UDC 004.056.55

The Quantum Distinguishing Attacks on Generalized Feistel Schemes

A. Zvychaina[1,a], A. Fesenko[1,b]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",*
Institute of Physics and Technology

Abstract

It turned out that in addition to problems with classical asymmetric cryptography in the post-quantum period, there are certain doubts about the strength of symmetric cryptographic schemes. This paper demonstrates that on Type III Generalized Feistel Scheme (GFS), by selectively fixing specific parts of the plaintext at the input to the GFS, it is possible to reduce the problem of distinguishing between random text and encrypted output of the same GFS to the Simon problem through different approaches. Our method enables the cracking of the cipher up to d rounds in polynomial time, while a more sophisticated approach based on different formulas from other paths of the cipher can crack $d + 1$ rounds with the same time complexity in quantum adversary model. These distinct approaches yield varying results in terms of scheme security, indicating the potential to break more rounds in the GFS using the same methodology.

Keywords: Generalized Feistel Schemes, Quantum Distinguishing Attack, Simon's Problem.

Introduction

In 1994, Daniel Simon introduced a significant problem in the field of quantum computing – the task of finding the period of a function, demonstrating its solvability within polynomial time in a quantum model [1]. This discovery opened the door to exploring the potential of quantum computing for solving complex computational problems efficiently. In 1996, Lov Grover made another breakthrough by reducing the time required to solve the problem of finding a unique element in an unstructured database using quantum algorithms, achieving a quadratic speedup [2]. The implications of quantum computing for symmetric cryptography did not capture widespread attention until 2010 when Kuwakado and Morii proposed a novel approach. They proposed a way to reduce the attack of distinguishing a random text from the ciphertext for the classical three-round Feistel scheme to the Simon problem [3]. This discovery marked the birth of post-quantum cryptanalysis of symmetric ciphers and this field that has gained increasing relevance due to the rapid advancement of quantum computers.

Over time, researchers have identified vulnerabilities and developed quantum attacks on various cryptographic schemes and constructions. These include attacks on Types I and II GFS [4], Even-Mansour scheme, authentication codes [5], FX-constructions [6], five-round Feistel scheme [7], 2/4K-Feistel scheme, 2/4K-DES [8]. Moreover, cryptographic primitives such as MISTY L/R, CAST-256, CLEFIA, MARS, SMS4, and Skipjack-A/B have also been subjected to quantum cryptanalysis [9].

In the context of this evolving landscape, this paper presents a comprehensive analysis of the strength of Type III GFS within the quantum adversary model. While it does not introduce a novel finding, it serves a crucial purpose by elucidating the difference between the strategy published in our work [10] (as well as in [11] that was gain independently) and that used in [12], enabling a better understanding of its security.

[a] azv-ipt23@lll.kpi.ua
[b] a.fesenko@kpi.ua

1. Preliminaries

Simon's algorithm is used in the quantum distinguisher attack on Type III GFS, therefore, there is a need to explicate it. This section also describes some of the theoretical foundations of quantum computing for further research.

1.1. Simon's problem.

Suppose for the function

$$f : \{0,1\}^n \to \{0,1\}^n$$

there exists such a that $f(x) = f(y)$ if and only if $y = x \oplus a$, where $\oplus$ is an exclusive disjunction (XOR). Simon's problem is to find a.

Obviously, in the classical case, the solution of this problem requires an exponential number of steps and memory; however, in the quantum model of computation, Daniel Simon showed that the complexity of finding a is polynomial [1]. To understand how he did it, we have to introduce some definitions and claim.

Definition 1. *n-qubit quantum register* is a quantum system whose wave function is defined as follows:

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

where $|\cdot\rangle$ is a ket vector as in Dirac notation, and amplitudes α_i satisfy the normalization condition:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

It is important to emphasise that when someone talks about quantum computations it means the application of unitary operators in order to change state vectors.

One of the well-known operators is the *Hadamard operator* (or corresponding *Hadamard gate*).

Definition 2. The *Hadamard operator (gate)* is a unitary operator that is defined as follows:

$$H_n = H_{n-1} \otimes H, \text{ where } H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$\otimes$ is the Kronecker product, n is the dimension of the quantum system to which we want to apply the Hadamard operator.

At this point, it is inconvenient to use such definition in the general case, thereby for our purposes we employ an alternative formulation, which is given below.

Claim 1. *The Hadamard gate applied to a vector $|x\rangle$ of some system with n qubits can be represented as:*

$$H_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{\langle x|y\rangle} |y\rangle,$$

where $\langle x|y\rangle$ is a scalar product of vectors x and y.

It should be noted that a quantum oracle is a formal model that performs the work of some function f, the internal structure of which is unknown to us. Then, based on the fact that in the quantum computational model everything is described by unitary operators, it becomes clear that the quantum oracle must implement such operator U_f which is invertible. Usually, the *standard oracle model* is used:

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle.$$

It is plain to see that U_f does not affect the value of $|x\rangle$, although uses it to determine the value of the function $f(x)$, what justifies the inversion of this operator. Furthermore, substituting different values in the registers $|x\rangle$ and $|y\rangle$, it is easy to make sure that all possible values of the function $f(x)$ are realised.

Theorem 1. *Simon's problem is solved in a quantum computational model in polynomial time [1, 3, 4, 7].*

Proof.

1) Let us set two quantum registers, to the input of which we give n-qubit zeros, i.e. $|0\rangle^n |0\rangle^n$. Then we apply the Hadamard transformation to the first of them:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle^n.$$

Thus, we received all possible input data.

2) To obtain the value of the function $f(x)$, we make a query to the quantum oracle, i.e. we apply the unitary operator U_f to two registers:

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

3) Since Simon's problem is a period finding problem, we have:

$$\frac{1}{\sqrt{2^n}}\sum_{\substack{x=0,\\ x\neq x\oplus a}}^{2^n-1}(|x\rangle+|x\oplus a\rangle)\,|f(x)\rangle.$$

4) We measure the state of the second register, then we get the value of the function f and the sum of its preimages:

$$\tfrac{1}{\sqrt{2}}(|x\rangle+|x\oplus a\rangle)\,|f(x)\rangle.$$

5) Again, we apply the Hadamard transformation to the first register:

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{y=0}^{2^n-1}(-1)^{\langle x|y\rangle}\,|y\rangle+$$
$$\frac{1}{\sqrt{2^{n+1}}}\sum_{y=0}^{2^n-1}(-1)^{\langle x\oplus a|y\rangle}\,|y\rangle.$$

6) If $\langle a|y\rangle\neq 0$, then the coefficient for $|y\rangle$ is zero. Accordingly, Simon's algorithm reduces the brute force of all register's states to the solution of the linear equation $\langle a|y\rangle=0$, which can be done efficiently in time $O(n)$.

■

1.2. Three-round Feistel scheme quantum distinguisher with polynomial time

Hidenori Kuwakado and Masakatu Morii in [3] showed why the ciphertext

$$y=y_1\parallel y_2\in\{0,1\}^{2n},\text{ where }y_1,y_2\in\{0,1\}^n$$

of the scheme in the Fig. 1 is not a random permutation in the quantum adversary model by reducing the question of the randomness of its output to Simon's problem when for the classical case Luby and Rackoff proved in 1988 that the Feistel scheme is resistant to distinguishing attacks.

Let the input to the scheme in the Fig. 1 be defined as follows:

$$x=x_1\parallel x_2\in\{0,1\}^{2n},\text{ where }x_1,x_2\in\{0,1\}^n.$$

We assume that P_1,P_2,P_3 are random permutations on n-bit vectors, therefore at the output of the encryption scheme E we get:

$$E(x)=E(x_1\parallel x_2)=P_2(P_1(x_2)\oplus x_1)\oplus x_2\parallel$$
$$P_3(P_2(P_1(x_2)\oplus x_1)\oplus x_2)\oplus(P_1(x_2)\oplus x_1)=$$
$$y_1\parallel y_2.$$

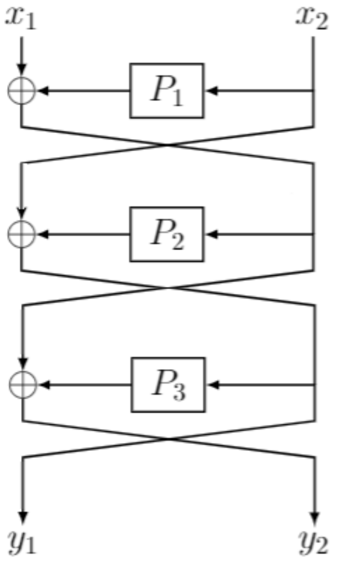

Figure 1: Classical three-round Feistel scheme

To restore the plaintext when the inverse permutations to P_1,P_2,P_3 are unknown, we only need to analyze one part of the ciphertext from the third round, either y_1 or y_2, as both contain x_1 and x_2. Let's focus on y_1 and define function W as:

$$W(x)=W(x_1\parallel x_2)=P_2(P_1(x_2)\oplus x_1)\oplus x_2.$$

Let f be a function that maps $(n+1)$-bit vectors to n-bit vectors. f operates as follows, where α and β are arbitrary n-bit constants:

$$f(b\parallel x_1)=\begin{cases}W(x_1\parallel\alpha)\oplus\beta, & \text{if } b=0,\\ W(x_1\parallel\beta)\oplus\alpha, & \text{if } b=1.\end{cases}$$

Lemma 1. *The ciphertext in the third round of the classical Feistel scheme (see Fig. 1) is not a random permutation in the quantum adversary model.*

Proof. Show that $f(b\parallel x_1)=f(b^{'}\parallel x_1^{'})$ if and only if $b^{'}=b\oplus 1$ and $x_1^{'}=x_1\oplus a$, where period $a=P_1(\alpha)\oplus P_1(\beta)$.
Necessary condition proof. Let $b=b^{'}=0$, then:

$$f(0\parallel x_1)=W(x_1\parallel\alpha)\oplus\beta=$$
$$P_2(P_1(\alpha)\oplus x_1)\oplus\alpha\oplus\beta,$$
$$f(0\parallel x_1^{'})=W(x_1^{'}\parallel\alpha)\oplus\beta=$$
$$P_2(P_1(\alpha)\oplus x_1^{'})\oplus\alpha\oplus\beta.$$

Since $f(0\parallel x_1)=f(0\parallel x_1^{'})$ and P_2 is a random permutation, we have:

$$x_1=x_1^{'}\text{ and }b\parallel x_1=b^{'}\parallel x_1^{'}.$$

If $b = 0,\ b^{'} = 1$, then:

$$f(1 \parallel x_1^{'}) = W(x_1^{'} \parallel \beta) \oplus \alpha = \\ P_2(P_1(\beta) \oplus x_1^{'}) \oplus \beta \oplus \alpha.$$

Since $f(0 \parallel x_1) = f(1 \parallel x_1^{'})$ and P_2 is a random permutation, we have:

$x_1^{'} = x_1 \oplus a$, where period $a = P_1(\alpha) \oplus P_1(\beta)$.

A similar proof for the cases where $b = 1,\ b^{'} = 1$ and $b = 1, b^{'} = 0$.
Sufficient condition proof. Let $b = 0, b^{'} = 1$, then:

$$f(1 \parallel x_1^{'}) = W(x_1^{'} \parallel \beta) \oplus \alpha = \\ P_2(P_1(\beta) \oplus x_1^{'}) \oplus \beta \oplus \alpha = P_2(P_1(\beta) \oplus x_1 \oplus \\ P_1(\alpha) \oplus P_1(\beta)) \oplus \beta \oplus \alpha = f(0 \parallel x_1).$$

A similar proof for the case where $b = 0,\ b^{'} = 1$. ■

2. Type III GFS quantum distinguisher with polynomial time

Dong, Li, and Wang in [4] proposed a way to reduce the problem of distinguishing a random text from the ciphertext for Types I and II GFS to the Simon problem. A similar result can be shown for Type III.

2.1. Cracking d rounds of the Type III GFS

We consider the scheme in the Fig. 2 and trace the outputs of each of the three rounds. Let us suppose that the input message to this scheme is a $3n$-bit vector:

$$x = x_1 \parallel x_2 \parallel x_3, \text{ where } x_1, x_2, x_3 \in \{0,1\}^n.$$

Let P_i^j stands for the permutation function, where i is the number of the round, and j is the number of the permutation function in the round (we assume that the numbering starts with 1). The second block y_2 in the third round equals

$$W(x) = W(x_1 \parallel x_2 \parallel x_3) = \\ P_3^1(P_2^1(P_1^1(x_2) \oplus x_1) \oplus x_3) \oplus P_1^2(x_3) \oplus x_2.$$

Suppose f be function that maps $(2n+1)$-bit to n-bit vector, and operates on the constants α, β and a fixed n-bit vector x_3, as follows:

$$f(b \parallel x_1 \parallel x_3) = \begin{cases} \text{if } b = 0: \\ W(x_1 \parallel \alpha \parallel x_3) \oplus \beta, \\ \text{if } b = 1: \\ W(x_1 \parallel \beta \parallel x_3) \oplus \alpha. \end{cases}$$

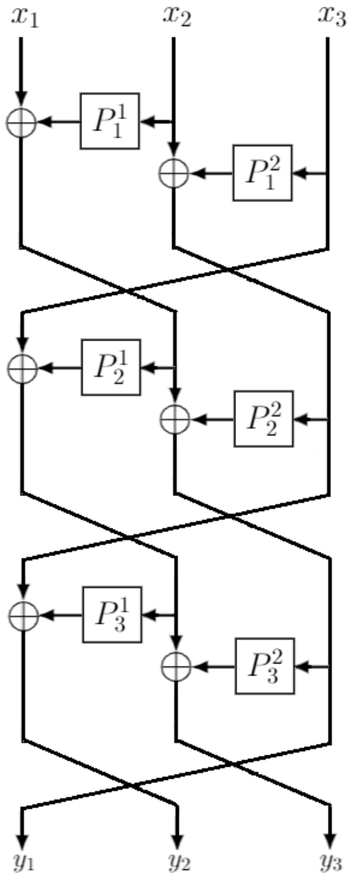

Figure 2: Type III GFS where the plaintext is divided into three parts at the entrance to the encryption scheme

Lemma 2. *The ciphertext in the third round of the Type III Generalized Feistel Scheme where the plaintext is divided into three parts (see Fig.2) is not a random permutation in the quantum adversary model [10].*

Proof. Show that $f(b \parallel x_1 \parallel x_3) = f(b^{'} \parallel x_1^{'} \parallel x_3)$ if and only if $b^{'} = b \oplus 1$ and $x_1^{'} = x_1 \oplus a$, where period $a = P_1^1(\alpha) \oplus P_1^1(\beta)$.
Necessary condition proof. Let $b = b^{'} = 0$, then:

$$f(0 \parallel x_1 \parallel x_3) = W(x_1 \parallel \alpha \parallel x_3) \oplus \beta = \\ P_3^1(P_2^1(P_1^1(\alpha) \oplus x_1) \oplus x_3) \oplus P_1^2(x_3) \oplus \alpha \oplus \beta;$$

$$f(0 \parallel x_1^{'} \parallel x_3) = W(x_1^{'} \parallel \alpha \parallel x_3) \oplus \beta = \\ P_3^1(P_2^1(P_1^1(\alpha) \oplus x_1^{'}) \oplus x_3) \oplus P_1^2(x_3) \oplus \alpha \oplus \beta.$$

Since $f(0 \parallel x_1 \parallel x_3) = f(0 \parallel x_1^{'} \parallel x_3)$ and P_2^1 is a random permutation, we have:

$$x_1 = x_1^{'} \text{ and } b \parallel x_1 \parallel x_3 = b^{'} \parallel x_1^{'} \parallel x_3.$$

If $b = 0,\ b^{'} = 1$, then:

$$f(1 \parallel x_1^{'} \parallel x_3) = W(x_1^{'} \parallel \beta \parallel x_3) \oplus \alpha = \\ P_3^1(P_2^1(P_1^1(\beta) \oplus x_1^{'}) \oplus x_3) \oplus P_1^2(x_3) \oplus \beta \oplus \alpha.$$

Since $f(0 \parallel x_1 \parallel x_3) = f(1 \parallel x_1^{'} \parallel x_3)$ and P_2^1 is a random permutation, we have:

$x_1^{'} = x_1 \oplus a$, where period $a = P_1^1(\alpha) \oplus P_1^1(\beta)$.

A similar proof for the cases where $b = 1$, $b^{'} = 1$ and $b = 1, b^{'} = 0$.
Sufficient condition proof. Let $b = 1, b^{'} = 0$, then:

$$f(1 \parallel x_1^{'} \parallel x_3) = W(x_1^{'} \parallel \beta \parallel x_3) \oplus \alpha = P_3^1(P_2^1(P_1^1(\beta) \oplus x_1^{'}) \oplus x_3) \oplus P_1^2(x_3) \oplus \beta \oplus \alpha = P_3^1(P_2^1(P_1^1(\beta) \oplus x_1 \oplus P_1^1(\alpha) \oplus P_1^1(\beta)) \oplus x_3) \oplus P_1^2(x_3) \oplus \beta \oplus \alpha = f(0 \parallel x_1 \parallel x_3).$$

A similar proof for the case where $b = 0$, $b^{'} = 1$. ■

Let us consider the Type III GFS where the plaintext is divided into four parts at the entrance to the encryption scheme and trace the outputs of each of the four rounds. We suppose that the input message to this scheme is a $4n$-bit vector:

$$x = x_1 \parallel x_2 \parallel x_3 \parallel x_4, \text{ where } x_1, x_2, x_3, x_4 \in \{0,1\}^n.$$

Permutation functions, as in the previous case, we denote as P_i^j, where i is the number of the round, j is the number of the permutation function in the round. The second block y_2 in the fourth round equals

$$W(x) = W(x_1 \parallel x_2 \parallel x_3 \parallel x_4) = P_4^1(P_3^1(P_2^1(P_1^1(x_2) \oplus x_1) \oplus x_4) \oplus P_1^3(x_4) \oplus x_3) \oplus P_2^3(P_1^3(x_4) \oplus x_3) \oplus P_1^2(x_3) \oplus x_2.$$

Let us redefine the function f. Now it takes a vector from the set of $(3n+1)$-bit vectors and returns a vector from the set of n-bit vectors. The function f works as follows (α and β are n-bit arbitrary constants, x_3, x_4 are fixed):

$$f(b \parallel x_1 \parallel x_3 \parallel x_4) = \begin{cases} \text{if } b = 0: \\ W(x_1 \parallel \alpha \parallel x_3 \parallel x_4) \oplus \beta, \\ \text{if } b = 1: \\ W(x_1 \parallel \beta \parallel x_3 \parallel x_4) \oplus \alpha. \end{cases}$$

Lemma 3. *The ciphertext in the fourth round of the Type III Generalized Feistel Scheme where the plaintext is divided into four parts is not a random permutation in the quantum adversary model [10].*

Proof. Show that $f(b \parallel x_1 \parallel x_3 \parallel x_4) = f(b \parallel x_1^{'} \parallel x_3 \parallel x_4)$ if and only if $b^{'} = b \oplus 1$ and $x_1^{'} = x_1 \oplus a$, where $a = P_1^1(\alpha) \oplus P_1^1(\beta)$. Since x_3 and x_4 are fixed, then for convenience we denote $K = P_1^3(x_4) \oplus x_3$.
Necessary condition proof. Let $b = b^{'} = 0$, then:

$$f(0 \parallel x_1 \parallel x_3 \parallel x_4) = W(x_1 \parallel \alpha \parallel x_3 \parallel x_4) \oplus \beta = P_4^1(P_3^1(P_2^1(P_1^1(\alpha) \oplus x_1) \oplus x_4) \oplus K) \oplus P_2^3(K) \oplus P_1^2(x_3) \oplus \alpha \oplus \beta,$$

$$f(0 \parallel x_1^{'} \parallel x_3 \parallel x_4) = W(x_1^{'} \parallel \alpha \parallel x_3 \parallel x_4) \oplus \beta = P_4^1(P_3^1(P_2^1(P_1^1(\alpha) \oplus x_1^{'}) \oplus x_4) \oplus K) \oplus P_2^3(K) \oplus P_1^2(x_3) \oplus \alpha \oplus \beta.$$

Since $f(0 \parallel x_1 \parallel x_3 \parallel x_4) = f(0 \parallel x_1^{'} \parallel x_3 \parallel x_4)$ and P_2^1 is a random permutation, we have:

$$x_1 = x_1^{'} \text{ and } b \parallel x_1 \parallel x_3 \parallel x_4 = b^{'} \parallel x_1^{'} \parallel x_3 \parallel x_4.$$

If $b = 0$, $b^{'} = 1$, then:

$$f(1 \parallel x_1^{'} \parallel x_3 \parallel x_4) = W(x_1^{'} \parallel \beta \parallel x_3 \parallel x_4) \oplus \alpha = P_4^1(P_3^1(P_2^1(P_1^1(\beta) \oplus x_1^{'}) \oplus x_4) \oplus K) \oplus P_2^3(K) \oplus P_1^2(x_3) \oplus \beta \oplus \alpha.$$

Since $f(0 \parallel x_1) = f(1 \parallel x_1^{'})$ and P_2^1 is a random permutation, we have

$x_1^{'} = x_1 \oplus a$, where period $a = P_1^1(\alpha) \oplus P_1^1(\beta)$.

A similar proof for the cases where $b = 1$, $b^{'} = 1$ and $b = 1$, $b^{'} = 0$.
Sufficient condition proof. Let $b = 1, b^{'} = 0$, then:

$$f(0 \parallel x_1^{'} \parallel x_3 \parallel x_4) = W(x_1^{'} \parallel \alpha \parallel x_3 \parallel x_4) \oplus \beta = P_4^1(P_3^1(P_2^1(P_1^1(\alpha) \oplus x_1^{'}) \oplus x_4) \oplus K) \oplus P_2^3(K) \oplus P_1^2(x_3) \oplus \alpha \oplus \beta = P_4^1(P_3^1(P_2^1(P_1^1(\alpha) \oplus x_1 \oplus P_1^1(\alpha) \oplus P_1^1(\beta)) \oplus x_4) \oplus K) \oplus P_2^3(K) \oplus P_1^2(x_3) \oplus \alpha \oplus \beta = f(1 \parallel x_1 \parallel x_3 \parallel x_4).$$

A similar proof for the case where $b = 0$, $b^{'} = 1$. ■

Corollary 1. *From Lemmas 1 and 2, it becomes clear that the d-round Type III GFS where the plaintext is divided into d parts is not resistant to attacks of distinguishing a random text from the ciphertext [10].*

2.2. Cracking $d + 1$ rounds of the Type III GFS

However, in 2022, Zhang, Wu, Sui, and Wang discovered a polynomial time quantum attack on $d + 1$ rounds of a Type III GFS.

They analyzed the scheme depicted in Fig. 3, where α and β are arbitrary n-bit constants, and $x_2^1, ..., x_{d-1}^1 \in \{0,1\}^n$ are fixed. They defined an n-bit function f using $E_i(\cdot)$ to represent the result of the i-th round in Type III GFS:

$$f^{E_{d+1}}(x) = x_d^{d+2} \oplus x_d^{\prime d+2},$$

where E_{d+1} is a quantum oracle that provides outputs of $E_{d+1}(\alpha, x_2^1, ..., x_{d-1}^1, x)$ and $E_{d+1}(\beta, x_2^1, ..., x_{d-1}^1, x)$.

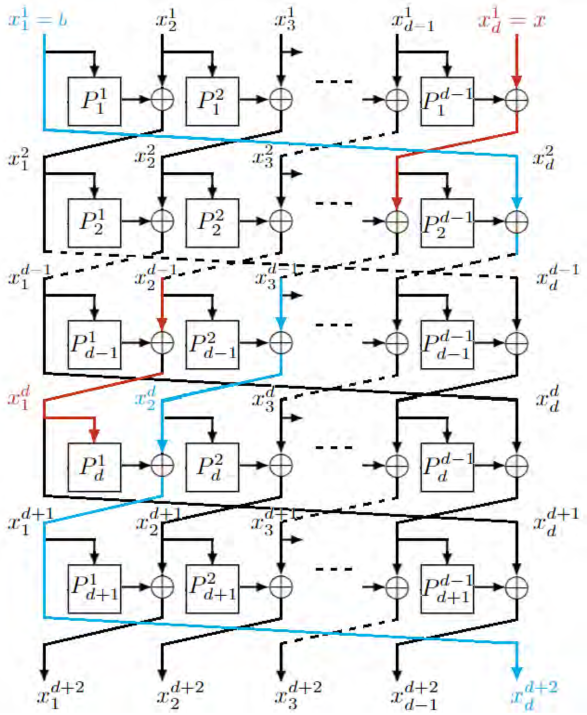

Figure 3: (d+1)-round distinguisher on Type III GFS

Lemma 4. *Let E_{d+1} is a quantum oracle, then for any n-bit x, we can get*

$$f^{E_{d+1}}(x) = f^{E_{d+1}}(x \oplus s), \textit{ where}$$

$$s = P_{d-1}^1(F_{d-1}^1(\alpha, x_2^1, ..., x_{d-1}^1)) \oplus$$
$$P_{d-1}^1(F_{d-1}^1(\beta, x_2^1, ..., x_{d-1}^1)) \textit{ is a period of } f^{E_{d+1}},$$
F_{d-1}^1 is a fixed function [12].

Proof. Let us examine the output value of the first $(d-1)$ rounds $(b \in \{\alpha, \beta\})$:

$$(x_1^d, x_2^d, ..., x_{d-1}^d, x_d^d) = E_{d-1}(b, x_2^1, ..., x_{d-1}^1, x).$$

Using the equations below, we can obtain x_1^d and x_2^d since b has shifted to the second position from the left:

$$x_1^d = P_{d-1}^1(x_1^{d-1}) \oplus x_2^{d-1},$$
$$x_1^{d-1} = P_{d-2}^1(x_1^{d-2}) \oplus x_2^{d-2},$$
$$x_2^{d-1} = P_{d-2}^2(x_2^{d-2}) \oplus x_3^{d-2},$$
$$...$$
$$x_1^2 = P_1^1(b) \oplus x_2^1,$$
$$...$$
$$x_{d-2}^2 = P_1^{d-2}(x_{d-2}^1) \oplus x_{d-1}^1,$$
$$x_{d-1}^2 = P_1^{d-1}(x_{d-1}^1) \oplus x,$$

and

$$x_2^d = P_{d-1}^2(x_2^{d-1}) \oplus x_3^{d-1},$$
$$x_2^{d-1} = P_{d-2}^2(x_2^{d-2}) \oplus x_3^{d-2},$$
$$x_3^{d-1} = P_{d-2}^3(x_3^{d-2}) \oplus x_4^{d-2},$$
$$...$$
$$x_2^3 = P_2^2(x_2^2) \oplus x_3^2,$$
$$...$$
$$x_{d-2}^3 = P_2^{d-2}(x_{d-2}^2) \oplus x_{d-1}^2,$$
$$x_{d-1}^3 = P_2^{d-1}(x_{d-1}^2) \oplus b,$$
$$x_2^2 = P_1^2(x_2^1) \oplus x_3^1,$$
$$...$$
$$x_{d-2}^2 = P_1^{d-2}(x_{d-2}^1) \oplus x_{d-1}^1,$$
$$x_{d-1}^2 = P_1^{d-1}(x_{d-1}^1) \oplus x.$$

Substituting the equations into each other, we can get

$$x_1^d = x \oplus P_1^{d-1}(x_{d-1}^1) \oplus$$
$$P_2^{d-2}(F_2^{d-2}(x_{d-2}^1, x_{d-1}^1)) \oplus$$
$$P_{d-2}^2(F_{d-2}^2(x_2^1, x_{d-1}^1)) \oplus$$
$$...$$
$$\oplus P_{d-1}^1(F_{d-1}^1(b, x_2^1, ..., x_{d-1}^1))$$

and

$$x_2^d = b \oplus P_2^{d-1}(F_2^{d-1}(x_{d-1}^1, x)) \oplus$$
$$...$$
$$\oplus P_{d-1}^2(F_{d-1}^2(x_2^1, ..., x_{d-1}^1, x)),$$

where $F_2^{d-2}, ..., F_{d-1}^1$, and $F_2^{d-1}, ..., F_{d-1}^2$ are fixed functions that output n-bit values.

Denoting

$$\Gamma_b = P_1^{d-1}(x_{d-1}^1) \oplus P_2^{d-2}(F_2^{d-2}(x_{d-2}^1, x_{d-1}^1))$$
$$\oplus ... \oplus P_{d-2}^2(F_{d-2}^2(x_2^1, ..., x_{d-1}^1)) \oplus$$
$$P_{d-1}^1(F_{d-1}^1(b, x_2^1, ..., x_{d-1}^1))$$

and

$$\Lambda_x = P_2^{d-1}(F_2^{d-1}(x_{d-1}^1, x)) \oplus ... \oplus$$
$$P_{d-1}^2(F_{d-1}^2(x_2^1, ..., x_{d-1}^1, x)),$$

we can say that $x_1^d = x \oplus \Gamma_b$ and $x_2^d = b \oplus \Lambda_x$. As $x_2^1, ..., x_{d-1}^1$ are arbitrary n-bit constants, Γ_b and Λ_x are functions of b and x respectively, we have

$$x_d^{d+2} = x_1^{d+1} = b \oplus \Lambda_x \oplus P_d^1(x \oplus \Gamma_b),$$

and, as a result, we get

$$f^{E_{d+1}}(x) = x_d^{d+2} \oplus x_d^{\prime d+2} = \\ \alpha \oplus \beta \oplus P_d^1(x \oplus \Gamma_\alpha) \oplus P_d^1(x \oplus \Gamma_\beta)$$

that means that $f^{E_{d+1}}(x \oplus \Gamma_\alpha \oplus \Gamma_\beta) = f^{E_{d+1}}(x)$, where the period of derived function is

$$s = \Gamma_\alpha \oplus \Gamma_\beta = P_{d-1}^1(F_{d-1}^1(\alpha, x_2^1, ..., x_{d-1}^1)) \oplus \\ P_{d-1}^1(F_{d-1}^1(\beta, x_2^1, ..., x_{d-1}^1)).$$

■

Conclusions

In this paper, we delve into the vulnerability assessment of the Type III Generalized Feistel Scheme (GFS) within the context of the quantum adversary model. Our investigation employs a multifaceted approach to ascertain the susceptibility of this cryptographic scheme. To successfully distinguish a random text from the ciphertext on $d+1$ rounds of the Type III GFS it is sufficient that the plaintext at the entrance to the encryption scheme is divided into d parts.

Open discussion: a more meticulous analysis of the parts of the plaintext inputs may potentially break more than $d+1$ encryption rounds in a reasonable time. The ramifications extend beyond the Type III GFS, raising concerns about the security of other cipher types, therefore, we may crack more rounds of Type I and Type II GFS, leading to improved attacks on Type I ciphers such as CAST-256 and MAME, as well as Type II ciphers like RC6 and CLEFIA.

References

[1] D. Simon, “On the power of quantum computation,” in Proceedings 35th Annual Symposium on Foundations of Computer Science, Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994.

[2] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96, ACM Press, 1996.

[3] H. Kuwakado and M. Morii, “Quantum distinguisher between the 3-round feistel cipher and the random permutation,” in 2010 IEEE International Symposium on Information Theory, IEEE, 2010.

[4] X. Dong, Z. Li, and X. Wang, “Quantum cryptanalysis on some generalized feistel schemes,” Science China Information Sciences, vol. 62, no. 2, 2019.

[5] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, “Breaking symmetric cryptosystems using quantum period finding,” in Advances in Cryptology – CRYPTO 2016, pp. 207–237, Springer Berlin Heidelberg, 2016.

[6] G. Leander and A. May, “Grover meets simon – quantumly attacking the FX-construction,” in Advances in Cryptology – ASIACRYPT 2017, pp. 161–178, Springer International Publishing, 2017.

[7] X. Dong and X. Wang, “Quantum key-recovery attack on feistel structures,” Science China Information Sciences, vol. 61, no. 10, 2018.

[8] 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.

[9] J. Cui, J. Guo, and S. Ding, “Applications of simon’s algorithm in quantum attacks on feistel variants,” Quantum Information Processing, vol. 20, no. 3, 2021.

[10] A. Zvychaina, “Cryptoanalysis of the lightweight symmetric block cipher «cypress»,” bachelor thesis : 113 Applied mathematics. – Kyiv, 2021. – 92 pp., 2021.

[11] S. Hodžić, L. Knudsen, R., and B. Kidmose, A., “On quantum distinguishers for type-3 generalized feistel network based on separability,” in Post-Quantum Cryptography, pp. 461–480, Springer International Publishing, 2020.

[12] Z. Zhang, W. Wu, H. Sui, and B. Wang, “Quantum attacks on type-3 generalized feistel scheme and unbalanced feistel scheme with expanding functions,” Chinese Journal of Electronics, vol. 32, no. 2, pp. 209–216, 2023.