diff.	Data RX-diff.	Data diff.
0	000114	(000000||000110)	000002||000004
1	000008	(000004||000000)	000000||000002
2	000004	(000000||000004)	000002||000000
3	000000	(000000||000000)	000004||000002
4	000002	(000000||000000)	
5	000006	(000002||000000)	
6	000002	(000000||000002)	
7	000000	(000000||000000)	
8	000008	(000000||000000)	
9	000005	(000008||000000)	
10	000007	(000015||000008)	
11	000015	(000000||000015)	
12	000000	(000000||000000)	
13	000008	(000000||000000)	
14	000019	(000008||000000)	
15	000013	(000009||000008)	
16	00001e	(000000||000009)	
17		(000017||000000)	
Prob.	2^{-32}	2^{-18}	2^{-4}

B Detail on RXDR distinguishers of Simon and Simeck

In section 4.3, we show some longer RXDR distinguishers. The detailed structures and probabilities of the longest RXDR distinguishers are shown in Table 18.

Table 18. Some optimal RXDR distinguishers of Simon and Simeck.

Version	Round	Input RX-diff.	Output diff.	Data prob. ($> 2^{-2n}$)	Key prob.
Simon32/64	16 (6 + 10)	(0x0, 0x6)	(0x2022, 0x8)	$2^{-63.98}$	1
Simon48/72	16 (7 + 9)	(0x0, 0x3e)	(0x222, 0x80)	$2^{-89.78}$	1
Simon48/96	17 (8 + 9)	(0x0, 0x180016)	(0x222, 0x80)	$2^{-89.78}$	1
Simeck32	16 (9 + 7)	(0x0, 0x4)	(0x15, 0x8)	$2^{-63.76}$	2^{-6}
Simeck48	21 (14 + 7)	(0x0, 0x110)	(0x28, 0x10)	$2^{-94.52}$	2^{-24}

Moreover, the specific rotational-XOR characteristics and optimal differential characteristics, from which we chose the output difference of multiple differentials, are listed in Table 19, 20, 21 and 22. The 6-round and 8-round rotational-XOR characteristics of Simon32 and Simon48/96 can be seen in Table 13 and 15.

Table 19. The 7-round rotational-XOR characteristic of Simon48/72.

Round	Key RX-diff.	Data RX-diff.
0	00003e	(000000‖00003e)
1	000020	(000000‖000000)
2	000080	(000020‖000000)
3	000020	(000000‖000020)
4	000020	(000000‖000000)
5	000080	(000020‖000000)
6	284900	(000000‖000020)
7		(284900‖000000)
Prob.	1	2^{-4}

Table 20. The 7-round optimal differential characteristics of Simeck32 (left) and Simeck48 (right).

Round	Data diff.	Data diff.
0	0008||0015	000010||000028
1	0005||0008	000008||000010
2	0002||0005	000000||000008
3	0001||0002	000008||000000
4	0000||0001	000010||000008
5	0001||0000	000028||000010
6	0002||0001	000040||000028
7	0005||0002	0000a8||000040
Prob.	2^{-14}	2^{-14}

Table 21. The 9-round (left) and 14-round (right) rotational-XOR characteristics of Simeck32 and Simeck48.

Round	Key RX-diff.	Data RX-diff.	Key RX-diff.	Data RX-diff.
0	0004	(0000||0004)	000114	(000000||000110)
1	0000	(0000||0000)	000008	(000004||000000)
2	0000	(0000||0000)	000004	(000000||000004)
3	0000	(0000||0000)	000000	(000000||000000)
4	0002	(0000||0000)	000002	(000000||000000)
5	0006	(0002||0000)	000006	(000002||000000)
6	0006	(0002||0002)	000002	(000000||000002)
7	0002	(0000||0002)	000000	(000000||000000)
8	000e	(0000||0000)	000008	(000000||000000)
9		(000e||0000)	000005	(000008||000000)
10			000007	(000015||000008)
11			000015	(000000||000015)
12			000000	(000000||000000)
13			00006f	(000000||000000)
14				(00006f||000000)
Prob.	2^{-6}	2^{-4}	2^{-24}	2^{-12}

Table 22. The 10-round (left) and 12-round (right) optimal differential characteristics of Simon32 and Simon48.

Round	Data diff.	Data diff.
0	0008||2022	000080||000222
1	2002||0008	000022||000080
2	8000||2002	000008||000022
3	2000||8000	000002||000008
4	0000||2000	000000||000002
5	2000||0000	000002||000000
6	8020||2000	000008||000002
7	0002||8020	000022||000008
8	8028||0002	000080||000022
9	0020||8028	000222||000080
10	80a8||0020	020808||000222
11		002200||020808
12		008008||002200
Prob.	2^{-25}	2^{-35}

C Algorithm to Calculate $\tilde{q}$ for Simon-like Ciphers

Algorithm 2: Calculate multiple differentials of SIMON-like ciphers

```
   Input: The output difference $\delta = (\delta_L, \delta_R)$, the window $w$ and the round $\mathtt{R}$.
   Output: The values of $\hat{q}_B$ (probability of the best differential) and $\tilde{q}$.
1  Initialize $q[2^w] = 0$, $space[2^w] = \emptyset$, $\hat{q}_B = 0$ and $\tilde{q} = 0$;
2  for $\mu$ from $0$ to $2^w - 1$ do
3      for $\nu$ from $0$ to $2^w - 1$ do
4          Calculate the probability $\Pr(\mu \to \nu)$ according to Theorem 1;
5          if $\Pr(\mu \to \nu) > 0$ then
6              $q[\mu] \leftarrow \Pr(\mu \to \nu)$;
7              Add $\nu$ to the set $space[\mu]$;
8          end
9      end
10 end
11 Initialize $X[2^w][2^w] = 0$;
12 $X[\delta_R][\delta_L] \leftarrow 1$; /* Regard $(\delta_R, \delta_L)$ as the input difference */
13 /* From line 14-34, $i$ and $j$ denote differences of the left and right branches
     respectively in the $r$-round differential propagation. */
14 for $r$ from $1$ to $\mathtt{R}$ do
15     Initialize $Y[2^w][2^w] = 0$;
16     for $i$ from $0$ to $2^w - 1$ do
17         for $j$ from $0$ to $2^w - 1$ do
18             if $X[i][j] > 0$ and $q[i] > 0$ then
19                 for $\nu$ in $space[i]$ do
20                     $Y[\nu \oplus j][i] \leftarrow Y[\nu \oplus j][i] + q[i] \cdot X[i][j]$;
21                 end
22             end
23         end
24     end
25     $X \leftarrow Y$;
26 end
27 for $i$ from $0$ to $2^w - 1$ do
28     for $j$ from $0$ to $2^w - 1$ do
29         $\tilde{q} \leftarrow \tilde{q} + (X[i][j])^2$; /* According to Equation (4). */
30         if $X[i][j] > \hat{q}_B$ then
31             $\hat{q}_B \leftarrow X[i][j]$;
32         end
33     end
34 end
35 return $(\hat{q}_B, \tilde{q})$.
```