Chinese Journal of Electronics
Vol.32, No.2, Mar. 2023

# Quantum Attacks on Type-3 Generalized Feistel Scheme and Unbalanced Feistel Scheme with Expanding Functions

ZHANG Zhongya[1,2,3], WU Wenling[1,2], SUI Han[1,4], and WANG Bolin[1,2]

(1. *Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China*)

(2. *University of Chinese Academy of Sciences, Beijing 100049, China*)

(3. *Luoyang Normal University, Luoyang 471934, China*)

(4. *State Key Laboratory of Cryptology, Beijing 100178, China*)

**Abstract — Quantum algorithms are raising concerns in the field of cryptography all over the world. A growing number of symmetric cryptography algorithms have been attacked in the quantum setting. Type-3 generalized Feistel scheme (GFS) and unbalanced Feistel scheme with expanding functions (UFS-E) are common symmetric cryptography schemes, which are often used in cryptographic analysis and design. We propose quantum distinguishing attacks on Type-3 GFS and UFS-E in the quantum chosen plaintext attack setting. The results of key recovery are better than those based on exhaustive search in the quantum setting.**

**Key words — Quantum attacks, Block ciphers, Unbalanced Feistel scheme with expanding functions, Type-3 generalized Feistel scheme.**

## I. Introduction

It is well known that the development of quantum computing has a significant impact on cryptographic algorithms. Particularly, there has been a turning point in quantum cryptanalysis in accordance with the advent that a new quantum attack was identified [1], [2]. Even-Mansour (EM) cipher [3] and 3-round Feistel scheme [4] can be attacked in polynomial time. Subsequently, quantum cryptanalysis of symmetric cryptography has become a hot spot in the current cryptography. Over the past decade, based on the acceleration advantage of quantum algorithms [5], [6] in previous research, various symmetric crypto-graphic schemes have been attacked in the quantum setting [7]–[16].

Feistel scheme [17] is very important and widely studied. Many standards ciphers are designed based on Feistel. Zheng *et al.* [18] summarize some generalized Feistel schemes (GFSs) as Type-1/2/3 GFS. CAST-256, RC6, CLEFIA, FMix and AEGIS are designed based on the three GFSs. In addition, unbalanced Feistel scheme (UFS) with contracting functions is denoted as UFS-C, SMS4 is designed based on this scheme. The block cipher MARS and the hash function CRUNCH is based on UFS with expanding functions (UFS-E) [19].

Because of the importance of the Feistel schemes, studying the security of GFS, UFS-E, and UFS-C is of great significance in postquantum conditions. Dong *et al.* [8] propose quantum distinguishing attacks and key recovery attacks on Type-1 and Type-2 GFSs in the quantum chosen plaintext attack (qCPA) setting, respectively. In PQCrypto 2020 [12], Hodžić *et al.* propose the quantum polynomial cryptanalysis of 4-round 4-branch Type-3 GFS, while the complexity of the distinguishing attack of 5-round Type-3 GFS is exponential level. You *et al.* propose a 6-round distinguisher of SMS4 in the qCPA setting in polynomial time [14]. In INDOCRYPT 2020 [15], Cid *et al.* investigate the quantum security of 7-round SMS4, and prove that 7-round SMS4 is insecure. Qian *et al.* study the quantum security of UFS-E [16]. They propose two quantum chosen ciphertext attack (qCCA) setting, respectively.

**Our contributions** We carry out quantum at-

Manuscript Received Sept. 30, 2021; Accepted Dec. 31, 2021. This work was supported by the National Natural Science Foundation of China (62072445) and the National Key Research and Development Program of China (2021YFB3100100).
 DOI:10.23919/cje.2021.00.294

tacks on the Type-3 GFS and UFS-E in this paper. Our results are better than those of Hodžić *et al.*'s [12] and Qian *et al.*'s [16]. Our main results are shown in Table 1 and Table 2.

**Table 1. The quantum distinguishing attacks on the Type-3 GFS and UFS-E**

| Schemes | Settings | #Branches | #Rounds | Complexity | Source |
|---|---|---|---|---|---|
| Type-3 GFS | qCPA | $d$ | $d+1$ | $O(n)$ | Section III |
| | | 4 | 4 | $O(n)$ | [12] |
| | | | 5 | $O(n)$ | Section III |
| | | | | $O(2^n)$ | [12] |
| UFS-E | qCPA | $d$ | $d+1$ | $O(n)$ | Section IV |
| | | $d$ | $d$ | $O(n)$ | [16] |
| | qCCA | $d$ | $d+1$ | $O(n)$ | [16] |

**Table 2. The quantum key-recovery on the Type-3 GFS and UFS-E**

| Schemes | #Branches | #Rounds | Complexity (log) | Trivial bound (log) |
|---|---|---|---|---|
| Type-3 GFS | $d$ | $r \geq d+2$ | $(d-1)(r-d-1)k/2$ | $(d-1)rk/2$ |
| UFS-E | $d$ | $d+2 \leq r \leq 2d$ | $(r-d-1)(r-d)k/4$ | $(d-1)rk/2$ |
| | | $r > 2d$ | $(d-1)(2r-3d)k/4$ | $(d-1)rk/2$ |

Firstly, a quantum distinguishing analysis on Type-3 GFS is proposed in the qCPA setting. We construct a periodic function by using the XOR of two different outputs of the same branch, and give a distinguisher of reduced round Type-3 GFS in the qCPA setting. The quantum query complexity of distinguishing attack is polynomial time. Note that, Hodžić *et al.* show that the 5-round Type-3 GFS with 4-branch is secure in the qCPA setting in PQCrypto 2020. In addition, we give key recovery on Type-3 GFS. Assume that the sub-keys are independent. Our result is better than that based on exhaustive search in the quantum setting.

Secondly, we also evaluate UFS-E against quantum attacks, and it has not been addressed in previous works. In the qCPA setting, we construct a periodic function of UFS-E by using the XOR of two different outputs of the same branch and exchanging two different terms, and give a distinguisher of UFS-E. The quantum query complexity is polynomial time. In addition, we give key recovery on UFS-E. We assume that the sub-keys are independent of each other. Our results are better than those based on exhaustive search.

**Organization** To begin with, we introduce some preliminaries in Section II. Section III illustrates our quantum attacks on Type-3 GFS. Section IV demonstrates the quantum attacks of UFS-E. Finally, this paper concludes in Section V.

## II. Preliminaries

### 1. Simon's algorithm

We briefly introduce Simon's problem and Simon's algorithm [4] firstly.

Simon's problem. Assume function $f:\{0,1\}^n \to \{0,1\}^n$ has a period $s \in \{0,1\}^n$, and $x' = x \oplus s \Leftrightarrow f(x) = f(x')$ for $x \neq x'$, our goal is to find the period $s$.

One needs $O(2^{n/2})$ queries to find $s$ in the classical setting. Simon's algorithm could find $s$ with $O(n)$ queries. The algorithm repeats the following quantum steps.

Step 1: Giving two quantum registers with state $|0\rangle|0\rangle$, then Hadamard transform is applied to the first register.

Step 2: Querying to $f(x)$, get $2^{-n/2}\sum_x |x\rangle|f(x)\rangle$.

Step 3: Applying Hadamard transform on the first register, then gives $2^{-n/2}\sum_{x,y}(-1)^{y\cdot x}|y\rangle|f(x)\rangle$.

If $x'{=}x\oplus s \Leftrightarrow f(x'){=}f(x)$, we can get $|y\rangle|f(x\oplus s)\rangle = |y\rangle|f(x)\rangle$. Then, we get $2^{-n/2}\sum_{x,y}(-1)^{y\cdot x}|y\rangle|f(x)\rangle = 2^{-n}\sum_{x\in V,y}((-1)^{y\cdot x}(1+(-1)^{y\cdot s}))|y\rangle|f(x)\rangle$, where $V$ is a linear sub-space. $\{0,1\}^n$ is divided into $V+s$ and $V$. Consequently, if we measure the state, we can get a random vector such that $y\cdot s = 0$. By repeating these steps $O(n)$ times, we can obtain adequate independent vectors with high probability.

### 2. Quantum distinguisher

The function $f$ has to satisfy $x' = x\oplus s \Leftrightarrow f(x) = f(x')$ to get $s$ based on Simon's algorithm. Nonetheless, the condition can be relaxed in distinguishing attack. If we get an oracle $\mathcal{O}:\{0,1\}^n \to \{0,1\}^n$ which is either a permutation $\Pi$ or an encryption algorithm $E_K$, and our question is how do we distinguish the two cases. Let oracle $U_{\mathcal{O}}$ be given in quantum circuit. We can apply the distinguisher in [13] to a function $f^{\mathcal{O}}$, which is $\{0,1\}^n \to \{0,1\}^n$. When $\mathcal{O} = E_K$, $f^{\mathcal{O}}$ has a non-zero period $s$. We expect that $f^{\Pi}$ does not have any period, and the probability is very high. The distinguisher is shown as follows:

Step 1: Starting with a set $\mathcal{Y}$, which is empty.

Step 2: Measure the first register for $\eta$ times, then add the values of vector $y$ to set $\mathcal{Y}$ and span to a vector space.

Step 3: Compute the dimension $d$ of the vector space.

Step 4: Output $\mathcal{O}=\Pi$, if $d=l$; while output $\mathcal{O}=E_K$, if $d<l$.

If $s$ is the period of $f^{\mathcal{O}}$, it is orthogonal to $y$. Thus, dimension $d$ is at most $l-1$. On the other side, $d$ can reach $l$ if $f^{\mathcal{O}}$ does not have a period. Therefore, the two cases can be distinguished by examining the dimension. To analyze the probability when the distinguisher succeeds, let $\pi$ be a fixed permutation, we define

$$\epsilon_f^{\pi}=\max_{t\in\{0,1\}^l\setminus\{0^l\}} \Pr_x[f^{\pi}(x)=f^{\pi}(x\oplus t)]$$

Take an arbitrary constant $0\leq\delta<1$. If $\epsilon_f^{\pi}>1-\delta$, we say $\pi$ is irregular permutation. What is more, we define the irregular permutations set as

$$\mathrm{irr}_f^{\delta}=\{\pi\in\mathrm{Perm}(n)|\epsilon_f^{\pi}>1-\delta\}$$

The following theorem is proved in [13].

**Theorem 1** (Theorem 2 in [13]) Assume that one has a quantum circuit, which has $O(poly(l,m))$ qubits. The quantum circuit can compute $f^{\mathcal{O}}$ by making $O(1)$ queries. When the distinguisher takes $O(\eta)$ queries, we can distinguish the two cases with probability

$$1-\frac{2^l}{e^{\delta\eta/2}}-\Pr_{\Pi}[\Pi\in\mathrm{irr}_f^{\delta}]$$

## III. Quantum Attacks on Type-3 GFS

We propose a distinguishing attack of $(d+1)$-round Type-3 GFS in polynomial time in the qCPA setting in this section. Then the 5-round 4-branch Type-3 GFS is studied as an example. We construct a periodic function by using the XOR of two different outputs of the same branch, and then offset a same term about the input variable. The result shows that the $(d+1)$-round Type-3 GFS is insecure in the qCPA setting. In addition, we propose key recovery attacks on Type-3 GFS, and give the comparison with quantum exhaustive search.

### 1. Specification of Type-3 GFS

Let Type-3 GFS have $d$ branches, where $d\geq 3$ and each branch has an $n$-bit sub-block. Let $E_r^{\text{type}-3}$ denote the $r$-round Type-3 and $R^{i,j}$ $(1\leq j\leq d-1)$ be keyed sub-round functions from $\{0,1\}^n$ to $\{0,1\}^n$. Let $R^{i,j}$ take a $k$-bit independent round key $k^{i,j}$ as the input, and the round function $R^i$ is defined as $R^i=(R^{i,1},\dots,R^{i,d-1})$. $E_r^{\text{type}-3}$ inputs a plaintext $(x_0^0,\dots,x_{d-1}^0)\in(\{0,1\}^n)^d$, and outputs a ciphertext $(x_0^r,\dots,x_{d-1}^r)\in(\{0,1\}^n)^d$, and the $i$th-round Type-3 GFS is shown in Fig.1.

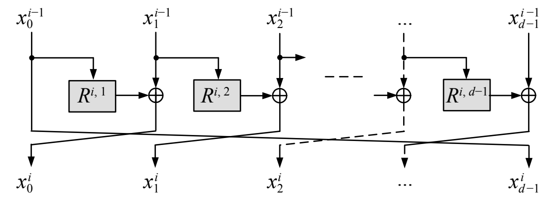


Fig. 1. The round function of Type-3 GFS.

### 2. Distinguishing attacks on the $(d+1)$-round Type-3 GFS

Let $\alpha_0,\alpha_1\in\{0,1\}^n$ be constants, which are arbitrary distinct. And $x_1^0,\dots,x_{d-2}^0\in\{0,1\}^n$ be arbitrary constants (as shown in Fig.2). If we get the oracle $\mathcal{O}$, we can define

$$\begin{aligned}f^{\mathcal{O}}:\{0,1\}^n&\rightarrow\{0,1\}^n\\ x&\mapsto z_{d-1}\oplus {z'}_{d-1}\end{aligned}$$

where $z_{d-1}$ and ${z'}_{d-1}$ are the last branches of the outputs of $\mathcal{O}(\alpha_0,x_1^0,\dots,x_{d-2}^0,x)$ and $\mathcal{O}(\alpha_1,x_1^0,\dots,x_{d-2}^0,x)$ respectively. If $\mathcal{O}$ is $E_{d+1}^{\text{Type-3}}$, $f^{\mathcal{O}}$ is described as

$$f^{\mathcal{O}}(x)=x_{d-1}^{d+1}\oplus {x'}_{d-1}^{d+1}$$

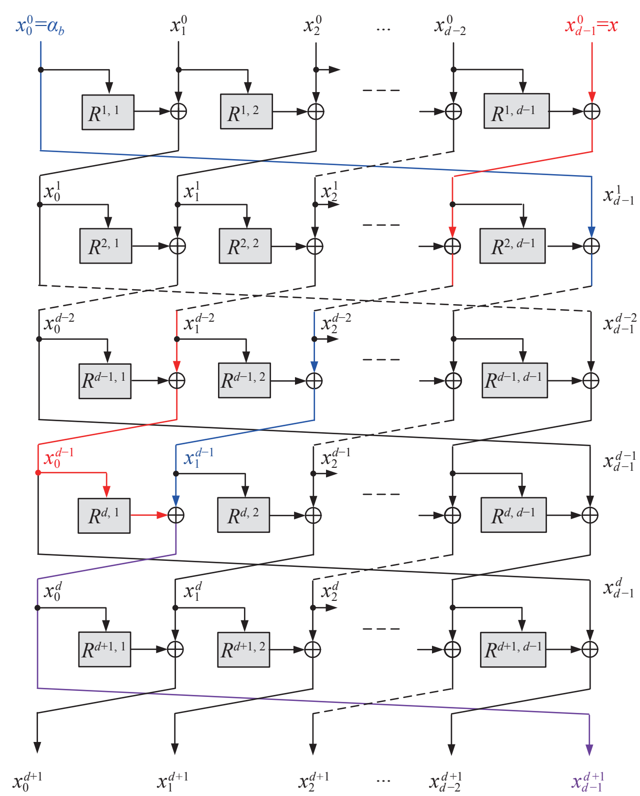


Fig. 2. $(d+1)$-round distinguisher on Type-3 GFS.

The following lemma is our main observation for $(d+1)$-round Type-3 GFS.

**Lemma 1** If the oracle $\mathcal{O}$ is $E_{d+1}^{\text{Type-3}}$, then for any $x\in\{0,1\}^n$, we can get

$$
\begin{aligned}
f^{\mathcal{O}}(x) =& f^{\mathcal{O}}(x \oplus R^{d-1,1}(F^{d-1,1}(\alpha_0, x_1^0, \dots, x_{d-2}^0)) \\
& \oplus R^{d-1,1}(F^{d-1,1}(\alpha_1, x_1^0, \dots, x_{d-2}^0)))
\end{aligned}
$$

That is, $s = R^{d-1,1}(F^{d-1,1}(\alpha_0, x_1^0, \dots, x_{d-2}^0)) \oplus R^{d-1,1}(F^{d-1,1}(\alpha_1, x_1^0, \dots, x_{d-2}^0))$ is the period of $f^{\mathcal{O}}$, where $F^{d-1,1}$ is a fixed function.

**Proof** Firstly, we consider the value of the output of the first $(d-1)$ rounds:

$$(x_0^{d-1}, x_1^{d-1}, \dots, x_{d-1}^{d-1}) = E_{d-1}^{\text{type-3}}(\alpha_b, x_1^0, \dots, x_{d-2}^0, x)$$

Meanwhile, $\alpha_b$ reaches the second position from left. Then, we can get $x_0^{d-1}$ and $x_1^{d-1}$ by the following equations:

$$
\begin{aligned}
x_0^{d-1} &= R^{d-1,1}(x_0^{d-2}) \oplus x_1^{d-2} \\
x_0^{d-2} &= R^{d-2,1}(x_0^{d-3}) \oplus x_1^{d-3} \\
x_1^{d-2} &= R^{d-2,2}(x_1^{d-3}) \oplus x_2^{d-3} \\
&\vdots \\
x_0^{1} &= R^{1,1}(\alpha_b) \oplus x_1^{0} \\
&\vdots \\
x_{d-3}^{1} &= R^{1,d-2}(x_{d-3}^{0}) \oplus x_{d-2}^{0} \\
x_{d-2}^{1} &= R^{1,d-1}(x_{d-2}^{0}) \oplus x
\end{aligned}
$$

and

$$
\begin{aligned}
x_1^{d-1} &= R^{d-1,2}(x_1^{d-2}) \oplus x_2^{d-2} \\
x_1^{d-2} &= R^{d-2,2}(x_1^{d-3}) \oplus x_2^{d-3} \\
x_2^{d-2} &= R^{d-2,3}(x_2^{d-3}) \oplus x_3^{d-3} \\
&\vdots \\
x_1^{2} &= R^{2,2}(x_1^{1}) \oplus x_2^{1} \\
&\vdots \\
x_{d-3}^{2} &= R^{2,d-2}(x_{d-3}^{1}) \oplus x_{d-2}^{1} \\
x_{d-2}^{2} &= R^{2,d-1}(x_{d-2}^{1}) \oplus \alpha_b \\
&\vdots \\
x_1^{1} &= R^{1,2}(x_1^{0}) \oplus x_2^{0} \\
&\vdots \\
x_{d-3}^{1} &= R^{1,d-2}(x_{d-3}^{0}) \oplus x_{d-2}^{0} \\
x_{d-2}^{1} &= R^{1,d-1}(x_{d-2}^{0}) \oplus x
\end{aligned}
$$

So, we can easily get

$$
\begin{aligned}
x_0^{d-1} =& x \oplus R^{1,d-1}(x_{d-2}^0) \oplus R^{2,d-2}(F^{2,d-2}(x_{d-3}^0, x_{d-2}^0)) \\
& \oplus \cdots \oplus R^{d-2,2}(F^{d-2,2}(x_1^0, \dots, x_{d-2}^0)) \\
& \oplus R^{d-1,1}(F^{d-1,1}(\alpha_b, x_1^0, \dots, x_{d-2}^0))
\end{aligned}
$$

and

$$
\begin{aligned}
x_1^{d-1} =& \alpha_b \oplus R^{2,d-1}(F^{2,d-1}(x_{d-2}^0, x)) \\
& \oplus \cdots \oplus R^{d-1,2}(F^{d-1,2}(x_1^0, \dots, x_{d-2}^0, x))
\end{aligned}
$$

where $F^{2,d-2}, \dots, F^{d-1,1}$ and $F^{2,d-1}, \dots, F^{d-1,2}$ are all fixed functions with an output length of $n$-bit.

For $b = 0, 1$, let

$$
\begin{aligned}
\Gamma_{\alpha_b} =& R^{1,d-1}(x_{d-2}^0) \oplus R^{2,d-2}(F^{2,d-2}(x_{d-3}^0, x_{d-2}^0)) \\
& \oplus \cdots \oplus R^{d-2,2}(F^{d-2,2}(x_1^0, \dots, x_{d-2}^0)) \\
& \oplus R^{d-1,1}(F^{d-1,1}(\alpha_b, x_1^0, \dots, x_{d-2}^0))
\end{aligned}
$$

and

$$
\begin{aligned}
\Lambda_x =& R^{2,d-1}(F^{2,d-1}(x_{d-2}^0, x)) \\
& \oplus \cdots \oplus R^{d-1,2}(F^{d-1,2}(x_1^0, \dots, x_{d-2}^0, x))
\end{aligned}
$$

We can get $x_0^{d-1} = x \oplus \Gamma_{\alpha_b}$ and $x_1^{d-1} = \alpha_b \oplus \Lambda_x$. As $x_1^0, \dots, x_{d-2}^0$ are arbitrary $n$-bit constants, thus $\Gamma_{\alpha_b}$ is a function about $\alpha_b$, $\Lambda_x$ is a function about $x$. Finally, as we have seen, $x_{d-1}^{d+1} = x_0^d = \alpha_b \oplus \Lambda_x \oplus R^{d,1}(x \oplus \Gamma_{\alpha_b})$, we have

$$
\begin{aligned}
f^{\mathcal{O}}(x) &= x_{d-1}^{d+1} \oplus x'^{d+1}_{d-1} \\
&= \alpha_0 \oplus \alpha_1 \oplus R^{d,1}(x \oplus \Gamma_{\alpha_0}) \oplus R^{d,1}(x \oplus \Gamma_{\alpha_1})
\end{aligned}
$$

So, we can get

$$f^{\mathcal{O}}(x \oplus \Gamma_{\alpha_0} \oplus \Gamma_{\alpha_1}) = f^{\mathcal{O}}(x)$$

So, $f^{\mathcal{O}}(x)$ has the period

$$
\begin{aligned}
s =& \Gamma_{\alpha_0} \oplus \Gamma_{\alpha_1} \\
=& R^{d-1,1}(F^{d-1,1}(\alpha_0, x_1^0, \dots, x_{d-2}^0)) \\
& \oplus R^{d-1,1}(F^{d-1,1}(\alpha_1, x_1^0, \dots, x_{d-2}^0))
\end{aligned}
$$

Hence the lemma follows.

Since the output of $(d+1)$-round Type-3 GFS could be truncated based on the approach in SCN 2018 [20], $f^{\mathcal{O}}(x)$ could be used as the oracle in quantum cryptanalysis based on Simon's algorithm. As $f^{\mathcal{O}}(x)$ has period $s$, $(d+1)$-round Type-3 GFS can be distinguished based on the quantum distinguisher in Section II in polynomial time. The Simon's function for $(d+1)$-round Type-3 GFS is illustrated in Fig.3 , where $E_{d+1,(\alpha_i)}^{d-1}$ denotes the output of the last branch when the input of $(d+1)$-round Type-3 GFS is $(\alpha_i, x_1^0, \dots, x_{d-2}^0, x)$, $i \in \{0, 1\}$.

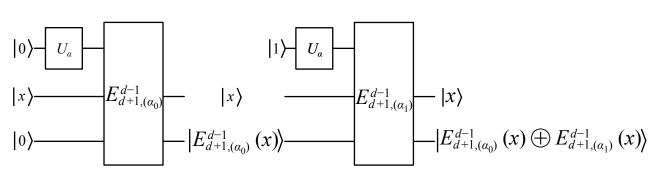


Fig. 3. Simon's function for $(d+1)$-round Type-3 GFS.

We use $\eta = 4n$ and $\delta = 1/2$, $(2/e)^n$ and $\Pr_\Pi[\Pi \in \text{irr}_f^\delta]$ are both small values. The success probability is at least $1 - (2/e)^n - \Pr_\Pi[\Pi \in \text{irr}_f^\delta]$ with measuring $4n$

times.

Next, the attack of 4-branch Type-3 GFS is included to illustrate the computational procedure.

Example of 4-branch Type-3 GFS. When the number of branch $d$ is 4, we get a 5-round quantum distinguisher (as shown in Fig.4).

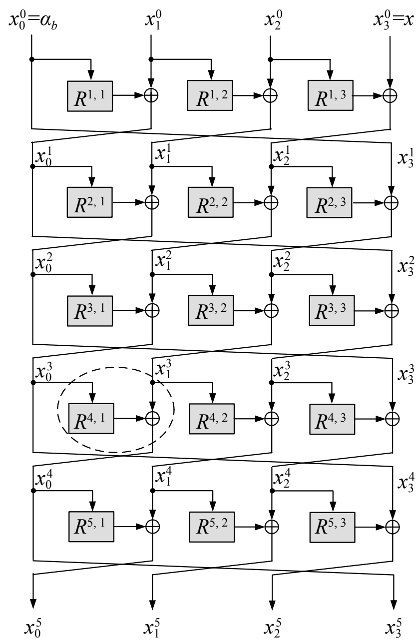


Fig. 4. 5-round distinguisher on 4-branch Type-3 GFS.

Based on the Lemma 1, we can get

$$\begin{aligned} x_{d-1}^{d+1} =x_3^5 &= \alpha_b \oplus R^{2,3}(x \oplus R^{1,3}(x_2^0)) \\ &\oplus R^{3,2}(x \oplus R^{1,3}(x_2^0) \oplus R^{2,2}(x_2^0 \oplus R^{1,2}(x_1^0))) \\ &\oplus R^{4,1}(x \oplus R^{1,3}(x_2^0) \oplus R^{2,2}(x_2^0 \oplus R^{1,2}(x_1^0)) \\ &\oplus R^{3,1}(x_2^0 \oplus R^{1,2}(x_1^0) \oplus R^{2,1}(x_1^0 \oplus R^{1,1}(\alpha_b)))) \end{aligned}$$

Given the oracle $\mathcal{O}$ of 5-round Type-3 GFS, we can define

$$\begin{aligned} f^{\mathcal{O}} : \{0,1\}^n &\to \{0,1\}^n \\ x &\mapsto x_3^5 \oplus x'^5_3 \end{aligned}$$

where $x_3^5$ and $x'^5_3$ are the last branches of the outputs of $\mathcal{O}(\alpha_0, x_1^0, x_2^0, x)$ and $\mathcal{O}(\alpha_1, x_1^0, x_2^0, x)$ respectively. Then, we can get

$$\begin{aligned} f^{\mathcal{O}}(x) =& \alpha_0 \oplus \alpha_1 \\ &\oplus R^{4,1}(x \oplus R^{1,3}(x_2^0) \oplus R^{2,2}(x_2^0 \oplus R^{1,2}(x_1^0))) \\ &\oplus R^{3,1}(x_2^0 \oplus R^{1,2}(x_1^0) \oplus R^{2,1}(x_1^0 \oplus R^{1,1}(\alpha_0))) \\ &\oplus R^{4,1}(x \oplus R^{1,3}(x_2^0) \oplus R^{2,2}(x_2^0 \oplus R^{1,2}(x_1^0))) \\ &\oplus R^{3,1}(x_2^0 \oplus R^{1,2}(x_1^0) \oplus R^{2,1}(x_1^0 \oplus R^{1,1}(\alpha_1))) \end{aligned}$$

The period for $f^{\mathcal{O}}(x)$ is

$$\begin{aligned} s =& R^{3,1}(x_2^0 \oplus R^{1,2}(x_1^0) \oplus R^{2,1}(x_1^0 \oplus R^{1,1}(\alpha_0))) \\ &\oplus R^{3,1}(x_2^0 \oplus R^{1,2}(x_1^0) \oplus R^{2,1}(x_1^0 \oplus R^{1,1}(\alpha_1))) \end{aligned}$$

Similar to the above attack, the 5-round 4-branch Type-3 GFS can be distinguished in polynomial time.

### 3. Key recovery attack on Type-3 GFS

Based on the $(d+1)$-round distinguisher, we introduce how to solve the keys of $r$-round Type-3 GFS. When the output of the $(d+2)$-round Type-3 GFS is known (shown in Fig.5), we can get

$$x_{d-1}^{d+1} = R^{d+2,d-1}(\cdots(R^{d+2,1}(x_{d-1}^{d+2}) \oplus x_0^{d+2}) \oplus \cdots) \oplus x_{d-2}^{d+2}$$

That is, when we get the output of $(d+2)$-round Type-3 GFS, we need to guess $d-1$ sub-keys for a total of $(d-1)k$ bits to recover the intermediate state $x_{d-1}^{d+1}$.

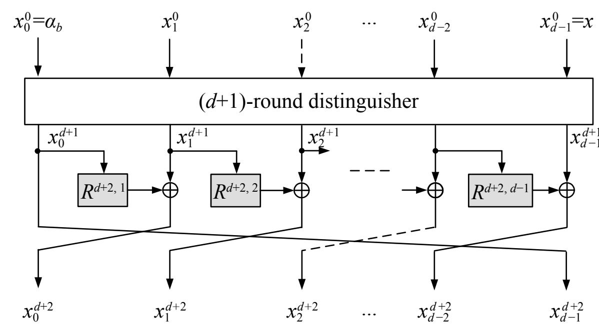


Fig. 5. Key recovery attack on Type-3 GFS.

For $r \geq d+2$, when the output of the $r$-round Type-3 GFS is known, we need to guess the value of $(d-1)(r-d-1)$ sub-keys for a total of $(d-1)(r-d-1)k$ bits to recover the intermediate state $x_{d-1}^{d+1}$. With the $(d+1)$-round distinguisher in qCPA setting, we can solve the key in time $O(2^{(d-1)(r-d-1)k/2})$ combining Simon's and Grover's algorithms.

For $r$-round $d$-branch Type-3 GFS, $(d-1)rk$ bits key need to be found by using the quantum exhaustive search to recover the key, and the time complexity is $O(2^{(d-1)rk/2})$. Therefore, this attack is better than the exhaustive search by factor $2^{(d-1)rk/2-(d-1)(r-d-1)k/2} = 2^{(d^2-1)k/2}$.

## IV. Quantum Attacks on UFS-E

In this section, we give a distinguishing attack of $(d+1)$-round $d$-branch UFS-E with polynomial time in the qCPA setting. The quantum attack of UFS-E shows that the $(d+1)$-round is insecure in the qCPA setting, however, the $(d+1)$-round is PRP in the classical setting. In addition, we carry out key recovery attacks on UFS-E.

### 1. Specification of UFS-E

Let UFS-E have $d$ branches, where $d \geq 3$ and each branch has an $n$-bit sub-block. Let $E_r^{\mathrm{UFS-E}}$ denote the $r$-

round UFS-E and $R^{i,j}(1 \le j \le d-1)$ be keyed sub-round functions from $\{0,1\}^n$ to $\{0,1\}^n$. Let $R^{i,j}$ take a $k$-bit independent round key $k^{i,j}$ as input, and the round function $R^i$ is defined as $R^i = (R^{i,1}, \ldots, R^{i,d-1})$. $E_r^{\text{UFS-E}}$ inputs a plaintext $(x_0^0, \ldots, x_{d-1}^0) \in (\{0,1\}^n)^d$, and outputs a ciphertext $(x_0^r, \ldots, x_{d-1}^r) \in (\{0,1\}^n)^d$. The $i$th-round UFS-E is shown in Fig.6.

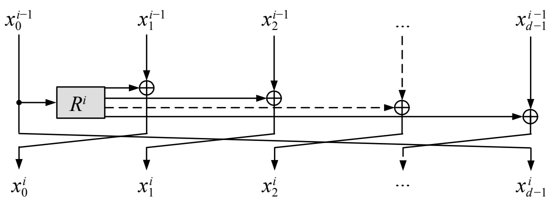


Fig. 6. The round function of UFS-E.

## 2. Distinguishing attacks on the $(d+1)$-round UFS-E

Let $\alpha_0, \alpha_1 \in \{0,1\}^n$ be constants, which are arbitrary distinct. And $x_1^0, \ldots, x_{d-2}^0 \in \{0,1\}^n$ be arbitrary constants (as shown in Fig.7). If we get the oracle $\mathcal{O}$, we can define

$$\begin{aligned} f^{\mathcal{O}} &: \{0,1\}^n \to \{0,1\}^n \\ &x \mapsto z_{d-1} \oplus z'_{d-1} \end{aligned}$$

where $z_{d-1}$ and $z'_{d-1}$ are the last branches of the outputs of $\mathcal{O}(\alpha_0, x_1^0, \ldots, x_{d-2}^0, x)$ and $\mathcal{O}(\alpha_1, x_1^0, \ldots, x_{d-2}^0, x)$ respectively. If the oracle $\mathcal{O}$ is $E_{d+1}^{\text{UFS-E}}$, $f^{\mathcal{O}}$ is described as

$$f^{\mathcal{O}}(x) = z_{d-1} \oplus z'_{d-1} = x_{d-1}^{d+1} \oplus {x'}_{d-1}^{d+1}$$

The following lemma is our main observation for $(d+1)$-round UFS-E.

**Lemma 2** If the oracle $\mathcal{O}$ is $E_{d+1}^{\text{UFS-E}}$, then for any $x$, we can get

$$f^{\mathcal{O}}(x \oplus \Gamma_{\alpha_0} \oplus \Gamma_{\alpha_1}) = f^{\mathcal{O}}(x)$$

That is, $f^{\mathcal{O}}$ has the period $s = \Gamma_{\alpha_0} \oplus \Gamma_{\alpha_1}$, where

$$\begin{aligned} \Gamma_{\alpha_b} =& R^{1,d-1}(\alpha_b) \oplus R^{2,d-2}(F^{2,d-2}(\alpha_b, x_1^0)) \\ &\oplus \cdots \oplus R^{d-1,1}(F^{d-1,1}(\alpha_b, x_1^0, \ldots, x_{d-2}^0)) \end{aligned}$$

and $F^{2,d-2}, \ldots, F^{d-1,1}$ are fixed functions with $n$-bit output.

**Proof** Firstly, we consider the value of the outputs of the first $(d-1)$ rounds:

$$(x_0^{d-1}, x_1^{d-1}, \ldots, x_{d-1}^{d-1}) = E_{d-1}^{\text{UFS-E}}(\alpha_b, x_1^0, \ldots, x_{d-2}^0, x)$$

Meanwhile, $\alpha_b$ reaches the second position from left. Similar as Lemma 1, we can get:

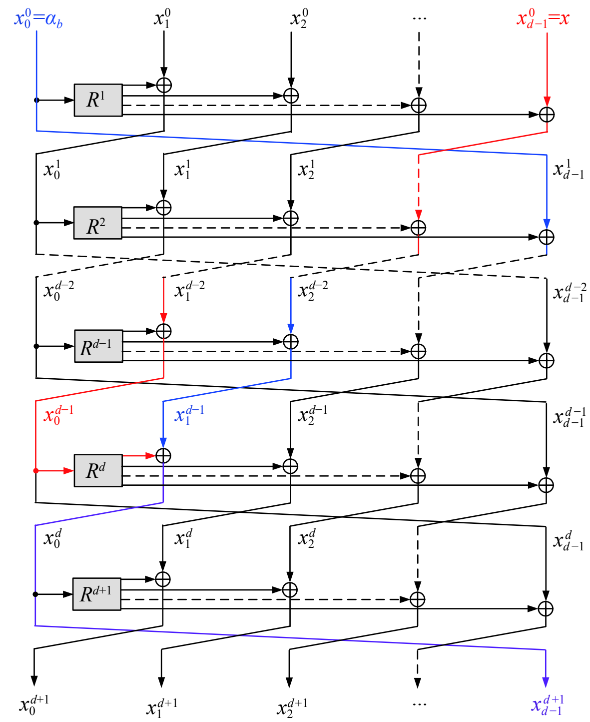


Fig. 7. $(d+1)$-round distinguisher on UFS-E.

$$\begin{aligned} x_0^{d-1} =& x \oplus R^{1,d-1}(\alpha_b) \oplus R^{2,d-2}(F^{2,d-2}(\alpha_b, x_1^0)) \\ &\oplus \cdots \oplus R^{d-1,1}(F^{d-1,1}(\alpha_b, x_1^0, \ldots, x_{d-2}^0)) \end{aligned}$$

$$\begin{aligned} x_1^{d-1} =& \alpha_b \oplus R^{2,d-1}(F^{2,d-1}(\alpha_b, x_1^0)) \\ &\oplus R^{3,d-2}(F^{3,d-2}(\alpha_b, x_1^0, x_2^0)) \\ &\oplus \cdots \oplus R^{d-1,2}(F^{d-1,2}(\alpha_b, x_1^0, \ldots, x_{d-2}^0)) \end{aligned}$$

where $F^{2,d-1}, \ldots, F^{d-1,2}$ and $F^{2,d-2}, \ldots, F^{d-1,1}$ are all fixed functions with $n$-bit output.

For $b = 0, 1$, let

$$\begin{aligned} \Lambda_{\alpha_b} =& \alpha_b \oplus R^{2,d-1}(F^{2,d-1}(\alpha_b, x_1^0)) \\ &\oplus R^{3,d-2}(F^{3,d-2}(\alpha_b, x_1^0, x_2^0)) \\ &\oplus \cdots \oplus R^{d-1,2}(F^{d-1,2}(\alpha_b, x_1^0, \ldots, x_{d-2}^0)) \end{aligned}$$

and

$$\begin{aligned} \Gamma_{\alpha_b} =& R^{1,d-1}(\alpha_b) \oplus R^{2,d-2}(F^{2,d-2}(\alpha_b, x_1^0)) \\ &\oplus \cdots \oplus R^{d-1,1}(F^{d-1,1}(\alpha_b, x_1^0, \ldots, x_{d-2}^0)) \end{aligned}$$

We can get $x_1^{d-1} = \Lambda_{\alpha_b}$ and $x_0^{d-1} = x \oplus \Gamma_{\alpha_b}$. As $x_1^0, \ldots, x_{d-2}^0$ are arbitrary $n$-bit constants, thus $\Lambda_{\alpha_b}$ and $\Gamma_{\alpha_b}$ are functions of $\alpha_b$.

Finally, as we have seen, $x_{d-1}^{d+1} = x_0^d = \Lambda_{\alpha_b} \oplus R^{d,1}(x \oplus \Gamma_{\alpha_b})$, and

$$\begin{aligned} f^{\mathcal{O}}(x) &= x_{d-1}^{d+1} \oplus {x'}_{d-1}^{d+1} \\ &= \Lambda_{\alpha_0} \oplus R^{d,1}(x \oplus \Gamma_{\alpha_0}) \oplus \Lambda_{\alpha_1} \oplus R^{d,1}(x \oplus \Gamma_{\alpha_1}) \end{aligned}$$

The function $f^{\mathcal{O}}$ has the claimed period since it satisfies

$$f^{\mathcal{O}}(x \oplus \Gamma_{\alpha_0} \oplus \Gamma_{\alpha_1}) = f^{\mathcal{O}}(x)$$

That is, $f^{\mathcal{O}}$ has the period $s = \Gamma_{\alpha_0} \oplus \Gamma_{\alpha_1}$.

Hence the lemma follows.

Since the output of $(d+1)$-round UFS-E could be truncated based on the approach in SCN2018 [20], $f^{\mathcal{O}}$ could be used as the oracle in quantum cryptanalysis based on Simon's algorithm. As $f^{\mathcal{O}}$ has the period $s$, $(d+1)$-round UFS-E can be distinguished based on the quantum distinguisher in Section II in polynomial time. The Simon's function of $(d+1)$-round UFS-E and the success probability are the same as those of $(d+1)$-round Type-3 GFS.

**3. Key recovery attack on UFS-E**

Based on the $(d+1)$-round distinguisher, we introduce how to solve the keys of $r$-round UFS-E. When the output of the $(d+2)$-round UFS-E is known (as shown in Fig.8), we can get

$$x_{d-1}^{d+1} = R^{d+2,d-1}(x_{d-1}^{d+2}) \oplus x_{d-2}^{d+2}$$

That is, when we get the output of $(d+2)$-round UFS-E, we need to guess the one sub-key for a total of $k$ bits to recover the intermediate state $x_{d-1}^{d+1}$.

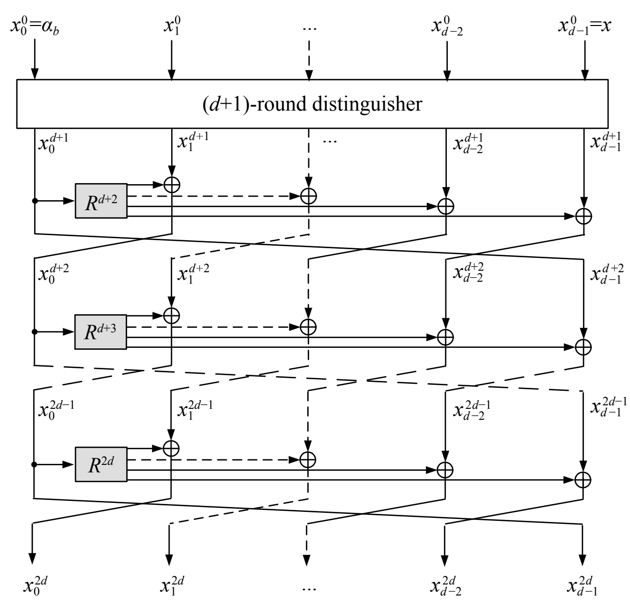


Fig. 8. Key recovery attack on UFS-E.

When the output of the $r$-round UFS-E is known, we need to guess the value of $(r-d)(r-d-1)/2$ sub-keys for a total of $(r-d)(r-d-1)k/2$ bits to recover the intermediate state $x_{d-1}^{d+1}$. With the distinguisher, we can solve the key of UFS-E in time $O(2^{(r-d)\cdot(r-d-1)\cdot k/4})$ by combining Grover's and Simon's algorithms when $d+2 \le r \le 2d$.

If we attack $r > 2d$ rounds, we need to guess the value of

$$(2d-d)(2d-d-1)/2+(r-2d)(d-1) = (r-3d/2)(d-1)$$

sub-keys for a total of $(r-\frac{3d}{2})(d-1)k$ bits to recover the intermediate state $x_{d-1}^{d+1}$. With the $(d+1)$-round distinguisher, we can solve the key of the $r$-round UFS-E in time $O(2^{(2r-3d)(d-1)k/4})$ combining Grover's and Simon's algorithm.

For $r$-round $d$-branch UFS-E, $r(d-1)k$ bits key need to be found by using the quantum exhaustive search to recover the key, the complexity is $O(2^{r(d-1)k/2})$. For $d+2 \le r \le 2d$ and $r > 2d$, our attacks are better than the exhaustive search by factors $2^{r(d-1)k/2-(r-d)(r-d-1)k/4} = 2^{(4rd-d^2-d-r^2-r)k/4}$ and $2^{r(d-1)k/2-(2r-3d)(d-1)k/4} = 2^{3d(d-1)k/4}$, respectively.

## V. Conclusions

In this paper, the quantum security of Type-3 GFS and UFS-E are studied. The 5-round 4-branch Type-3 GFS has been proved secure in the qCPA setting in previous work, while $(d+1)$-round $d$-branch UFS-E has not been studied in the qCPA setting.

For $d$-branch Type-3 GFS and UFS-E, we propose quantum distinguishing attacks on $(d+1)$-round Type-3 GFS and $(d+1)$-round UFS-E in polynomial time in the qCPA setting. The results show that the $(d+1)$-round Type-3 GFS and $(d+1)$-round UFS-E which proved to be PRP are not secure in the quantum setting. In addition, based on Grover's and Simon's algorithm, we give key recovery on the Type-3 GFS and UFS-E, which are better than the quantum exhaustive search.

### References


[1] H. Kuwakado and M. Morii, "Quantum distinguisher between the 3-round feistel cipher and the random permutation," in *Proceedings of the 2010 IEEE International Symposium on Information Theory*, Austin, TX, USA, pp.2682–2685, 2010.

[2] H. Kuwakado and M. 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, pp.312–316, 2012.

[3] S. Even and Y. Mansour, "A construction of a cipher from a single pseudorandom permutation," *J. Cryptology*, vol.10, no.3, pp.151–162, 1997.

[4] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," *SIAM J. Comput*, vol.17, no.2, pp.373–386, 1988.

[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, Philadelphia, PA, USA, pp.212–219, 1996.

[6] D. R. Simon, "On the power of quantum computation,"

*SIAM J. Comput.*, vol.16, no.5, pp.1474–1483, 1997.
[7] G. Leander and A. May, "Grover meets Simon – quantumly attacking the FX construction," in *Proceedings of the 23rd International Conference on the Theory and Applications of Cryptology and Information Security,* Hong Kong, China, pp.161–178, 2017.
[8] X. Y. Dong, Z. Li, and X. Y. Wang, "Quantum cryptanalysis is on some generalized Feistel schemes," *Science China (Information Sciences)*, vol.62, no.2, pp.180–191, 2019.
[9] X. Y. Dong and X. Y. Wang, "Quantum key-recovery attack on Feistel structures," *Science China (Information Sciences)*, vol.61, no.10, pp.1–7, 2018.
[10] X. Dong, B. Dong, and X. Wang, "Quantum attacks on some Feistel block ciphers," *Designs, Codes and Cryptography*, vol.88, no.6, pp.1179–1203, 2020.
[11] X. Dong, S. Sun, D. Shi, F Gao, *et al.*, "Quantum collision attacks on AES-like hashing with low quantum random access memories," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, Daejeon, South Korea, pp.727–757, 2020.
[12] S. Hodžić, L. Ramkilde, and A. Kidmose, "On quantum distinguishers for Type-3 generalized Feistel network based on separability," in *Proceedings of International Conference on Post-Quantum Cryptography (PQCrypto 2020)*, Paris, France, pp.461–480, 2020.
[13] G. Ito, A. Hosoyamada, R. Matsumoto, *et al.*, "Quantum chosen ciphertext attacks against Feistel ciphers," in *Proceedings of the Cryptographers' Track at the RSA Conference 2019 (CT-RSA 2019)*, San Francisco, CA, USA, pp.391–411, 2019.
[14] Q. D. You, X. Qian, X. Zhou, *et al.*, "Research on quantum cryptanalysis on SMS4-like structure and NBC algorithm," *Journal of Cryptologic Research*, vol.7, no.6, pp.864–874, 2020. (in Chinese)
[15] C. Cid, A, Hosoyamada, Y. Liu, *et al*, "Quantum cryptanalysis on contracting Feistel structures and observation on related-key settings," in *Proceedings of International Conference on Cryptology in India (INDOCRYPT 2020)*, Bangalore, India, pp.373–394, 2020.
[16] X. Qian, Q. D. You, X. Zhou, *et al.*, "Quantum attack on MARS-like Feistel schemes," *Journal of Cryptologic Research*, vol.8, no.3, pp.417–431, 2021. (in Chinese)
[17] H. Feistel, W. A. Notz, and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," *Proc. of the IEEE* , vol.63, no.11, pp.1545–1554, 1975.
[18] Y. Zheng, T. Matsumoto, and H. Imai, "On the construction of block ciphers provably secure and not relying on any unproved hypotheses," in *Proceedings of Conference on the Theory and Application of Cryptology (CRYPTO 1989)*, Santa Barbara, CA, USA, pp.461–480, 1990.
[19] S. Moriai and S. Vaudenay, "On the pseudorandomness of top-level schemes of block ciphers," in *Proceedings of International Conference on the Theory and Application of Cryptology and Information Security,* Singapore, pp.289–302, 2000.
[20] A. Hosoyamada and Y. Sasaki, "Quantum Demiric-Sel¸cuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions," in *Proceedings of International Conference on Security and Cryptography for Networks (SCN 2018)*, Amalfi, Italy, pp.386–403, 2018.

**ZHANG Zhongya** was born in 1985. He is a Ph.D. candidate in cyberspace security. His main research interests include design and cryptanalysis of block ciphers and quantum computing.
(Email: zzycrypto@163.com)

**WU Wenling** was born in 1966. She is a Researcher, and Ph.D. Supervisor in Chinese Academy of Sciences. Her main research interests include design and cryptanalysis of block ciphers.
(Email: wenling@iscas.ac.cn)

**SUI Han** was born in 1986. She is working at Institute of Software, Chinese Academy of Sciences. Her research direction include the provable security theory of symmetric cryptography, and the design and analysis of authenticated encryption ciphers. ciphers.
(Email: suihan@iscas.ac.cn)

**WANG Bolin** was born in 1995. She is currently working toward the Ph.D. degree at Institute of Software, Chinese Academy of Sciences. Her main research interests include design and analysis of block ciphers.
(Email: bolin2018@iscas.ac.cn)