Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions

Jacques Patarin[1], Valérie Nachef[2], and Côme Berbain[3]

[1] Université de Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
[2] CNRS(UMR 8088) and Department of Mathematics
Université de Cergy-Pontoise
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
[3] France Telecom Research and Development
38-40 rue du Général Leclerc, 92794 Issy-les-Moulineaux, France
jacques.patarin@prism.uvsq.fr
valerie.nachef@u-cergy.fr
come.berbain@orange-ftgroup.com

Abstract. Unbalanced Feistel schemes with expanding functions are used to construct pseudo-random permutations from kn bits to kn bits by using random functions from n bits to $(k-1)n$ bits. At each round, all the bits except n bits are changed by using a function that depends only on these n bits. Jutla [6] investigated such schemes, which he denotes by F_k^d, where d is the number of rounds. In this paper, we describe novel Known Plaintext Attacks (KPA) and Non-Adaptive Chosen Plaintext Attacks (CPA-1) against these schemes. With these attacks we will often be able to improve the results of Jutla.

Key words: Unbalanced Feistel permutations, pseudo-random permutations, generic attacks on encryption schemes, Block ciphers.

1 Introduction

A Feistel scheme from $\{0,1\}^l$ to $\{0,1\}^l$ with d rounds is a permutation built from round functions $f_1, \ldots, f_d$. When these round functions are randomly chosen, we obtain what is called a "Random Feistel Scheme". The attacks on these "random Feistel schemes" are called "generic attacks" since these attacks are valid for most of the round functions $f_1, \ldots, f_d$.

When $l = 2n$ and when the f_i functions are from $\{0,1\}^n$ to $\{0,1\}^n$ we obtain the most classical Feistel schemes, also called "balanced" Feistel schemes. Since the famous paper of Luby and Rackoff [10], many results have been obtained on the security of such classical Feistel schemes (see [11] for an overview of these results). When the number of rounds is lower than 5, we know attacks with less than $2^l (= 2^{2n})$ operations: for 5 rounds, an attack in $O(2^n)$ operations is given in [14] and for 3 or 4 rounds an attack in $\sqrt{2^n}$ is given in [1, 12]. When

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

the functions are permutations, similar attacks for 5 rounds are given in [7, 9]. Therefore, for security, at least 6 rounds are recommended, i.e. each bit will be changed at least 3 times.

When $l = kn$ and when the round functions are from $(k-1)n$ bits to n bits, we obtain what is called an "Unbalanced Feistel Scheme with contracting functions". In [11] some security proofs are given for such schemes when for the first and the last rounds pairwise independent functions are used instead of random contracting functions. At Asiacrypt 2006 [15] generic attacks on such schemes have been studied.

When $l = kn$ and when the rounds functions are from n bits to $(k-1)n$ bits, we obtain what is called an "Unbalanced Feistel Scheme with expanding functions", also called "complete target heavy unbalanced Feistel networks" [16]. Generic attacks on Unbalanced Feistel Schemes with expanding functions is the theme of this paper. One advantage of these schemes is that it requires much less memory to store a random function of n bits to $(k-1)n$ bits than a random function of $(k-1)n$ bits to n bits. BEAR and LION [2] are two block ciphers which employ both expanding and contracting unbalanced Feistel networks. The AES-candidate MARS is also using a similar structure.

Attacks on Unbalanced Feistel Schemes with expanding functions have been previously studied by Jutla [6]. We will often be able to improve his attacks by attacking more rounds, or by using a smaller complexity. Moreover we will generalize these attacks by analyzing KPA (Known Plaintext Attacks), not only CPA-1 (non adaptive plaintext attacks) and by giving explicit formulas for the complexities. We will not introduce adaptive attacks, or chosen plaintext and chosen ciphertext attacks, since we have not found anything significantly better than CPA-1.

The paper is organized as follows. First, we give our notation. Then we describe the different families of attacks we have studied. We will have three families of attacks called "2-point attacks" (TWO), "rectangle attacks" (SQUARE, R1, R2, R3, R4) and "Multi-Rectangle attacks". In this paper, we will study in detail TWO and rectangle attacks, but we will give only a few comment on "Multi-Rectangle attacks" (Multi-Rectangle attacks are still under investigation). It can be noticed that $k = 2$ is very different from $k \geq 3$.

2 Notation

Our notation is very similar to [15]. An unbalanced Feistel scheme with expanding functions F_k^d is a Feistel scheme with d rounds. At each round j, we denote by f_j the round function from n bits to $(k-1)n$ bits. f_j is defined as $f_j = (f_j^{(1)}, f_j^{(2)}, \ldots, f_j^{(k-1)})$, where each function $f_j^{(l)}$ is defined from $\{0,1\}^n$ to $\{0,1\}^n$. On some input $[I^1, I^2, \ldots, I^k]$ F_k^d produces an output denoted by $[S^1, S^2, \ldots, S^k]$ by going through d rounds. At round j, the first n bits of the round entry are used as an input to the round function f_j, which produces $(k-1)n$ bits. Those bits are xored to the $(k-1)n$ last bits of the round entry and the result is rotated by n bits. We introduce the internal variable X^j: it

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

is the n-bit value produced by round j, which will be the input of next round function f_{j+1}. For example, we have:

$$\begin{aligned} X^1 &= I^2 \oplus f_1^{(1)}(I^1) \\ X^2 &= I^3 \oplus f_1^{(2)}(I^1) \oplus f_2^{(1)}(X^1) \\ X^3 &= I^4 \oplus f_1^{(3)}(I^1) \oplus f_2^{(2)}(X^1) \oplus f_3^{(1)}(X^2) \\ &\dots \end{aligned}$$

The first round is represented on Figure 1 below :

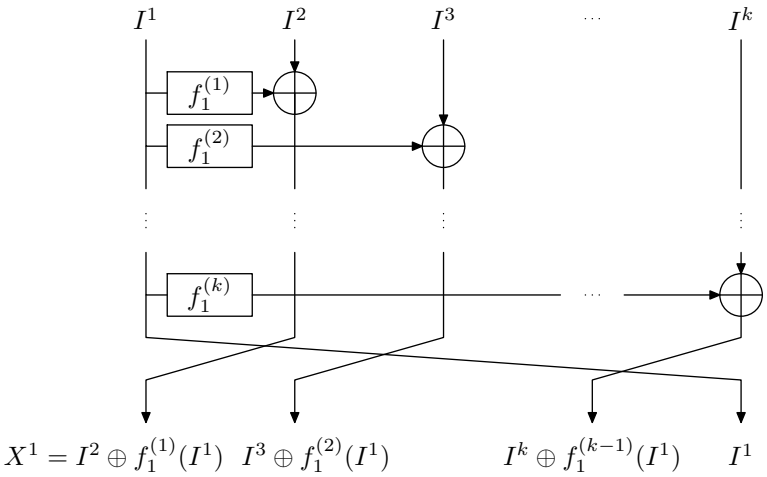

Fig. 1. First Round of F_k^d

After d rounds ($d \geq k+1$), the output $[S^1, S^2, \dots, S^k]$ can be expressed by using the introduced values X^j:

$$\begin{aligned} S^k &= X^{d-1} \\ S^{k-1} &= X^{d-2} \oplus f_d^{(k-1)}(X^{d-1}) \\ S^{k-2} &= X^{d-3} \oplus f_{d-1}^{(k-1)}(X^{d-2}) \oplus f_d^{(k-2)}(X^{d-1}) \\ &\dots \end{aligned}$$

3 Overview of the Attacks

We investigated several attacks allowing to distinguish F_k^d from a random permutation. Depending on the values of k and d some attacks are more efficient than others. All our attacks are using sets of plaintext/ciphertext pairs : the sets can be simply couples (for attack TWO) or a rectangle structure with either four

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

plaintext/ciphertext pairs (attack SQUARE) or more (attacks R1, R2, R3, and R4). Depending on the number of rounds, it is possible to find some relations between the input variables and output variables of the pairs of a set. Those relations can appear at random or due to equalities of some internal variables due to the structure of the Feistel scheme.

The TWO attack consists in using m plaintext/ciphertexts pairs and in counting the number $\mathcal{N}_{F_k^d}$ of couples of these pairs that satisfy the relations between the input and output variables. We then compare $\mathcal{N}_{F_k^d}$ with $\mathcal{N}_{perm}$ where $\mathcal{N}_{perm}$ is the number of couples of pairs for a random permutation instead of F_k^d. The attack is successful, i.e. we are able to distinguish F_k^d from a random permutation if the difference $|E(\mathcal{N}_{F_k^d}) - E(\mathcal{N}_{perm})|$ is much larger than the standard deviation σ_{perm} and than the standard deviation $\sigma_{F_k^d}$, where E denotes the expectancy function. In order to compute these values, we need to take into account the fact that the structures obtained from the m plaintext/ciphertext tuples are not independent. However their mutual dependence is very small. To compute σ_{perm} and $\sigma_{F_k^d}$, we will use this well-known formula as in [15] that we will call the "Covariance Formula":

$$V(\sum x_i) = \sum_i V(x_i) + \sum_{i<j} \big[E(x_i, x_j) - E(x_i)E(x_j)\big]$$

where the x_i are random variables.

In the attacks R1, R2, R3, and R4, we use a rectangle structure: we consider φ plaintext/ciphertext pairs where φ is an even number and is the total number of indexes of the rectangle. We will fix some conditions on the inputs of the φ pairs. On the case of F_k^d, those conditions will turn into conditions on the internal state variables X^j due to the structure of the Feistel scheme. These conditions will imply equations on the outputs. On the case of a random permutation, equations on the outputs will only appear at random. By counting the sets of φ pairs satisfying the conditions on inputs and outputs, we can distinguish between F_k^d and a random permutation, since in the case of F_k^d the equations on the outputs appear not only at random, but a part of them is due to the conditions we set. However, those attacks are not always able to distinguish between F_k^d and a random permutation, since it requires some internal collision to appear in the structure of the Feistel scheme. For some instances of F_k^d the desired collision will not exist and the attacks will fail. There exists a probability ϵ which is a strictly positive constant independent of n such that rectangle structures appear for F_k^d. How to compute this probability can be found in the extended version. Consequently, in order to verify that we are able to distinguish between the family of F_k^d permutations and the family of random permutations, we can apply our attacks on several randomly chosen instances of F_k^d or of random permutation, count the number of instances were the attack is working and compare this number for F_k^d and for a random permutation. Attacks R1, R2, R3, and R4 all share this principle but the conditions imposed on the plaintexts and ciphertexts are different.

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

The SQUARE attack is a special case of attack R1, when $\varphi = 4$. In the next sections, we will give more precise definitions of these attacks and examples for attack TWO and attack R1. Finally we will consider attacks with more than 2^{kn} computations, i.e. attacks against generators of pseudo-random permutations. All the results are summarized in Section 9.

For a fixed value of k, attack TWO is very efficient for small values of d. When d increases, first SQUARE, which is a variant of R1, then R1 will become the best known attack. Then, when d increases again, R2, R3 or R4 will become the best known attack. Finally, for very large d, TWO will become again the best known attack.

4 Attack "TWO"

In this section, we describe a family of attacks called "TWO". These attacks will use correlations on pairs of plaintext/ciphertext. Therefore, they can be called "2-point" attacks. When $k = 2$ i.e. on classical balanced Feistel Schemes, these attacks give the best known generic attacks [14]. However these attacks have not been studied in [6]. As we will see, TWO attacks are sometimes more efficient than the attacks of [6] for example when the number of rounds is very small.

The principle of attack TWO is to concentrate on one of the equations linking an output word S^i with some of the internal variables X^i. By fixing the first n-bit blocks of the input I we fix the value of some of the internal variables and a simple equality between the remaining input blocks and the output word becomes true assuming that a collision on some of the internal variable occurs. If the number of plaintext/ciphertext pairs is sufficiently large, this collision will appear and the attack succeeds.

In order to illustrate attack TWO, we now present the attack against F_k^d, $k + 2 \leq d \leq 2k - 1$. We will concentrate the attack on the equation:

$$S^{2k-d} = X^{k-1} \oplus \bigoplus_{i=k}^{d-1} f_{i+1}^{(2k-i-1)}(X^i)$$

The i-th pair is denoted by $[I^1(i), I^2(i), \ldots, I^k(i)]$ for the plaintext and by $[S^1(i), S^2(i), \ldots, S^k(i)]$ for the ciphertext. We will count the number $\mathcal{N}$ of (i, j) such that $I^1(i) = I^1(j), I^2(i) = I^2(j), \ldots, I^{k-1}(i) = I^{k-1}(j), S^k(i) = S^k(j)$, $S^{k-1}(i) = S^{k-1}(j), \ldots, S^{2k-d+1}(i) = S^{2k-d+1}(j)$ and $S^{2k-d}(i) \oplus S^{2k-d}(j) = I^k(i) \oplus I^k(j)$. For F_k^d, this last equation is a consequence of the other equations, i.e. of these $k - 1$ equations in I and $d - k$ equations in S. Therefore, the attack will succeed in KPA when $m^2 \geq 2^{(d-1)n}$, i.e. when $m \geq 2^{\frac{d-1}{2}n}$. In CPA-1, we will fix $I^1, I^2, \ldots, I^k$ to some values, and we will do this α times. The attack will succeed with $\alpha = 2^{(d-k-2)n}$ and the complexity in CPA-1 is $\alpha \cdot 2^n = 2^{(d-k-1)n}$.

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

5 "R1" Attack

5.1 Definition of R1

We now give a definition of attack R1. Let us consider φ plaintext/ciphertext pairs. We first set the following conditions on the input variables:

$$(I) = \begin{cases} I^1(1) = I^1(2),\ I^1(3) = I^1(4),\ I^1(5) = I^1(6), \ldots,\ I^1(\varphi - 1) = I^1(\varphi) \\ \forall i,\ 2 \leq i \leq k,\ I^i(1) \oplus I^i(2) = I^i(3) \oplus I^i(4) = \ldots = I^i(\varphi - 1) \oplus I^i(\varphi) \end{cases}$$

Conditions on the first block I^1 are here to cancel the impact of function f_1, while conditions on other blocks are used to obtain differential equations on the internal state variables. These equations will then propagate to other rounds with some probability until they turn to equations on the outputs, which then can be detected.

In order for the previous conditions to propagate with high probability, we need some extra conditions on the internal state variables. We have $d-2$ internal state variables $X^1, X^2, \ldots, X^{d-2}$ and $X^{d-1} = S^k$ is an output variable.

Let a be an integer, $1 \leq a \leq d-1$. We will choose a values of $\{1, 2, \ldots, d-k\}$. Let $\mathcal{E}$ be the set of these a values, and let $\mathcal{F}$ be the set of all integers i, $1 \leq i \leq d-1$ such that $i \notin \mathcal{E}$. We have $|\mathcal{E}| = a$ and $|\mathcal{F}| = d - a - 1$. Let (X) be the set of the following equalities:

$$(X) = \begin{cases} \forall i \in \mathcal{E},\ X^i(1) = X^i(3) = \ldots = X^i(\varphi - 1) \\ \forall i \in \mathcal{F},\ X^i(1) = X^i(2) \end{cases}$$

Between two different plaintext/ciphertext pairs i and j, $i \neq j$, we can have at most $k-1$ successive equalities on the variables $I^1, X^1, X^2, \ldots, X^{d-1}$. Otherwise from k successive equalities we would get $I^1(i) = I^1(j), I^2(i) = I^2(j), \ldots, I^k(i) = I^k(j)$, so the two messages would be the same. Therefore we must have: $\lfloor \frac{d}{k} \rfloor \leq a \leq d - 1 - \lfloor \frac{d-1}{k} \rfloor$. For the same reason we must have $\{d-k\} \in \mathcal{E}$ since $d-1$, $d-2$, ..., $d-k+1$ are in $\mathcal{F}$.

From the conditions (I) and (X) and considering the equalities that we can derive from them with probability one, we will have:

$$(S) = \begin{cases} \forall i,\ 2 \leq i \leq k,\ S^i(1) = S^i(2),\ S^i(3) = S^i(4), \ldots\ S^i(\varphi - 1) = S^i(\varphi) \\ S^1(1) \oplus S^1(2) = S^1(3) \oplus S^1(4) = \ldots = S^1(\varphi - 1) \oplus S^1(\varphi) \end{cases}$$

Consequently the conditions (S) can appear by chance, or due to the conditions (X).

Our KPA attack consists in counting the number $\mathcal{N}$ of rectangle sets of plaintext/ciphertext pairs satisfying the conditions (I) and (S). The obtained number can be divided into two parts: either the conditions (I) and (S) appear completely at random, or conditions (I) appear and conditions (S) are satisfied because (X) happened.

Figure 2 illustrates one rectangle set of our attack. Plaintext/ciphertext pairs are denoted by $1, 2, \ldots, \varphi$. Two points are joined by an edge if the values are equal (for example $I^1(1) = I^1(2)$). We draw a solid edge if the equality appears with probability $\frac{1}{2^n}$ and a dotted line if the equality follows conditionally with probability 1 from other imposed equalities.

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

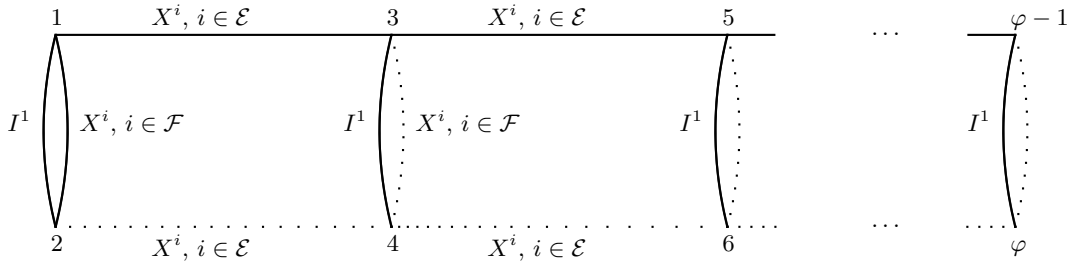

Fig. 2. Attack R1 on F_k^d

5.2 "R1" Attack on F_3^7

Before studying the general properties of R1, we will illustrate this attack with an example. We will now describe our "R1" attack on F_3^7. As we will see, we will obtain here a complexity in $O(2^{2n})$ in CPA-1 and in $O(2^{\frac{5n}{2}})$ in KPA. This is better than the $O(2^{3n})$ of the TWO attacks. In [6], Jutla shows that he can obtain on F_k^d attacks with complexity less than $O(2^{kn})$ when $d \leq 3k-3$. For $d=3$, this gives attacks up to only 6 rounds, unlike here where we will reach 7 rounds with the complexity less than 2^{3n}. We have $F_3^7[I^1, I^2, I^3] = [S^1, S^2, S^3]$.

Let i_1, i_2, i_3, i_4, i_5, i_6 be six indexes of messages (so these values are between 1 and m). We will denote by $[I^1(\alpha), I^2(\alpha), I^3(\alpha)]$ the plaintext of message i_α, and by $[S^1(\alpha), S^2(\alpha), S^3(\alpha)]$ the ciphertext of message i_α. (i.e. for simplicity we use the notation $I^1(\alpha)$ and $S^1(\alpha)$ instead of $I^1(i_\alpha)$ and $S^1(i_\alpha)$, $1 \leq \alpha \leq 6$). The idea of the attack is to count the number $\mathcal{N}$ of indexes $(i_1, i_2, i_3, i_4, i_5, i_6)$ such that:

$$\begin{cases} I^1(1) = I^1(2) \text{ and } I^1(3) = I^1(4) \text{ and } I^1(5) = I^1(6) \\ I^2(1) \oplus I^2(2) = I^2(3) \oplus I^2(4) = I^2(5) \oplus I^2(6) \\ I^3(1) \oplus I^3(2) = I^3(3) \oplus I^3(4) = I^3(5) \oplus I^3(6) \\ \quad \text{and} \\ S^3(1) = S^3(2) \text{ and } S^3(3) = S^3(4) \text{ and } S^3(5) = S^3(6) \\ S^2(1) = S^2(2) \text{ and } S^2(3) = S^2(4) \text{ and } S^2(5) = S^2(6) \\ S^1(1) \oplus S^1(2) = S^1(3) \oplus S^1(4) = S^1(5) \oplus S^1(6) \end{cases}$$

We will call the 7 first equations the "input equations" and we will call the 8 last equations the "output equations".

KPA. If the messages are randomly chosen, for a random permutation we will have $E(\mathcal{N}_{perm}) \simeq \frac{m^6}{2^{15n}}$. For a F_3^7 permutation we will have about 2 times more solutions since the 8 output equations can occur at random, or due to the following 8 internal equations:

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

$$\begin{cases} X^1(1) = X^1(3) = X^1(5) \\ X^2(1) = X^2(2) \\ X^3(1) = X^3(2) \\ X^4(1) = X^4(3) = X^4(5) \\ X^5(1) = X^5(2) \\ X^6(1) = X^6(2) \end{cases}$$

We get the following conditions on the internal variables:

$$\begin{cases} X^2(1) = X^2(2) \text{ gives } X^2(3) = X^2(4) \text{ and } X^2(5) = X^2(6) \\ X^3(1) = X^3(2) \text{ gives } X^3(3) = X^2(4) \text{ and } X^3(5) = X^3(6) \\ X^4(1) = \ X^4(3) = X^4(5) \text{ gives } X^4(2) = X^4(4) = X^4(6) \\ X^5(1) = X^5(2) \text{ gives } X^5(3) = X^5(4) \text{ and } X^5(5) = X^5(6) \\ X^6(1) = X^6(2) \text{ gives } X^6(3) = X^6(4) \text{ and } X^6(5) = X^6(6) \end{cases}$$

Now since $S^3 = X^6$, $S^2 = X^5 \oplus f_7^{(2)}(X^6)$ and $S^1 = X^4 \oplus f_6^{(2)}(X^5) \oplus f_7^{(1)}(X^6)$, we get the 8 output equations written above. Therefore, in KPA, for a F_3^7 permutation, the expectancy of $\mathcal{N}_{F_3^7}$ is larger than for a random permutation by a value of about $\frac{m^6}{2^{15n}}$ (since we have 8 equations in X and 7 in I), i.e. we expect to have about 2 times more solutions for $\mathcal{N}$: $E(\mathcal{N}) \simeq \frac{2m^6}{2^{15n}}$ for F_3^7. So we will be able to distinguish with a high probability F_3^7 from a random permutation by counting $\mathcal{N}$ when $\mathcal{N} \neq 0$ with a high probability, i.e. when $m^6 \geq O(2^{15n})$, or $m \geq O(2^{\frac{5n}{2}})$. We have found here a KPA with $O(2^{\frac{5n}{2}})$ complexity and $O(2^{\frac{5n}{2}})$ messages. This is better than the $O(2^{3n})$ complexity of the attack TWO, and it shows that we can attack 7 rounds, not only 6 with a complexity less than 2^{3n}.

CPA-1

We can transform this KPA in CPA-1. We will choose only 3 fixed different values c_1, c_2, c_3 for I^1: $\frac{m}{3}$ plaintexts will have $I^1 = c_1$, $\frac{m}{3}$ plaintexts will have $I^1 = c_2$, and $\frac{m}{3}$ plaintexts will have $I^1 = c_3$. We will generate all (or almost all) possible messages $[I^1, I^2, I^3]$ with such I^1. Therefore, $m = 3 \cdot 2^{2n}$. We can derive from these m messages $\frac{2m^4}{27}$ tuples $(i_1, i_2, i_3, i_4, i_5, i_6)$ satisfying our 7 input equations. For a random permutation we will have $E(\mathcal{N}_{perm}) \simeq \frac{2m^4}{27 \cdot 2^{8n}}$ (since we have 8 output equations). For a permutation F_3^7, we will have $E(\mathcal{N}_{F_3^7}) \simeq \frac{4m^4}{27 \cdot 2^{8n}}$, i.e. about 2 times more solutions, since the 8 output equations can occur at random, or due to 8 internal equations in X as we have seen. So this CPA-1 will succeed when $\mathcal{N} \neq 0$ with a high probability, i.e. when $m^4 \geq O(2^{8n})$, or $m \geq O(2^{2n})$. Here we have $m \simeq 3 \cdot 2^{2n}$, the probability of success is not negligible. Moreover if it fails for some values (c_1, c_2, c_3) for I^1, we can start again with another (c_1, c_2, c_3). Therefore this CPA-1 is in $O(2^{2n})$ complexity and $O(2^{2n})$ messages. (This is better than the $O(2^{3n})$ we have found with the TWO attack).

5.3 Properties of R1

We now describe the general properties of R1. We will denote by n_I the number of equalities in (I), and by n_S the number of equalities in (S). Similarly, we will

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

denote by n_X the number of equalities in (X). Therefore n_X is the number of independent equalities in the X^i variables needed in order to get (S) from (I) (in the previous example presented in Section 5.2, we have $n_I = 7$, $n_S = 8$ and $n_X = 8$). In this attack R1 we have:

$$\begin{cases} n_I = \frac{k\varphi}{2} - k + 1 \\ n_S = \frac{k\varphi}{2} - 1 \\ n_X = a(\frac{\varphi}{2} - 2) + d - 1 \end{cases}$$

The idea of R1 is to minimize the total number $n_I + n_X$ of needed equations in I and X. When this criteria is dominant, R1 will be the best attack.

The value $\mathcal{N}$ is expected to be larger for a F_k^d than for a random permutation due to the fact that (S) can come from random reasons or from (X) in F_k^d. Therefore, it is natural, in order to get necessary and sufficient condition of success for R1, to evaluate the expectancy and the standard deviation of $\mathcal{N}$ in the case of F_k^d and in the case of random permutations. This can be done (by using the covariance formula as in [15] or by using approximation as in [6]) and we have found that each time that R1 was better than TWO, we had $n_X \leq n_S$. However, when $n_X \leq n_S$ we can easily obtain sufficient condition of success for R1 without computing the standard deviations, since when $n_X \leq n_S$ we will have for most permutations about 2 times more (or more) solutions with F_k^d than with this random permutation. Therefore, a sufficient condition of success for R1 when $n_X \leq n_S$ is to have that (X) and (I) can be satisfied with a non-negligible probability. A sufficient condition for this is to have:

In KPA

Condition 1: $n_X \leq n_S$.

Condition 2: $m^\varphi \geq 2^{n(n_I+n_X)}$.

Condition 3: $m^2 \geq 2^{(d-a)n}$.

Condition 4: $m^3 \geq 2^{dn}$ and more generally $\forall i$, $0 \leq i \leq \frac{\varphi}{2}-1$, $m^{3+i} \geq 2^{(d+ia)n}$.

Condition 5: $m^4 \geq 2^{(d+k)n}$.

(Conditions 2, 3, 4, 5 are necessary. Conditions 1, 2, 3, 4, 5 are sufficient for success. Condition 1 is not necessary, but the computation of $\sigma(\mathcal{N})$ shows that R1 is not better than TWO when $n_X > n_S$.)

Condition 2 comes from the fact that we have about m^φ rectangles with φ points, and the probability that (I) and (X) are satisfied on one rectangle is $\frac{1}{2^{n(n_I+n_X)}}$.

Condition 3 comes from the fact that between points 1 and 2 we have $|\mathcal{F}|$ equations in X^i, and one equation in I^1. Therefore in KPA we must have $m^2 \geq 2^{(|\mathcal{F}|+1)n} = 2^{(d-a)n}$.

Condition 4 comes from the fact that between points 1, 2 and 3 we have $d-1$ equations in X^i, and one equation in I^1. Therefore we must have $m^3 \geq 2^{dn}$. Similarly between the points 1, 2, 3, 5, we must have: $m^4 \geq 2^{(d+a)n}$. And similarly between the points 1, 2, 3, 5, 7, ..., $(\varphi - 1)$, we must have: $m^{\frac{\varphi}{2}+1} \geq 2^{(d+a(\frac{\varphi}{2}-2))n}$.

Condition 5 comes from the fact that between points 1, 2, 3, 4, we have $d-1$ equations in X^i, 2 equations in I^1 and $(k-1)$ in I^2, I^3, ..., I^{k-1}.

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

It is easy to see that the conditions on any points are consequences of these 5 conditions. Moreover, if $m \geq 2^{an}$ (we will often, but not always, choose a like this), condition 4 can be changed with only $m^3 \geq 2^{dn}$.

CPA-1

In CPA-1 the sufficient conditions when $m \leq 2^{(k-1)n}$ are:

Condition 1: $n_X \leq n_S$.

Condition 2: $m^{(\frac{\varphi}{2}+1)} \geq 2^{n \cdot n_X}$.

Condition 3: $m^2 \geq 2^{(d-a-1)n}$.

Condition 4 and Condition 5: $m^3 \geq 2^{(d-1)n}$.

From these conditions we can compute the best parameters a and φ for any d and k, when d and k are fixed.

Remark. If we choose $n_X < n_S$ (instead of $n_X \leq n_S$), the attacks are slightly less efficient but more spectacular since with a non-negligible probability (I) and (S) are satisfied with F_k^d and not with random permutations. Moreover with $n_X < n_S$ it is still possible (with R2) to attack $3k-1$ rounds with less than 2^{kn} complexity.

6 "R2", "R3", "R4" Attacks for any $k \geq 3$ with $d \geq k$

R2, R3, and R4 attacks are very similar to attack R1 but the conditions on the variables are not the same.

6.1 R2 attacks

In the R2 attack, we will choose a values of $\{1, 2, \ldots, d-k\}$. Let $\mathcal{E}$ be the set of these a values, and let $\mathcal{F}$ be the set of all integers i, $1 \leq i \leq d-1$ such that $i \notin \mathcal{E}$. We have $|\mathcal{E}| = a$, $|\mathcal{F}| = d-a-1$, and $\mathcal{F}$ contains all the $k-1$ values i, $d-k+1 \leq i \leq d-1$. For R2 we have:

$$(I) = \begin{cases} I^1(1) = I^1(3) = I^1(5) = \ldots = I^1(\varphi - 1) \\ I^1(2) = I^1(4) = I^1(6) = \ldots = I^1(\varphi) \\ \forall i,\ 2 \leq i \leq k,\ I^i(1) \oplus I^i(2) = I^i(3) \oplus I^i(4) = \ldots = I^i(\varphi - 1) \oplus I^i(\varphi) \end{cases}$$

$$(X) = \begin{cases} \forall i \in \mathcal{E},\ X^i(1) = X^i(3) = \ldots = X^i(\varphi - 1) \\ \forall i \in \mathcal{F},\ X^i(1) = X^i(2) \end{cases}$$

$$(S) = \begin{cases} \forall i,\ 2 \leq i \leq k,\ S^i(1) = S^i(2),\ S^i(3) = S^i(4), \ldots,\ S^i(\varphi - 1) = S^i(\varphi) \\ S^1(1) \oplus S^1(2) = S^1(3) \oplus S^1(4) = \ldots = S^1(\varphi - 1) \oplus S^1(\varphi) \end{cases}$$

The equations (X) have been chosen such that (S) is just a consequence of (I) and (X). Our attacks consist in counting the number $\mathcal{N}$ of rectangle sets of plaintext/ciphertext pairs satisfying the conditions (I) and (S). Figure 3 illustrates the equations for R2.

Between two different plaintext/ciphertext pairs i and j, $i \neq j$, we can have at most $k-1$ successive equalities on the variables I^1, X^1, ..., X^{d-1}. Therefore, for R2, we have $\lfloor \frac{d-1}{k} \rfloor \leq a \leq d-1-\lfloor \frac{d}{k} \rfloor$, and

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

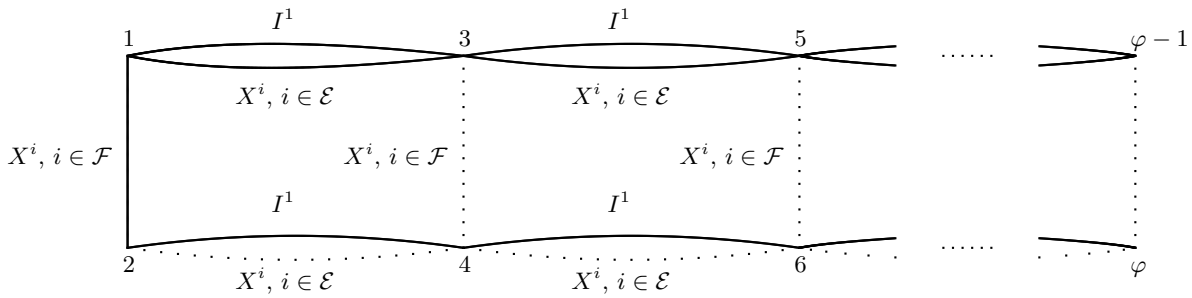

Fig. 3. Attack R2 on F_k^d

$$\begin{cases} n_I = \frac{k\varphi}{2} + \frac{\varphi}{2} - k - 1 \\ n_S = \frac{k\varphi}{2} - 1 \\ n_X = a(\frac{\varphi}{2} - 2) + d - 1 \end{cases}$$

As we have explained for R1, sufficient conditions of success for R2 in KPA are the following 5 conditions:

Condition 1: $n_X \leq n_S$.
Condition 2: $m^\varphi \geq 2^{n(n_I+n_X)}$.
Condition 3: $m^3 \geq 2^{dn}$.
Condition 4: $m^2 \geq 2^{(d-a-1)n}$.
Condition 5: $m^4 \geq 2^{(d+k)n}$.

Example for R2

In the R2 attack on F_3^8, we have: $\varphi = 8$, $a = 2$, $n_I = 12$, $n_S = 11$ and $n_X = 11$. Details are in the extended version of the paper.

6.2 R3 Attack

In the R3 attack, we set the following conditions on the input variables:

$$(I) = \begin{cases} I^1(1) = I^1(2),\ I^1(3) = I^1(4),\ I^1(5) = I^1(6), \ldots,\ I^1(\varphi - 1) = I^1(\varphi) \\ \forall i,\ 2 \leq i \leq k,\ I^i(1) \oplus I^i(2) = I^i(3) \oplus I^i(4) = \ldots = I^i(\varphi - 1) \oplus I^i(\varphi) \end{cases}$$

Then the conditions on the internal variables (with $|\mathcal{E}| = d - a - 1$ and $|\mathcal{F}| = a$ and if $d - k + 2 \leq i \leq d - 1$ then $i \in \mathcal{F}$) are:

$$(X) = \begin{cases} \forall i \in \mathcal{E},\ X^i(1) = X^i(2) \\ \forall i \in \mathcal{F},\ X^i(1) = X^i(3) = \ldots = X^i(\varphi - 1) \end{cases}$$

Finally, the conditions on the output variables are given by:

$$(S) = \begin{cases} S^1(1) \oplus S^1(2) = S^1(3) \oplus S^1(4) = \ldots = S^1(\varphi - 1) \oplus S^1(\varphi) \\ S^2(1) \oplus S^2(2) = S^2(3) \oplus S^2(4) = \ldots = S^2(\varphi - 1) \oplus S^2(\varphi) \\ \forall i,\ 3 \leq i \leq k,\ S^1(1) = S^1(3) = S^1(5) = \ldots = S^1(\varphi - 1) \\ \forall i,\ 3 \leq i \leq k,\ S^1(2) = S^1(4) = S^1(6) = \ldots = S^1(\varphi) \end{cases}$$

Then, the R3 attack proceeds exactly the same as R1 and R2 attacks.

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

6.3 R4 Attack

In the R4 attack, we have the following conditions on the input, internal and output variables:

$$(I) = \begin{cases} I^1(1) = I^1(3) = I^1(5) = \ldots = I^1(\varphi - 1) \\ I^1(2) = I^1(4) = I^1(6) = \ldots = I^1(\varphi) \\ \forall i,\, 2 \le i \le k,\, I^i(1) \oplus I^i(2) = I^i(3) \oplus I^i(4) = \ldots = I^i(\varphi - 1) \oplus I^i(\varphi) \end{cases}$$

$$(X) = \begin{cases} \forall i \in \mathcal{E},\, X^i(1) = X^i(2) \\ \forall i \in \mathcal{F},\, X^i(1) = X^i(3) = \ldots = X^i(\varphi - 1) \end{cases}$$

(with $|\mathcal{E}| = d - a - 1$ and $|\mathcal{F}| = a$ and if $d - k + 3 \le i \le d - 1$ then $i \in \mathcal{F}$)

$$(S) = \begin{cases} S^1(1) \oplus S^1(2) = S^1(3) \oplus S^1(4) = \ldots = S^1(\varphi - 1) \oplus S^1(\varphi) \\ S^2(1) \oplus S^2(2) = S^2(3) \oplus S^2(4) = \ldots = S^2(\varphi - 1) \oplus S^2(\varphi) \\ S^3(1) \oplus S^3(2) = S^3(3) \oplus S^3(4) = \ldots = S^3(\varphi - 1) \oplus S^3(\varphi) \\ \forall i,\, 4 \le i \le k,\, S^1(1) = S^1(3) = S^1(5) = \ldots = S^1(\varphi - 1) \\ \forall i,\, 4 \le i \le k,\, S^1(2) = S^1(4) = S^1(6) = \ldots = S^1(\varphi) \end{cases}$$

Example for R4

We will now present how to attack F_k^{3k-1} when $k \ge 5$ with a complexity less than 2^{kn}. This example is interesting since $3k - 1$ is the maximum number of rounds that we can attack with a complexity lower than 2^{kn} (for $d = 3k$ the complexity of the best known attacks become $O(2^{kn})$ and for $d \ge 3k+1$ we need more than $O(2^{kn})$ computations). It is also interesting since in [6] Jutla was able to attack only $3k - 3$ rounds with a complexity less than 2^{kn}. We will present only the main ideas. We will use the attack R4 with $a = k - 1$, i.e. between 1 and 3 we have these $k - 1$ equations: X^{d-1}, X^{d-2}, ..., X^{d-k+3}, plus X^k and X^{2k}.

Remark. With R2 (but not with R1) we can also attack F_k^{3k-1} (with $\varphi = 2k + 2$ and $a = k - 1$) with a complexity less than 2^{kn}, but the complexity of R4 will be slightly better.

In R4 with $a = k - 1$, we have:

$$\begin{cases} n_I = \frac{k\varphi}{2} + \frac{\varphi}{2} - k - 1 \\ n_S = k\varphi - \frac{3\varphi}{2} - 2k + 3 \\ n_X = \frac{k\varphi}{2} + d - 2k - \frac{\varphi}{2} + 1 \end{cases}$$

Therefore when $d = 3k-1$, we have $n_X = \frac{k\varphi}{2} + k - \frac{\varphi}{2}$. $n_X \le n_S$ gives $\varphi \ge 6 + \frac{6}{k-2}$. For $k \ge 5$, this means $\varphi \ge 8$ (φ is always even). Now if we look at all the 5 conditions for the complexity, these conditions give: $m \ge 2^{(k-\frac{1}{8})n}$ in KPA, and $m \ge 2^{(k-\frac{1}{2})n}$ in CPA-1. These complexities are less than 2^{kn} as claimed.

7 Experimental Results

We have implemented the CPA-1 attacks SQUARE and R1 against F_3^6, F_3^7, and F_3^8. The attack against F_3^6 uses 4 points and $2^{\frac{5n}{3}}$ plaintexts, the attack against

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

F_3^7 uses 6 points and 2^{2n} plaintexts, and the attack against F_3^8 uses 8 points and $2^{2.5n}$ plaintexts. Our experiments confirm our ability to distinguish between F_3^6 or F_3^7 or F_3^8 and a random permutation. Our experiments were done as follows:

- choose randomly an instance of F_3^6 or F_3^7 or F_3^8
- choose randomly a permutation: for this we use classical balanced Feistel scheme with a large number of rounds (more than 20)
- launch the attack in CPA-1
- count the number of structures satisfying the input and output relations for the F_3^6 or F_3^7 or F_3^8 permutation and for the permutation
- if this number is higher or equal to a fixed threshold (generally 1 or 2), declare the function to be a F_3^6 or F_3^7 or F_3^8 permutation and otherwise a random permutation

All these procedures are iterated a large number of time (at least 1000 times) to evaluate the effectiveness of our distinguisher. We give the percentage of success, i.e. the number of F_3^6 or F_3^7 or F_3^8 that have been correctly distinguished and the percentage of false alarm, i.e. the number of random permutation that have incorrectly been declared as F_3^6 or F_3^7 or F_3^8.

Table 1. Experimental results for CPA-1 attacks

scheme	n	threshold	Percentage of success of the attack	Percentage of false alarm
F_3^6	8	2	54%	4%
F_3^7	6	1	33%	1%
F_3^8	6	1	38%	1%

We give some details in the F_3^7 case: here are the numbers of rectangles sets for 100 instances of F_3^7.

$$2, 0, 25, 1, 0, 3, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 2, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 12, 1, 4, 1,$$
$$0, 1, 4, 18, 0, 1, 1, 0, 0, 2, 0, 0, 0, 2, 0, 0, 0, 0, 1, 0, 0, 0, 3, 0, 0, 0, 0, 0, 1, 0, 1, 13, 0, 1, 6, 0,$$
$$0, 0, 33, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 1, 0, 3, 36, 1, 14, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0$$

The corresponding numbers for 100 random permutations are composed of 99 zero and a single one. This clearly shows that we can distinguish between the two cases.

Our experiments show that the distinguisher on F_3^6 is more efficient than the one on F_3^7 and than the one on F_3^8. But in all case they confirm our ability to distinguish.

8 Attack by the Signature

It can be proved that all the permutations F_k^d have an even signature. The proof of this result is quite similar to the proof in the case of a symmetric

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

Feistel scheme [13]. Therefore, by computing the signature of F_k^d we are able to distinguish F_k^d from a random permutation with a non-negligible probability and $O(2^{kn})$ computations if all the 2^{kn} plaintext/ciphertext are known. However if we do not have access to the complex codebook of size 2^{kn}, or if we want to distinguish F_k^d from a random permutation with an even signature, this "attack" obviously fails.

9 Summary of the results on F_k^d, $k \geq 3$, on TWO, SQUARE and Rectangle attacks

The following table shows the results we have obtained with our different attacks.

Table 2. Results on F_k^d for $k = 3$, on TWO, SQUARE and Rectangle attacks (i.e. without Multi-rectangle attacks). CAUTION: Multi-Rectangle attacks may have sometimes better complexities.

	KPA	CPA-1
F_3^1	1	1
F_3^2	$2^{\frac{n}{2}}$, TWO	2
F_3^3	2^n, TWO	2
F_3^4	$2^{\frac{3}{2}n}$, TWO	$2^{\frac{n}{2}}$, TWO
F_3^5	2^{2n}, TWO	2^n, TWO
F_3^6	$2^{\frac{9}{4}n}$, SQUARE	$2^{\frac{5}{3}n}$, SQUARE
F_3^7	$2^{\frac{5}{2}n}$, M1, $\varphi = 6$	2^{2n}, M1, $\varphi = 6$
F_3^8	$2^{\frac{23}{8}n}$, R2, $\varphi = 8$	$2^{\frac{5}{2}n}$, R2, $\varphi = 8$
F_3^9	2^{3n}, R2, $\varphi \geq 10$	2^{3n}, R2, $\varphi \geq 10$
F_3^{10}	2^{7n}, TWO	2^{7n}, TWO
F_3^{11}	2^{8n}, TWO	2^{8n}, TWO
F_3^d, $d \geq 10$	$2^{(d-6+\lfloor \frac{d}{3} \rfloor)n}$, TWO	$2^{(d-6+\lfloor \frac{d}{3} \rfloor)n}$, TWO

10 Multi-Rectangle attacks

An interesting problem is to design better attacks than 2-point attacks, or rectangle attacks. We have tried attacks with different geometries of equations (hexagons instead of rectangles, multi-dimensional cubes instead of 2-dimension rectangles, etc...). So far the best new attacks that we have found are "Multi-Rectangle attacks", i.e. attacks where some "rectangles" in I equations are linked with S equations. We will present here only two examples. More details are given in the extended version of this paper. These new attacks are very promising asymptotically (i.e. when n becomes large) but their efficiency from a practical point of view and the design optimality are still under investigation.

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

Table 3. Results on F_k^d for $k > 3$, on TWO, SQUARE and Rectangle attacks (i.e. without Multi-rectangle attacks). CAUTION: Multi-Rectangle attacks may have sometimes better complexities.

	KPA	CPA-1
F_k^1	1	1
F_k^2	$2^{\frac{n}{2}}$, TWO	2
F_k^3	2^n, TWO	2
F_k^d, $2 \leq d \leq k$	$2^{\frac{d-1}{2}n}$,TWO	2
F_k^{k+1}	$2^{\frac{k}{2}n}$, TWO	$2^{\frac{n}{2}}$, TWO
F_k^{k+2}	$2^{\frac{k+1}{2}n}$, TWO and SQUARE	2^n, TWO
F_k^{k+3}	$2^{\frac{2k+3}{4}n}$, SQUARE	2^{2n},TWO or $2^{\frac{k+2}{3}n}$, SQUARE
F_k^d, $k+2 \leq d \leq 2k$	$2^{\frac{d+k}{4}n}$, SQUARE	$2^{(d-k-1)n}$,TWO or $2^{\frac{d-1}{3}n}$, SQUARE
F_k^{2k}	$2^{\frac{3k}{4}n}$, SQUARE	$2^{\frac{2k-1}{3}n}$,SQUARE
$\vdots$	$\vdots$	$\vdots$
F_k^{3k-1}	$2^{(k-\frac{1}{8})n}$, R3 $k=4$, R4 $k \geq 5$	$2^{(k-\frac{1}{2})n}$, R2 $k=4$, R4 $k \geq 5$
F_k^{3k}	2^{kn}, R2	2^{kn}, R2
F_k^d, $3k \leq d \leq k^2$	$2^{(d-2k)n}$, R2	$2^{(d-2k)n}$, R2

Example 1. With a 2-rectangle attack (as in Figure 4 below), it seems that we can attack F_6^{18} with a complexity strictly less than 2^{6n}. Therefore this attack is expected to be better than rectangle attacks. However we have to use 2 rectangles of about 2×20 points. Consequently we will have a large constant in the complexity and therefore such a theoretical attack might be of no practical interest.

Example 2. It seems that we can attack F_k^d when $d \leq k^2 + k$ with a complexity less than $O(2^{kn})$ with a Multi-Rectangle attack when k is fixed (with a huge coefficient depending of k and not of n in the O).This attacks is based on arrays of $k+1$ dimensional hypercubes. This attack is still under investigation.

Multi-Rectangle attacks are also of interest for less rounds, for example in order to attack F_k^{2k} with a smaller complexity than rectangle attacks.

11 Conclusion

In [6], Jutla has introduced "Rectangle attacks" against unbalanced Feistel schemes. To improve the attacks of Jutla, we have first made a systematic analysis of the different ways to optimize the parameters. We have obtained like this 5 different kinds of "rectangle attacks" that we have called SQUARE, R1, R2, R3 and R4. By computing the optimal parameters, we have shown that we can attack $3k-1$ rounds in KPA instead of $3k-3$ in CPA-1 for Jutla with a complexity strictly lower than 2^{kn} with these "Rectangle attacks" (This was confirmed with experimental simulations). Moreover, we have also described two other families

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

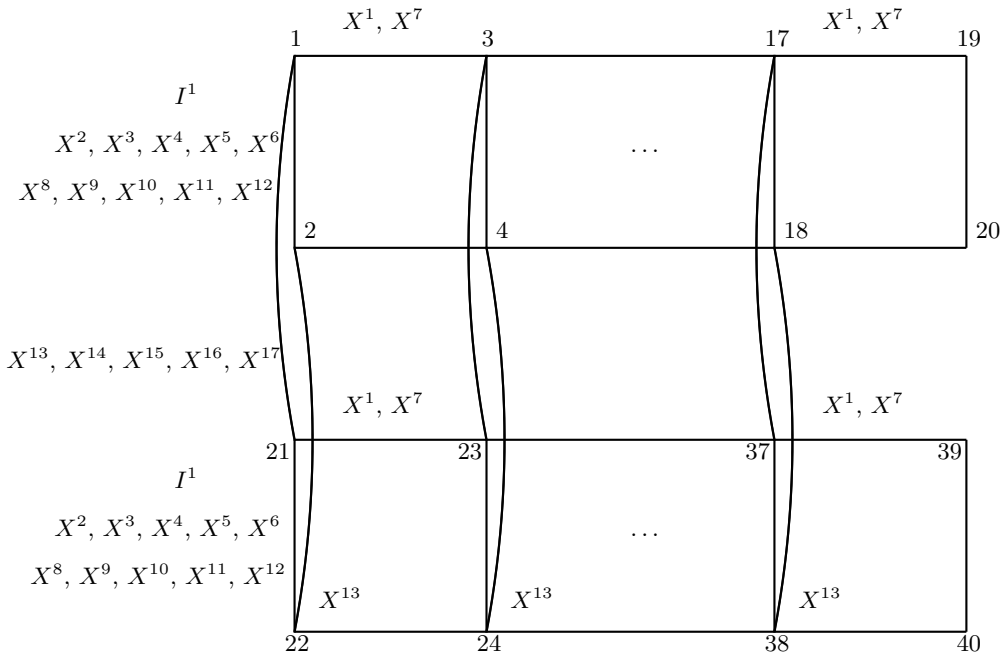

Fig. 4. Example of a multi-rectangle attack on F_6^{18}

of attacks that we have called TWO (for 2-point attacks) and "Multi-Rectangle attacks". We have shown that sometimes TWO attacks are the best, and sometimes it is SQUARE, R1, R2, R3, R4 or Multi-Rectangle attacks, depending of the choices of d and k. For example, for very small values of d, TWO attacks are the best. Multi-Rectangle attacks seem to be very promising from a theoretical point of view. For example, we may attack much more than $3k-1$ rounds with a complexity strictly lower than 2^{kn}, and we may attack F_k^{2k} with a complexity better than with rectangle attacks. However the precise properties of Multi-Rectangle attacks are not yet known since these attacks are still under investigation.

In conclusion, there are much more possibilities for generic attacks on unbalanced Feistel schemes with expanding functions than with other Feistel schemes (classical or with contracting functions). So these constructions must be designed with great care and with sufficiently many rounds. However, if sufficiently many rounds are used, these schemes are very interesting since the memory needed to store the functions is much smaller compared with other generic Feistel schemes.

More examples and more simulations can be found in the extended version of this paper.

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.

References

1. William Aiello and Ramarathnam Venkatesan. Foiling Birthday Attacks in Length-Doubling Transformations - Benes: A Non-Reversible Alternative to Feistel. In Ueli M. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 307–320. Springer-Verlag, 1996.
2. Ross J. Anderson and Eli Biham. Two Practical and Provably Secure Block Ciphers: BEARS and LION. In Dieter Gollman, editor, *Fast Software Encryption*, volume 1039 of *Lecture Notes in Computer Science*, pages 113–120. Springer-Verlag, 1996.
3. Don Coppersmith. Another Birthday Attack. In Hugh C. Williams, editor, *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 14–17. Springer-Verlag, 1985.
4. Don Coppersmith. Luby-Rackoff: Four rounds is not enough. Technical Report RC20674, IBM Research Report, December 1996.
5. Marc Girault, Robert Cohen, and Mireille Campana. A Generalized Birthday Attack. In C. G. Gnther, editor, *Advances in Cryptology – EUROCRYPT '88*, volume 330 of *Lecture Notes in Computer Science*, pages 129–156. Springer-Verlag, 1988.
6. Charanjit S. Jutla. Generalized Birthday Attacks on Unbalanced Feistel Networks. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 186–199. Springer-Verlag, 1998.
7. Lars R. Knudsen. DEAL - A 128-bit Block Cipher. Technical Report 151, University of Bergen, Department of Informatics, Norway, february 1998.
8. Lars R. Knudsen, Xuejia Lai, and Bart Preneel. Attacks on Fast Double Block Length Hash Functions. *J. Cryptology*, 11(1):59–72, 1998.
9. Lars R. Knudsen and Vincent Rijmen. On the Decorrelated Fast Cipher (DFC) and Its Theory. In Lars R. Knudsen, editor, *Fast Software Encrytion – FSE '99*, volume 1636 of *Lecture Notes in Computer Science*, pages 81–94. Springer-Verlag, 1999.
10. Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
11. Moni Naor and Omer Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *J. Cryptology*, 12(1):29–66, 1999.
12. Jacques Patarin. New Results on Pseudorandom Permutation Generators Based on the DES Scheme. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 301–312. Springer-Verlag, 1991.
13. Jacques Patarin. Generic Attacks on Feistel Schemes. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 222–238. Springer-Verlag, 2001.
14. Jacques Patarin. Security of Random Feistel Schemes with 5 or More Rounds. In Matthew K. Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer-Verlag, 2004.
15. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 396–411. Springer-Verlag, 2006.
16. Bruce Schneier and John Kelsey. Unbalanced Feistel Networks and Block Cipher Design. In Dieter Gollmann, editor, *Fast Software Encrytion – FSE '96*, volume 1039 of *Lecture Notes in Computer Science*, pages 121–144. Springer-Verlag, 1996.

Appeared in Kaoru Kurosawa(Ed.): ASIACRYPT 2007, LNCS 4833,pp. 325–341, 2007.