Quantum Attacks on Some Feistel Block Ciphers

Xiaoyang Dong, Bingyou Dong, Xiaoyun Wang

Abstract—Post-quantum cryptography has attracted much attention from worldwide cryptologists. However, most research works are related to public-key cryptosystem due to Shor's attack on RSA and ECC ciphers. At CRYPTO 2016, Kaplan et al. breaks many secret-key (symmetric) systems using quantum period finding algorithm, which arises researcher's attentions to evaluate the symmetric systems against quantum attackers.

In this paper, we continue to study the symmetric ciphers against quantum attackers. First, we convert the classical advanced slide attacks (introduced by Biryukov and Wagner) to a quantum one, that gains an exponential speed-up of the time complexity. Thus, we could break 2/4K-Feistel and 2/4K-DES in polynomial time. Second, we give a new quantum key-recovery attack on full-round GOST, a Russian standard, with 2^{112} Grover iterations, which is faster than a quantum brute force search attack by a factor 2^{16}.

Index Terms—Quantum key-recovery attack, GOST, DES, Symmetric cipher, Feistel, Grover.

1 Introduction

Post-quantum cryptography studies the security of cryptographic systems against quantum attackers. The most severe and notable quantum attack is Shor's algorithm [1] that breaks the most currently used public-key systems, such as RSA cryptosystem [2] and elliptic curve cryptography. There were not many known quantum threats against secret-key (symmetric) systems since then. The common belief was that quantum attacks on symmetric primitives are of minor concern, as they mainly consist of employing Grover's algorithm [3] to generically speed up search (sub-)problems.

Recently, researchers [4] find that quantum attackers, who are equipped with quantum computers, could break several secret-key schemes in polynomial time using superposition queries, such as Even-Mansour ciphers [5]. These pioneer works arise the attentions from the world wide cryptographic researchers to review the symmetric primitives against quantum attackers. To study the security of more classical and important cryptographic schemes against quantum attacks is urgently needed. At Asiacrypt 2017, NIST [6] reports the ongoing competition for post-quantum cryptographic algorithms, including signatures, encryptions and key-establishment. The ship for post-quantum crypto has sailed, cryptographic communities must get ready to welcome the post-quantum age.

Feistel block ciphers [7], which are important components of symmetric ciphers, are observed to be important and constitute one of the extensively researched cryptographic schemes. Several standard block ciphers, such as DES, Triple-DES, MISTY1, Camellia, CAST-128 [8] and the Russian GOST [9], are based on the Feistel design. Classically, researchers from academy and industry only care for the security of Feistel block ciphers against attackers who are only equipped with classical computers. In a quantum age, the adversaries are more powerful and equipped with quantum computers. They could make quantum queries on some superposition quantum states of the relevant cryptosystem, which is the so-called *quantum chosen-plaintext attacks* (qCPA) [10]. It is known that Grover's algorithm [3] could speed up brute force search. Given a block cipher with m-bit key, Grover's algorithm allows to quantum brute-force search the secret key using $\mathcal{O}(2^{m/2})$ quantum steps. It seems that doubling the key-length of one block cipher could achieve the same security against quantum attackers. However, Kuwakado and Morii [4] identified a new family of quantum attacks on certain generic constructions of secret key schemes. They showed that the Even-Mansour ciphers could be broken in polynomial time by Simon algorithm [11], which could find the period of a periodic function in polynomial time in a quantum computer. The following works by Kaplan *et al.* [12] revealed that many other secret key schemes could also be broken by Simon algorithm, such as CBC-MAC, PMAC, GMAC and some CAESAR candidates.

Our Contributions

In this paper, we focus on the study of the symmetric ciphers against quantum attackers. Combining with Simon's algorithm [11], we convert the classical advanced slide attacks (introduced by Biryukov and Wagner [13]) to a quantum one, that gains an exponential speed-up of the time complexity. Thus, we could break 2/4K-Feistel block ciphers and 2/4K-DES block ciphers in polynomial time. On the other hand, we give a new quantum key-recovery attack on the full-round GOST, a Russian block cipher standard, that breaks GOST in 2^{112} Grover iterations, which is faster than a quantum brute force search attack by a factor 2^{16}. The results are summarized in Table 1. Our paper alerts the academy and industry that it is not enough to just double the key length of the symmetric primitives to stand up to the attackers from the postquantum world.

2 Preliminaries

2.1 Attack Model

We consider attacks against classical cryptosystems using quantum resources. This general setting broadly defines the field of postquantum cryptography. But attacking specific cryptosystems requires a more precise definition of the operations the adversary is allowed to perform. The simplest

TABLE 1
Summary of key-recovery attacks on Feistel schemes in classical and quantum-CPA settings

Ciphers	Rounds	Key bits	Best Previous Classical Attacks			Quantum Brute-force Search	Ours
			Date	Time	Source	Time	
2K-Feistel	∞	n	$2^{0.25n}$	$2^{0.25n}$	[13]	$2^{0.5n}$	$\mathcal{O}(n)$
4K-Feistel	∞	$2n$	$2^{0.25n}$	$2^{0.25n}$	[13]	2^{n}	$\mathcal{O}(n)$
2K-DES	∞	96	2^{32}	2^{33}	[13]	2^{48}	$\mathcal{O}(1)$
4K-DES	∞	192	2^{32}	2^{33}	[13]	2^{96}	$\mathcal{O}(1)$
GOST	32	256	2^{32}	2^{224}	[14], [15]	2^{128}	2^{112}
	30	256	2^{32}	2^{224}	[16]	2^{128}	2^{112}

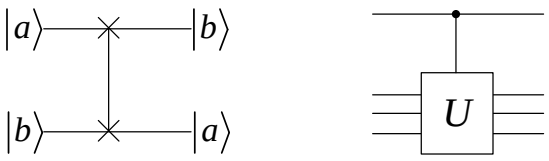

Fig. 1. Swap Circuit (left) and Controlled-U Gate (right).

setting allows the adversary to perform local quantum computation. For instance, this can be modeled by the quantum random oracle model, in which the adversary can query the oracle in an arbitrary superposition of the inputs.

The basic gate used in this paper are the negation (X), Hadamard (H). The circuits to swap two qubits, i.e., $|a, b\rangle \rightarrow |b, a\rangle$, and the control-$U$ gate are depicted in Figure 1.

2.2 Quantum Algorithms

Our quantum attacks are based on two of the most popular quantum algorithms, namely Simon's algorithm [11] and Grover's algorithm [3].

Simon's Problem. Given a Boolean function, $f : \{0,1\}^n \rightarrow \{0,1\}^n$, that is observed to be invariant under some n-bit XOR period a, find a. In other words, find a when $f(x) = f(y) \leftrightarrow x \oplus y \in \{0^n, a\}$ is given.

The optimal time to solve the problem is $\mathcal{O}(2^{n/2})$. However, Simon [11] presents a quantum algorithm that provides exponential speedup and requires only $\mathcal{O}(n)$ quantum queries to find a. The algorithm includes five quantum steps that are as follows:

I. Initialization of two n-bit quantum registers to state $|0\rangle^{\otimes n}|0\rangle^{\otimes n}$. Then apply the Hadamard transform to the first register to attain an equal superposition in the following manner:

$$H^{\otimes n}|0\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle. \tag{1}$$

II. A quantum query to the function f maps this to

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle.$$

III. While measuring the second register, the first register is observed to collapse to the following state:

$$\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus a\rangle).$$

IV. Applying the Hadamard transform to the first register, we obtain:

$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{y\cdot z}(1 + (-1)^{y\cdot a})|y\rangle.$$

V. The vectors, y, are selected such that $y \cdot a = 1$ depict an amplitude of zero. Hence, measuring the state yields a value, y, which depicts that $y \cdot a = 0$.

Repeat $\mathcal{O}(n)$ times, we can obtain a by solving a system of linear equations.

Kuwakado and Morii [4] used Simon's algorithm to break the Even-Mansour (EM) cipher [5]. For a given permutation P, the EM cipher is $Enc(x) = P(x \oplus k_1) \oplus k_2$. Classically, an EM cipher is secure for up to $2^{n/2}$ queries, where n is the input size of P. However, using Simon's algorithm [11], Kuwakado and Morii [4] presented a quantum key-recovery attack on EM ciphers with a time complexity of $\mathcal{O}(n)$. They define $f(x) = Enc(x) \oplus P(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$. Clearly, it is a periodic function that satisfies $f(x \oplus k_1) = f(x)$.

Grover's Algorithm. Given a set, X, in which some elements are marked, the objective is to find a marked element from X. We denote the subset of the marked elements by $M \subseteq X$. Classically, one can solve the problem in a time of $|X|/|M|$. However, in a quantum computer, the problem is solved with high probability in a time of $\sqrt{|X|/|M|}$ using Grover's algorithm. The steps of the algorithm are as follows:

1) Initialization of a n-bit register $|0\rangle^{\otimes n}$. Apply the Hadamard transform to the first register to attain an equal superposition that can be given as follows:

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle = |\varphi\rangle. \tag{2}$$

2) Construct an oracle $\mathcal{O}$: $|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$, where $f(x) = 1$ if x is the correct state; otherwise, $f(x) = 0$.
3) Apply Grover's iteration $R \approx \frac{\pi}{4}\sqrt{2^n}$ times that can be given as follows:

$$[(2|\varphi\rangle\langle\varphi| - I)\mathcal{O}]^R|\varphi\rangle \approx |x_0\rangle.$$

4) return x_0.

Further, Brassard *et al.* [17] generalized the Grover search as an amplitude amplification method.

Theorem 1. ***(Brassard, Hoyer, Mosca and Tapp [17]).*** *Let $\mathcal{A}$ be any quantum algorithm on q qubits that performs no measurement. Let $\mathcal{B} : \mathbb{F}_2^q \rightarrow \{0,1\}$ be a function that classifies the outcomes of $\mathcal{A}$ as either good or bad state. Let $p > 0$ be*

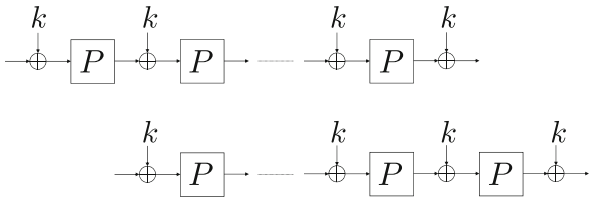

Fig. 2. Slide attack against iterated Even-Mansour cipher round keys of which are all the same

the initial success probability that the measurement of $\mathcal{A}|0\rangle$ is good. Set $k = \lceil \frac{\pi}{4\theta} \rceil$, where θ is defined using $sin^2(\theta) = p$. Furthermore, define the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$, where the operator $S_{\mathcal{B}}$ changes the sign of the good state,

$$|x\rangle \mapsto \begin{cases} -|x\rangle \text{ if } \mathcal{B}(x) = 1, \\ |x\rangle \text{ if } \mathcal{B}(x) = 0. \end{cases}$$

Further, S_0 changes the sign of the amplitude only in case of the zero state $|0\rangle$. Finally, after performing the computation of $Q^k\mathcal{A}|0\rangle$, the measurement yields a good state with probability a least max{1-p, p}.

Assume that $|\varphi\rangle = \mathcal{A}|0\rangle$ is the initial vector, whose projections on the good and the bad subspace are denoted by $|\varphi_1\rangle$ and $|\varphi_0\rangle$, respectively. The state $|\varphi\rangle = \mathcal{A}|0\rangle$ exhibits an θ with a bad subspace, where $sin^2(\theta) = p$. Each Q iteration increases the angle to 2θ. Hence, after $k \approx \frac{\pi}{4\theta}$, the angle is observed to be approximately equal to $\pi/2$. Therefore, the state after k iterations is almost orthogonal to that of the bad subspace. After measurement, it produces a good vector with high probability.

3 New Advanced Quantum Slide Attacks

3.1 Slide Attack and Advanced Slide Attack

Slide attack and advanced slide attack were proposed by Biryukov and Wagner [13], [18]. They are a set of powerful cryptanalysis tools. Classically, slide attack and advanced slide attack are launched against block ciphers with exponential time complexity. At CRYPTO 2016, Kaplan et al. [12] converted the slide attack on iterated Even-Mansour cipher into a quantum one by applying the slide attack and Simon's algorithm, shown in Figure 2. They define $F : \{0,1\}^{n+1} \to \{0,1\}^n$ as

$$F(b\|x) = \begin{cases} P(E_k^P(x)) \oplus x & \text{if } b = 0, \\ E_k^P(P(x)) \oplus x & \text{if } b = 1, \end{cases} \tag{3}$$

where $b \in \{0,1\}, x \in \{0,1\}^n$. For arbitrary $x \in \{0,1\}^n$, we have

$$\begin{aligned} &F(0\|x) = P(E_k^P(x)) \oplus x \\ &= E_k^P(P(x \oplus k)) \oplus (x \oplus k) = F(1\|(x \oplus k)). \end{aligned} \tag{4}$$

Thus, $s = 1\|k$ is the period of F. Finally, they could retrieve the secret key by applying Simon's algorithm with polynomial time complexity.

Feistel ciphers form an important special case for applying slide attacks. Kaplan *et al.*'s quantum slide attack against iterated Even-Mansour cipher could not applied to Feistel ciphers trivially. Thus, we will give some new quantum attacks on some Feistel ciphers.

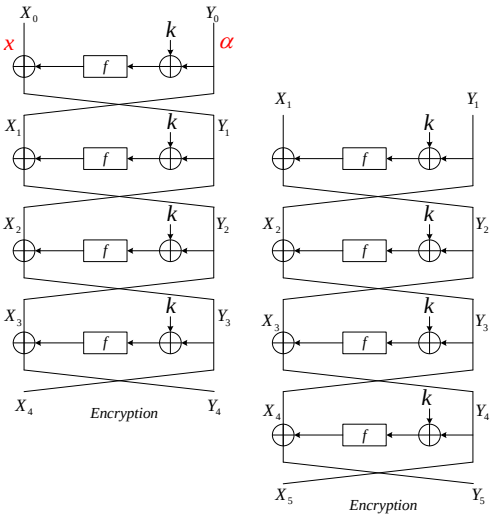

Fig. 3. Quantum Attacks on 1K-Feistel Block Cipher

In this section, we focus on the 1K-/2K-/4K-Feistel and 2K-/4K-DES block ciphers, which were introduced and studied by Biryukov and Wagner [13], [18]. They designed a novel advanced slide attack on these ciphers with exponential time complexities in classical computers. In this section, we will give some new advanced quantum slide attacks on 1K-/2K-/4K-Feistel block ciphers with polynomial time complexities in quantum computers.

2K-/4K-DES block ciphers are the modified DES examples given by Biryukov and Wagner [13], [18]. 2K-/4K-DES use two or four independent 48-bit keys and the key arrangement is the same with 2K-/4K-Feistel block ciphers. The total number of rounds of 2K-/4K-DES are 64 or more, thus they are resists to the conventional differential [19] and linear attacks [20]. Since 2K-/4K-DES block ciphers are trivially the concrete primitives of 2K-/4K-Feistel block ciphers, our attacks could be applied to 2K-/4K-DES trivially.

3.2 Advanced Quantum Slide Attack on 1K-Feistel

As shown in Figure 3, 1K-Feistel block cipher adopts repeating round subkeys and identical round functions f.

We first define the following functions using given random constant α:

$$\begin{aligned} &F : \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2} \\ &b, x \mapsto \begin{cases} E_K(x,\alpha)_R & \text{if } b = 0, \\ E_K(\alpha, f(\alpha) \oplus x)_L & \text{if } b = 1, \end{cases} \end{aligned} \tag{5}$$

where n is the block size of 1K-Feistel block cipher E_K, $E_K(\cdot)_L$ and $E_K(\cdot)_R$ are the left branch ($\frac{n}{2}$-bit) or right branch ($\frac{n}{2}$-bit) of $E_K(\cdot)$.

As shown in Figure 3, $E_K(x,\alpha)_R = Y_4$, $E_K(X_1, Y_1)_L = X_5 = Y_4$. $X_1 = \alpha$ and $Y_1 = f(k \oplus \alpha) \oplus x$. Thus,

$$\begin{aligned} &F(0,x) = E_K(x,\alpha)_R = E_K(\alpha, f(k \oplus \alpha) \oplus x)_L \\ &= F(1, x \oplus f(\alpha) \oplus f(k \oplus \alpha)). \end{aligned} \tag{6}$$

So $F(b,x)$ is a function with period $s = 1\|f(\alpha) \oplus f(k \oplus \alpha)$ and the period could be retrieved by applying Simons algorithm with polynomial time complexity.

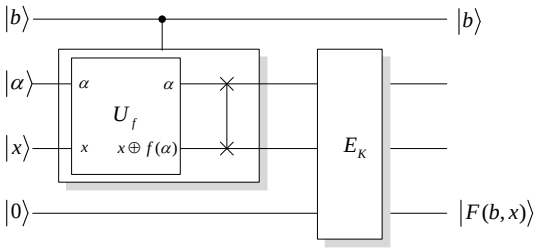

Fig. 4. Simon's function for the attack on 1K-Feistel

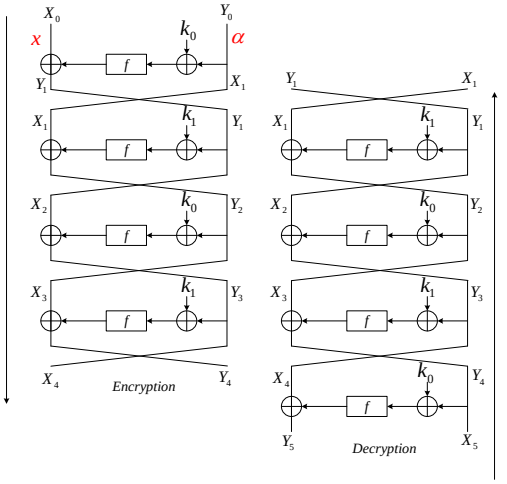

Fig. 5. Quantum Attacks on 2K-Feistel Block Cipher to Recover k_0

The quantum circuit of $F(b,x)$ is shown in Figure 4. If f is reversible, such as GOST [9], Camellia [8] etc., it is easy to get k with the knowledge s. If f is irreversible, it is easy to get the key by studying the internal structure of f, such as for DES and its variants.

3.3 Quantum Slide Attack on 2K-Feistel

As shown in Figure 5, 2K-Feistel block cipher adopts round subkeys (k_0, k_1) iteratively and identical round function f.

We first define the following functions using given random constant α:

$$F : \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$$
$$b, x \mapsto \begin{cases} E_K(x,\alpha)_R & \text{if } b = 0, \\ D_K(f(\alpha) \oplus x, \alpha)_R & \text{if } b = 1. \end{cases} \tag{7}$$

As shown in Figure 5, $E_K(x,\alpha)_R = Y_4$, $D_K(Y_1, X_1)_R = X_5 = Y_4$. $Y_1 = f(k_0 \oplus \alpha) \oplus x$, $X_1 = \alpha$. Thus,

$$\begin{aligned} F(0,x) &= E_K(x,\alpha)_R = D_K(f(k_0 \oplus \alpha) \oplus x, \alpha)_R \\ &= F(1, x \oplus f(\alpha) \oplus f(k_0 \oplus \alpha)). \end{aligned} \tag{8}$$

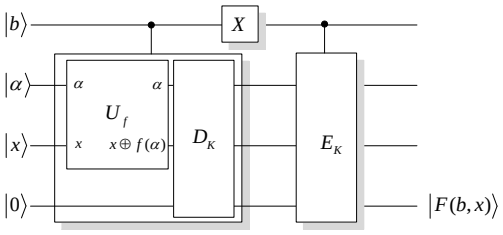

Fig. 6. Simon's function for 2K-Feistel

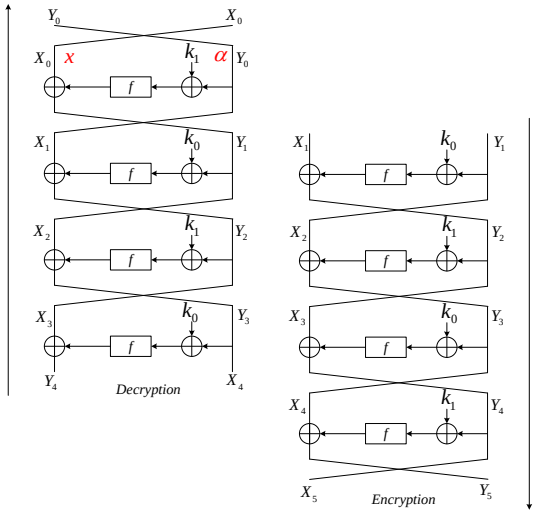

Fig. 7. Quantum Attacks on 2K-Feistel Block Cipher to Recover k_1

So $F(b,x)$ is a function with period $s = 1 \| f(\alpha) \oplus f(k_0 \oplus \alpha)$. The quantum circuit of $F(b,x)$ is shown in Figure 6. If f is reversible, such as GOST [9], Camellia [8], etc., it is easy to get k_0 with the knowledge s. If f is irreversible, it is easy to get the key by studying the internal structure of f, such as for DES and its variants. To get k_1, we design a similar quantum period function in Equation (9).

$$F : \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$$
$$b, x \mapsto \begin{cases} D_K(\alpha, x)_L & \text{if } b = 0, \\ E_K(\alpha, f(\alpha) \oplus x)_L & \text{if } b = 1. \end{cases} \tag{9}$$

As shown in Figure 7, $D_K(\alpha,x)_L = Y_4$, $E_K(X_1,Y_1)_L = X_5 = Y_4$. $Y_1 = f(k_1 \oplus \alpha) \oplus x$, $X_1 = \alpha$. Thus,

$$\begin{aligned} F(0,x) &= D_K(\alpha,x)_L = E_K(\alpha, f(k_1 \oplus \alpha) \oplus x)_L \\ &= F(1, x \oplus f(\alpha) \oplus f(k_1 \oplus \alpha)). \end{aligned} \tag{10}$$

So $F(b,x)$ is a function with period $s = 1 \| f(\alpha) \oplus f(k_1 \oplus \alpha)$, and k_1 is got consequently.

3.4 Quantum Slide Attack on 4K-Feistel

As shown in Figure 5, 4K-Feistel block cipher adopts round subkeys (k_0, k_1, k_2, k_3) iteratively and identical round func-

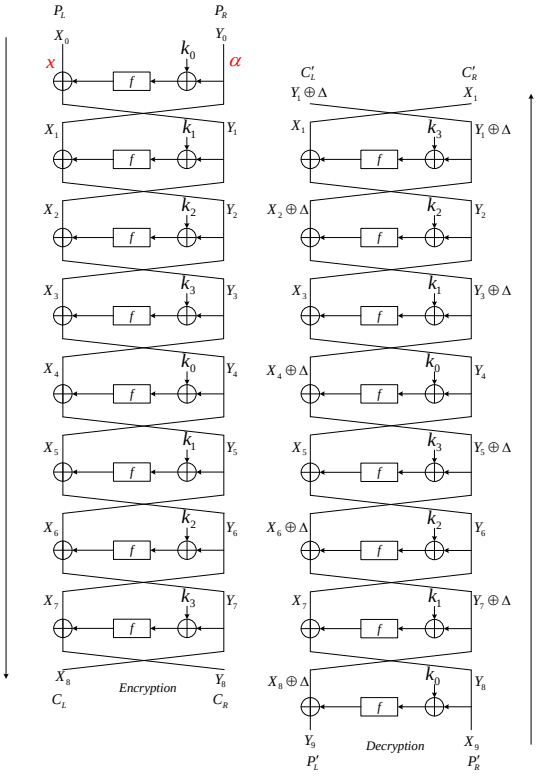

Fig. 8. Quantum Attacks on 4K-Feistel Block Cipher

tion f. Given arbitrary constant $\alpha \in \mathbb{F}_2^{n/2}$, define:

$$F : \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$$
$$b, x \mapsto \begin{cases} E_K(x,\alpha)_R & \text{if } b = 0, \\ D_K(f(\alpha) \oplus x, \alpha)_R & \text{if } b = 1. \end{cases} \tag{11}$$

As shown in Figure 8, $E_K(x,\alpha)_R = Y_8$, $D_K(Y_1 \oplus \Delta, X_1)_R = X_9 = Y_8$, where $\Delta = k_1 \oplus k_3$. $Y_1 = f(k_0 \oplus \alpha) \oplus x$, $X_1 = \alpha$. Thus,

$$F(0,x) = E_K(x,\alpha)_R = D_K(f(k_0 \oplus \alpha) \oplus x \oplus \Delta, \alpha)_R$$
$$= F(1, x \oplus f(\alpha) \oplus f(k_0 \oplus \alpha) \oplus \Delta). \tag{12}$$

So, $F(b,x)$ is a function with period $s = 1 \| f(\alpha) \oplus f(k_0 \oplus \alpha) \oplus \Delta$. Similar to the attack on 2K-Feistel, we could also design a similar period function, with period $s' = 1 \| f(\alpha) \oplus f(k_3 \oplus \alpha) \oplus \Delta'$, where $\Delta' = k_0 \oplus k_2$. We follow the the assumptions made by the 2K-/4K-Feistel's designers, i.e., Biryukov and Wagner, that the round function f is simple, just like the round function of GOST [9], Camellia [8], DES [8], etc. Hence, it is easy to get the secret keys by the knowledge of s and s', when look into the details of the round function.

4 Quantum Key-recovery Attack on GOST Block Cipher

4.1 GOST Block Cipher

GOST [9] is a block cipher designed during the 1970's by the Soviet Union as an alternative to the American DES. Similarly to DES, it has a 64-bit Feistel structure, employing 8 S-boxes and is intended for civilian use. Unlike DES, it has a significantly larger key (256 bits instead of just 56), more rounds (32 compared with DES's 16), and it uses different sets of S-boxes. After the USSR had been dissolved, GOST was accepted as a Russian standard.

Suppose the input state of i-th round function is (X_{i-1}, Y_{i-1}), where X_{i-1} and Y_{i-1} are the left and right branches of the i-th round function for $i = 1, 2, ..., 32$. The first round of GOST is given in Figure 10, the only difference for each round is the subkeys. The symbols used are

$+$	modular addition,
$-$	modular subtraction,
$\oplus$	bitwise addition,
$<<< j$	cyclic left rotation by j bits ,
$>>> j$	cyclic right rotation by j bits.
$X[i_1, .., i_j]$	the $i_1, .., i_j$th least significant bits of the 32-bit word X.

In the round function, the round key is (modular) added with 32-bit right branch; then the 32-bit state is substitute by S, which is composed of 8 4×4 s-boxes in parallel; then rotating left the 32-bit state by 11 bits. It has a simple key schedule: 256-bit key is divided into eight 32-bit words $k_0, k_1 \cdots, k_7$ and the sequence of round keys is given as $k_0, \cdots, k_7, k_0, \cdots, k_7, k_0, \cdots, k_7, k_7, k_6, \cdots, k_1, k_0$.

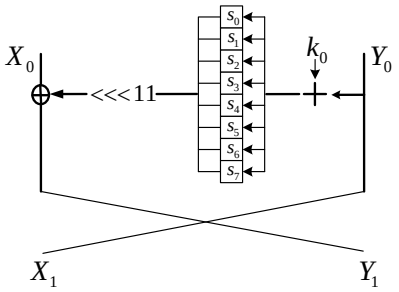

Fig. 9. The first round of GOST block cipher.

4.2 Quantum Attack on 30-round GOST Block Cipher

We first give some properties of GOST.

Property 1. *As shown in Figure 10, for a two round GOST, if we know (X_0, Y_0) and (X_2, Y_2), then $k_0 = S^{-1}((X_0 \oplus X_2) >>> 11) - Y_0$, $k_1 = S^{-1}((Y_0 \oplus Y_2) >>> 11) - X_2$.*

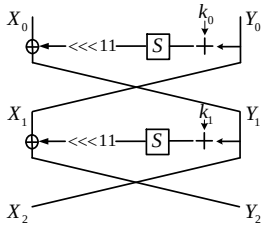

Fig. 10. 2-round of GOST block cipher

Property 2. *(***Reflection Property***) If the input state of the 25*th *round meets condition $X_{24} = Y_{24}$, then the last 16-round of*

*32-round GOST acts as an identity by ignoring the last swap function, i.e., the input of 17*th *round is* (X_{16}, Y_{16})*, and the output of 32*th *round is* $(X_{32}, Y_{32}) = (Y_{16}, X_{16})$.

Proof. As shown in Figure 11, it is easy to see that, $X_{23} = f_{k_8}(Y_{23}) \oplus Y_{24}$, $Y_{25} = f_{k_8}(Y_{24}) \oplus X_{24}$. Since $X_{24} = Y_{24}$ and $Y_{23} = X_{24}$, we get $X_{23} = Y_{25}$. While $Y_{23} = X_{24} = X_{25}$ holds. Thus, we get (X_{23}, Y_{23})=(Y_{25}, X_{25}).

$X_{22} = f_{k_7}(Y_{22}) \oplus Y_{23}$, $Y_{26} = f_{k_7}(Y_{25}) \oplus X_{25}$. Since (X_{23}, Y_{23})=(Y_{25}, X_{25}) and $Y_{22} = X_{23}$, we get $X_{22} = Y_{26}$. While $Y_{22} = X_{23} = Y_{25} = X_{26}$ holds. Thus, we get (X_{22}, Y_{22})=(Y_{26}, X_{26}). Iterating the above procedures, finally, we get the conclusion of Property 2, i.e., $(X_{32}, Y_{32}) = (Y_{16}, X_{16})$. □

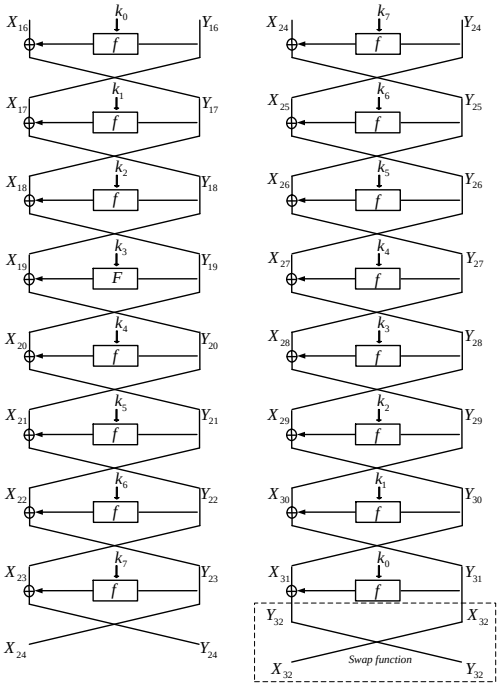

Fig. 11. Reflection Property of the last 16-rounds GOST block cipher.

In this section, we only consider the last 30-round reduced GOST block cipher (from 3*th* to 32*th* round), against quantum attackers. In case of a quantum computer, the adversaries were able to generate quantum queries on some superposition quantum states of the relevant cryptosystem, which is the so-called *quantum chosen-plaintext attacks* (qCPA) [10]. Since the key size of the 30-round GOST block cipher is 256-bit, if we trivially use quantum brute-force search (Grover's algorithm [3]) to find the key, it needs 2^{128} Grover iterations. In the following, we combine the reflection property and Grover's algorithm to attack 30-round GOST block cipher in 2^{112} Grover iterations. Note that the input and output are (X_2, Y_2) and (X_{32}, Y_{32}). We first construct the following quantum algorithm $\mathcal{A}$: Preparing the initial 32×7-bit register $|0\rangle^{\otimes 224}$. Apply Hadamard transform $H^{\otimes 224}$ to the register to attain an equal superposition (omitting the amplitudes):

$$\sum_{X_2,k_2,k_3,...,k_7 \in \{0,1\}^{32}} |X_2\rangle|k_2, k_3, ..., k_7\rangle = |\varphi\rangle, \tag{13}$$

where X_2 is the left half of the input of the 30-round GOST; the right half Y_2 is a constant.

According to the Reflection Property 2, when $X_{24} = Y_{24}$, the last 16-round is a identical transformation by ignoring the last swap function. Thus, given 2^{32} inputs (X_2, Y_2), it is expected that there is one (X_2, Y_2) pair that satisfies the condition $X_{24} = Y_{24}$, then $(X_{16} \| Y_{16}) = (Y_{32} \| X_{32})$.

Once we get the right (X_2, Y_2) somehow, we guess $k_2, k_3, ..., k_7$, then encrypt for round 3-8 to get the internal state (X_8, Y_8), decrypt $(X_{16} \| Y_{16})$ for round 11-16 to get (X_{10}, Y_{10}). According to Property 1, we could deduce k_0 and k_1 from (X_8, Y_8) and (X_{10}, Y_{10}).

Considering the superposition $|\varphi\rangle$, assume that we had a classifier $\mathcal{B} : \{0,1\}^{32\times 7} \mapsto \{0,1\}$, which partitions $|\varphi\rangle$ into a good subspace and a bad subspace: $|\varphi\rangle = |\varphi_1\rangle + |\varphi_0\rangle$, where $|\varphi_1\rangle$ and $|\varphi_0\rangle$ denotes the projection onto the good subspace and bad subspace, respectively. In the good subspace $|\varphi_1\rangle$, (X_2, Y_2) meets the Reflection Property and $k_2, k_3, ..., k_7$ are the right subkeys. For the good state $|x\rangle$, $\mathcal{B}(x) = 1$.

We construct the quantum classifier $\mathcal{B}$. Define $\mathcal{B} : \{0,1\}^{32\times 7} \mapsto \{0,1\}$ that maps $(X_2, k_2, k_3, ..., k_7) \mapsto \{0,1\}$:

1) For (X_2, Y_2), derive (X_{32}, Y_{32}) from the 30-round encryption oracle, note that Y_2 is a random given constant.
2) Use $(k_2, k_3, ..., k_7)$, (X_2, Y_2) and (X_{32}, Y_{32}) to derive k_0, k_1 from Property 1.
3) Check the derived $(k_0, k_1, k_2, ..., k_7)$ by 5 plaintext-ciphertext pairs using the 30-round encryption oracle. If the check is right, output 1. Else ouput 0.

We classify a state $|X_2\rangle|k_2, k_3, ..., k_7\rangle$ is a good state if and only if $\mathcal{B}(X_2, k_2, k_3, ..., k_7) = 1$. The classifier $\mathcal{B}$ outputs good under two conditions:

a) Condition 1. (X_2, Y_2) meets the Reflection Property. According to the above cryptanalysis, it is right with a probability of 2^{-32}.
b) Condition 2. $k_2, k_3, ..., k_7$ are the right subkeys. It is right with a probability 2^{-192}.

If we measure $|\phi\rangle$, it produces the good state with probability p:

$$\begin{aligned} p &= \Pr[|X_2\rangle|k_2, k_3, ..., k_7\rangle \texttt{ is good}] \\ &= \Pr[\mathcal{B}(X_2, k_2, k_3, ..., k_7) = 1] \\ &= \Pr[\texttt{Condition 1}] \cdot \Pr[\texttt{Condition 2}] \\ &\approx 2^{-32} \times 2^{-32\times 6} = 2^{-224}. \end{aligned} \tag{14}$$

Our classifier $\mathcal{B}$ defines a unitary operator $S_{\mathcal{B}}$ that conditionally change the sign of the quantum state $|X_2\rangle|k_2, k_3, ..., k_7\rangle$:

$$\begin{cases} - & |X_2\rangle|k_2, .., k_7\rangle \texttt{ if } \mathcal{B}(X_2, k_2, .., k_7) = 1 \\ & |X_2\rangle|k_2, .., k_7\rangle \texttt{ if } \mathcal{B}(X_2, k_2, .., k_7) = 0 \end{cases} \tag{15}$$

The complete amplification process is realized by repeatedly for t times applying the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$ to the state $|\varphi\rangle = \mathcal{A}|0\rangle$, i.e. $Q^t\mathcal{A}|0\rangle$.

Initially, the angle between $|\varphi\rangle = \mathcal{A}|0\rangle$ and the bad subspace $|\varphi_0\rangle$ is θ, where $sin^2(\theta) = p = \langle\varphi_1|\varphi_1\rangle$. When p is smaller enough, $\theta \approx arcsin(\sqrt{p}) \approx 2^{-\frac{224}{2}}$. According to Theorem 1, after $t = \lceil \frac{\pi}{4\theta} \rceil = \lceil \frac{\pi}{4\times 2^{-\frac{224}{2}}} \rceil \approx 2^{112}$ Grover iterations Q, the angle between resulting state and the bad subspace is roughly $\pi/2$. The probability P_{good} that the measurement yields a good state is about $sin^2(\pi/2) = 1$.

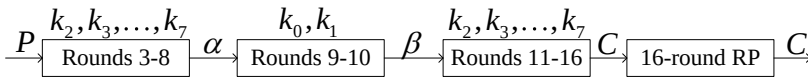

Fig. 12. Attack on 30-round reduced GOST

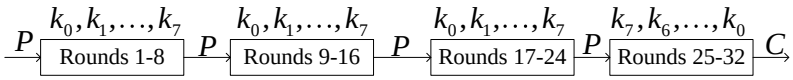

Fig. 13. Attack on the Full-round GOST

The whole attack needs 224 qubits and 2^{112} Grover iterations, which is more efficient than the trivial quantum search (256 qubits and 2^{128} Grover iterations).

4.3 Quantum Attack on Full-round GOST Block Cipher

Property 3. *(**Fixed Point Property**) As shown in Figure 13, assume that when we encrypt a 64-bit plaintext P =(X_0, Y_0), we obtain (X_8, Y_8)=(X_0, Y_0) after 8 encryption rounds. Since rounds 9-16 and 17-24 are identical to rounds 1-8, we obtain P after 16 and 24 encryption rounds as well. In rounds 25-32, the round keys $k_0, ..., k_7$ are applied in the reverse order, and we obtain some arbitrary ciphertext $C = (X_{32}, Y_{32})$. The knowledge of P and C immediately gives us the two input-output pairs of the first 8-round, i.e., $(P, P) = (X_0\|Y_0, X_0\|Y_0)$ and $(\bar{C}, \bar{P}) = (Y_{32}\|X_{32}, Y_0\|X_0)$. The probability to get a fix point of the first 8 rounds is 2^{-64}.*

Proof. As shown in Figure 13, once we get a input-output pair $(P, P) = (X_0\|Y_0, X_0\|Y_0)$ for the rounds 1-8, we get the input-output pair (P, C) for rounds 25-32. We focus on rounds 25-32 shown in Figure 11, different from rounds 1-8, the subkeys are in inverse order. If we consider rounds 25-32 in inverse direction, i.e., from 32th round to 25th round, the only difference from rounds 1-8 is that there is an additional swap function is in the first round but not in the last round. So, $(\bar{C}, \bar{P}) = (Y_{32}\|X_{32}, Y_0\|X_0)$ is also a input-output pair for rounds 1-8. □

Property 4. *As shown in Figure 14, if we know two valid input-output pairs of the 3-round GOST, i.e., $(X_5\|Y_5, X_8\|Y_8)$ and $(X'_5\|Y'_5, X'_8\|Y'_8)$, then we can easily determine the three subkeys k_5, k_6, k_7.*

Proof. As shown in Figure 14, we get

$$(S(Y_5 + k_5) <<< 11) \oplus X_5 = (S(X_8 + k_7) <<< 11) \oplus Y_8, \quad (16)$$

$$(S(Y'_5 + k_5) <<< 11) \oplus X'_5 = (S(X'_8 + k_7) <<< 11) \oplus Y'_8. \quad (17)$$

We rewrite Equation (16), as $S(Y_5 + k_5) \oplus S(X_8 + k_7) = (X_5 \oplus Y_8) >>> 8$. Note that S is composed of 8 4×4 s-boxes in parallel, we first guess the 4 least significant bits of k_5, i.e., $k_5[3, 2, 1, 0]$, then compute $s_0(Y_5[3, .., 0] + k_5[3, .., 0])$, where s_0 is the s-box applied to the 4 least significant bits of $Y_5 + k_5$, thus we could determine $X_8[3, .., 0] + k_7[3, .., 0]$ and get $k_7[3, .., 0]$ by (modular 2^4) subtract $X_8[3, .., 0]$. Similarly, by Equation (17), we could also derive another value of $k_7[3, .., 0]$, if they are not equal, then the guessing of $k_5[3, 2, 1, 0]$ is wrong. After we determine a right candidate $k_5[3, 2, 1, 0]$ and $k_7[3, 2, 1, 0]$, we could continue to guess and determine $k_5[7, 6, 5, 4]$ and $k_7[7, 6, 5, 4]$. Finally, we are expected to get the right candidate k_5, k_7. Then we compute $Y_6 = (S(Y_5 + k_5) <<< 11) \oplus X_5$. Thus we get $k_6 = S^{-1}((Y_5 \oplus X_8) >>> 11) - Y_6$. Totally, we only use $8 \times 2^4 \times 2 + 2 \times 8 = 272$ s-boxes operations, which approximates one encryption of GOST (it needs $8 \times 32 = 256$ s-boxes operations). □

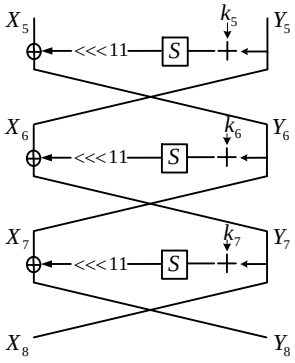

Fig. 14. 3-round GOST.

In our quantum attack on full-round GOST, we first construct the following quantum algorithm $\mathcal{A}$: Preparing the initial 32×7-bit register $|0\rangle^{\otimes 224}$. Apply Hadamard transform $H^{\otimes 224}$ to the register to attain an equal superposition (omitting the amplitudes):

$$\sum_{X_0, Y_0, k_0, k_1, ..., k_4 \in \{0,1\}^{32}} |X_0, Y_0\rangle |k_0, k_1, ..., k_4\rangle = |\varphi\rangle. \quad (18)$$

According to Property 3, once we get the right P =(X_0, Y_0) that meet the fix point property, we get two input-output pairs of the first 8 rounds.

Considering the superposition $|\varphi\rangle$, assume that we had a classifier $\mathcal{B} : \{0,1\}^{32\times 7} \mapsto \{0,1\}$, which partitions $|\varphi\rangle$ into a good subspace and a bad subspace: $|\varphi\rangle = |\varphi_1\rangle + |\varphi_0\rangle$, where $|\varphi_1\rangle$ and $|\varphi_0\rangle$ denotes the projection onto the good subspace and bad subspace, respectively. In the good subspace $|\varphi_1\rangle$, $P = (X_0, Y_0)$ meets the fixed point property and $k_0, k_1, ..., k_4$ are the right subkeys. For the state $|x\rangle$ in the good subspace, $\mathcal{B}(x) = 1$.

We construct the quantum classifier $\mathcal{B}$. Define $\mathcal{B}: \{0,1\}^{32\times 7} \mapsto \{0,1\}$ that maps $(X_0, Y_0, k_0, k_1, ..., k_4) \mapsto \{0,1\}$:

1) For (X_0, Y_0), derive (X_{32}, Y_{32}) from the encryption oracle of GOST.
2) Suppose (X_0, Y_0) meet the fix point property, use $(k_0, k_1, ..., k_4)$ to derive k_5, k_6, k_7 from Property 4.
3) Check the derived $(k_0, k_1, k_2, ..., k_7)$ by 5 plaintext-ciphertext pairs using the GOST encryption oracle. If the check is right, output 1. Else ouput 0.

We classify a state $|X_0, Y_0\rangle|k_0, k_1, ..., k_4\rangle$ is a good if and only if $\mathcal{B}(X_0, Y_0, k_0, k_1, ..., k_4) = 1$. The classifier $\mathcal{B}$ outputs good under two conditions:

a) Condition 1. (X_0, Y_0) meets the Property 3. It is right with a probability of 2^{-64}.
b) Condition 2. $k_0, k_1, ..., k_4$ are the right subkeys. It is right with a probability 2^{-160}.

If we measure $|\phi\rangle$, it produces the good state with probability p:

$$\begin{aligned} p &= \Pr[|X_0, Y_0\rangle|k_0, k_1, ..., k_4\rangle \texttt{ is good}] \\ &= \Pr[\mathcal{B}(X_0, Y_0, k_0, k_1, ..., k_4) = 1] \\ &= \Pr[\texttt{Condition 1}] \cdot \Pr[\texttt{Condition 2}] \\ &\approx 2^{-64} \times 2^{-32\times 5} = 2^{-224}. \end{aligned} \tag{19}$$

Our classifier $\mathcal{B}$ defines a unitary operator $S_{\mathcal{B}}$ that conditionally change the sign of the quantum state $|X_0, Y_0\rangle|k_0, k_1, ..., k_4\rangle$:

$$\begin{cases} -|X_0, Y_0\rangle|k_0, k_1, ..., k_4\rangle \texttt{ if } \mathcal{B}(X_0, Y_0, k_0, k_1, ..., k_4) = 1 \\ |X_0, Y_0\rangle|k_0, k_1, ..., k_4\rangle \texttt{ if } \mathcal{B}(X_0, Y_0, k_0, k_1, ..., k_4) = 0 \end{cases} \tag{20}$$

The complete amplification process is realized by repeatedly for t times applying the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$ to the state $|\varphi\rangle = \mathcal{A}|0\rangle$, i.e. $Q^t\mathcal{A}|0\rangle$.

Initially, the angle between $|\varphi\rangle = \mathcal{A}|0\rangle$ and the bad subspace $|\varphi_0\rangle$ is θ, where $sin^2(\theta) = p = \langle\varphi_1|\varphi_1\rangle$. When p is smaller enough, $\theta \approx arcsin(\sqrt{p}) \approx 2^{-\frac{224}{2}}$. According to Theorem 1, after $t = \lceil \frac{\pi}{4\theta} \rceil = \lceil \frac{\pi}{4\times 2^{-\frac{224}{2}}} \rceil \approx 2^{112}$ Grover iterations Q, the angle between resulting state and the bad subspace is roughly $\pi/2$. The probability P_{good} that the measurement yields a good state is about $sin^2(\pi/2) = 1$. The whole attack needs 224 qubits and 2^{112} Grover iterations.

5 Conclusion

In this paper, we have studied several Feistel block ciphers against quantum attackers, including the attacks on 2/4K-Feistel and 2/4K-DES in polynomial time and the attacks on GOST which is faster than a quantum brute force search attack by a factor 2^{16}. Our paper alerts the academy and industry that it is not enough to just double the key length of the symmetric primitives to stand up to the attackers from the post-quantum world.

References

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997, 26(5): 1484–1509.

[2] Rivest R L, Shamir A, Adleman L. A Method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 1978, 21(2): 120–126.

[3] Grover L K. A fast quantum mechanical algorithm for database search. In: Miller G L, eds. Proceedings of STOC 1996. ACM, 1996. 212–219.

[4] Kuwakado H, Morii M. Security on the quantum-type even-mansour cipher. In: International symposium on information theory and its applications, ISITA 2012. IEEE, 2012. 312–316.

[5] Even S, Mansour Y. A construction of a cipher from a single pseudorandom permutation. Journal of Cryptology, 1997, 10(2): 151–161.

[6] Takagi T, Peyrin T. Advances in Cryptology - ASIACRYPT 2017, Part I. Lecture Notes in Computer Science, Vol 10624. Berlin: Springer-Verlag, 2017. 1-813.

[7] Feistel H, Notz W A, Smith J L. Some cryptographic techniques for machine-to-machine data communications. In: Proceedings of the IEEE, 1975, 63(11): 1545–1554.

[8] International Organization for Standardization(ISO). International Standard- ISO/IEC 18033-3, Information technology-Security techniques-Encryption algorithms -Part 3: Block ciphers. 2010.

[9] National Soviet Bureau of Standards. Information Processing System - Cryptographic Protection - Cryptographic Algorithm GOST 28147-89 (1989)

[10] Boneh D, Zhandry M. Secure signatures and chosen ciphertext security in a quantum computing world. In: Canetti R, Garay J A, eds. Advances in Cryptology - CRYPTO 2013. Lecture Notes in Computer Science, Vol 8043. Berlin: Springer-Verlag, 2013. 361–379.

[11] Simon D R. On the power of quantum computation. SIAM Journal on Computing, 1997, 26(5):1474–1483.

[12] Kaplan M, Leurent G, Leverrier A, et al. Breaking symmetric cryptosystems using quantum period finding. In: Robshaw M, Katz J, eds. Advances in Cryptology - CRYPTO 2016. Lecture Notes in Computer Science, Vol 9815. Berlin: Springer-Verlag, 2016. 207–237.

[13] Biryukov A, Wagner D. Advanced Slide Attacks. In: Preneel B. eds. Advances in Cryptology ł EUROCRYPT 2000. Lecture Notes in Computer Science, Vol 1807. Springer, Berlin, Heidelberg, 2000. 589–606.

[14] Isobe T. A Single-Key Attack on the Full GOST Block Cipher. In: Joux A, eds. Fast Software Encryption, FSE 2011. Lecture Notes in Computer Science, Vol 6733. Berlin: Springer-Verlag, 2011. 290–305.

[15] Dinur I, Dunkelman O, Shamir A. Improved Attacks on Full GOST. In: Canteaut A, eds. Fast Software Encryption, FSE 2012. Lecture Notes in Computer Science, Vol 7549. Berlin: Springer-Verlag, 2012. 9–28.

[16] Kara O. Reflection cryptanalysis of some ciphers. In: Chowdhury D R, Rijmen V, Das A, eds. Progress in Cryptology - INDOCRYPT 2008. Lecture Notes in Computer Science, Vol 5365. Berlin: Springer-Verlag, 2008. 294–307.

[17] Brassard G, Hoyer P, Mosca M, et al. Quantum amplitude amplification and estimation. *arXiv: Quantum Physics*, 2000.

[18] Biryukov A, Wagner D. Slide Attacks. In: Knudsen L, eds. Fast Software Encryption, FSE 1999. Lecture Notes in Computer Science, Vol 1636. Springer, Berlin, Heidelberg, 1999. 245-259.

[19] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. J. Cryptology (1991) Vol 4, Issue 1. 3-72.

[20] Matsui M. Linear Cryptanalysis Method of DES Cipher. In: Helleseth T, eds. EUROCRYPT 1993. LNCS, Vol. 765. Springer, Heidelberg, 1994. 386C-397.