IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2024, No. 2, pp. 296–321. DOI:10.46586/tosc.v2024.i2.296-321

Links between Quantum Distinguishers Based on Simon's Algorithm and Truncated Differentials

Zejun Xiang[1,2], Xiaoyu Wang[3], Bo Yu[4], Bing Sun[4,5], Shasha Zhang[1], Xiangyong Zeng[3], Xuan Shen[6] and Nian Li[1]

[1] School of Cyber Science and Technology, Hubei University, Wuhan, Hubei, 430062, China
xiangzejun@hubu.edu.cn; amushasha@163.com; nian.li@hubu.edu.cn
[2] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China
[3] Faculty of Mathematics and Statistics, Hubei University, Wuhan, Hubei, 430062, China
wangxiaoyu@stu.hubu.edu.cn; xzeng@hubu.edu.cn
[4] College of Science, National University of Defense Technology, Changsha, Hunan, 410073, China
sunbing06@nudt.edu.cn; bo_yu99@outlook.com
[5] Center for Cryptologic Research, National University of Defense Technology, Changsha, Hunan, P.R. China, 410073
[6] College of Information and Communication, National University of Defense Technology, Wuhan, Hubei, 430010, China
shenxuan_08@163.com

Abstract. In this paper, we study the quantum security of block ciphers based on Simon's period-finding quantum algorithm. We explored the relations between periodic functions and truncated differentials. The basic observation is that truncated differentials with a probability of 1 can be used to construct periodic functions, and two such constructions are presented with the help of a new notion called *difference-annihilation matrix*. This technique releases us from the tedious manual work of verifying the period of functions. Based on these new constructions, we find an 8-round quantum distinguisher for LBlock and a 9/10/11/13/15-round quantum distinguisher for SIMON-32/48/64/96/128 which are the best results as far as we know. Besides, to explore the security bounds of block cipher structures against Simon's algorithm based quantum attacks, the unified structure, which unifies the Feistel, Lai-Massey, and most generalized Feistel structures, is studied. We estimate the exact round number of probability 1 truncated differentials that one can construct. Based on these results, one can easily check the quantum security of specific block ciphers that are special cases of unified structures, when the details of the non-linear building blocks are not considered.

Keywords: Simon's Algorithm · Truncated Differentials · LBlock · SIMON · Unified Structures

1 Introduction

With the development of physics and computation techniques, quantum computation has subverted the cognition of traditional theories of computation, and thus attracted extensive attention, especially in the field of cryptography, since the emergence of large-scale quantum computers affects the security of existing cryptographic schemes significantly.

The proposal of Shor's algorithm [Sho97] is a milestone in developing quantum computation. Shor's algorithm can solve problems such as the factorization of large integers and the computation of discrete logarithms in polynomial time, which leads to the cracking of the public key cryptography designed based on those problems in the quantum scenario.

Received: 2024-03-01 Accepted: 2024-05-01 Published: 2024-06-18

In addition, Grover's algorithm [Gro96] and Simon's algorithm [Sim97] also challenge the security of existing symmetric cryptographic schemes. Grover's algorithm quadratically accelerates the exhaustive key search for any cryptographic primitives. Simon's algorithm can be used to derive the period of periodic functions in polynomial time, by which the attacks on symmetric cryptographic structures can be conducted.

Various methods have been proposed to be used as cryptanalysis tools in the classical scenario, which should also be established for evaluating the post-quantum security of current cryptographic primitives and providing the necessary preparation for designing new quantum-resistant cryptographic primitives, as the authors suggested in [KLLN16a]. At present, quantum attacks on cryptographic primitives can be roughly divided into two categories. One is the use of existing quantum algorithms to quantize classical cryptanalysis techniques, such as quantum differential and linear attacks [KLLN16b], quantum Demirci and Selçuk meet-in-the-middle attacks [HS18, BNS19b], quantum slide attacks [DDW20, BNS19a], and quantum rebound attacks [HS20, DSS+20, CKS21]. The other, as classical cryptanalysis does, is to consider combining the problems that quantum algorithms can solve with the flaws that exist in cryptographic primitives to complete the attack. Along this line of research, Simon's algorithm has attracted much attention since it was used by Kuwakado and Morii to distinguish the 3-round Feistel structure in 2010 [KM10]. Later, Simon's algorithm was also applied in [KM12] to conduct a key recovery attack on the Even-Mansour structure, and the authors proved that the Even-Mansour structure was no longer secure under quantum scenarios.

Roughly, Simon's algorithm based quantum attacks can be divided into two categories. The first one is to distinguish a round-reduced block cipher, such as the 3-round distinguisher of Feistel structure presented in [KM10]. Soon after, quantum distinguishers for generalized Feistel structures [DLW19, HKK20, ZWSW23], improved quantum distinguishers for Type-1 generalized Feistel structures [NIDI19], and chosen-ciphertext distinguisher for Feistel and Feistel-FK structures [IHM+19] are proposed. Furthermore, Leander *et al.* presented a clever idea combining Grover's algorithm and Simon's algorithm at ASIACRYPT 2017 [LM17], and a key recovery attack for FX structure. Inspired by this idea, Dong and Wang [DW18] proposed a key recovery attack on the 5-round Feistel structure based on the 3-round distinguisher. The other line of research converts the weakness of modes of operations into recovering the period of well-designed periodic functions, such as the key recovery attack of the Even-Mansour cipher [KM12]. Following this idea, Kaplan *et al.* broke several modes of operations at CRYPTO 2016 [KLLN16a], such as CBC-MAC, GCM, and OCB. Usually, the period in such attacks contains the key information, thus, recovering the period can directly retrieve the key.

Although Simon's quantum algorithm has many applications in the cryptanalysis of symmetric ciphers, it requires access to a quantum encryption oracle to which it may acquire superposition states. Recently, this requirement has been removed by offline Simon's algorithms [BHN+19], where an attacker can only access a classical encryption oracle and run Simon's algorithm in an offline style with an increase in the time complexity. However, both Simon's algorithm and the offline Simon's algorithm need to devise a periodic function.

Our Contributions. In this paper, we focus on the quantum security of basic symmetric primitives and investigate the construction of periodic functions for round-reduced block ciphers. We establish the links between periodic functions and truncated differentials and present a classical view of quantum distinguishing attacks for the first time. Our contributions are threefold.

(1) We observe that a periodic function always exhibits a differential with probability 1, and prove that as long as there is an r-round truncated differential whose output differences can be annihilated, a periodic function can be constructed. Moreover, two types of periodic functions that cover most existing studies and general constructions for such

periodic functions from truncated differentials with probability 1 are presented, which prevents us from manually verifying the periodic property of constructed functions. Moreover, this indicates that the study of classical truncated differentials can be a guide for the study of quantum distinguishing attacks for a round-reduced block cipher.

(2) As an illustration, our general techniques are applied to `LBlock` and `SIMON` block ciphers. Regarding `LBlock`, an 8-round distinguisher which is 4 rounds longer than the previous generic result can be constructed. For the `SIMON` family block ciphers, we construct 9/10/11/13/15-round distinguishers for `SIMON`-32/48/64/96/128, while the best previous generic results cover 6 rounds for all `SIMON` variants. We provide a comparison table in Table 1. All our distinguishers can be easily verified from the view of truncated differentials.

(3) Finally, we study the quantum resistance of block cipher structures, where the details of non-linear components are not considered. The round number of quantum distinguishers for the unified structure is estimated. It's proved that for a d-branch unified structure with a few restrictions, one can always construct a $(2d-1)$-round quantum distinguisher. Specifically, this result applies to classical Feistel, MARS-like, and SM4-like structures.

Organization. This paper is organized as follows. Section 2 introduces some notations and briefly revisits Simon's quantum algorithm. We introduce a new technique on how to construct periodic functions from truncated differentials in Section 3. Section 4 presents an extended periodic function. Section 5 applies our technique to `LBlock` and `SIMON` block ciphers. We study the round number of such quantum distinguishers for unified structures in Section 6. Section 7 concludes the paper.

2 Preliminaries

2.1 Notation

This subsection introduces the notations that will be used throughout this paper. Let $\mathbb{F}_2$ denote the finite field with two elements, and $\mathbb{F}_2^n$ denote the n-dimensional vector space over $\mathbb{F}_2$. All vectors that appear in this paper are treated as column vectors. With a bit of abuse of notations, we let $a = (a_1, ..., a_n) \in \mathbb{F}_2^n$ denote a column vector, where we omit the transpose notation for clarity. 0^n represents an n-dimensional zero vector. Denote the bit-wise XOR and AND operations by $\oplus$ and $\&$, respectively. Let $b = (b_1, ..., b_n) \in \mathbb{F}_2^n$, $a \cdot b \triangleq a_1 b_1 \oplus \cdots \oplus a_n b_n$ denote the inner product of a and b. Let V be a subset of $\mathbb{F}_2^n$, $V^\perp = \{x \in \mathbb{F}_2^n \mid x \cdot y = 0, \ \forall\ y \in V\}$ is the orthogonal complement of V. If V is a subspace, $V^\perp$ is the orthogonal complement subspace of V. Let $S^j(x)$ denote the left cyclic shift of x by j bits for $x \in \mathbb{F}_2^n$.

2.2 Truncated Differential

The idea of truncated differentials was first introduced by Knudsen *et al.* in [Knu94] and later formalized in [BLN14, LTW18, ZSLS15]. Different from a classical differential, a truncated differential focuses on difference propagations from a set of input differences to a set of output differences. In this paper, we adopt the more general definition in [ZSLS15] shown below.

Definition 1 ([ZSLS15])**.** Let $E : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, $\Delta_I \subset \mathbb{F}_2^n$ and $\Delta_O \subset \mathbb{F}_2^n$ be two subsets. $\Delta_I \to \Delta_O = \{\alpha \to \beta \mid \exists\ \alpha \in \Delta_I, \beta \in \Delta_O, x \in \mathbb{F}_2^n, \text{s.t. } E(x \oplus \alpha) \oplus E(x) = \beta\}$ is called a truncated differential of E. Moreover, $\Pr(\Delta_I \to \Delta_O) = \Pr\{E(x) \oplus E(x \oplus \alpha) \in \Delta_O | \alpha \in \Delta_I\}$ is called the probability of $\Delta_I \to \Delta_O$.

Table 1: The Distinguishers of `SIMON` and `LBlock`.

Cipher	Round	Setting	Method	Ref.
LBlock	3	Quantum	qCPA	[IHM+19]
	4		qCCA	[IHM+19]
	8		qCPA	**Sect. 5.1**
	14	Classical	Differential	[WZ11]
	14		Linear	[WZ11]
	17		Integral	[WHG+19]
SIMON-32	5	Quantum	qCPA	[IHM+19]
	6		qCCA	[IHM+19]
	9		qCPA	**Sect. 5.2**
	14	Classical	Differential	[LLW17]
	14		Linear	[KLT15]
	14		Integral	[XZBL16]
SIMON-48	5	Quantum	qCPA	[IHM+19]
	6		qCCA	[IHM+19]
	10		qCPA	**Sect. 5.2**
	17	Classical	Differential	[KLT15]
	17		Linear	[KLT15]
	17		Integral	[XZBL16]
SIMON-64	5	Quantum	qCPA	[IHM+19]
	6		qCCA	[IHM+19]
	11		qCPA	**Sect. 5.2**
	23	Classical	Differential	[LLW17]
	22		Linear	[KLT15]
	18		Integral	[XZBL16]
SIMON-96	5	Quantum	qCPA	[IHM+19]
	6		qCCA	[IHM+19]
	13		qCPA	**Sect. 5.2**
	31	Classical	Differential	[LLW17]
	33		Linear	[LPS21]
	22		Integral	[XZBL16]
SIMON-128	5	Quantum	qCPA	[IHM+19]
	6		qCCA	[IHM+19]
	15		qCPA	**Sect. 5.2**
	41	Classical	Differential	[LLW17]
	42		Linear	[LPS21]
	26		Integral	[XZBL16]

Moreover, if $\Pr(\Delta_I \to \Delta_O) = 1$, we call it a probability 1 truncated differential.

2.3 Simon's Algorithm

In this subsection, we briefly introduce Simon's quantum algorithm [Sim97]. Throughout this paper, we assume that readers have basic knowledge about quantum computation. Simon's algorithm was originally proposed to solve the following problem.

Simon's problem Given a vectorial Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with the promise that there exists an $s \in \mathbb{F}_2^n \setminus \{0^n\}$, such that for any $x, y \in \mathbb{F}_2^n$, $f(x) = f(y) \Leftrightarrow x \oplus y \in \{0^n, s\}$, the goal is to find s.

The condition that $f(x) = f(y) \Leftrightarrow y = x \oplus s$ for any distinct x and y is called the *Simon's promise*. According to the birthday bound, $O(2^{n/2})$ queries are needed to find s in the classical setting, while only $O(n)$ quantum queries are required by Simon's algorithm in the quantum setting. We assume that the attacker has access to a quantum oracle U_f, which is defined as $U_f |x\rangle |y\rangle = |x\rangle |x \oplus f(y)\rangle$. Simon's algorithm works as follows:

1. Initialize two quantum registers $|0\rangle^{\otimes n}$ and $|0\rangle^{\otimes m}$.
2. Apply the Hadamard transform to the first register to obtain an equal superposition,
$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} |x\rangle |0\rangle .$$
3. Apply the unitary operator U_f to obtain the state
$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} |x\rangle |f(x)\rangle .$$
4. Measure the second register in the computational basis and get a random output value denoted by y. According to Simon's promise, there is a pair of input $\{x, x \oplus s\}$ such that $f(x) = f(x \oplus s) = y$. Thus, the quantum state of the first register after the measurement is
$$\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle).$$
5. Apply the Hadamard transform to the first register again to obtain the state
$$\frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \mathbb{F}_2^n} [(-1)^{z \cdot x}(1 + (-1)^{z \cdot s})] |z\rangle .$$
6. Measure the first register in the computational basis and get a random output value denoted by z. If $z \cdot s = 1$, the amplitude of $|z\rangle$ is 0, which means the probability of measuring such a z is 0. Therefore, one obtains $z \cdot s = 0$ from the above fact.

Repeating the above subroutine $O(n)$ times, $n - 1$ linearly independent vectors orthogonal to s can be obtained with a high probability. Furthermore, s can be recovered by solving linear equations.

2.4 The Extension of Simon's Algorithm

In practical settings, Simon's promise is not always completely satisfied in most cases. For example, when round functions are not permutations, there is no guarantee that the periodic function designed in [KM10] strictly satisfies Simon's promise. That is, one has a function f satisfying the only condition that $y = x \oplus s$ implies $f(x) = f(y)$ for any x. In

this case, Simon's algorithm no longer seems to work. In the following, we call such an f a *periodic function* and s a *period* of f.

In order to solve the shortcomings when the Simon's promise is not strictly satisfied, Kaplan *et al.* [KLLN16a] studied Simon's algorithm and they introduced the parameter $\varepsilon(f, s)$, where

$$\varepsilon(f, s) = \max_{t \in \{0,1\}^n \setminus \{0^n, s\}} \Pr[f(x) = f(x \oplus t)],$$

and concluded that as long as a periodic function f is constructed, which satisfies that there exists p_0 such that $\varepsilon(f, s) \leq p_0 < 1$, one can also use Simon's algorithm with f to recover the period s with probability at least $1 - (2(\frac{1+p_0}{2})^c)^n$ after cn queries. Although Kaplan *et al.*'s technique is applicable to any (vectorial) Boolean functions, it is tricky to evaluate an upper bound of $\varepsilon(f, s)$.

Later, Ito *et al.* [IHM+19] further relaxed the condition to design quantum distinguishers. Suppose that we are given an oracle $\mathcal{O} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ which is either a cryptographic primitive $E \in \mathrm{Perm}(n)$ or a random permutation $\Pi \in \mathrm{Perm}(n)$, where $\mathrm{Perm}(n)$ denotes the set of all permutations over n-bit strings, the goal is to distinguish these two cases. Suppose that the quantum oracles $U_{\mathcal{O}}$ and $U_{\mathcal{O}^{-1}}$ are given. Assume that a function $f^{\mathcal{O}} : \mathbb{F}_2^l \to \mathbb{F}_2^m$ can be constructed by querying the oracles $U_{\mathcal{O}}$ and $U_{\mathcal{O}^{-1}}$, which satisfies that it is a periodic function when $\mathcal{O} = E$, and it is not periodic with a high probability when $\mathcal{O}$ is a random permutation. Instead of recovering a period for constructing distinguishers, Ito *et al.* [IHM+19] focused on the dimension of the vector space spanned by those vectors returned by applying Simon's algorithm to $f^{\mathcal{O}}$. If $f^{\mathcal{O}}$ has a period s, the obtained vectors must be orthogonal to s. Hence the dimension of the vector space spanned is less than l. On the other hand, if $f^{\mathcal{O}}$ has no periods, the dimension can reach l. Thus, the evaluation of $\varepsilon(f, s)$ is no longer required. This means as long as a periodic function is constructed, it is not required to prove the period is unique and a distinguishing attack can be achieved.

2.5 Automatic Search of Periodic Functions

Recently, Canale *et al.* proposed a generic algorithm for the automatic search of period functions and presented the first efficient key-recovery attacks against constructions like 5-round MISTY L-FK and 5-round Feistel-FK using Simon's algorithm at CRYPTO 2022 [CLS22]. They represent those functions dependent on a round-reduced cipher E by a class of circuits, and these circuits can make use of oracle gates of E. Moreover, the oracle gates for several internal parts of E, such as the key-less round functions, are provided. Then, they automatically examine all circuits for periodicity.

Although their approach discovered many improved quantum distinguishers, this technique has several limitations. On the one hand, their approach is still quite complex in practice. On the other hand, their results do not cover periodic functions that have been constructed for some cryptographic primitives. In order to make the search algorithm practical, their approach just instantiates a reduced cipher with a small input size. Thus, the search algorithm may return an invalid periodic function, which further needs a verification process. Besides, the search algorithm requires exhaustively evaluating all possible combinations, whose complexity may be practically infeasible for more sophisticated ciphers. Compared with our approach which will be illustrated later, their approach fails to leverage the specific properties of the round function, while our approach exploits such properties in a difference-based technique, thus, potentially leading to longer distinguishers.

3 Links between Periodic Functions and Truncated Differentials

Revisiting the previous work [KM10, KM12, NIDI19, DLW19, HK20], the key to constructing a quantum distinguisher based on Simon's algorithm is to design a periodic function. Previous studies construct periodic functions by analyzing the properties of underlying primitives case by case. In this section, we present a more general way to design periodic functions, which makes it easier to verify their periods.

3.1 Observations on Periodic Functions

Before we formally introduce our general technique, we would like to first make an in-depth study on periodic functions. The general idea is to try to connect periodic functions with differentials.

Suppose $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a periodic function with a period s ($s \neq 0^n$), i.e., $f(x) = f(x \oplus s)$ for any $x \in \mathbb{F}_2^n$. Note that $(x, x \oplus s)$ is a natural input pair with an input difference s when considering differential cryptanalysis. Thus, we can restate periodic functions from the perspective of differential cryptanalysis.

Lemma 1. *$f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a periodic function if and only if there exists an s ($s \neq 0^n$), such that the difference transition from s to 0 is of probability 1, i.e., $\Pr[s \xrightarrow{f} 0] = 1$.*

However, it is unlikely to exist such an input-output difference pair for a symmetric cipher. For instance, if f is a block cipher, this difference pair indicates that there are two plaintexts that are encrypted to the same ciphertext, which will never happen for a block cipher as decryption is necessary. Thus, we consider a more general case for symmetric ciphers.

3.2 Constructing Periodic Functions from Truncated Differentials

In this section, we show how to construct periodic functions from the perspective of truncated differentials, before which we first present a new notion which we call the *differen ce-annihilation matrix*.

Definition 2. Let $\Delta_O \subset \mathbb{F}_2^n$ be a non-empty set of differences. Assume that there exists a non-zero matrix L and such that $Lx = \gamma$ for any $x \in \Delta_O$, where $\gamma \in \mathbb{F}_2^n$ is a fixed value. Then, we call L a difference-annihilation matrix of Δ_O.

Theorem 1. *Let $E : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which has a probability 1 truncated differential $\Delta_I \to \Delta_O$. Assume that there exists a difference-annihilation matrix $M \in \mathbb{F}_2^{k \times n}$ of Δ_O with a full row rank, such that $Mx = \gamma$ for any $x \in \Delta_O$. Let γ_0 and γ_1 be two k-bit constants, such that $\gamma_0 \oplus \gamma_1 = \gamma$. Define a function g as*

$$\begin{aligned} g : \mathbb{F}_2 \times \mathbb{F}_2^n &\to \mathbb{F}_2^k \\ (b, x) &\mapsto M \cdot E(x) \oplus \gamma_b. \end{aligned}$$

Then, g is a periodic function with $(1, s)$ being its period for any $s \in \Delta_I$.

Proof. $\forall\ s \in \Delta_I,\ \forall\ x \in \mathbb{F}_2^n$, since $\Pr[\Delta_I \xrightarrow{E} \Delta_O] = 1$, $E(x) \oplus E(x \oplus s) \in \Delta_O$ always holds. Thus we have

$$\begin{aligned} & g(0, x) \oplus g(1, x \oplus s) \\ =& M \cdot E(x) \oplus \gamma_0 \oplus M \cdot E(x \oplus s) \oplus \gamma_1 \\ =& M \cdot (E(x) \oplus E(x \oplus s)) \oplus \gamma \\ =& \gamma \oplus \gamma = 0^k. \end{aligned}$$

This proves that g is a periodic function, and $(1, s)$ is a period of g for any $s \in \Delta_I$. □

Remark 1 When $\gamma = 0$ in Theorem 1, one can check that all of $(0, s), (1, s)$ and $(1, 0)$ are periods of g. In this case, we can simplify the construction of g as $g(x) = M \cdot E(x)$, and s is a period of g for any $s \in \Delta_I$.

Remark 2 Denote $l = |\Delta_O|$ the number of vectors in Δ_O, and denote τ_i $(i = 0, 1, \ldots, l-1)$ the i-th vector of Δ_O. Let $\bar{\Delta}_O = \{\tau_i \oplus \tau_0 \mid i = 1, 2, \ldots, l-1\}$. Algorithm 1[1] can return such an M and the corresponding γ.

Algorithm 1: Evaluating the non-zero matrix M for any set $\Delta_O \subseteq \mathbb{F}_2^n$

Input: the output set Δ_O of truncated differential;
Output: difference-annihilation matrix M, fixed constant γ;
$\tau_0 \leftarrow$ the first vector of Δ_O;
Evaluate $\bar{\Delta}_O$ from Δ_O as in Remark 2;
$v_0, ..., v_{r-1} \leftarrow$ maximal linearly independent system of $\bar{\Delta}_O$;
if $r = n$ **then**
  return `Nonexistence`;
end
else
  Solving linear equations: $v_0 \cdot x = 0, ..., v_{r-1} \cdot x = 0$, and denote $u_0, ..., u_{k-1}$ a set of basis of the solution space; // $r \oplus k = n$
  $M \leftarrow (u_0, ..., u_{k-1})^{\mathrm{T}}$;
  $\gamma \leftarrow M\tau_0$;
  return M, γ;
end

Definition 3. Let $E : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which has an r-round truncated differential $\Delta_I \to \Delta_O$ with probability 1. If there exists a difference-annihilation matrix M of Δ_O, we call the periodic function as constructed in Theorem 1 a **Type-I periodic function** of E_r, where E_r is the r-round reduced version of E.

Example 1. The Feistel structure $\mathcal{E}^{\texttt{Feistel}} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$, has a 2-round truncated differential $\Delta_I = \{(0^n, \gamma)\} \to \Delta_O = \{(u, \gamma) \mid u \in \mathbb{F}_2^n\}$ with probability 1, where $\gamma \in \mathbb{F}_2^n$ and $\gamma \neq 0^n$. Take $(0^n, \gamma)$ as the first vector τ_0 of Δ_O, Algorithm 1 returns the following matrix $M_1 = (O\ I)$ and $\gamma = M_1\tau_0$, where I and O denote the $n \times n$ identity and zero matrices over $\mathbb{F}_2$. Let $\gamma_0, \gamma_1 \in \mathbb{F}_2^n$ be two arbitrarily chosen constants, such that $\gamma_0 \oplus \gamma_1 = \gamma$. According to Theorem 1, $g_1(b, y, z) = M_1 \cdot \mathcal{E}_2^{\texttt{Feistel}}(y, z) \oplus \gamma_b$ is a periodic function.

4 Extending Quantum Distinguishers

4.1 New Insights on the 3-Round Distinguisher by Kuwakado and Morii

If we try to use a Type-I periodic function to construct a distinguisher for the Feistel structure, we can only get a 2-round distinguisher as in Example 1. However, there exists a 3-round quantum distinguisher given by Kuwakado and Morii as shown in Figure 1. The periodic function g_1' used by such a distinguisher is defined as follows.

$$\begin{aligned} g_1' : \mathbb{F}_2 \times \mathbb{F}_2^n &\to \mathbb{F}_2^n \\ (b, x) &\mapsto R_3 \oplus \gamma_b, \end{aligned}$$

where $(L_3, R_3) = \mathcal{E}_3^{\texttt{Feistel}}(\gamma_b, x)$, γ_0 and γ_1 are two fixed n-bit constants.

[1] As in most cases, the truncated differential is constructed by evaluating which bits have active differences, and this results in a well-structured output difference set. In this case, the maximal linearly independent system is constructed by traversing its differentially active bits.

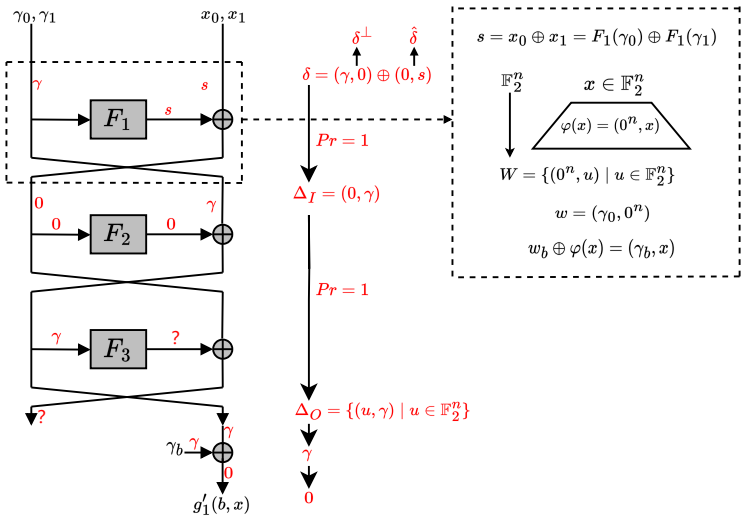

Figure 1: The 3-round Distinguisher of the Feistel structure.

According to Figure 1, in order to construct such a 3-round quantum distinguisher, the left branch of the input needs to be fixed to two distinct constants (γ_0 and γ_1) with a difference $\gamma = \gamma_0 \oplus \gamma_1$, such that the output difference of the first round function is a fixed unknown value $s = F_1(\gamma_0) \oplus F_1(\gamma_1)$, which is key-related. In this case, if the difference of the right branch equals the output difference of the first round function, the left branch of the input to the second round has a zero input difference. As $\{(0^n, \gamma)\} \to \{(u, \gamma) \mid u \in \mathbb{F}_2^n\}$ is a truncated differential of 2-round Feistel structure with probability 1. Thus, g'_1 is a periodic function, and the 3-round quantum distinguisher can be constructed.

4.2 Type-II Periodic Function

Inspired by the 3-round distinguisher of the Feistel structure, we further extend the Type-I periodic functions to construct new periodic functions.

Theorem 2. *Let $E : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which has an r_2-round truncated differential $\Delta_I \to \Delta_O$ with probability 1. Assume that there exists a difference-annihilation matrix $M \in \mathbb{F}_2^{k \times n}$ of full row rank with $Mx = \gamma$ for any $x \in \Delta_O$. Moreover, assume that the r_1-round difference transition from $\delta \to \Delta_I$ has a probability of 1 when one of the inputs belongs to a t-dimensional[2] ($t < n$) affine space $w \oplus W$, where $W = \mathrm{span}\{\zeta_1, \zeta_2, ..., \zeta_t\}$ (i.e., $\zeta_1, \zeta_2, ..., \zeta_t$ constitute a basis of W). Denote $\delta^\perp$ the projection of δ to $W^\perp$, and $\hat{\delta}$ the projection of δ to W. Let φ be a bijective linear transformation, and φ is defined as*

$$\begin{aligned} \varphi : \mathbb{F}_2^t &\to W \\ (x_1, ..., x_t) &\mapsto x_1\zeta_1 \oplus \cdots \oplus x_t\zeta_t. \end{aligned}$$

Let $w_0 = w$, $w_1 = w \oplus \delta^\perp$, and γ_0, γ_1 be two constants such that $\gamma = \gamma_0 \oplus \gamma_1$. Let g be defined as

$$\begin{aligned} g : \mathbb{F}_2 \times \mathbb{F}_2^t &\to \mathbb{F}_2^k \\ (b, x) &\mapsto M \cdot E_{r_1+r_2}(w_b \oplus \varphi(x)) \oplus \gamma_b. \end{aligned}$$

Then, g is a periodic function with a period $(1, s)$, where $s = \varphi^{-1}(\hat{\delta})$.

[2] If $t = n$, the affine space is the full space $\mathbb{F}_2^n$ and one can construct $(r_1 + r_2)$-round probability 1 truncated differentials with no input restrictions.

Proof. Since $\varphi(x) \in W$ for any $x \in \mathbb{F}_2^t$,

$$w_0 \oplus \varphi(x) = w \oplus \varphi(x) \in w \oplus W.$$

Thus, $w_0 \oplus \varphi(x)$, as one of the input to $E_{r_1+r_2}$, falls into $w \oplus W$. Moreover,

$$[w_0 \oplus \varphi(x)] \oplus [w_1 \oplus \varphi(x \oplus \varphi^{-1}(\hat{\delta}))] = w_0 \oplus w_1 \oplus \hat{\delta} = \delta^{\perp} \oplus \hat{\delta} = \delta.$$

According to the fact that the difference transition $\delta \to \Delta_I$ has a probability of 1 when one of the inputs belongs to $w \oplus W$, it can deduced that

$$E_{r_1}(w_0 \oplus \varphi(x)) \oplus E_{r_1}(w_1 \oplus \varphi(x \oplus \varphi^{-1}(\hat{\delta})) \in \Delta_I.$$

Let $s = \varphi^{-1}(\hat{\delta})$, $E_{r_2} \circ E_{r_1}(w_0 \oplus \varphi(x)) \oplus E_{r_2} \circ E_{r_1}(w_1 \oplus \varphi(x \oplus s)) \in \Delta_O$ always holds, due to $\Pr[\Delta_I \overset{E_{r_2}}{\to} \Delta_O] = 1$. Thus,

$$\begin{aligned} & g(0,x) \oplus g(1, x \oplus s) \\ =& M \cdot E_{r_1+r_2}(w_0 \oplus \varphi(x)) \oplus \gamma_0 \oplus M \cdot E_{r_1+r_2}(w_1 \oplus \varphi(x \oplus s)) \oplus \gamma_1 \\ =& M \cdot (E_{r_2} \circ E_{r_1}(w_0 \oplus \varphi(x)) \oplus E_{r_2} \circ E_{r_1}(w_1 \oplus \varphi(x \oplus s))) \oplus \gamma \\ =& \gamma \oplus \gamma = 0^k. \end{aligned}$$

This proves that g is a periodic function, and $(1, s)$ is a period. □

Remark 3 Figure 2 illustrates the construction of periodic functions in Theorem 2 from a differential point of view. Given an input x, the left and right branches of Figure 2 represent the encryption procedure of a differential pair with input difference $\varphi^{-1}(\hat{\delta})$. Besides, in order to obtain identical outputs, w_i and γ_i are XORed to the left and right branches for $i = 0$ and 1, respectively. What marked with red in the middle of Figure 2 presents the intermediate differences during the encryption procedure.

Remark 4 It should be noted that w_i and γ_i $(i = 0, 1)$ are explicitly XORed to the two branches in Figure 2, thus, they should be known to the attacker. In this case, one can get identical outputs if the inputs have a difference of $\varphi^{-1}(\hat{\delta})$, and this results in a periodic function whose period $\varphi^{-1}(\hat{\delta})$ can be recovered by Simon's algorithm. This observation confirms the fact that only $\delta^{\perp}$ is used to construct the periodic function in Theorem 2.

Definition 4. Let $E : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which has an r_2-round truncated differential $\Delta_I \to \Delta_O$ of probability 1, and an r_1-round truncated differential $\delta \to \Delta_I$ of probability 1 with the restriction that one of the inputs belongs to an affine space $w \oplus W$. If there exists a difference-annihilation matrix $M \in \mathbb{F}_2^{k \times n}$ of Δ_O and the projection of δ to $W^{\perp}$ is known, we call the periodic function as constructed in Theorem 2 a **Type-II periodic function** of $E_{r_1+r_2}$, where $E_{r_1+r_2}$ is the $(r_1 + r_2)$-round reduced version of E.

Example 2. Reconsidering the 3-round quantum distinguisher of the Feistel structure by Kuwakado and Morii, the periodic function used in such a distinguisher is a Type-II periodic function as shown in Figure 1. The symbols marked with red present the difference transition $\delta = (\gamma, s) \to (?, \gamma)$ for the 3-round Feistel structure, where γ is a fixed constant and $s = F_1(\gamma_0) \oplus F_1(\gamma_1)$ with $\gamma_0 \oplus \gamma_1 = \gamma$ (F_1 is the first round function). In this case, $r_2 = 2$, $r_1 = 1$, and the input affine space is $w \oplus W = (\gamma_0, 0^n) \oplus \{(0^n, u) \mid u \in \mathbb{F}_2^n\}$. The 2-round truncated differential $\{(0^n, \gamma)\} \to \{(u, \gamma) \mid u \in \mathbb{F}_2^n\}$ holds with probability 1 for and input. Define φ as $\varphi(x) = (0^n, x)$, where $x \in \mathbb{F}_2^n$. Moreover, it can be checked that $\delta^{\perp} = (\gamma, 0^n) \in W^{\perp}, \hat{\delta} = (0^n, s) \in W$. In this case, the 1-round difference transition from $\delta^{\perp} \oplus \hat{\delta} = \delta = (\gamma, s) \to \{(0^n, \gamma)\}$ has a probability of 1 when one of the inputs belongs to $w \oplus W$. Let $w_0 = w = (\gamma_0, 0^n)$, $w_1 = w \oplus \delta^{\perp} = (\gamma_1, 0^n)$. Thus, according to Theorem 2, we can reconstruct Kuwakado and Morii's 3-round distinguisher as $g_1' = M_1 \cdot \mathcal{E}_3^{\texttt{Feistel}}(w_b \oplus \varphi(x)) \oplus \gamma_b = M_1 \cdot \mathcal{E}_3^{\texttt{Feistel}}(\gamma_b, x) \oplus \gamma_b = R_3 \oplus \gamma_b$, where M_1 is defined as in Example 1.

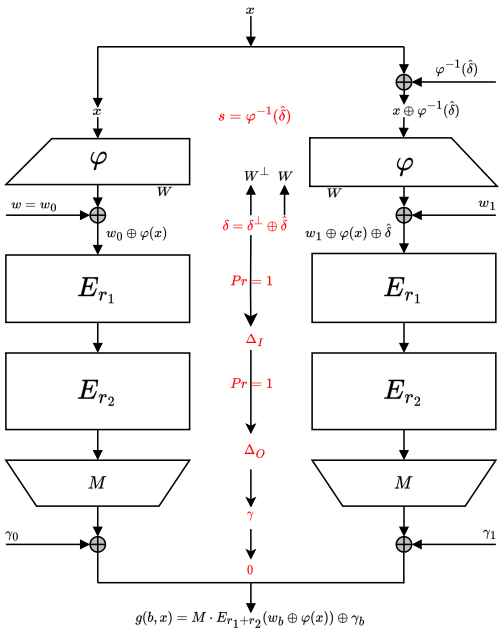

Figure 2: An illustration of **Type-II** periodic functions.

In addition to the Feistel structure, the period functions used in the quantum distinguishers of Type-1 GFS [DLW19, CGD21, NIDI19], Type-2 GFS [DLW19, CGD21], the Lai-Massey structure [MGWH22], `SM4` [HK20, CGD21, CHLS20], `MARS` [CGD21] and `Skipjack-A/B` [CGD21] are also Type-II periodic functions.

5 Applications to `LBlock` and `SIMON`

5.1 8-Round Distinguisher of `LBlock`

`LBlock` is designed from a variant of Feistel structures with the only difference that a left circular shift is performed on the right branch. Therefore, the 4-round quantum distinguisher of Feistel structure designed in [IHM+19] is also applicable to `LBlock`. However, when considering the details of the round function from truncated differentials with probability 1, longer quantum distinguishers can be devised.

The round function of `LBlock` adopts the SPN structure as shown in Figure 3. Let a single Sbox in the round function be differentially active (as a single active Sbox leads to a slower diffusion) to construct probability 1 truncated differentials. We found that each of the eight possible active Sboxes leads to the same round number of probability 1 truncated differentials. Specifically, we can deduce that if an input difference $\delta_I \in V_i$, the output difference $\delta_O \in V_{\mathtt{index}(i)}$ for $0 \le i \le 7$, where $\mathtt{index} = \{2, 0, 3, 1, 6, 4, 7, 5\}$ and

$$V_i = \{(x_0, ..., x_7) \in (\mathbb{F}_2^4)^8 \mid x_i \in \mathbb{F}_2^4, x_j = 0^4 \text{ for } j \neq i\},\ 0 \le i \le 7.$$

Thus, let $0^{32} \neq \alpha \in V_0, \alpha_0$ and α_1 be two 32-bit constants with $\alpha_0 \oplus \alpha_1 = \alpha$. Figure 3 illustrates a 7-round truncated differential $\Delta_I = \{(0^{32}, \alpha)\} \to \Delta_O$ with probability 1 for `LBlock`, where

$$\Delta_O = \{(u, y) \in (\mathbb{F}_2^{32})^2 \mid u \in \mathbb{F}_2^{32}, y \in V_1 \oplus V_2 \oplus V_3 \oplus V_4 \oplus V_5 \oplus V_6 \oplus V_7\}.$$

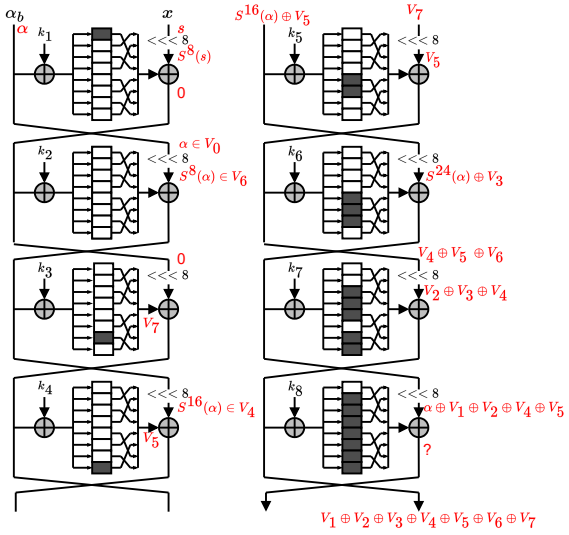

Figure 3: The 8-round distinguisher of `LBlock`.

Furthermore, there exists $W = \{(0^{32}, u) \mid u \in \mathbb{F}_2^{32}\}$,$w = (\alpha_0, 0^{32})$, $\delta^{\perp} = (\alpha, 0^{32}) \in W^{\perp}$, $\hat{\delta} = (0^{32}, s) \in W$, $s = F_1(\alpha_0) \oplus F_1(\alpha_1)$, such that the 1-round difference transition $\delta^{\perp} \oplus \hat{\delta} = (\alpha, s) \to \{(0^{32}, \alpha)\}$ has a probability of 1 when one of the inputs belongs to $w \oplus W$. Let $w_0 = w = (\alpha_0, 0^{32})$, $w_1 = w \oplus \delta^{\perp} = (\alpha_1, 0^{32})$. The corresponding linear transformation φ is defined as $\varphi(x) = (0^{32}, x)$, where $x \in \mathbb{F}_2^{32}$. Applying Algorithm 1 to Δ_O, it returns a difference-annihilation matrix M_2, where the row vectors of M_2 constitute a basis of $\Delta_O^{\perp} = \{(0^{32}, u) \mid u \in V_0\}$. According to Theorem 2, we can construct a Type-II periodic function for the 8-round `LBlock` $\mathcal{E}_8^{\texttt{LBlock}}$ as

$$\begin{aligned} g_2 : \mathbb{F}_2 \times \mathbb{F}_2^{32} &\to \mathbb{F}_2^4 \\ (b, x) &\mapsto M_2 \cdot \mathcal{E}_8^{\texttt{LBlock}}(\alpha_b, x). \end{aligned}$$

5.2 7/9-Round Distinguisher of `SIMON-32`

In [IHM+19], Ito *et al.* presented a 6-round distinguisher for Feistel-FK structures. Thus, a 6-round distinguisher for the `SIMON` family can be obtained directly. In the following, we take `SIMON-32` as an example to illustrate how to construct longer distinguishers.

7-Round Distinguisher of `SIMON-32` The round function of `SIMON-32` without the round key is defined as

$$F(x) = S^8(x) \& S^1(x) \oplus S^2(x), x \in \mathbb{F}_2^{16}.$$

Figure 4 illustrates a 6-round truncated differential

$$\Delta_I = \{(0^{16}, \alpha)\} \to \Delta_O = \{(u, y) \in (\mathbb{F}_2^{16})^2 \mid u \in \mathbb{F}_2^{16}, y \in V_{1,15}\}$$

with probability 1 for `SIMON-32`, where $\alpha = (1, 0^{15}) \in \mathbb{F}_2^{16}$, and $V_{1,15} = \{(y_0, \ldots, y_{15}) \in \mathbb{F}_2^{16} \mid y_1 = 0, y_{15} = 0\}$. Let $\alpha_0, \alpha_1 \in \mathbb{F}_2^n$, such that $\alpha_0 \oplus \alpha_1 = \alpha$. Then, there exists $W = \{(0^{16}, u) \mid u \in \mathbb{F}_2^{16}\}$, $w = (\alpha_0, 0^{16})$, $\delta^{\perp} = (\alpha, 0^{16}) \in W^{\perp}$, $\hat{\delta} = (0^{16}, s) \in W$, $s = F_1(\alpha_0) \oplus F_1(\alpha_1)$, where F_1 is the first round function of the 7-round reduced `SIMON-32`. One can verify that the 1-round difference transition $\delta^{\perp} \oplus \hat{\delta} = (\alpha, s) \to \Delta_I = \{(0^{16}, \alpha)\}$ has a probability of 1 when one of the inputs belongs to $w \oplus W$. Let $w_0 = w = (\alpha_0, 0^{16})$,

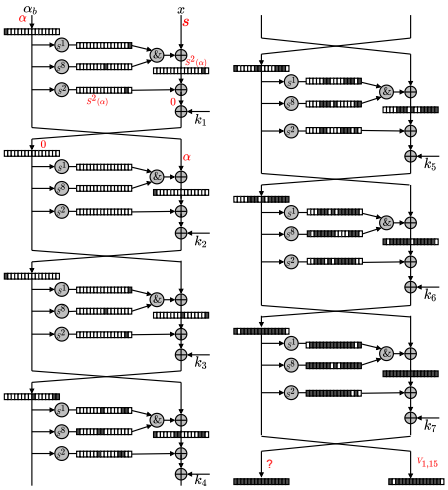

Figure 4: The 7-Round distinguisher of SIMON-32.

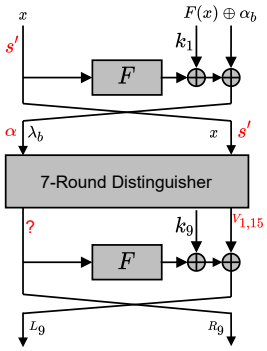

Figure 5: The 9-Round Distinguisher of SIMON-32.

$w_1 = w \oplus \delta^{\perp} = (\alpha_1, 0^{16})$, and the corresponding linear transformation φ is defined as $\varphi(x) = (0^{16}, x), x \in \mathbb{F}_2^{16}$. Then, the 7-round Type-II periodic function of SIMON-32 is

$$\begin{aligned} g_3 : \mathbb{F}_2 \times \mathbb{F}_2^{16} &\to \mathbb{F}_2^2 \\ (b, x) &\mapsto M_3 \cdot \mathcal{E}_7^{\texttt{SIMON}}(\alpha_b, x), \end{aligned}$$

where the row vectors of M_3 are composed of a set of basis of $\Delta_O^{\perp} = \{(0^{16}, u) \mid u \in V_{1,15}^{\perp}\}$.

9-round Distinguisher of SIMON-32 [IHM+19] presented a technique to construct longer distinguishers for Feistel-FK structures, which is also applicable to the SIMON family. The 9-round distinguisher for SIMON-32 can be obtained by placing the 7-round one from the second round to the eighth round, and adding one round before and after the 7-round distinguisher, respectively.

Since $(1, s)$ is a period of g_3, and $s = F_1(\alpha_0) \oplus F_1(\alpha_1) = F(\alpha_0) \oplus F(\alpha_1)$, where F is the round function of SIMON without the round key, which implies that the period does not contain any key information. Let $\lambda_b = \alpha_b \oplus k_1$ for $b \in \mathbb{F}_2$, where k_1 is the first round key of the 9-round reduced SIMON-32. Thus, $\lambda_0, \lambda_1 \in \mathbb{F}_2^n$ are two distinct and unknown constants with $\lambda_0 \oplus \lambda_1 = \alpha_0 \oplus \alpha_1 = \alpha$. Replacing α_b involved in the above 7-round distinguisher by

λ_b. Furthermore, we define

$$g_3' : \mathbb{F}_2 \times \mathbb{F}_2^{16} \to \mathbb{F}_2^2$$
$$(b, x) \mapsto M_3'(F(R_9) \oplus L_9),$$

where $(L_9, R_9) = \mathcal{E}_9^{\texttt{SIMON}}(x, F(x) \oplus \alpha_b)$, the row vectors of M_3' are composed of a set of basis of $V_{1,15}^{\perp}$. As illustrated in Figure 5, g_3' is a periodic function for the 9-round reduced `SIMON-32`, and $s' = F(\lambda_0) \oplus F(\lambda_1) = F(\alpha_0 \oplus k_1) \oplus F(\alpha_1 \oplus k_1)$ is a period.

Distinguishers for other `SIMON` variants Similarly, one can also construct longer distinguishers for other `SIMON` variants. The results are listed in Table 2, where Δ_I and Δ_O denote the input and output difference of the corresponding truncated differentials, and R_1 represents the round number of truncated differentials with probability 1, respectively. $W_{n;\Gamma} = \{(u, y) \in (\mathbb{F}_2^n)^2 \mid u \in \mathbb{F}_2^n, y = (y_0, y_1 \ldots, y_{n-1}) \in \mathbb{F}_2^n, y_i = 0, i \in \Gamma\}$, and $\Gamma \subset \{0, 1, \ldots, n-1\}$. Since one can always extend the truncated differentials for one round, and add two rounds using the technique in [IHM+19]. Thus, $R = R_1 + 3$ represents the round number of quantum distinguishers.

Table 2: Quantum Distinguishers of the `SIMON` Family.

Block size	R_1	Δ_I	Δ_O	R
32	6	$\{(0^{16}, 1, 0^{15})\}$	$W_{16;\{1,15\}}$	9
48	7	$\{(0^{24}, 1, 0^{23})\}$	$W_{24;\{1\}}$	10
64	8	$\{(0^{32}, 1, 0^{31})\}$	$W_{32;\{1,31\}}$	11
96	10	$\{(0^{48}, 1, 0^{47})\}$	$W_{48;\{1,47\}}$	13
128	12	$\{(0^{64}, 1, 0^{63})\}$	$W_{64;\{1,63\}}$	15

Note It is not difficult to observe that the periodic functions used to construct quantum distinguishes for `LBlock` and `SIMON` have a few output bits. Specifically, the periodic functions for `LBlock` and `SIMON`-32/48/64/96/128 have output sizes of 4 and 2/1/2/2/2 bits, respectively. However, this feature does not affect the distinguishing properties. It has been proved in [MS22] that Simon's algorithm still works with a small (approximately doubled) overhead even if the output size of periodic functions is a single bit.

6 Quantum Distinguishers of Cipher Structures

From previous sections, we can deduce that both Type-I and Type-II periodic functions contain a truncated differential with probability 1. This motivates us to study the round number that such truncated differentials can reach. Note that the periodic function for the 3-round Feistel structure holds for any bijective round functions, which is a structural property of the Feistel structure. Although, one can find longer distinguishers when focusing on a particular Feistel block cipher, such as `LBlock` and `SIMON`. It's necessary to study the weakness of such cipher structures against quantum distinguishing attacks. Thus, in order to study the round number of truncated differentials with probability 1, we may ignore the details of non-linear components as in [SLR+15], where the authors presented the idea of *structures* to characterize ciphers' properties which are independent of the specific details of non-linear components.

6.1 The Unified Structure

In this section, we briefly revisit the structure theory [SLR+15] and the unified structure [LSL+22].

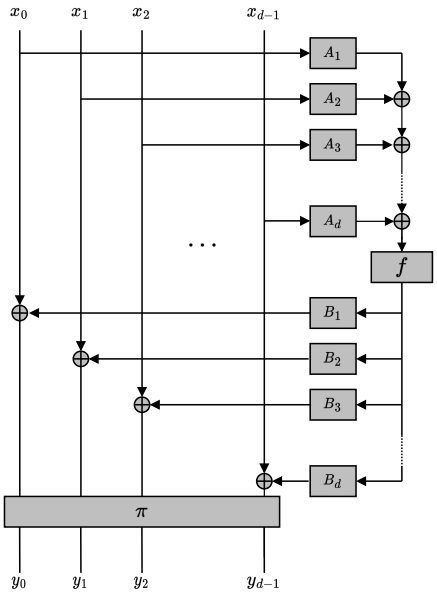

Figure 6: The Unified Structure $\mathcal{F}_{A,B,\pi}$.

Definition 5 ([SLR+15])**.** Let $E : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher with bijective S-boxes as the basic non-linear components. A structure $\mathcal{E}^E$ on $\mathbb{F}_2^n$ is defined as a set of block ciphers that are exactly the same as E except that the S-boxes can take all possible bijective transformations on the corresponding domains.

Basically, a structure is a set of block ciphers that differ only in their non-linear components. When studying cryptographic properties, one only needs to focus on those holding for all instances within the structure, i.e., irrelevant to the particular details of non-linear components. In the following, when we state a specific property of a structure, it holds for all instances of this structure. In [LSL+22], the authors revisited the Feistel and Lai-Massey structures and presented a conversion between these two classical cipher structures. As a result, they presented a unified structure covering these two structures as well as most generalized Feistel structures. The unified structure is illustrated in Figure 6.

In a unified structure, the input is divided into d branches and the width of each branch is n bits. Each round is composed of four steps: the first step applies linear transformations to each input branch, which is denoted by A_i for the i-th branch, where A_i is an $m \times n$ matrix for $i = 1, 2, \ldots, d$; the second step first sums the output of the first step and then applies a permutation $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$ to the sum; the third step applies a linear transformation B_i to the output of f and sums the output to the i-th branch, where B_i is an $n \times m$ matrix for $i = 1, 2, \ldots, d$; the last step applies a branch permutation denoted by π to all branches. In the following, we will denote an r-round unified structure by $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$, where f_i is the i-the round function. Moreover, it has been proved in [LSL+22] that $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$ is invertible if and only if $\sum_{i=1}^{d} A_i B_i = O$. Denote $A = (A_1 \ \cdots \ A_d)$ which is an $m \times dn$ matrix, and $B = (B_1^{\mathrm{T}} \ \cdots \ B_d^{\mathrm{T}})^{\mathrm{T}}$ which is a $dn \times m$ matrix. Since π is a permutation on d branches and each branch is of n bits, we will interchangeably use π as either a $d \times d$ matrix over $\mathbb{F}_2^n$ or a $dn \times dn$ matrix over $\mathbb{F}_2$ without

causing ambiguity. Denote

$$\mathcal{A}^r = \begin{pmatrix} A \\ A\pi \\ \vdots \\ A\pi^r \end{pmatrix}, \mathcal{B}^r = (B\ \pi B\ \cdots\ \pi^r B)\,.$$

6.2 Probability 1 Truncated Differentials

[LSL+22] has shown that $\mathrm{rank}(\mathcal{A}^{d-1}) < nd$ always leads to the existence of a truncated differential with probability 1 for any rounds. In this section, we will illustrate that $\mathrm{rank}(\mathcal{B}^{d-1}) < nd$ also leads to a truncated differential with probability 1.

Theorem 3. *Given a unified structure $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$. If $\mathrm{rank}(\mathcal{B}^{d-1}) < nd$, there always exists a truncated differential with probability 1 for any r.*

Proof. Since $\mathrm{rank}(\mathcal{B}^{d-1}) < nd$, there exists an $(nd - \mathrm{rank}(\mathcal{B}^{d-1})) \times nd$ non-zero matrix L of full row rank such that $L\mathcal{B}^{d-1} = O$. Taking $\mathrm{ord}(\pi) = d$ into consideration, for any integer i, we have $L\pi^i B = O$.

Let $0 \neq \Delta_0 \in \mathbb{F}_2^{nd}$ be the input difference to $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$. Let the input and output differences to f_i be α_i and $\beta_i \in \mathbb{F}_2^n$, and Δ_i be the output difference of the i-th round, where $i = 1, 2, \ldots, r$. Then we have

$$\begin{cases} \Delta_0 = \pi\Delta_0 \oplus \pi B\beta_1, \\ \Delta_1 = \pi^2\Delta_0 \oplus \pi^2 B\beta_1 \oplus \pi B\beta_2, \\ \quad\ \vdots \\ \Delta_r = \pi^r\Delta_0 \oplus \pi^r B\beta_1 \oplus \pi^{r-1} B\beta_2 \oplus \cdots \oplus \pi B\beta_r. \end{cases}$$

Therefore,

$$\begin{aligned} L\Delta_r &= L\left(\pi^r\Delta_0 \oplus \pi^r B\beta_1 \oplus \pi^{r-1} B\beta_2 \oplus \cdots \oplus \pi B\beta_r\right) \\ &= L\pi^r\Delta_0 \oplus L\pi^r B\beta_1 \oplus L\pi^{r-1} B\beta_2 \oplus \cdots \oplus L\pi B\beta_r \\ &= L\pi^r\Delta_0. \end{aligned}$$

Thus, for any input difference Δ_0, L annihilates the difference $\pi^r B\beta_1 \oplus \pi^{r-1} B\beta_2 \oplus \cdots \oplus \pi B\beta_r$ and $\{\Delta_0\} \to \{\Delta_r \mid L\Delta_r = L\pi^r\Delta_0\}$ is a truncated differential with probability 1. □

Consequently, $\mathcal{A}^{d-1}$ and $\mathcal{B}^{d-1}$ should have a rank of nd to prevent an attacker from constructing probability 1 truncated differentials for arbitrary rounds. In Proposition 1, we present the exact round number for such differentials.

Proposition 1. *Denote $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$ a unified structure with d branches and each of size n bits. Let A_i and B_i as denoted above with $\sum_{i=1}^{d} A_i B_i = O$, and f_i's are bijective. Then, there always exists an $(r_1 + r_2)$-round probability 1 truncated differential, where r_1 is the minimal number such that $\mathrm{rank}(\mathcal{A}^{r_1}) = nd$, and r_2 is the minimal number such that $\mathrm{rank}(\mathcal{B}^{r_2}) = nd$.*

Proof. According to the definition of r_1, the matrix $\mathcal{A}^{r_1-1}$ is not of full column rank. Thus, there exists a non-zero vector $\Delta_0 \in \mathbb{F}_2^{nd}$ such that $\mathcal{A}^{r_1-1}\Delta_0 = 0$. Let Δ_0 be the input difference to $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$, it can be verified that the input difference to f_1 is $A\Delta_0 = 0$. Therefore, the output difference of the first round is $\Delta_1 = \pi\Delta_0$ and the input difference to f_2 is $A\pi\Delta_0$ which is also equal to zero. Similarly, it can be deduced that the input difference to the first r_1 round functions is zero, and the output difference of the first r_1 rounds is thus deterministically being $\Delta_{r_1} = \pi^{r_1}\Delta_0$.

Since $\mathcal{B}^{r_2-1} = (B\ \pi B\ \cdots\ \pi^{r_2-1}B)$ is not of full row rank, we can find a non-zero matrix M such that $M(B\ \pi B\ \cdots\ \pi^{r_2-1}B) = O$. Denote the output difference of f_{r_1+i} by β_{r_1+i} where $i = 1, ..., r_2$. Thus, the output difference of the (r_1+1)-th round is $\Delta_{r_1+1} = \pi(\pi^{r_1}\Delta_0 \oplus B\beta_{r_1+1})$. Moreover, the output difference of the (r_1+r_2)-th round is $\Delta_{r_1+r_2} = \pi^{r_1+r_2}\Delta_0 \oplus \pi^{r_2}B\beta_{r_1+1} \oplus \pi^{r_2-1}B\beta_{r_1+2} \oplus \cdots \oplus \pi B\beta_{r_1+r_2}$. Left multiplying the matrix $M\pi^{-1}$ to $\Delta_{r_1+r_2}$, one can get

$$M\pi^{r_1+r_2-1}\Delta_0 \oplus M\pi^{r_2-1}B\beta_{r_1+1} \oplus \cdots \oplus MB\beta_{r_1+r_2} = M\pi^{r_1+r_2-1}\Delta_0. \tag{1}$$

Thus, $M\pi^{-1}$ is a difference-annihilation matrix and it annihilates $\pi^{r_2}B\beta_{r_1+1} \oplus \pi^{r_2-1}B\beta_{r_1+2} \oplus \cdots \oplus \pi B\beta_{r_1+r_2}$. Therefore, a truncated differential from $\{\Delta_0\}$ to $\{\eta \in \mathbb{F}_2^{nd} \mid M\pi^{-1}\eta = M\pi^{r_1+r_2-1}\Delta_0\}$ can be constructed for $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$ with probability 1. □

Example 3. Let $\mathcal{E}^{\mathtt{SM4}} : \mathbb{F}_2^{128} \to \mathbb{F}_2^{128}$ denote the unified structure derived from `SM4`, which means $\mathcal{E}^{\mathtt{SM4}}$ is a set of block ciphers identical to `SM4` except the round functions. The corresponding parameters are as follows. $A_1 = B_2 = B_3 = B_4 = O$, $B_1 = A_2 = A_3 = A_4 = I$, where O and I denote the 32×32 zero and identity matrices over $\mathbb{F}_2$, respectively. Moreover, the branch permutation is

$$\pi = \begin{pmatrix} O & I & O & O \\ O & O & I & O \\ O & O & O & I \\ I & O & O & O \end{pmatrix}.$$

Thus, $A = (O\ I\ I\ I)$, $B = (I\ O\ O\ O)^{\mathrm{T}}$. Since

$$\mathcal{A}^3 = \begin{pmatrix} O & I & I & I \\ I & O & I & I \\ I & I & O & I \\ I & I & I & O \end{pmatrix}, \mathcal{B}^3 = \begin{pmatrix} I & O & O & O \\ O & O & O & I \\ O & O & I & O \\ O & I & O & O \end{pmatrix}$$

are full rank matrices, we have $r_1 = r_2 = 3$.

Furthermore, $\mathcal{A}^2(\alpha, \alpha, \alpha, 0) = 0$, where $0 \neq \alpha \in \mathbb{F}_2^{32}$, and there exists the following non-zero matrix $M = (O\ I\ O\ O)$ such that $M(B\ \pi B\ \pi^2 B) = (O\ O\ O)$.

Accordingly, we can get $\{\eta \in \mathbb{F}_2^{128} \mid M\pi^{-1}\eta = M\pi^5(\alpha, \alpha, \alpha, 0)\} = \{(\alpha, u_2, u_3, u_4) \mid u_2, u_3, u_4 \in \mathbb{F}_2^{32}\}$. Thus a truncated differential $\{(\alpha, \alpha, \alpha, 0)\} \to \{(\alpha, u_2, u_3, u_4) \mid u_2, u_3, u_4 \in \mathbb{F}_2^{32}\}$ with probability 1 and covering 6 rounds can be constructed for $\mathcal{E}^{\mathtt{SM4}}$, which can be obtained directly from Figure 7.

6.3 Bounding Probability 1 Truncated Differentials

Proposition 1 presents a lower bound for probability 1 truncated differentials that one can construct. Conversely, if the round number $r > r_1 + r_2$, it can be proved that, for any fixed input difference Δ_0, one cannot find a truncated differential with probability 1 such that all instance of $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$ conforming it.

Proposition 2. *Denote $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$ a unified structure with d branches and each of size n bits. Let A_i and B_i as denoted above with $\sum_{i=1}^{d} A_i B_i = O$. Assume $A\pi^i B$'s $(i = 1, 2, \ldots, d-1)$ are invertible matrices, and f_i's are bijective. Then, there doesn't exists an r-round probability 1 truncated differential when $r > r_1 + r_2$, where r_1 is the minimal number such that* $\mathrm{rank}(\mathcal{A}^{r_1}) = nd$, *and r_2 is the minimal number such that* $\mathrm{rank}(\mathcal{B}^{r_2}) = nd$.

Proof. For any given non-zero input difference Δ_0 to the structure, assume that the first r' rounds have a zero difference to the round function. According to the proof of Proposition 1, it can be deduced that $r' \leq r_1$.

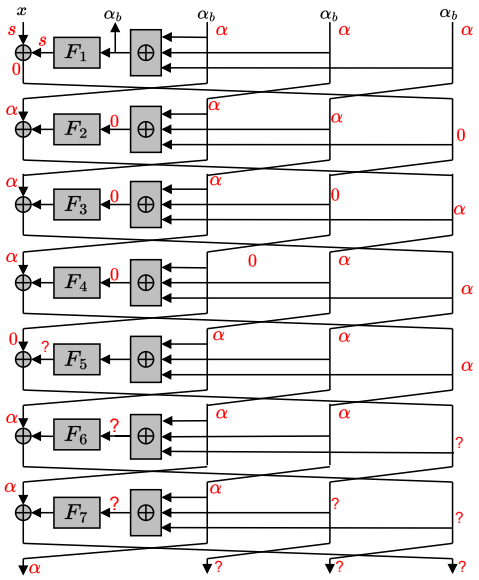

Figure 7: A 7-Round distinguisher of SM4.

Denote the output difference of $f_{r'+i}$ by $\beta_{r'+i}$, then the input difference to the $(r'+i)$-th round is

$$\Delta_{r'+i} = \pi^{r'+i-1}\Delta_0 \oplus \pi^{i-1}B\beta_{r'+1} \oplus \cdots \oplus \pi B\beta_{r'+i-1}$$

for $i = 1, 2, \ldots, r - r'$, and the input difference to $f_{r'+i}$ is

$$\alpha_{r'+i} = A\pi^{r'+i-1}\Delta_0 \oplus A\pi^{i-1}B\beta_{r'+1} \oplus \cdots \oplus A\pi B\beta_{r'+i-1}.$$

When $i = 1$, $\alpha_{r'+1} = A\pi^{r'}\Delta_0 \neq 0$. Thus, $\beta_{r'+1}$ can take any non-zero difference. Since $\alpha_{r'+2} = A\pi^{r'+1}\Delta_0 \oplus A\pi B\beta_{r'+1}$, $\beta_{r'+2}$ can take any non-zero difference when $A\pi^{r'+1}\Delta_0 = 0$. Moreover, $\beta_{r'+2}$ can be zero if $A\pi^{r'+1}\Delta_0 \neq 0$ and $A\pi^{r'+1}\Delta_0 \oplus A\pi B\beta_{r'+1} = 0$. Similarly, $\alpha_{r'+i} = A\pi^{r'+i}\Delta_0 \oplus A\pi^{r'+i-1}B\beta_{r'+1} \oplus \cdots \oplus A\pi B\beta_{r'+i-1}$, thus $\beta_{r'+i}$ can take any difference for $i \geq 3$.

Assume that there exists a matrix M such that

$$M \cdot \Delta_{r+1} = M \cdot \pi^{r}\Delta_0 \oplus M \cdot \pi^{r-r'}B\beta_{r'+1} \oplus \cdots \oplus M \cdot \pi B\beta_{r}$$

is a fixed constant. For any fixed $\beta_{r'+1}, \beta_{r'+2}, \ldots, \beta_{r-1}$, there are two possibilities for the input difference α_r to f_r. The first case is that $\alpha_r \neq 0$ and β_r can take any non-zero difference. Since

$$M \cdot \Delta_{r+1} \oplus M \cdot \pi^{r}\Delta_0 \oplus M \cdot \pi^{r-r'}B\beta_{r'+1} \oplus \cdots \oplus M \cdot \pi^2 B\beta_{r-1}$$

is fixed and equal to $M \cdot \pi B\beta_r$. It requires that $M \cdot \pi B = 0$. The other case is that $\alpha_r = 0$, and we can choose other values for $\beta_{r'+1}, \beta_{r'+2}, \ldots, \beta_{r-1}$ such that $\alpha_r \neq 0$. Therefore, it can be deduced that $M \cdot \pi B = O$. Thus, $M \cdot \pi B$ must be a zero matrix in either case. Similarly, $M \cdot \pi^{r-r'}B = \cdots = M \cdot \pi^2 B = O$, and $M\pi(B\ \pi B\ \cdots\ \pi^{r-r'-1}B) = O$. Since $r - r' - 1 \geq r_2$, it can be inferred that $(B\ \pi B\ \cdots\ \pi^{r-r'-1}B)$ is of full row rank, and M must be a zero matrix. □

This subsection presents the upper bound on the round number of probability 1 truncated differentials for a unified structure. Thus, we have the following results.

Proposition 3. *Denote $\mathcal{F}_{A,B,\pi}(f_1,...,f_r)$ a unified structure with d branches and each of size n bits. Let $\sum_{i=1}^{d} A_iB_i = O$. Assume that $A\pi^iB$'s $(i = 1, 2, \ldots, d-1)$ are invertible matrices, and f_i's are bijective. Then, a Type-I periodic function covers at most $(r_1 + r_2)$ rounds for $\mathcal{F}_{A,B,\pi}(f_1,...,f_r)$, where r_1 is the minimal number such that* $\mathrm{rank}(\mathcal{A}^{r_1}) = nd$, *and r_2 is the minimal number such that* $\mathrm{rank}(\mathcal{B}^{r_2}) = nd$.

It should be noted that Proposition 3 presents an upper bound for Type-I periodic functions for a unified structure. If one considers a specific instance within the structure, longer Type-I periodic functions may exist.

6.4 On the Extension of Probability 1 Truncated Differentials

A Type-I periodic function is constructed directly from a truncated differential with probability 1. However, a Type-II periodic function is constructed from a truncated differential by extending it backward for several rounds. To make the difference transition hold deterministically when extending backward, one has to restrict the input to a subset. This subsection further discusses the extension of probability 1 truncated differentials for unified structures.

Given a unified structure $\mathcal{F}_{A,B,\pi}(f_1,...,f_r)$ with a truncated differential $\Delta_I \to \Delta_O$ of probability 1, we only consider the case that $|\Delta_I| = 1$, i.e., there is only a single input difference as this is the common case. Denote the difference in Δ_I by Δ, which is a fixed and known constant. Assume that we propagate Δ backward for r rounds. And we denote the round index from -1 to $-r$ when extending backward. Let x be the input to the structure. Let u_{-i} and v_{-i} denote the input and output of f_{-i} for $i = 1, 2, \ldots, r$. Then,

$$\begin{aligned} u_{-r} =& Ax, \\ u_{1-r} =& A\pi x \oplus A\pi B v_{-r}, \\ & \vdots \\ u_1 =& A\pi^{r-1}x \oplus A\pi^{r-1}Bv_{-r} \oplus \cdots \oplus A\pi B v_{-2}. \end{aligned}$$

To make differences propagate deterministically, the input u_{-i}'s to the first r round functions should be constants. Note that v_{-i}'s are the output of the round function, which are also constants. Thus, $A\pi^i x$ should be fixed constant for $i = 0, 1, \ldots, r-1$. Without loss of generality, we assume that $\mathcal{A}^{r-1}x = 0$. and denote W the solution space of $\mathcal{A}^{r-1}x = 0$. Thus, $W^{\perp}$, which is the orthogonal complement of W, is the linear space spanned by the row vectors of $\mathcal{A}^{r-1}$.

In this case, when we consider a pair of inputs with a given input difference, the output difference of the r-round encryption is an unknown constant, as the input to each round function is fixed which results in an unknown fixed round function output difference. Denote the input and output difference of f_{-i} by α_{-i} and β_{-i}, the input difference of the $(-i)$-th round by Δ_{-i}. Then,

$$\begin{cases} \Delta_{-1} =& \pi^{-1}\Delta \oplus B\beta_{-1}, \\ \Delta_{-2} =& \pi^{-2}\Delta \oplus \pi^{-1}B\beta_{-1} \oplus B\beta_{-2}, \\ & \vdots \\ \Delta_{1-r} =& \pi^{1-r}\Delta \oplus \pi^{2-r}B\beta_{-1} \oplus \cdots \oplus B\beta_{1-r}, \\ \Delta_{-r} =& \pi^{-r}\Delta \oplus \pi^{1-r}B\beta_{-1} \oplus \cdots \oplus B\beta_{-r}. \end{cases}$$

It should be noted that Δ is a fixed and known constant. β_{-i}'s are fixed and unknown constants. According to Theorem 2, the projection of Δ_{-r} to $W^{\perp}$ should be a known

constant. That is,

$$\begin{aligned}&\begin{pmatrix} A \\ A\pi \\ \vdots \\ A\pi^{r-1} \end{pmatrix} \begin{pmatrix} B & \pi^{-1}B & \cdots & \pi^{1-r}B \end{pmatrix} \begin{pmatrix} \beta_{-r} \\ \beta_{1-r} \\ \vdots \\ \beta_{-1} \end{pmatrix} \\ =&\begin{pmatrix} AB & A\pi^{-1}B & \cdots & A\pi^{1-r}B \\ A\pi B & AB & \cdots & A\pi^{2-r}B \\ \vdots & \vdots & \ddots & \vdots \\ A\pi^{r-1}B & A\pi^{r-2}B & \cdots & AB \end{pmatrix} \begin{pmatrix} \beta_{-r} \\ \beta_{1-r} \\ \vdots \\ \beta_{-1} \end{pmatrix}\end{aligned} \tag{2}$$

should be a constant known to the attacker. This indicates that the extended round number is related to specific forms of $A\pi^i B$. In the following, we discuss two commonly used generalized Feistel structures to illustrate the backward extension.

Case 1 $A\pi^i B = I$ for $i = 1, 2, ..., d-1$, where d is the branch number. Note that the classical two-branch Feistel network, SM4-like, and MARS-like structures fall into this case.

Case 2 $A\pi B = I$ and $A\pi^i B = O$ for $i = 2, 3, ..., d-1$, where d is the branch number. This case applies to the Type-1 generalized Feistel structure.

For the first case, Equation (2) indicates that

$$\begin{pmatrix} O & I & \cdots & I \\ I & O & \cdots & I \\ \vdots & \vdots & \ddots & \vdots \\ I & I & \cdots & O \end{pmatrix} \begin{pmatrix} \beta_{-r} \\ \beta_{1-r} \\ \vdots \\ \beta_{-1} \end{pmatrix} = \begin{pmatrix} \beta_{1-r} \oplus \beta_{2-r} \oplus \cdots \oplus \beta_{-1} \\ \beta_{-r} \oplus \beta_{2-r} \oplus \cdots \oplus \beta_{-1} \\ \vdots \\ \beta_{-r} \oplus \beta_{1-r} \oplus \cdots \oplus \beta_{-2} \end{pmatrix} \tag{3}$$

should be known constants. When $r = 1$, Equation (3) is equivalent to $AB\beta_1 = 0$, which is a fixed and known constant. Thus, one can always extend a probability 1 truncated differential for one round. However, when $r \geq 2$, Equation (3) involves some unknown constants β_i's, and this prevents us from extending the distinguisher for more than one round.

Proposition 4. *Denote $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$ a unified structure with d branches and each of size n bits. Let $\sum_{i=1}^{d} A_i B_i = O$. Assume that $A\pi^i B = I$ for $i = 1, 2, \ldots, d-1$, and f_i's are bijective. Then, there exists an $(r_1 + r_2 + 1)$-round quantum distinguisher for $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$, where r_1 is the minimal number such that $\mathrm{rank}(\mathcal{A}^{r_1}) = nd$, and r_2 is the minimal number such that $\mathrm{rank}(\mathcal{B}^{r_2}) = nd$.*

Example 4. Take `SM4` in Example 3 as an example again. A 6-round truncated differential from $\{(\alpha, \alpha, \alpha, 0)\}$ to $\{(\alpha, u_2, u_3, u_4) | u_2, u_3, u_4 \in \mathbb{F}_2^{32}\}$ can be constructed for $\mathcal{E}^{SM4}$ with probability 1. This extension requires $W = \{x \in \mathbb{F}_2^{128} | Ax = 0\} = \{(u_0, u_1, u_2, u_1 \oplus u_2) \mid u_0, u_1, u_2 \in \mathbb{F}_2^{32}\}$. Moreover, we note that $\{(u, 0, 0, 0) \mid u \in \mathbb{F}_2^{32}\}$ is a subspace of W. So we can take $W = \{(u, 0, 0, 0) \mid u \in \mathbb{F}_2^{32}\}$, $w = (0, \alpha_0, \alpha_0, \alpha_0)$, the input difference $\delta = (s, \alpha, \alpha, \alpha)$, where α_0, α_1 are fixed and known constants, $\alpha_0 \oplus \alpha_1 = \gamma$, and $s = F_1(\alpha_0) \oplus F_1(\alpha_1)$. Clearly the projection of δ to $W^\perp$ equals $(0, 0, \alpha, 0)$, which is a known constant. which can be obtained directly from Figure 7.

For the second case, we can still make a similar analysis. However, this situation is a bit tricky here, and we focus on extending the input difference which is constructed as presented in Section 6.2.

Proposition 5. *Denote $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$ a unified structure with d branches and each of size n bits. Let $\sum_{i=1}^{d} A_i B_i = O$. Assume that $A\pi B = I$, $A\pi^i B = O$ $(i = 2, 3, \ldots, d-1)$,*

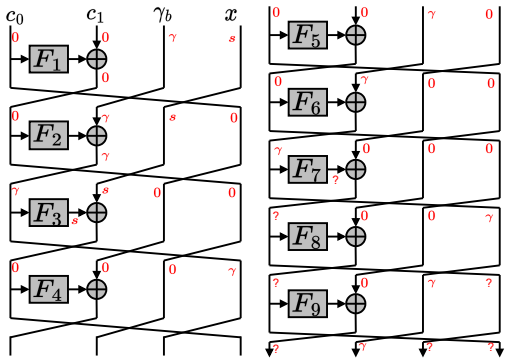

Figure 8: 9-Round Distinguisher of 4-branch Type-1 GFS.

and f_i's are bijective. Assume that $r_1 = d-1$ is the minimal number such that $\mathrm{rank}(\mathcal{A}^{r_1}) = nd$ *and r_2 is the minimal number such that* $\mathrm{rank}(\mathcal{B}^{r_2}) = nd$*. Then, there exists an $(2r_1+r_2)$-round quantum distinguisher for $\mathcal{F}_{A,B,\pi}(f_1, ..., f_r)$.*

Proof. According to Section 6.2, we can construct an (r_1+r_2)-round probability 1 truncated differential, whose input difference Δ satisfies $A\Delta = A\pi\Delta = \cdots = A\pi^{r_1-1}\Delta = 0, A\pi^{r_1}\Delta \neq 0$. Therefore, we consider propagating Δ backward for $r = r_1$ rounds.

Since $AB = O$, $A\pi B = I$, and $A\pi^i B = O$ for $i = 2, 3, \ldots, d-1$, it follows that $\alpha_{-i} = A\Delta_{-i} = A\pi^{-i}\Delta$ for $i = 1, 2, \ldots, r_1$. As $A\Delta = A\pi\Delta = \cdots = A\pi^{r_1-1}\Delta = 0$, we have $A\pi^{r_1-i}\Delta = 0$ for $i = 1, \ldots, r_1$. Thus, $\alpha_{-i} = A\pi^{d-i}\Delta = A\pi^{r_1-(i-1)}\Delta = 0$ for $i = 2, 3, \ldots, r_1$, and this results to $\beta_{-2} = \beta_{-3} = \cdots = \beta_{-r_1} = 0$. With a similar deduction as in Proposition 4, Equation (2) indicates that

$$\begin{pmatrix} O & O & \cdots & O & O \\ I & O & \cdots & O & O \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & \cdots & I & O \end{pmatrix} \begin{pmatrix} \beta_{-r_1} \\ \beta_{1-r_1} \\ \vdots \\ \beta_{-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \beta_{-r_1} \\ \vdots \\ \beta_{-2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{4}$$

Thus, the projection of Δ_{-r_1} to W is indeed a known constant, and one can extend such a probability 1 truncated differential for $r_1 = d-1$ rounds. □

Example 5. Figure 8 illustrates a 9-round distinguisher for the 4-branch Type-1 generalized Feistel structure that can be constructed according to Proposition 5, where $r_1 = r_2 = 3$. This distinguisher is constructed based on the 6-round truncated differential $\{(0,0,0,\gamma)\} \to \{(u_1, \gamma, u_2, u_3) \mid u_1, u_2, u_3 \in \mathbb{F}_2^n\}$ with probability 1, where $\gamma \in \mathbb{F}_2^n, \gamma \neq 0$. Then, one can extend the input difference backward for 3 rounds. This extension requires

$$W = \{x \in \mathbb{F}_2^{4n} \mid \mathcal{A}^2 x = 0\} = \{(0,0,0,u) \mid u \in \mathbb{F}_2^n\}.$$

And we can take $w = (c_0, c_1, \gamma_0, 0)$, the input difference $\delta = (0, 0, \gamma, s)$, where $c_0, c_1, \gamma_0, \gamma_1$ are fixed and known constants, $\gamma_0 \oplus \gamma_1 = \gamma$, and

$$s = F_3(F_2(F_1(c_0) \oplus c_1) \oplus \gamma_0) \oplus F_3(F_2(F_1(c_0) \oplus c_1) \oplus \gamma_1).$$

Clearly the projection of δ to $W^{\perp}$ equals $(0, 0, \gamma, 0)$, which is a known constant.

It should be noted that Proposition 4 and 5 present a structural property of cipher structures, which holds for all instances within such a structure. In particular, the 7-round quantum distinguish holds for all SM4 variants with a different permutation round function. However, one should realize that longer quantum distinguishers may exist if the round function details are considered.

7 Conclusion

In this paper, we established the links between quantum distinguishers and truncated differentials with probability 1 for the first time. This enables us to use classic truncated differential cryptanalysis techniques to analyze the quantum security of block ciphers. Moreover, a general approach to constructing quantum distinguishers from truncated differentials is proposed in this paper, which can serve as a generic quantum cryptanalysis vector applicable to any block cipher. Moreover, this technique releases us from the tedious manual work of verifying the periodic property functions. As an illustration of our technique, we found better distinguishers for `SIMON` and `LBlock`.

On the other hand, we studied quantum resistance against unified structures. We established an upper bound on the length of probability 1 truncated differential, which bounds the round number of quantum distinguishers constructed from Type-I periodic functions. Although longer quantum distinguishers may exist for a specific cipher, this upper bound reflects the structural property of the underlying cipher structure. It can help with the cipher designs to evaluate its linear building blocks.

Acknowledgments

We would like to thank Professor Santanu Sarkar for his guidance and the anonymous reviewers for their valuable comments and suggestions. This work was supported by the National Natural Science Foundation of China (No: 62272147, U2336209, 62272470), the Science and Technology on Communication Security Laboratory Foundation (No: 6142103012207), the Innovation Group Project of the Natural Science Foundation of Hubei Province of China (No: 2023AFA021), the Wuhan Science and Technology Bureau (No: 2022010801020328), the Scientific Research Plan of National University of Defense Technology (No: ZK21-36), and the Innovation Program for Quantum Science and Technology (No: 2021ZD0302902).

References

[BHN+19] Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher. Quantum attacks without superposition queries: The offline simon's algorithm. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 552–583. Springer, 2019. 1

[BLN14] Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-linear cryptanalysis revisited. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 411–430. Springer, 2014. 2.2

[BNS19a] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. On quantum slide attacks. In Kenneth G. Paterson and Douglas Stebila, editors, *Selected Areas in Cryptography - SAC 2019 - 26th International Conference, Waterloo, ON, Canada, August 12-16, 2019, Revised Selected Papers*, volume 11959 of *Lecture Notes in Computer Science*, pages 492–519. Springer, 2019. 1

[BNS19b] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. Quantum security analysis of AES. *IACR Trans. Symmetric Cryptol.*, 2019(2):55–93, 2019. 1

[CGD21] Jingyi Cui, Jiansheng Guo, and Shuzhen Ding. Applications of simon's algorithm in quantum attacks on Feistel variants. *Quantum Inf. Process.*, 20(3):117, 2021. 4.2

[CHLS20] Carlos Cid, Akinori Hosoyamada, Yunwen Liu, and Siang Meng Sim. Quantum cryptanalysis on contracting feistel structures and observation on related-key settings. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 373–394. Springer, 2020. 4.2

[CKS21] Amit Kumar Chauhan, Abhishek Kumar, and Somitra Kumar Sanadhya. Quantum free-start collision attacks on double block length hashing with round-reduced AES-256. *IACR Trans. Symmetric Cryptol.*, 2021(1):316–336, 2021. 1

[CLS22] Federico Canale, Gregor Leander, and Lukas Stennes. Simon's algorithm and symmetric crypto: Generalizations and automatized applications. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, volume 13509 of *Lecture Notes in Computer Science*, pages 779–808. Springer, 2022. 2.5

[DDW20] Xiaoyang Dong, Bingyou Dong, and Xiaoyun Wang. Quantum attacks on some Feistel block ciphers. *Des. Codes Cryptogr.*, 88(6):1179–1203, 2020. 1

[DLW19] Xiaoyang Dong, Zheng Li, and Xiaoyun Wang. Quantum cryptanalysis on some generalized Feistel schemes. *Sci. China Inf. Sci.*, 62(2):22501:1–22501:12, 2019. 1, 3, 4.2

[DSS+20] Xiaoyang Dong, Siwei Sun, Danping Shi, Fei Gao, Xiaoyun Wang, and Lei Hu. Quantum collision attacks on AES-like hashing with low quantum random access memories. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 727–757. Springer, 2020. 1

[DW18] Xiaoyang Dong and Xiaoyun Wang. Quantum key-recovery attack on Feistel structures. *Sci. China Inf. Sci.*, 61(10):102501:1–102501:7, 2018. 1

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996. 1

[HK20] Samir Hodzic and Lars R. Knudsen. A quantum distinguisher for 7/8-round SMS4 block cipher. *Quantum Inf. Process.*, 19(11):411, 2020. 3, 4.2

[HKK20] Samir Hodzic, Lars Ramkilde Knudsen, and Andreas Brasen Kidmose. On quantum distinguishers for type-3 generalized Feistel network based on separability. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings*, volume 12100 of *Lecture Notes in Computer Science*, pages 461–480. Springer, 2020. 1

[HS18] Akinori Hosoyamada and Yu Sasaki. Quantum demiric-selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, volume 11035 of *Lecture Notes in Computer Science*, pages 386–403. Springer, 2018. 1

[HS20] Akinori Hosoyamada and Yu Sasaki. Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 249–279. Springer, 2020. 1

[IHM+19] Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata. Quantum chosen-ciphertext attacks against Feistel ciphers. In Mitsuru Matsui, editor, *Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings*, volume 11405 of *Lecture Notes in Computer Science*, pages 391–411. Springer, 2019. 1, 1, 2.4, 5.1, 5.2, 5.2, 5.2

[KLLN16a] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237. Springer, 2016. 1, 2.4

[KLLN16b] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(1):71–94, 2016. 1

[KLT15] Stefan Kölbl, Gregor Leander, and Tyge Tiessen. Observations on the SIMON block cipher family. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 161–185. Springer, 2015. 1

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2682–2685. IEEE, 2010. 1, 2.4, 3

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 312–316. IEEE, 2012. 1, 3

[Knu94] Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer, 1994. 2.2

[LLW17] Zhengbin Liu, Yongqiang Li, and Mingsheng Wang. Optimal differential trails in SIMON-like ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(1):358–379, 2017. 1

[LM17] Gregor Leander and Alexander May. Grover meets simon - quantumly attacking the FX-construction. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 161–178. Springer, 2017. 1

[LPS21] Gaëtan Leurent, Clara Pernot, and André Schrottenloher. Clustering effect in Simon and Simeck. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I*, volume 13090 of *Lecture Notes in Computer Science*, pages 272–302. Springer, 2021. 1

[LSL+22] Jiajie Liu, Bing Sun, Guoqiang Liu, Xinfeng Dong, Li Liu, Hua Zhang, and Chao Li. New wine old bottles: Feistel structure revised. *IEEE Transactions on Information Theory*, 2022. 6.1, 6.1, 6.1, 6.2

[LTW18] Gregor Leander, Cihangir Tezcan, and Friedrich Wiemer. Searching for subspace trails and truncated differentials. *IACR Trans. Symmetric Cryptol.*, 2018(1):74–100, 2018. 2.2

[MGWH22] Shuping Mao, Tingting Guo, Peng Wang, and Lei Hu. Quantum attacks on Lai-Massey structure. In Jung Hee Cheon and Thomas Johansson, editors, *Post-Quantum Cryptography - 13th International Workshop, PQCrypto 2022, Virtual Event, September 28-30, 2022, Proceedings*, volume 13512 of *Lecture Notes in Computer Science*, pages 205–229. Springer, 2022. 4.2

[MS22] Alexander May and Lars Schlieper. Quantum period finding is compression robust. *IACR Trans. Symmetric Cryptol.*, 2022(1):183–211, 2022. 5.2

[NIDI19] Boyu Ni, Gembu Ito, Xiaoyang Dong, and Tetsu Iwata. Quantum attacks against type-1 generalized Feistel ciphers and applications to CAST-256. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Hyderabad, India, December 15-18, 2019, Proceedings*, volume 11898 of *Lecture Notes in Computer Science*, pages 433–455. Springer, 2019. 1, 3, 4.2

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. 1

[Sim97] Daniel R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997. 1, 2.3

[SLR+15] Bing Sun, Zhiqiang Liu, Vincent Rijmen, Ruilin Li, Lei Cheng, Qingju Wang, Hoda AlKhzaimi, and Chao Li. Links among impossible differential, integral and zero correlation linear cryptanalysis. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 95–115. Springer, 2015. 6, 6.1, 5

[WHG+19] Senpeng Wang, Bin Hu, Jie Guan, Kai Zhang, and Tairong Shi. Milp-aided method of searching division property using three subsets and applications. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III*, volume 11923 of *Lecture Notes in Computer Science*, pages 398–427. Springer, 2019. 1

[WZ11] Wenling Wu and Lei Zhang. LBlock: A lightweight block cipher. In Javier López and Gene Tsudik, editors, *Applied Cryptography and Network Security - 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings*, volume 6715 of *Lecture Notes in Computer Science*, pages 327–344, 2011. 1

[XZBL16] Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 648–678, 2016. 1

[ZSLS15] Guangyao Zhao, Bing Sun, Chao Li, and Jinshu Su. Truncated differential cryptanalysis of PRINCE. *Secur. Commun. Networks*, 8(16):2875–2887, 2015. 2.2, 1

[ZWSW23] Zhongya Zhang, Wenling Wu, Han Sui, and Bolin Wang. Quantum attacks on type-3 generalized Feistel scheme and unbalanced Feistel scheme with expanding functions. *Chinese Journal of Electronics*, 32(2):209–216, 2023. 1