Chapter 2
Balanced Feistel Ciphers, First Properties

Abstract Feistel ciphers are named after Horst Feistel who studied these schemes in the 1960s. In this chapter, we will only present classical Feistel ciphers, i.e. balanced Feistel ciphers with the $\oplus$ group law (Xor). In Chaps. 8, 9 and 10, we will see that there are many variants of these ciphers.

2.1 Introduction

2.2 Definition of Classical Feistel Ciphers

Classical Feistel ciphers are also known as *balanced* Feistel ciphers. We start with the definition of the 1-round Feistel transformation.

Definition 2.1. Let $f \in \mathscr{F}_n$. The *1-round balanced Feistel network* associated with f, denoted $\Psi(f)$, is the function from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$ defined by (see also Fig. 2.1):

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

It is quite easy to see that for any function f, $\Psi(f)$ is actually a permutation of $\{0,1\}^{2n}$, as we show in the following proposition. Recall that σ denotes the permutation of $\{0,1\}^{2n}$ that swaps the two n-bit halves of its argument.

Proposition 2.1. *For any function $f \in \mathscr{F}_n$, $\Psi(f)$ is a permutation of $\{0,1\}^{2n}$ and its inverse is $\Psi(f)^{-1} = \sigma \circ \Psi(f) \circ \sigma$.*

Proof.

$$\Psi(f)([L,R]) = [S,T] \iff \begin{cases} S = R \\ T = L \oplus f(R). \end{cases}$$

V. Nachef et al., *Feistel Ciphers*, DOI 10.1007/978-3-319-49530-9_2

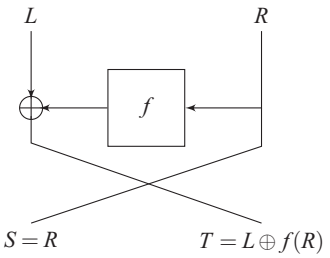

Fig. 2.1 The basic (1-round) balanced Feistel network associated with round function f

Therefore, for all $[S, T]$ we have exactly one solution $[L, R]$ and $\Psi(f)$ is a permutation of $\{0,1\}^{2n}$. Moreover, its inverse is given by

$$\begin{aligned}\Psi(f)^{-1}[S,T] &= [T \oplus f(S), S] \\ &= \sigma([S, T \oplus f(S)]) \\ &= \sigma(\Psi(f)([T,S])) \\ &= \sigma(\Psi(f)(\sigma([S,T]))),\end{aligned}$$

hence the result. □

Before going further in the description of Feistel ciphers, we will make comments on this first round. Notice that $\Psi(f_1)$ is always a permutation even though f_1 is not bijective. This is an important property of Feistel ciphers. In contrast, in some other ciphers like AES for example, designers manage to have bijective transformations. Here the choice for f_1 is much larger since we do not have to take into account the bijective feature of f_1. However, clearly one round of a Feistel cipher is not enough to obtain a pseudo-random permutation: indeed the left-hand part of the output is exactly the right-hand part of the input. It was not encrypted at all. However, if we compose several bijections, we still get a bijection. This is what we are going to do below. Thus even though one round of a Feistel cipher is not good to hide the inputs, this will not be the case anymore after several rounds as we will see. An architect who builds a tower with one floor that collapses will not consider the possibility of constructing a tower by adding several floors of the same kind and hope that the tower will be solid. However, this is what we will do, but this construction will be justified by the security results we will obtain. Cryptography with bijections does not behave like the architecture of towers!

Definition 2.2. Let $r \geq 1$ and let $f_1, f_2, \ldots, f_r$ be r functions in $\mathscr{F}_n$. The *r-round balanced Feistel network* associated with $f_1, \ldots, f_r$, denoted $\Psi^r(f_1, \ldots, f_r)$, is the function from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$ defined by (see also Fig. 2.2)

$$\Psi^r(f_1, \ldots, f_r) = \Psi(f_r) \circ \cdots \circ \Psi(f_2) \circ \Psi(f_1).$$

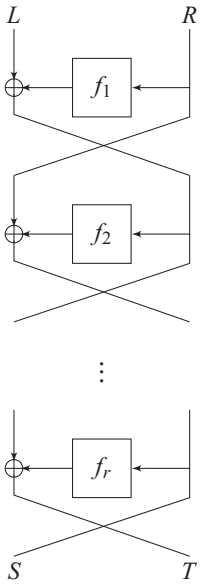

Fig. 2.2 The r-round balanced Feistel network associated with round functions $f_1, \ldots, f_r$

Theorem 2.1. *For any functions* $f_1, \ldots, f_r \in \mathscr{F}_n$, $\Psi^r(f_1, \ldots, f_r)$ *is a permutation of* $\{0,1\}^{2n}$ *and*

$$(\Psi^r(f_1, \ldots, f_r))^{-1} = \sigma \circ \Psi^r(f_r, \ldots, f_1) \circ \sigma.$$

Proof. $\Psi^r(f_1, \ldots, f_r)$ is a permutation of $\{0,1\}^{2n}$ since it is the composition of r permutations of $\{0,1\}^{2n}$. Moreover, by Proposition 2.1, and since σ^2 is the identity function, one has

$$\begin{aligned}(\Psi^r(f_1, \ldots, f_r))^{-1} &= (\Psi(f_1))^{-1} \circ \cdots \circ (\Psi(f_r))^{-1} \\ &= \sigma \circ \Psi(f_1) \circ \sigma \circ \cdots \circ \sigma \circ \Psi(f_r) \circ \sigma \\ &= \sigma \circ \Psi(f_1) \circ \cdots \circ \Psi(f_r) \circ \sigma,\end{aligned}$$

from which the result follows. □

Up to the initial and final application of the "swapping" function σ, the inverse of an r-round balanced Feistel network is simply another r-round Feistel network where the round functions $f_1, \ldots, f_r$ are used in the reverse order. Since the computation of σ is very fast, we see that the computation of $\Psi^r(f_1, \ldots, f_r)$ should take about the same time in the forward or backward direction (i.e., when encrypting or decrypting).

Definition 2.3. Let $r \geq 1$. The *r-round Feistel transformation*, denoted Ψ^r, maps a tuple of functions $(f_1, \ldots, f_r) \in (\mathscr{F}_n)^r$ to the permutation $\Psi^r(f_1, \ldots, f_r)$ of $\{0,1\}^{2n}$ as defined by Def. 2.2.

Remark 2.1. Balanced Feistel networks can be defined on any group $(G, *)$, not only $(\{0,1\}^n, \oplus)$.

From Feistel networks, we can finally define Feistel ciphers, by letting round functions depend on secret keys.

Definition 2.4. Let $r \geq 1$ and let $F = (f_K)$ be a family of functions in $\mathscr{F}_n$ indexed by a set $\mathscr{K}$. The *r-round balanced Feistel cipher* associated with F is the block cipher with key space $\mathscr{K}^r$ and message space $\{0,1\}^{2n}$ which maps a key $(K_1, \ldots, K_r) \in \mathscr{K}^r$ and a plaintext $[L, R] \in \{0,1\}^{2n}$ to the ciphertext $\Psi^r(f_{K_1}, \ldots, f_{K_r})([L, R])$. In other words, the permutation of $\{0,1\}^{2n}$ associated with key $(K_1, \ldots, K_r)$ is the Feistel network $\Psi^r(f_{K_1}, \ldots, f_{K_r})$.

2.3 Signature of Balanced Feistel Networks

Theorem 2.2 ([4]). *When $n \geq 2$, the signature of a Feistel permutation is even, i.e.,*

$$\forall f_1, f_2, \ldots, f_r \in \mathscr{F}_n,\ \Psi^r(f_1, \ldots, f_r) \in \mathscr{A}_{2n}.$$

Proof. Let f_1 be a function of F_n. Let $\Psi'(f_1)([L, R]) = [L \oplus f_1(R), R]$. We will show that the signature of both σ and $\Psi'(f_1)$ is even. Since $\Psi(f_1) = \sigma \circ \Psi'(f_1)$, $\Psi(f_1)$ has an even signature as well, and by composition, any Feistel permutations has an even signature.

Consider σ: All its cycles have 1 or 2 elements since $\sigma \circ \sigma$ is the identity. There are exactly 2^n cycles with 1 element since $\sigma([L, R]) = [L, R]$ if and only if $L = R$ (and a cycle with 1 element has an even signature). Hence, there are $(2^{2n} - 2^n)/2$ cycles with 2 elements, which is even for $n \geq 2$.

Consider now $\Psi'(f_1)$: All the cycles have 1 or 2 elements since $\Psi'(f_1) \circ \Psi'(f_1)$ is the identity. Moreover $\Psi'(f_1)([L, R]) = [L, R]$ if and only if $f_1(R) = 0$, so the number of cycles with 2 elements is $k \cdot 2^n/2$, with k being the number of values R such that $f_1(R) \neq 0$. So when $n \geq 2$ the signature of $\Psi'(f_1)$ is even. □

The fact that Feistel ciphers have always an even signature is not in general cryptographic security problem. Indeed, this property has influence only when you know the images of all inputs (except may 2 which can be deduced from the others). Thus this property is mathematically interesting but it has a small cryptographic impact.

2.4 Random Feistel Ciphers

As we have seen, when the functions $f_1, \ldots, f_d$ are randomly and independently chosen in $\mathscr{F}_n$ (or when they are generated from a pseudo-random generator), $\Psi^d(f_1, \ldots, f_d)$ is called a `Random Feistel Cipher`, or a `Luby-Rackoff` construction, since we will see in Chap. 4 some very famous security results on these ciphers proved by Luby and Rackoff [3]. On the contrary, many important Feistel ciphers are designed with functions $f_1, \ldots, f_d$ which are not random or pseudo-random, for example DES variants as we will see in Part III.

From the Luby-Rackoff theorem that we will see in Chap. 4, it is possible to prove that random Feistel ciphers provide a PRPG (Pseudo-random Permutation Generator) from a PRFG (Pseudo-Random Function Generator). Moreover, in cryptography, it is also proved that is possible to generate a PRFG from a PGNG (Pseudo-Random Number Generator) and a PRNG from any one-way function (see Fig. 2.3). However, this is not the topic of this book. The interested reader is referred to [1] and [2]. Since a proof of the existence of a one-way function will provide a proof of the famous theoretical open computer science problem $P \neq NP$, this design of a PRPG is interesting but do not provide the existence of a PRPG. Moreover, Feistel ciphers that are based on functions $f_1, \ldots, f_d$ that are not pseudo-random (like 3DES) are often much more computationally efficient than random Feistel ciphers as constructed in Fig. 2.3.

2.5 Efficient Attacks for One, Two, and Three Rounds

We show that for one, two, and three rounds, balanced Feistel ciphers can be broken very efficiently with a *constant* number of queries, independently of the size parameter n. These attacks are generics, i.e., they work for any round functions.

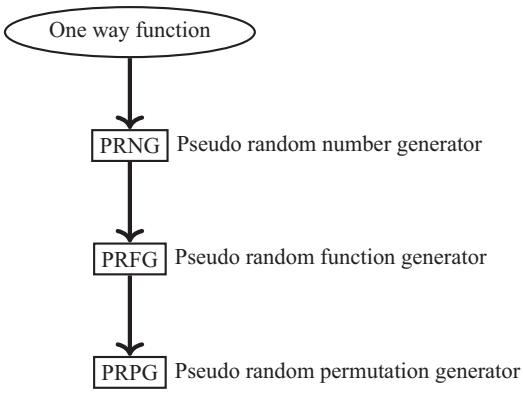

Fig. 2.3 A possible construction of PRPG from any one-way function

2.5.1 KPA for One Round with $q = 1$

Consider the following KPA-distinguisher D:

1. D makes a query to the oracle, and receives a random plaintext $[L, R]$ together with $[S, T] = \mathscr{O}([L, R])$;
2. is $S = R$, D outputs 1, otherwise it outputs 0.

Clearly, when $\mathscr{O} = \Psi^1(f_1)$, D *always* outputs 1 since

$$\Psi^1(f_1)([L, R]) = [S, T] \iff \begin{cases} S = R \\ T = L \oplus f_1(R). \end{cases}$$

On the other hand, when $\mathscr{O}$ is a random permutation of $\{0,1\}^{2n}$, then $[S, T]$ is uniformly random in $\{0,1\}^{2n}$, and the probability that $S = R$ (and hence that D outputs 1) is exactly 2^{-n}. Therefore, by definition of the advantage (cf. Def. 1.3) we have

$$\mathbf{Adv}_{\Psi^1}(\mathsf{D}) = 1 - \frac{1}{2^n}.$$

Since $\mathscr{D}$ makes exactly one query, it follows that

$$\mathbf{Adv}^{\mathrm{KPA}}_{\Psi^1}(D) \geq 1 - \frac{1}{2^n}.$$

Hence, there is a very efficient known-plaintext attack against Ψ^1, making only one query and distinguishing Ψ^1 from a random permutation with probability negligibly close to one.

2.5.2 NCPA for Two Rounds with $q = 2$

Consider the following NCPA-distinguisher D:

1. D chooses $L, L', R \in \{0,1\}^n$, with $L \neq L'$, and queries $[S, T] := \mathscr{O}([L, R])$ and $[S', T'] := \mathscr{O}([L', R])$;
2. D checks whether $S \oplus S' = L \oplus L'$; if this holds, D outputs 1, otherwise D outputs 0.

Note that D chooses L, L', and R *before* making any query to the oracle, hence it is non-adaptive. By definition of Ψ^2, we have

$$\Psi^2(f_1, f_2)([L, R]) = [S, T] \iff \begin{cases} S = L \oplus f_1(R) \\ T = R \oplus f_2(L \oplus f_1(R)). \end{cases}$$

Hence, when $\mathscr{O} = \Psi^2(f_1, f_2)$, one has

$$S \oplus S' = L \oplus f_1(R) \oplus L' \oplus f_1(R) = L \oplus L',$$

so that D always outputs 1.

On the other hand, when $\mathscr{O}$ is a random permutation of $\{0,1\}^{2n}$, then $[S', T']$ is uniformly random in $\{0,1\}^{2n} \setminus \{[S,T]\}$. Since there are exactly 2^n possible values of $[S', T']$ in $\{0,1\}^{2n} \setminus \{[S,T]\}$ such that $S' = S \oplus L \oplus L'$ (because $L \oplus L' \neq 0$), D outputs 1 with probability

$$\frac{2^n}{2^{2n}-1}.$$

Hence, we have, by definition of the advantage,

$$\mathbf{Adv}_{\Psi^2}(\mathsf{D}) = 1 - \frac{2^n}{2^{2n}-1}.$$

Since D makes exactly two queries, this implies

$$\mathbf{Adv}^{\mathrm{NCPA}}_{\Psi^2}(\mathsf{D}) \geq 1 - \frac{2^n}{2^{2n}-1}.$$

Hence, there is a very efficient non-adaptive chosen-plaintext attack against Ψ^2, making only two queries and distinguishing Ψ^2 from a random permutation with probability negligibly close to one.

2.5.3 CCA for Three Rounds with $q = 3$

We consider the following CCA-distinguisher D:

1. D chooses $L, L', R \in \{0,1\}^n$, with $L \neq L'$, and queries $[S,T] := \mathscr{O}([L,R])$ and $[S', T'] := \mathscr{O}([L', R])$;
2. D asks for the value $[L'', R''] := \mathscr{O}^{-1}([S', T' \oplus L \oplus L'])$.
3. D checks if $R'' = S' \oplus S \oplus R$; if this holds, D outputs 1. Otherwise D outputs 0.

If $\mathscr{O}$ is a permutation randomly chosen, the probability that D outputs 1 is $\simeq 1/2^n$.

Now assume that $\mathscr{O} = \Psi^3(f_1, f_2, f_3)$.

Then $\mathscr{O}([L,R]) = [S,T] \Leftrightarrow \begin{cases} S = R \oplus f_2(L \oplus f_1(R)) \\ T = L \oplus f_1(R) \oplus f_3(R \oplus f_2(L \oplus f_1(R)). \end{cases}$

And $\mathscr{O}^{-1}[S,T] = [L,R] \Leftrightarrow \begin{cases} L = T \oplus f_3(S) \oplus f_1(S \oplus f_2(T \oplus f_3(S)))) \\ R = S \oplus f_2(T \oplus f_3(S)) \end{cases}$

Thus $\mathscr{O}^{-1}[S', T' \oplus L \oplus L'] = [L'', R''] \Rightarrow R'' = S' \oplus \underbrace{f_2(\underbrace{T' \oplus L \oplus L' \oplus f_3(S')}_{L \oplus f_1(R)})}_{S \oplus R}$

Therefore $R'' = S' \oplus S \oplus R$.

Thus the probability that D outputs 1 when $\mathscr{O} = \Psi^3(f_1, f_2, f_3)$ is 1 and we obtain that

$$\mathbf{Adv}^{CCA}_{\Psi^3}(\mathsf{D}) \geq 1 - \frac{1}{2^n}.$$

This attack is able to distinguish $\Psi(f_1, f_2, f_3)$ when f_1, f_2, and f_3 are randomly and independently chosen in $\mathscr{F}_n$ from a truly random permutation of $\mathscr{P}_{2n}$ with a high probability when we can choose 2 plaintext/ciphertext pairs and obtain the corresponding ciphertexts, and then choose 1 ciphertext and obtain the plaintext. This attack is a CCA with $q = 3$ plaintext/ciphertext pairs.

This attack can be found as follows. The idea is to create a "circle" in R, S, X, as in Fig. 2.4, where $X_i = L_i \oplus f_1(R_i)$, i.e. to have $R_2 = R_1$, $S_3 = S_2$ and $X_3 = X_1$. We always have:

$$R_i = R_j \Rightarrow L_i \oplus L_j = X_i \oplus X_j \tag{2.1}$$

$$X_i = X_j \Rightarrow R_i \oplus R_j = S_i \oplus S_j \tag{2.2}$$

$$S_i = S_j \Rightarrow X_i \oplus X_j = T_i \oplus T_j \tag{2.3}$$

First, we choose $R_2 = R_1$ and $L_2 \neq L_1$. So from 2.1, we have:

$$X_2 \oplus X_1 = L_1 \oplus L_2 \ . \tag{2.4}$$

Second, we choose $S_3 = S_2$. So from 2.3, we have:

$$X_2 \oplus X_3 = T_2 \oplus T_3 \ . \tag{2.5}$$

So from 2.4 and 2.5 we can impose $X_3 = X_1$ by choosing $T_3 = T_2 \oplus L_1 \oplus L_2$. Then from 2.2 we will have: $R_3 = R_1 \oplus S_1 \oplus S_3$ $(= R_1 \oplus S_1 \oplus S_2)$.

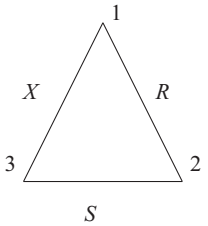

Fig. 2.4 A "circle" in R, S, X (here it looks more as a triangle)

2.6 Conclusion

We have seen that it is possible to mount attacks on Feistel ciphers with 1, 2, and 3 rounds even when the round functions are perfect. This shows that these ciphers are not secure if we apply only 1, 2, or 3 rounds. Several questions arise. They will be the topic of the following chapters. Do there exist similar attacks for 4 rounds or more? This is studied in Chap. 6. On the contrary, is it possible to obtain security results? For 3 rounds, was it unavoidable to use a more complex attack (CCA instead of KPA or NCPA)? We will get an answer with Luby-Rackoff Theorems in Chap. 4. Can we design more general Feistel ciphers? Examples will be given in Chaps. 8, 9, 10.

Problems

2.1. Is $\Psi^3(f,f,f)$ secure in CPA? Here $f_1 = f_2 = f_3$. Similarly, is $\Psi^7(f_1,f_2,f_3,f_4,f_3,f_2,f_1)$ secure in CPA?

2.2. Let $G = F_2 \circ F_1$ where F_1 is a Feistel cipher with a key k_1 of 40 bits, and F_2 is also a Feistel cipher with a key k_2 of 40 bits. Can G be a secure cipher? Here F_1 and F_2 have many rounds and we assume that the computation of F_1 and F_2 is not very slow.

2.3. Let F be a Feistel cipher with 10 rounds and a secret key of 256 bits that generates permutations on 40 bits. Can F be a secure cipher?

2.4. In a foreign country, the law asks for all cryptographic permutations to have a key with a maximal length of 50 bits. How can we build an efficient and secure permutation according to such a law?

References

1. Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. J. ACM **33**, 792–807 (1986)
2. Hastad J., Impagliazzo, R., Levin, L., Luby, M.: Construction of a pseudo-random generator from any one-way function. SIAM J. Comput. **28**, 12–24 (1993)
3. Luby, M., Rackoff, C.: How to construct pseudo-random permutations from pseudo-random functions. SIAM J. Comput. **17**, 373–386 (1988)
4. Patarin, J.: Generic Attacks on Feistel Schemes. In: Cryptology ePrint Archive: Report 2008/036

http://www.springer.com/978-3-319-49528-6

Feistel Ciphers
Security Proofs and Cryptanalysis
Nachef, V.; Patarin, J.; Volte, E.
2017, XV, 309 p. 39 illus., 6 illus. in color., Hardcover
ISBN: 978-3-319-49528-6