



Quantum Cryptanalysis of 5 Rounds Feistel Schemes and Benes Schemes

Maya Chartouny, Jacques Patarin, Ambre Toulemonde

► To cite this version:

Maya Chartouny, Jacques Patarin, Ambre Toulemonde. Quantum Cryptanalysis of 5 Rounds Feistel Schemes and Benes Schemes. 4th International Conference on Codes, Cryptology and Information Security, C2SI 2023, May 2023, Rabat, Morocco. 10.1007/978-3-031-33017-9_13 . hal-04268886

HAL Id: hal-04268886

<https://hal.science/hal-04268886>

Submitted on 3 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Quantum Cryptanalysis of 5 rounds Feistel schemes and Benes schemes

Maya Chartouny^{1,2}, Jacques Patarin^{1,2}, and Ambre Toulemonde²

¹ Thales DIS, Meudon, France

{maya.saab-chartouni, jacques.patarin}@thalesgroup.com

² Université de Versailles Saint-Quentin-en-Yvelines, Versailles, France
ambre.toulemonde@orange.fr

Abstract. In this paper, we provide new quantum cryptanalysis results on 5 rounds (balanced) Feistel schemes and on Benes schemes. More precisely, we give an attack on 5 rounds Feistel schemes in $\Theta(2^{2n/3})$ quantum complexity and an attack on Benes schemes in $\Theta(2^{2n/3})$ quantum complexity, where n is the number of bits of the internal random functions.

Keywords: Feistel ciphers · Pseudo-random permutation · Quantum cryptanalysis · Luby–Rackoff block cipher · Benes network

1 Introduction

There exist several methods to build pseudo-random permutations and pseudo-random functions.

A random Feistel cipher also known as Luby–Rackoff block cipher is a symmetric structure used in the construction of block ciphers. The benefit of the Feistel network is that the same structure can be used for encryption and decryption, and both consist of iteratively running a function called a “round function” a fixed number of times. The most studied way to build pseudo-random permutations from random functions or random permutations is the r -round Feistel construction. The Feistel construction is important from a practical point of view since it is used to develop many block ciphers such as DES [2], 3DES [2] and Simon [7]. We study generic attacks on Feistel schemes where we assume that the internal round functions f_1, \dots, f_r are randomly chosen.

The plaintext message of a Feistel scheme is denoted by $[L, R]$ that stands for *Left* and *Right*, and the ciphertext message after applying r rounds is denoted by $[S, T]$. The first round of a Feistel scheme takes as input $[L, R]$ and it outputs $[R, L \oplus f(R)]$ with f a secret function from n bits to n bits.

A Benes scheme is a composition of two schemes called “Butterflies”. It allows to construct, from random functions from n bits to n bits, a pseudorandom function from $2n$ bits to $2n$ bits. For many cryptographic primitives, e.g., hashing and pseudorandom functions, doubling the output length is useful even if the doubling transformation is not reversible.

The plaintext message of a Benes scheme is denoted by $[L, R]$ that stands for *Left* and *Right*, and the ciphertext message is denoted by $[S, T]$.

Our Contribution. In this paper, we describe a non-adaptive quantum chosen plaintext attack (QCPA) against 5-round balanced Feistel schemes. This attack allows to distinguish Feistel network from random permutations with quantum complexity of $\mathcal{O}(2^{2n/3})$ instead of 2^n for the best known attack (before our attack). We also describe a QCPA against the Benes schemes. This attack allows to distinguish a Benes scheme from random functions with quantum complexity of $\mathcal{O}(2^{2n/3})$ instead of 2^n for the best known attack (before our attack).

Organization. Section 2 recalls the Feistel and Benes schemes. Section 3 gives an overview of previous works and the new results provided in this paper. Section 4 recall Zhandry's quantum algorithm. Finally, in Section 5 and Section 6, we present our QCPA against the Feistel schemes with 5 rounds and our QCPA against the Benes schemes.

2 Feistel and Benes constructions

In this section, we recall the definition of a classical (aka balanced) Feistel scheme and the definition of a Benes scheme. Let $\mathcal{F}_{m,n}$ be the set of all functions from $\{0,1\}^m$ to $\{0,1\}^n$. When $m = n$, the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$ will be denoted by \mathcal{F}_n .

2.1 Feistel scheme

First round Feistel scheme. Let $f \in \mathcal{F}_n$. The first round balanced Feistel scheme associated with f , denoted by $\Psi(f)$, is the function in \mathcal{F}_{2n} defined by:

$$\forall (L, R) \in (\{0,1\}^n)^2, \Psi(f)([L, R]) = [S, T] \iff \begin{cases} S = R, \\ T = L \oplus f(R). \end{cases}$$

For any function f , $\Psi(f)$ is a permutation of $\{0,1\}^{2n}$.

The figure of the Feistel scheme for the first round is given in Figure 1.

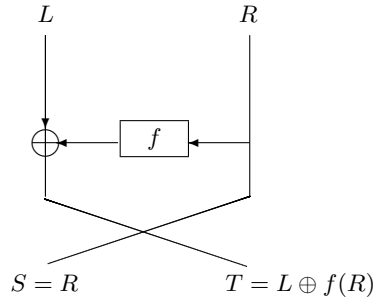


Fig. 1: First round of Feistel scheme

r –round Feistel scheme. Let f_1, f_2, \dots, f_r be r functions in \mathcal{F}_n . The r –round balanced Feistel network associated with f_1, \dots, f_r , denoted by $\Psi^r(f_1, \dots, f_r)$, is the function in \mathcal{F}_{2n} defined by:

$$\Psi^r(f_1, \dots, f_r) = \Psi^r(f_r) \circ \dots \circ \Psi^1(f_1).$$

5–round Feistel scheme. We describe now in detail the equations of the Feistel network for the first five rounds.

$$\begin{aligned} \text{1 round: } & \begin{cases} S = R \\ T = L \oplus f_1(R) = X^1 \end{cases} & \text{4 rounds: } & \begin{cases} S = X^3 \\ T = X^2 \oplus f_4(X^3) = X^4 \end{cases} \\ \text{2 rounds: } & \begin{cases} S = X^1 \\ T = R \oplus f_2(X^1) = X^2 \end{cases} & \text{5 rounds: } & \begin{cases} S = X^4 \\ T = X^3 \oplus f_5(X^4) = X^5 \end{cases} \\ \text{3 rounds: } & \begin{cases} S = X^2 \\ T = X^1 \oplus f_3(X^2) = X^3 \end{cases} \end{aligned}$$

2.2 Benes scheme

To give a definition of the Benes transformation, we need to recall first the definition of a butterfly transformation.

Butterfly transformation. Let f_1, \dots, f_4 be four functions in \mathcal{F}_n . A Butterfly transformation is the function in \mathcal{F}_{2n} which takes as input $(L_i, R_i) \in (\{0, 1\}^n)^2$ and gives as output (X_i, Y_i) where,

$$\begin{cases} X_i = f_1(L_i) \oplus f_2(R_i), \\ Y_i = f_3(L_i) \oplus f_4(R_i). \end{cases}$$

The figure of the Butterfly scheme is given in Figure 2.

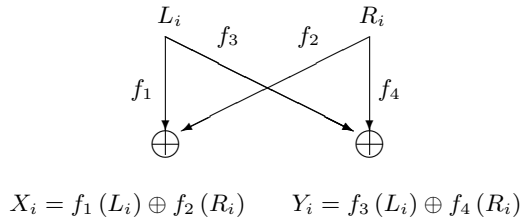


Fig. 2: Butterfly scheme

Benes transformation. Let f_1, \dots, f_8 be functions in \mathcal{F}_n . A Benes transformation (back to back Butterfly) is the function in \mathcal{F}_{2n} which takes as input $(L_i, R_i) \in (\{0, 1\}^n)^2$ and gives as output (S_i, T_i) where,

$$\begin{cases} S_i = f_5(\underbrace{f_1(L_i) \oplus f_2(R_i)}_{X_i}) \oplus f_6(\underbrace{f_3(L_i) \oplus f_4(R_i)}_{Y_i}) = f_5(X_i) \oplus f_6(Y_i), \\ T_i = f_7(f_1(L_i) \oplus f_2(R_i)) \oplus f_8(f_3(L_i) \oplus f_4(R_i)) = f_7(X_i) \oplus f_8(Y_i). \end{cases}$$

The figure of the Benes scheme is given in Figure 3.

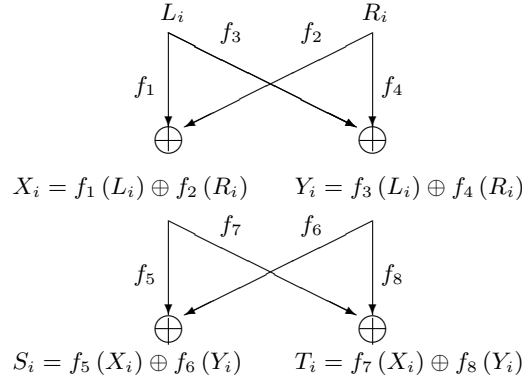


Fig. 3: Benes scheme

3 Overview of cryptanalysis on Feistel schemes

In this section, we review the best known cryptanalysis results of the state of the art on the Feistel schemes and we point out the new results of this paper. Note that before, the attacks used against the Feistel schemes gave a polynomial complexity instead of exponential thanks to Simon's algorithm [7]. Whereas now, our attack remains exponential but we are able to gain a round.

In Figure 4, we summarize the cryptanalysis results on few rounds of Feistel schemes based on the distinguishing attacks presented in [3] and in [5] together with our new contributions.

We have not found a better attack for QCCA (quantum chosen ciphertext attack) than the one of the QCPA. Notice that any QCPA can be transformed into a QCCA.

4 Quantum Collision

In this section, we recall the results of the quantum algorithm that we use in our quantum cryptanalysis. The full details on how the algorithm works can be found in [1] and in [8].

| | KPA | CPA | CCA | QCPA | QCCA |
|----------|------------|-----------|-----------|----------------------------------|----------------------------------|
| Ψ^1 | 1 | 1 | 1 | 1 | 1 |
| Ψ^2 | $2^{n/2}$ | 2 | 2 | 2 | 2 |
| Ψ^3 | $2^{n/2}$ | $2^{n/2}$ | 3 | n | 3 |
| Ψ^4 | 2^n | $2^{n/2}$ | $2^{n/2}$ | $2^{n/2}$ | n |
| Ψ^5 | $2^{3n/2}$ | 2^n | 2^n | This paper: $2^{2n/3}$ | This paper: $2^{2n/3}$ |
| Ψ^6 | 2^{2n} | 2^{2n} | 2^{2n} | 2^{2n} | 2^{2n} |

Fig. 4: Number of computations to distinguish Feistel schemes (with 1, 2, 3, 4, 5 and 6 rounds) from random permutations (best known attacks)

Theorem 1. Let f be a random function with domain size M and codomain size N . Assume $M = \Omega(N^{1/2})$. Then the quantum query complexity of finding a collision with constant probability is $\Theta(N^{1/3})$.

Note that if $M = o(N^{1/2})$ then there are no collisions with probability approaching 1, so the collision problem becomes meaningless. Thus, Theorem 1 completely characterizes the quantum query complexity of the collision problem for all sensible parameters.

5 Quantum cryptanalysis on Feistel network

In this section, we first describe a non quantum attack that distinguishes a 5-round Feistel scheme from a $2n$ bits random function with a complexity of 2^n presented in [5]. Then, we describe our quantum chosen plaintext attack that distinguishes a 5-round Feistel scheme from a $2n$ bits random function with a complexity of $2^{2n/3}$.

Classical attack. We can choose messages $[L_i, R_i]$ and $[L_j, R_j]$ such that $R_i = R_j$, $\forall i, j$. Then, we can check whether S_i is equal to S_j and $L_i \oplus L_j$ is equal to $T_i \oplus T_j$, i.e., we count the number of (i, j) such that:

$$\begin{cases} S_i = S_j, \\ L_i \oplus L_j = T_i \oplus T_j. \end{cases}$$

For a 5-round Feistel scheme, we have two times more such collision than for truly random permutations. Indeed, for a truly random permutation if $R_i = R_j$, the numbers of (i, j) , $1 \leq i < j \leq m$, where $m \simeq 2^n$, such that $S_i = S_j$ and $T_i \oplus T_j = L_i \oplus L_j$ is approximately $\frac{m(m-1)}{2} \frac{1}{2^{2n}}$.

However, for a 5-round Feistel scheme we have:

$$\begin{cases} T_i = L_i \oplus f_1(R_i) \oplus f_3(R_i \oplus f_2(L_i \oplus f_1(R_i))) \oplus f_5(S_i), \\ T_j = L_j \oplus f_1(R_j) \oplus f_3(R_j \oplus f_2(L_j \oplus f_1(R_j))) \oplus f_5(S_j). \end{cases}$$

Let us suppose that $R_i = R_j$ and $S_i = S_j$, hence, $T_i \oplus T_j = L_i \oplus L_j$ is equivalent to

$$f_3(R_i \oplus f_2(L_i \oplus f_1(R_i))) = f_3(R_j \oplus f_2(L_j \oplus f_1(R_j))),$$

which can occur either if $f_2(L_i \oplus f_1(R_i)) = f_2(L_j \oplus f_1(R_j))$ with an approximate probability of $\frac{1}{2^n}$ or if these values are distinct but when Xored with R , they have the same images by f_3 with an approximate probability of $\frac{1}{2^n}$.

Hence, $\forall(i, j), i < j$, the probability that $S_i = S_j$ and $T_i \oplus T_j = L_i \oplus L_j$ when $R_i = R_j$ is approximately $\frac{m(m-1)}{2} \frac{2}{2^{2n}}$.

Thus we have two times more such collision for a 5-round Feistel scheme compared to a truly random permutation. This has also been demonstrated with the H-coefficient technique in [4].

Therefore, we search for collision of the form of $S_i || L_i \oplus T_i$ and the complexity is in 2^n from the birthday paradox. For more details see [5].

Note that there are several attacks on Ψ_5 with the same complexity but we choose this one to be able to detect collisions in quantum.

Quantum attack. In quantum we detect collisions, when they exist, faster than on classical computers. In fact, we use the same attack in quantum to detect these collisions.

We apply Theorem 1 with $M = 2^n$ and $N = 2^{2n}$ ($M = \Omega(N^{1/2})$). Hence, the quantum complexity to detect such a collision is in $N^{1/3} = 2^{2n/3}$ (unlike 2^n as seen before). Therefore, we can distinguish 5-round Feistel schemes from truly random permutations with a quantum complexity of $2^{2n/3}$.

6 Quantum distinguishing attack on Benes scheme

In this section, we first describe a non quantum attack that distinguishes a Benes scheme from a random function with a complexity of 2^n presented in [6]. Then, we describe a quantum chosen plaintext attack that distinguishes a Benes scheme from a random function with a complexity of $2^{2n/3}$.

Classical attack. We can choose messages $[L_i, R_i]$, then, we check whether S_i is equal to S_j and T_i is equal to T_j .

For a truly random permutation, the numbers $(i, j), 1 \leq i < j \leq m$ such that $S_i = S_j$ and $T_i = T_j$ is approximately $\frac{m(m-1)}{2} \frac{1}{2^{2n}}$.

However, for Benes scheme we have

$$\begin{cases} S_i = f_5(X_i) \oplus f_6(Y_i), \\ T_i = f_7(X_i) \oplus f_8(Y_i). \end{cases}$$

Hence, $S_i = S_j$ and $T_i = T_j$ is equivalent to $f_5(X_i) \oplus f_6(Y_i) = f_5(X_j) \oplus f_6(Y_j)$ and $f_7(X_i) \oplus f_8(Y_i) = f_7(X_j) \oplus f_8(Y_j)$. This can occur either if $X_i = X_j$ and $Y_i = Y_j$ or if these values are distinct but $S_i = S_j$ and $T_i = T_j$.

Thus, $\forall(i, j)$, $i < j$, the probability that $S_i = S_j$ and $T_i = T_j$ is approximately $\frac{m(m-1)}{2} \frac{2}{2^{2n}}$ so we have two times more such collision for a Benes scheme compared to a random function. More details can be found in [6].

The number of computations needed for this attack is about 2^n from the birthday paradox.

Quantum attack. We use the same attack in quantum to detect these collisions faster.

We apply Theorem 1 with $M = 2^{2n}$ and $N = 2^{2n}$ ($M = \Omega(N^{1/2})$). Hence, the quantum complexity to detect such a collision is in $N^{1/3} = 2^{2n/3}$ (unlike 2^n as seen before). Therefore, we can distinguish Benes schemes from truly random functions with a quantum complexity of $2^{2n/3}$.

References

1. Ambainis, A.: Quantum walk algorithm for element distinctness. In: 45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings. pp. 22–31. IEEE Computer Society (2004)
2. IBM: Data encryption standard. Federal Information Processing Standards Publication (1999)
3. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round feistel cipher and the random permutation. 2010 IEEE International Symposium on Information Theory pp. 2682–2685 (2010)
4. Patarin, J.: Etude des generateurs de permutations pseudo-aleatoires bases sur le schema du d. E. S. Ph.D. thesis (1991), <http://www.theses.fr/1991PA066601>
5. Patarin, J.: Generic attacks on feistel schemes. IACR Cryptol. ePrint Arch. p. 36 (2008)
6. Patarin, J., Montreuil, A.: Benes and butterfly schemes revisited. In: Won, D., Kim, S. (eds.) Information Security and Cryptology - ICISC 2005, 8th International Conference, Seoul, Korea, December 1-2, 2005, Revised Selected Papers. Lecture Notes in Computer Science, vol. 3935, pp. 92–116. Springer (2005)
7. Simon, D.R.: On the Power of Quantum Computation. SIAM J. Comput. **26**(5), 1474–1483 (1997)
8. Zhandry, M.: A note on the quantum collision and set equality problems. CoRR **abs/1312.1027** (2013)