Differential Attacks on Generalized Feistel Schemes

Valérie Nachef[1],and Emmanuel Volte[1],Jacques Patarin[2]

Department of Mathematics
University of Cergy-Pontoise
CNRS UMR 8088
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
and Université de Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
valerie.nachef@u-cergy.fr
emmanuel.volte@u-cergy.fr
jacques.patarin@prism.uvsq.fr

Abstract. While generic attacks on classical Feistel schemes and unbalanced Feistel schemes have been studied a lot, generic attacks on several generalized Feistel schemes like type-1, type-2 and type-3 and Alternating Feistel schemes, as defined in [6], have not been systematically investigated. This is the aim of this paper. We give our best Known Plaintext Attacks and non-adaptive Chosen Plaintext Attacks on these schemes and we determine the maximum number of rounds that we can attack. It is interesting to have generic attacks since there are well known block cipher networks that use generalized Feistel schemes: CAST-256 (type-1), RC-6 (type-2), MARS (type-3) and BEAR/LION (alternating). Also, Type-1 and Type-2 Feistel schemes are respectively used in the construction of the hash functions *Lesamnta* and $SHAvite - 3_{512}$.

Key words: generalized Feistel schemes, generic attacks on encryption schemes, block ciphers

1 Introduction

Classical Feistel Schemes have been extensively studied since the seminal work of Luby and Rackoff [11]. These schemes allow to construct permutations from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$ by using round functions from n bits to n bits and they are used in DES. When the number of rounds is less than 5, there are attacks with less than 2^{2n} operations: for 5 rounds, an attack with $O(2^n)$ inputs is given in [15, 16] and there are attacks with $\sqrt{2^n}$ inputs for 3 and 4 rounds in [1] and [14]. When the round functions are permutations, attacks are studied in [9, 10, 20]. We define generalized Feistel schemes as Feistel-like ciphers as follows: the input belongs to $\{0,1\}^{kn}$ and we apply different kinds of round functions on some parts of the input in order to construct permutations from kn bits to kn bits.
When the rounds functions are from $(k-1)n$ bits to n bits, we obtain an Unbalanced Feistel Scheme with Contracting Functions. Attacks on these schemes were studied in [17]. When the round functions are from n bits to $(k-1)n$ bits, we have Unbalanced Feistel Schemes with Expanding Functions. Attacks on these Schemes are given in [8, 18, 19, 21]. Alternating Feistel Schemes alternate between contracting and expanding steps. They are described in [2] and are used in the BEAR/LION block cipher. There are also Type-1, Type-2 and Type-3 Feistel Schemes (they are described in Section 2, see also [7, 23]). These schemes are used respectively in the block ciphers CAST-256, RC6 and MARS. In [4], Attacks are given on some particular instances if type-1 and type-2 Feistel schemes. They give attacks on the hash functions $Lesamnta$ and $SHAvite-3_{512}$ whose construction is based on type-1 and type-2 Feistel schemes. Some attacks on instances of generalized Feistel schemes are also given in [3]
Important security results have been obtained for most of these schemes. For classical Feistel schemes the different results are given in [6, 16, 13], unbalanced Feistel schemes with contracting functions have been studied in [6, 12, 13, 22] and for unbalanced Feistel Schemes with expanding functions, type-1, type-2, type-3 Feistel Schemes, the results are in [6].
This paper is devoted to the study of generic attacks on type-1, type-2, type-3 and alternating generalized Feistel schemes. By generic attacks, we mean attacks that are valid for most round functions. Our attacks will be differential attacks. While security results are given in [6], attacks on these schemes have not been performed so far (except for some very particular instances of the round functions, see [4] for example). We provide Known Plaintext Attacks (KPA) and non-adaptive Chosen Plaintext Attacks (CPA-1). For each kind of scheme we will give the maximum number of rounds that we can attack in KPA and CPA-1 and we will describe our best attacks. We only give CPA-1 attacks with a complexity less or equal to $2^{(k-1)n}$, that is why the maximum number of rounds attacked is higher with the KPA. We show that for type-1 Feistel schemes, we can attack k^2+2k-2 in KPA and k^2+k-1 in CPA-1. For type-2 (resp. type-3) Feistel schemes we give attacks up to $2k+2$ (resp. $k+\frac{k}{2}+1$ for k even, $k+\frac{k-1}{2}+1$ for k odd) in KPA and $2k+1$ (resp. $k+1$) in CPA-1. For Alternating Feistel Schemes, we attack up to $3k$ rounds in KPA and $3k-2$ rounds in CPA-1. We also provide the complexities of attacks on intermediate rounds.

The paper is organized as follows. In Section 2, we give the notation and define type-1, type-2, type-3 and alternating Feistel schemes. Section 3 is devoted to an overview of the attacks. In Section 4 we detail the attacks. For type-1 Feistel schemes, we also provide results of simulations. In the Appendices, we give an example of computations of the variance, needed to get the complexity of our attacks.

2 Notation - Definitions of the Schemes

Fig. 1. Round one for Feistel schemes type-1 and type-2

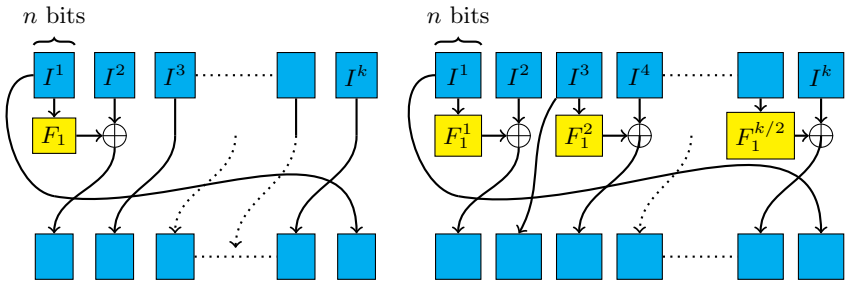
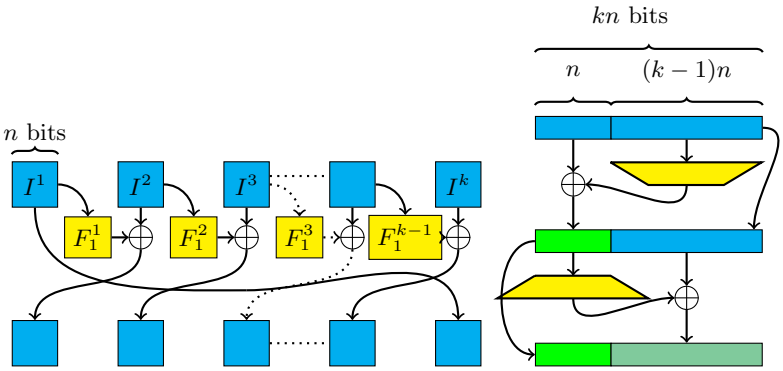


Fig. 2. Round one for type-3 Feistel Scheme and first two rounds of Alternating Feistel Scheme



The input is always denoted by $[I^1, I^2, \ldots, I^k]$ and the output by $[S^1, S^2, \ldots, S^k]$ where each I^s, S^s is an element of $\{0,1\}^n$. When we have m messages, $I^s(i)$ represents part s of the input of message number i. The same notation is used for the outputs. We will give differential attacks, i.e. attacks where we study

how differences on pairs of input variables will propagate following a differential path, and give relations between pairs of input/output variables. d denotes the number of rounds. We now define our schemes.

1. *Type-1 Feistel Schemes (Fig. 1)*
   After one round, the output is given by $[I^2 \oplus F_1(I^1), I^3, I^4, \ldots, I^k, I^1]$ where F_1 is a function from n bits to n bits.
2. *Type-2 Feistel Schemes (Fig. 1)*
   Here k is even and we set $k = 2\ell$. After one round, the output is given by $[I^2 \oplus F_1^1(I^1), I^3, I^4 \oplus F_1^2(I^3), \ldots, I^{2\ell} \oplus F_1^\ell(I^{2\ell-1}), I^1]$ where each F_1^s, $1 \leq s \leq \ell$ is a function from n bits to n bits.
3. *Type-3 Feistel Schemes (Fig. 2)*
   After one round, the output is given by $[I^2 \oplus F_1^1(I^1), I^3 \oplus F_1^2(I^2), I^4 \oplus F_1^3(I^3), \ldots, I^k \oplus F_1^{k-1}(I^{k-1}), I^1]$ where each F_1^s, $1 \leq s \leq k-1$ is a function from n bits to n bits.
4. *Alternating Feistel Schemes (Fig. 2)*
   On the input $[I^1, I^2, \ldots, I^k]$, for the first round, we apply a contracting round, i.e. we use a function F_1 from $(k-1)n$ bits to n bits and the output is given by $[I^1 \oplus F_1([I^2, \ldots, I^k]), I^2, \ldots, I^k]$. Then for the second round, we apply an expanding round, i.e. we use a function $G_2 = (G_2^1, G_2^2, \ldots, G_2^k)$ where each G_2^s is a function from n bits to n bits. We set $X_1 = I^1 \oplus F_1([I^2, \ldots, I^k])$ and then the output after the second round is given by $[X_1, I^2 \oplus G_2^1(X_1), \ldots, I^k \oplus G_2^k(X_1)]$. X_1 is called an internal variable. After 2 rounds, we have new internal variables. Then we alternate contracting rounds and expanding rounds. We can also start with an expanding round. In this paper, we will always begin with a contracting round.

We now explain the differential notation. We use plaintext/ciphertexts pairs. In KPA, on the input variables, suppose we set $[\mathbf{0}, \mathbf{0}, \Delta_0^3, \Delta_0^4, \ldots, \Delta_0^k]$, this means that the pair of messages (i, j) satisfies $I^1(i) = I^1(j)$, $I^2(i) = I^2(j)$, and $I^s(i) \oplus I^s(j) = \Delta_0^s$, $3 \leq s \leq k$. In CPA-1, the same notation means that we choose I^1 and I^2 to be constant. We want that the relations between the input variables propagate. Thus we will impose conditions on the internal variables for some round. When we impose conditions on the internal variables in order to get a differential path, we use the notation $\boxed{0}$ to mean that the corresponding internal variables are equal in messages i and j.

3 Overview of the attacks

We present attacks that allow us to distinguish a permutation computed by the scheme from a random permutation. A permutation computed from an alternating Feistel scheme will be named an alternating permutation. We use the same convention for other schemes. Depending on the number of rounds, it is possible to find some relations between the input and output variables. These relations hold conditionally to equalities of some internal variables due

to the structure of the Feistel scheme. Our attacks consist in using m plaintext/ciphertexts pairs and in counting the number $\mathcal{N}$ of couples of these pairs that satisfy the relations between the input and output variables. We then compare $\mathcal{N}_{scheme}$, the number of such couples we obtain with a generalized scheme, with $\mathcal{N}_{perm}$, the corresponding number for a random permutation. The attack is successful, i.e. we are able to distinguish a permutation generated by a generalized Feistel scheme from a random permutation if the difference $|E(\mathcal{N}_{scheme}) - E(\mathcal{N}_{perm})|$ is larger than both standard deviations $\sigma_{\mathcal{N}_{perm}}$ and $\sigma_{\mathcal{N}_{scheme}}$, 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 $\sigma_{\mathcal{N}_{perm}}$ and $\sigma_{\mathcal{N}_{scheme}}$, we will use this well-known formula (see [5], p.97), that we will call the "Covariance Formula": if $x_1, \dots x_n$ are random variables, then if V represents the variance, we have $V(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} V(x_i) + 2\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\big[E(x_i, x_j) - E(x_i)E(x_j)\big]$. These kind of computations are also performed in [17].

4 Best attacks on the schemes

For each scheme, we give examples of attacks and describe more precisely KPA and CPA-1 that allow to attack the maximum number of rounds. We always suppose that $k \geq 3$.

4.1 Type-1 Feistel Schemes

For 1 to $k-1$ rounds, one message is enough, since after t rounds, $1 \leq t \leq k-1$, we have $S^{k-t+1} = I^1$. This condition is satisfied with probability 1 with a type-1 Feistel scheme and with probability $\frac{1}{2^n}$ when we deal with a random permutation. Thus with one message we can distinguish a type-1 Feistel scheme from a random permutation in KPA and CPA-1.
In Table 1 (left part), we give the general pattern of KPA.

The conditions after $pk-2$ rounds ($p \geq 3$) are given by

$$(2)\ \begin{cases} S^2(i) = S^2(j) \\ I^1(i) \oplus I^1(j) = S^3(i) \oplus S^3(j) \end{cases}.$$

We count the number of indices (i, j) such that these conditions are satisfied. Let $\mathcal{N}_{perm}$ (resp. $\mathcal{N}_{scheme}$) be the number obtained with a random permutation (resp. with a scheme). With a random permutation, these conditions appear at random and we compute the mean value we obtain $E(\mathcal{N}_{perm}) \simeq \frac{m^2}{2^{2n}}$ and $E(\mathcal{N}_{scheme}) \simeq \frac{m^2}{2^{2n}} + \frac{m^2}{2^{(p-1)n}}$. The standard deviations satisfy $\sigma(\mathcal{N}_{perm}) \simeq \sqrt{E(\mathcal{N}_{perm})}$ and $\sigma(\mathcal{N}_{scheme}) \simeq \sqrt{E(\mathcal{N}_{scheme})} \simeq \sqrt{E(\mathcal{N}_{perm})}$ when $p \geq 4$. This means that we can distinguish between a random permutation and an Type-1 Feistel scheme as soon as $\frac{m^2}{2^{(p-1)n}} \geq \frac{m}{2^n}$. This gives the condition $m \geq 2^{(p-2)n}$. Since the maximum number of messages is 2^{kn}, these attacks work for $p-2 \leq k$ and then with $p = k+2$, we can attack up to $(k+2)k - 2 = k^2 + 2k - 2$ rounds.

Table 1. KPA and CPA-1 on type-1 Feistel Schemes

round	Δ_0^1	Δ_0^2	Δ_0^3	...	Δ_0^{k-1}	Δ_0^k
1				...		Δ_0^1
2				...	Δ_0^1	
⋮						
$k-1$	$\boxed{0}$	Δ_0^1		...		
k	Δ_0^1			...		0
$k+1$				...		Δ_0^1
⋮						
$pk-2$		0	Δ_0^1	...		
$pk-1$	$\boxed{0}$	Δ_0^1		...		
pk	Δ_0^1			...		0
⋮						
$(p+1)k-2$		0	Δ_0^1	...		

round	**0**	Δ_0^2	Δ_0^3	...	Δ_0^{k-1}	Δ_0^k
1	Δ_0^2	Δ_0^3		...		0
2				...	0	Δ_0^2
⋮						
$k-1$		0	Δ_0^2	...		
k	$\boxed{0}$	Δ_0^2		...		
$k+1$	Δ_0^2			...	0	
$k+2$				...	0	Δ_0^2
⋮						
$pk-1$		0	Δ_0^2	...		
pk	$\boxed{0}$	Δ_0^2		...		
⋮						
$(p+1)k-1$		0	Δ_0^2	...		

In CPA-1, we know that for 1 to $k-1$ rounds, one message is enough. For k to $2k-1$ rounds, we have a CPA-1 with 2 messages such that $\forall s, 1 \leq s \leq k-1$, $I^s(1) = I^s(2)$. Then with a type-1 Feistel scheme, we obtain with probability 1 that at round t, $S^{2k-t}(1) \oplus S^{2k-t}(2) = I^k(1) \oplus I^k(2)$. With a random permutation, the probability to obtain this equality is $\frac{1}{2^n}$. For each round, we have to consider different conditions on the input variables. We give now CPA-1 on $pk-1$ rounds. As shown in Table 1 (right part), we choose the messages such that I^1 takes only one value for all messages. The conditions after $pk-1$ rounds are given by (3) $\begin{cases} S^2(i) = S^2(j) \\ I^2(i) \oplus I^2(j) = S^3(i) \oplus S^3(j) \end{cases}$. We count the number of indices (i,j) such that these conditions are satisfied. In the appendices, we show that for this CPA-1, we have for a random permutation $E(\mathcal{N}_{perm}) \simeq \frac{m^2}{2^{2n}}$ and for a scheme $E(\mathcal{N}_{scheme}) \simeq \frac{m^2}{2^{2n}} + \frac{m^2}{2^{(p-1)n}}$. Using the computation of the variances (see the appendices), we can distinguish between a random permutation and a scheme as long as $\frac{m^2}{2^{(p-1)n}} \geq \frac{m}{2^n}$. This gives the condition $m \geq 2^{(p-2)n}$. Since the maximum number of messages is $2^{(k-1)n}$, these attacks work for $p-2 \leq k-1$ and then with $p = k+1$, we can attack up to $(k+1)k-1 = k^2+k-1$ rounds. Table 3 summarizes the complexities for type-1 Feistel schemes. We also give the results of our simulations in Table 2.

4.2 Type-2 Feistel Schemes

Table 4 represents KPA.

We begin with a KPA on $2k+2 = 2(k+1)$ rounds where the conditions are: (4) $\begin{cases} I^1(i) = I^1(j) \\ I^2(i) \oplus I^2(j) = S^{2\ell}(i) \oplus S^{2\ell}(j) \end{cases}$. We count the number of indices (i,j) such that these conditions are satisfied. For a random permutation this is about $\frac{m^2}{2^{2n}}$.

Table 2. Experimental results for CPA-1 against type-1 Feistel Scheme with k^2+k-1 rounds

k	n	% of success -% of false alarm	# iteration
6	2	67%	10000
8	2	66,5%	10000
9	2	66%	10000
6	4	95%	10000
8	4	96%	1000
4	6	99,5%	10000

Table 3. Complexities of the attacks on type-1 Feistel Schemes

d	KPA
$1 \to k-1$	1
$k \to 2k-1$	$2^{n/2}$
$2k \to 3k-2$	2^n
$\vdots$	
$pk-2$	$2^{(p-2)n}$
$pk-1$	$2^{(p-3/2)n}$
pk	
$\vdots$	$2^{(p-1)n}$
$(p+1)k-2$	
$\vdots$	
k^2+2k-2	2^{kn}

d	CPA-1	d	CPA-1
1			
$\vdots$	1	$\vdots$	
$k-1$			
k		$pk-(p-2)$	
$\vdots$	2	$\vdots$	$2^{(p-2)n}$
$2k-2$		$(p+1)k-p$	
$2k-1$			
$\vdots$	$2^{n/2}$	$\vdots$	
$3k-2$			
$3k-1$		k^2+k	
$\vdots$	2^n	$\vdots$	$2^{(k-1)n}$
$4k-3$		k^2+k-1	

For a scheme, we obtain $\frac{m^2}{2^{2n}} + \frac{m^2}{2^{(k+1)n}}$. As previously, the computation of the standard deviations shows that we can distinguish between a random permutation and a scheme as long as $\frac{m^2}{2^{(k+1)n}} \geq \frac{m}{2^n}$. This gives the condition $m \geq 2^{kn}$, which is the maximum number of messages. More generally, after $2p$ rounds, $p \geq 3$, we use the same attack with the conditions:

(5) $\begin{cases} I^1(i) = I^1(j) \\ I^2(i) \oplus I^2(j) = S^s(i) \oplus S^s(j) \end{cases}$. where t is defined by $s = k - 2(p-1)$ if $1 \leq p \leq \ell$

$s = k - 2(u-1)$ if $p = k + 2u$, $1 \leq u \leq \ell$

$s = 2k - 2(u-1)$ if $p = 2k + 2u$, $1 \leq u \leq 2$

We count the number of indices (i, j) such that these conditions are satisfied. For a random permutation this is about $\frac{m^2}{2^{2n}}$. For a scheme, we obtain $\frac{m^2}{2^{2n}} + \frac{m^2}{2^{pn}}$. Again we can distinguish between a random permutation and a scheme as long as $\frac{m^2}{2^{pn}} \geq \frac{m}{2^n}$ and we obtain that the number of messages is $2^{(p-1)n}$. Thus for $p = k+1$, we have the maximum number of messages.

Table 4. KPA on type-2 Feistel Schemes

round	**0**	Δ_0^2	Δ_0^3	Δ_0^4	...	$\Delta_0^{2\ell-3}$	$\Delta_0^{2\ell-2}$	$\Delta_0^{2\ell-1}$	$\Delta_0^{2\ell}$
1	Δ_0^2				...				0
2					...			$\boxed{0}$	Δ_0^2
3					...		0	Δ_0^2	
$\vdots$									
$k-1$		0	Δ_0^2		...				
k	$\boxed{0}$	Δ_0^2			...				
$k+1$	Δ_0^2				...				0
$k+2$					...			$\boxed{0}$	Δ_0^2
$\vdots$									
$2k-1$		0	Δ_0^2		...				
$2k$	$\boxed{0}$	Δ_0^2			...				
$2k+1$	Δ_0^2				...				0
$2k+2$					...				Δ_0^2

After $2p+1$ rounds, $p \geq 3$,
we have the conditions: (6) $\begin{cases} I^1(i) = I^1(j) \\ I^2(i) \oplus I^2(j) = S^t(i) \oplus S^t(j) \\ S^{t-1}(i) = S^{t-1}(j) \end{cases}$, where t is defined by $t = k - 2(p-1) - 1$ if $0 \leq p \leq \ell - 1$
$t = k - 2(u-1) - 1$ if $p = k + 2u + 1$, $0 \leq u \leq \ell - 1$
$t = 2k - 2(u-1) - 1$ if $p = 2k + 2u + 1$, $0 \leq u \leq 2$

We count the number of indices (i, j) such that this condition is satisfied. For a random permutation this is about $\frac{m^2}{2^{3n}}$. For a scheme, we obtain $\frac{m^2}{2^{3n}} + \frac{m^2}{2^{(p+1)n}}$. The variance is about the square root of the mean value. Thus we can distinguish between a random permutation and a scheme as long as $\frac{m^2}{2^{(p+1)n}} \geq \frac{m}{2^{3n/2}}$ and we obtain that the number of messages is $2^{(p-1/2)n}$.

For CPA-1, we can impose conditions on a given number of input variables. We give in Table 5 an example of an attack for which we consider messages where I^1, I^2, I^3 are given constant values. Then we will generalize.

The conditions after $2k-1$ rounds are given by
(7) $\begin{cases} S^4(i) = S^4(j) \\ I^4(i) \oplus I^4(j) = S^5(i) \oplus S^5(j) \end{cases}$. We count the number of indices (i, j) such that these conditions are satisfied. For a random permutation this is about $\frac{m^2}{2^{2n}}$. For a scheme, we obtain $\frac{m^2}{2^{2n}} + \frac{m^2}{2^{(k-2)n}}$. Since again the variance is about the square root of the mean value, we can distinguish between a random permutation and a scheme as long as $\frac{m^2}{2^{(k-2)n}} \geq \frac{m}{2^n}$. This gives the condition $m \geq 2^{(k-3)n}$. Since the maximum number of messages is $2^{(k-3)n}$, we get a CPA-1 for $2k-1$ rounds. For round $2k-2$, we can perform the following attack: we do not impose the condition on the fifth coordinate (see Table 5) and then we count the number of

Table 5. CPA-1 on type-2 Feistel Schemes

round	**0**	**0**	**0**	Δ_0^4	Δ_0^5	Δ_0^6	...	Δ_0^{k-3}	Δ_0^{k-2}	Δ_0^{k-1}	Δ_0^k
1	0	0	Δ_0^4				...				0
2	0	Δ_0^4					...				0
3	Δ_0^4						...				0
4							...			$\boxed{0}$	Δ_0^4
5							...		0	Δ_0^4	
$\vdots$											
k			$\boxed{0}$	Δ_0^4			...				
$k+1$		0	Δ_0^4				...				
$k+2$	$\boxed{0}$	Δ_0^4					...				
$k+3$	Δ_0^4						...				0
$\vdots$											
$2k-2$					$\boxed{0}$	Δ_0^4	...				
$2k-1$				0	Δ_0^2		...				

(i,j) such that $(8)\, S^6(i) = S^6(j)$. For a random permutation this is about $\frac{m^2}{2^n}$. For a scheme, we obtain $\frac{m^2}{2^{2n}} + \frac{m^2}{2^{(k-3)n}}$. The variance is about the square root of the mean value. Thus we can distinguish between a random permutation and a scheme as long as $\frac{m^2}{2^{(k-3)n}} \geq \frac{m}{2^{n/2}}$. This gives the condition $m \geq 2^{(k-3-1/2)n}$. Since the maximum number of messages is $2^{(k-3)n}$, we get a CPA-1 for $2k-2$ rounds. More generally, if we suppose that for the input variables, we have $I^1, \ldots, I^p$ are constant ($p \leq k-1$), we can perform the same kind of attacks. It is easy to check that we can attack up to $2k-p+2$ rounds and we need exactly $2^{(k-p)n}$. In order to get the best CPA-1 for each round, we will change the conditions on the input variables. For example, for $k+1$, $k+2$ and $k+3$ rounds, we choose $I^1, \ldots I^{k-1}$ to be constant, then we will have $I^1, \ldots I^{k-2}$ constant, and so on.

Table 6 summarizes the complexities for type-2 Feistel schemes.

4.3 Type-3 Feistel Schemes

We will present our attacks when $k = 2\ell$ is even and give only the results for k odd. We begin with KPA. For one round, we need one message, we just have to check if $I^1 = S^{2\ell}$. With a random permutation, this happens with probability $\frac{1}{2^n}$ and with a scheme with probability one. Suppose we want to attack d rounds with $2 \leq d \leq k$. We wait until we have 2 messages such that $I^1(1) = I^1(2), \ldots, I^{d-1}(1) = I^{d-1}(2)$. Then we test if $I^{d-1}(1) \oplus I^{d-1}(2) = S^k(1) \oplus S^k(2)$. With a random permutation, this happens with probability $\frac{1}{2^n}$ and with a scheme with probability one. Moreover, from the birthday paradox, if we have $2^{\frac{(d-1)n}{2}}$ messages, we get 2 messages with the given conditions with a high probability. We give in Table 7 (left part) an attack on $k+4$ rounds, where we suppose that $4 \leq \ell + 1$.

Table 6. Complexities of the a attacks on type-2 Feistel Schemes

d	KPA
1	1
2	$2^{n/2}$
3	$2^{n/2}$
$\vdots$	
$2p$	$2^{(p-1)n}$
$2p+1$	$2^{(p-1/2)n}$
$\vdots$	
$2k$	$2^{(k-1)n}$
$2k+1$	$2^{(k-1/2)n}$
$2k+2$	2^{kn}

d	CPA-1
1	1
2	
$\vdots$	2
k	
$k+1$	$2^{n/2}$
$k+2$	$2^{n/2}$
$\vdots$	
$k+v$	$2^{(v-2)n}$
$\vdots$	
$2k+1$	$2^{(k-1)n}$

Table 7. KPA and CPA-1 on type-3 Feistel Schemes

round	**0**	...	**0**	**0**	**0**	**0**	Δ_0^k
1	0	...	0	0	0	Δ_0^k	0
2	0	..	0	0	Δ_0^k		0
3	0	..	0	Δ_0^k			0
$\vdots$							
$k-1$	Δ_0^k	...					0
k		...	$\boxed{0}$	$\boxed{0}$	$\boxed{0}$	$\boxed{0}$	Δ_0^k
$k+1$		...	0	0	0	Δ_0^k	
$k+2$		...	0	0	Δ_0^k		
$k+3$		...	0	Δ_0^k			
$k+4$		...	Δ_0^k				

round	**0**	**0**	...	**0**	**0**	**0**	**0**	Δ_0^k
1	0	0	...	0	0	0	Δ_0^k	0
2	0	0	..	0	0	Δ_0^k		0
3	0	0	..	0	Δ_0^k			0
$\vdots$								
$k-1$	Δ_0^k		...					0
k			...				$\boxed{0}$	Δ_0^k
$k+1$			...	0	0	0	Δ_0^k	

The conditions are given by (9) $\begin{cases} I^1(i) = I^1(j) \\ I^2(i) = I^2(j) \\ \vdots \\ I^{k-1}(i) = I^{k-1}(j) \\ I^k(i) \oplus I^k(j) = S^{k-5}(i) \oplus S^{k-5}(j) \end{cases}$

We count the number of indices (i, j) such that these conditions are satisfied. For a random permutation this is about $\frac{m^2}{2^{kn}}$. For a scheme, we obtain $\frac{m^2}{2^{kn}} + \frac{m^2}{2^{(k+3)n}}$. We can distinguish between a random permutation and a scheme as long as $\frac{m^2}{2^{(k+3)n}} \geq \frac{m}{2^{ln}}$. This gives $m \geq 2^{(l+3)n}$. We can perform the same kind of attack for $k+t$ rounds, with $t \leq \ell + 1$. We can attack up to $k + \ell + 1$ rounds. For $k + \ell + 1$, we need the maximum number of messages i.e. 2^{kn}.

For CPA-1, it is easy to see that after one round, one message is sufficient. We just have to check if $S^k = I^1$. For 2 rounds, we choose 2 messages such that $I^1(1) = I^1(2)$ and we check if $S^k(1) \oplus S^k(2) = I^2(1) \oplus I^2(2)$. With a random permutation this happens with probability $\frac{1}{2^n}$, but with a scheme, the probability is one. Thus

we can distinguish between the two permutations with only 2 messages. More generally, for d rounds with $d \leq k$, we choose 2 messages such that $I^s(1) = I^s(2)$ for $1 \leq s \leq k-1$ and then we check if $S^k(1) \oplus S^k(2) = I^d(1) \oplus I^d(2)$. With a random permutation this happens with probability $\frac{1}{2^n}$, but with a scheme, the probability is one. Thus we can distinguish between the two permutations with only 2 messages. We can attack up to k rounds. For $k+1$ rounds, we have the following CPA-1 described in Table 7 (right part). We choose m messages such that $I^1, I^2, \ldots, I^{k-1}$ have a constant value. We count the number of (i, j) such that $I^k(i) \oplus I^k(j) = S^{k-1}(i) \oplus S^{k-1}(j)$. For a random permutation this is about $\frac{m^2}{2^n}$. For a scheme, we obtain $\frac{m^2}{2^n} + \frac{m^2}{2^n}$. We can distinguish between a random permutation and a scheme when the number of messages m is about $2^{n/2}$. Table 8 gives KPA complexities for $d \leq k + \ell + 1$ and CPA-1 ones for $d \leq k + 1$.

Table 8. Attacks on type-3 Feistel Schemes

d	KPA, k even	CPA-1, $k = 2\ell$
1	1	1
2	$2^{n/2}$	2
3	2^n	2
$\vdots$		
k	$2^{(k-1)n/2}$	2
$k+1$	$2^{\ell n}$	$2^{n/2}$
$k+2$	$2^{(\ell+1)n}$	
$\vdots$		
$k+t$	$2^{(\ell+t-1)n}$	
$\vdots$		
$k+\ell+1$	2^{kn}	

d	KPA, k odd	CPA-1, $k = 2\ell+1$
1	1	1
2	$2^{n/2}$	2
3	2^n	2
$\vdots$		
k	$2^{(k-1)n/2}$	2
$k+1$	$2^{(\ell+1/2)n}$	$2^{n/2}$
$k+2$	$2^{(\ell+3/2)n}$	
$\vdots$		
$k+t$	$2^{(\ell+t-1/2)n}$	
$\vdots$		
$k+\ell+1$	$2^{(k-1/2)n}$	

4.4 Alternating Feistel Schemes

Here we will describe our best attacks on alternating Feistel schemes. After one round, we have $[I^2, I^3, \ldots, I^k] = [S^2, S^3, \ldots, S^k]$. Thus we choose one message and we check if this condition is satisfied. With a random permutation, this happens with probability $\frac{1}{2^{(k-1)n}}$ and with a scheme the probability is one. Thus with one message we can distinguish a random permutation from a permutation obtained with an alternating scheme. After 2 rounds, in CPA-1, we choose 2 messages such that $\forall s,\ 2 \leq s \leq k,\ I^s(1) = I^s(2)$ and then we check if $I^1(1) \oplus I^1(2) = S^1(1) \oplus S^1(2)$. The probability to have this condition satisfied is $\frac{1}{2^n}$ with a random permutation and 1 with an alternating scheme. We can transform this CPA-1 into a KPA. We generate m messages and from the birthday paradox, when $m \simeq 2^{\frac{(k-1)n}{2}}$ with a good probability, we can find (i, j) such that $\forall s,\ 2 \leq s \leq k,\ I^s(i) = I^s(j)$ and then we test if $I^1(i) \oplus I^1(j) = S^1(i) \oplus S^1(j)$. But there

are better KPA, as we can see now. We have the following CPA-1, described in table 9 (right part), where Δ denotes $[\Delta_0^2, \Delta_0^3, \Delta_0^4, \ldots, \Delta_0^k]$.

At each odd round, the probability to have the first zero is $1/2^n$. So we have the probability of $1/2^{np}$ to have the equalities on the output: $S^2(1) \oplus S^2(2) = I^2(1) \oplus I^2(2)$ and $S^1(1) = S^1(2)$ when we follow the path. But we can also have this equalities without the path. For a random permutation, the probability to have this is equal to $\frac{1}{2^n} \times \frac{1}{2^{(k-1)n}} = \frac{1}{2^{kn}}$. So the number of such pair of points will be greater for an alternating scheme when $p \leq k$, i.e. $d = 2p$. The number of messages is $m = 2^{np/2} = 2^{nd/4}$. This is a CPA-1 complexity of course, but we can transform slightly the attack in order to have the same complexity in KPA and CPA-1, as shown in Table 9 (left part). For example,

Table 9. KPA and CPA-1 on Alternating Feistel Schemes

round	Δ_1	Δ
1	$\boxed{0}$	Δ
2	0	Δ
3	$\boxed{0}$	Δ
4	0	Δ
$\vdots$	$\vdots$	
$2p-1$	$\boxed{0}$	Δ
$2p$	0	Δ

round	$\mathbf{0}$	Δ
1	$\boxed{0}$	Δ
2	0	Δ
3	$\boxed{0}$	Δ
4	0	Δ
$\vdots$	$\vdots$	
$2p-1$	$\boxed{0}$	Δ
$2p$	0	Δ

we obtain here, after 2 rounds a KPA with $2^{\frac{n}{2}}$ messages (notice that the CPA-1 complexity of the previous attack was better). These attacks are valid until we reach $2k$ rounds. We explain now how to attack more rounds if we use the covariance formula as mentioned in Section 3. We keep the same kind of attacks. After $2p$ rounds with $p \geq k$, in KPA, we count the number of (i, j) such that

$$(1) \begin{cases} S^1(i) = S^1(j) \\ \forall s,\ 2 \leq s \leq k,\ I^s(i) \oplus I^s(j) = S^s(i) \oplus S^s(j) \end{cases}$$

Let $\mathcal{N}_{perm}$ (resp. $\mathcal{N}_{scheme}$) be the number obtained with a random permutation (resp. with a scheme). With a random permutation, these conditions appear at random. Thus $E(\mathcal{N}_{perm}) \simeq \frac{m^2}{2^{kn}}$. For a scheme, we obtain $E(\mathcal{N}_{scheme}) = \frac{m(m-1)}{2}\left(\frac{1}{2^{kn}} + \frac{1}{2^{pn}} + \frac{1}{2^{(k+p-1)n}}\right) \simeq \frac{m^2}{2^{kn}} + \frac{m^2}{2^{pn}}$. As usual, the standard deviations satisfy $\sigma(\mathcal{N}_{perm}) \simeq \sqrt{E(\mathcal{N}_{perm})}$ and $\sigma(\mathcal{N}_{scheme}) \simeq \sqrt{E(\mathcal{N}_{scheme})} \simeq \sqrt{E(\mathcal{N}_{perm})}$. This means that we can distinguish between a random permutation and an alternating scheme as soon as $\frac{m^2}{2^{pn}} \geq \frac{m}{2^{kn/2}}$, i.e. $m \geq 2^{(p-\frac{k}{2})n}$. Thus we obtain a KPA with about $2^{(p-\frac{k}{2})n}$ messages. Since the number of messages cannot exceed 2^{kn}, we obtain the condition $p \leq 3k/2$. If k is even, then $p = 3k/2$ and the number of rounds is $3k$. If k is odd, then $p = \frac{k-1}{2}$ and we can attack $3k-1$ rounds. In CPA-1, since we impose the condition that for all messages, I^1 is constant, we can generate at most $2^{(k-1)n}$ messages. Thus we can attack $3k-2$ rounds for k even and $3k-3$ rounds for k odd. Here we have given the complexity for even

rounds. If we want to attack an odd round, for example round $2p-1$, the last condition on the internal variable is imposed at round $2p-3$ and then we will count the number of (i,j) such that $\forall s,\ 2 \leq s \leq k,\ I^s(i) \oplus I^s(j) = S^s(i) \oplus S^s(j)$. By computing the mean values and the standard deviations, we obtain that $m \simeq 2^{(p-\frac{(k-1)}{2})n}$. We now summarize all the complexities in Table 10.

Table 10. Complexities of the attacks on Alternating Feistel Schemes

d	KPA, k even	CPA-1, k even	KPA, k odd	CPA-1, k odd
1	1	1	1	
2	$2^{n/2}$	2	$2^{n/2}$	2
3	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
$\vdots$				
$2p-1,\ 2 \leq p \leq k$	$2^{\frac{(p-1)n}{2}}$	$2^{\frac{(p-1)n}{2}}$	$2^{\frac{(p-1)n}{2}}$	$2^{\frac{(p-1)n}{2}}$
$2p,\ 2 \leq p \leq k$	$2^{\frac{pn}{2}}$	$2^{\frac{pn}{2}}$	$2^{\frac{pn}{2}}$	$2^{\frac{pn}{2}}$
$\vdots$				
$2k$	$2^{\frac{kn}{2}}$	$2^{\frac{kn}{2}}$	$2^{\frac{kn}{2}}$	$2^{\frac{kn}{2}}$
$\vdots$				
$2p-1,\ p \geq k$	$2^{(p-\frac{(k-1)}{2})n}$	$2^{(p-\frac{(k-1)}{2})n}$	$2^{(p-\frac{(k-1)}{2})n}$	$2^{(p-\frac{(k-1)}{2})n}$
$2p,\ p \geq k$	$2^{(p-\frac{k}{2})n}$	$2^{(p-\frac{k}{2})n}$	$2^{(p-\frac{k}{2})n}$	$2^{(p-\frac{k}{2})n}$
$\vdots$				
$3k-3$	$2^{(k-3/2)n}$	$2^{(k-3/2)n}$	$2^{(k-1)n}$	$2^{(k-1)n}$
$3k-2$	$2^{(k-1)n}$	$2^{(k-1)n}$	$2^{(k-1/2)n}$	
$3k-1$	$2^{(k-1/2)n}$		2^{kn}	
$3k$	2^{kn}			

5 Conclusion

In this paper, we have given our best differential generic attacks (KPA and CPA-1) on different kinds of generalized Feistel Schemes: alternating, type-1, type-2 and type-3 Feistel schemes. For example, we show in this paper that type-1 Feistel Scheme can be attacked up to 22 rounds in KPA when $k = 4$. In [4] for very specific function only 21 rounds are attacked with an integral attack. Since these schemes are used in well known block ciphers, it is interesting to find the maximum number of rounds that we can attack. We also gave the complexity of attacks on intermediate rounds. In our attacks, the computations of the mean values and the standard deviations are very useful. We generally stop attacking schemes, when we need the maximum number of possible messages to perform the attack. A way to overcome this problem is to attack permutation generators instead of a single permutation.

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: BEAR and LION. In Dieter Gollman, editor, *Fast Software Encryption*, volume 1039 of *Lecture Notes in Computer Science*, pages 113–120. Springer-Verlag, 1996.
3. Andrey Bogdanov and Vincent Rijmen. Zero-Correlation Linear Cryptanalysis on Block Cipher. *Cryptology ePrint archive: 2011/123: Listing for 2011*.
4. Charles Bouillaguet, Orr Dunkelamn, Gaetan Laurent, and Pierre-Alain Fouque. Attacks on hash Functions based on Generalized Feistel schemes. Application to Reduced-Round *Lesamnta* and $SHAvite - 3_{512}$. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptographyl – SAC '10*, volume 6544 of *Lecture Notes in Computer Science*, pages 18–35. Springer-Verlag, 2010.
5. Paul G.Hoel, Sidney C.Port, and Charles J.Stone. *Introduction to Probability Theory*. Houghton Mifflin Company, 1971.
6. Viet Tung Hoang and Phillip Rogaway. On Generalized Feistel Networks. In Tel Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 613–630. Springer-Verlag, 2110.
7. Subariah Ibrahim and f Mohd Aizaini Mararof. Diffusion Analysis of Scalable Feistel Networks. *World Academy of Science, Engineering and Technology*, 5:98–101, 2005.
8. 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.
9. Lars R. Knudsen. DEAL - A 128-bit Block Cipher. Technical Report 151, University of Bergen, Department of Informatics, Norway, february 1998.
10. 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.
11. Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
12. Moni Naor and Omer Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *J. Cryptology*, 12(1):29–66, 1999.
13. Jacques Partarin. Security of balanced and unbalanced Feistel schemes with linear non equalities. *Cryptology ePrint archive: 2010/293: Listing for 2010*.
14. 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.
15. 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.
16. 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.

17. 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.
18. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions. In Kaoru Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 325–341. Springer-Verlag, 2007.
19. 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.
20. Joana Treger and Jacques Patarin. Generic Attacks on Feistel Networks with Internal Permutations. In Bart Preneel, editor, *Progresses in Cryptology – AFRICACRYPT '09*, volume 5580 of *Lecture Notes in Computer Science*, pages 41–59. Springer-Verlag, 2009.
21. Emmanuel Volte, Valérie Nachef, and Jacques Patarin. Improved Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions. In Kaoru Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 94–111. Springer-Verlag, 2007.
22. Aaram Yun, Je Hong Park, and Jooyoung Lee. Lai-Massey Scheme and Quasi-Feistel Networks. *Cryptology ePrint archive: 2007/347: Listing for 2007.*
23. Y. Zhen, T. Matsumoto, and H. Imai. On the Construction of Block Ciphers provably secure and not relying on any unproved Hypotheses. In Gilles Brassard, editor, *Advances in Cryptology – CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 461–480. Springer-Verlag, 1990.

A An example of Computation of the Mean Value and the Variance for Random Permutations

Very often in cryptographic attacks based on the computations of variance V and mean value E we have $V \simeq E$, particularly when we deal with differential attacks. We will prove this precisely here for the CPA-1 given in section 4.1. Similar proofs have also been done for other cases.

First we compute the mean value denoted by $E(\mathcal{N}_{perm})$. We have $\forall i,\ 1 \leq i \leq m,\ I_1(i) = 0$. Here $m \simeq 2^{(p-2)n}$. The inputs are pairwise distinct. Let $\delta_{ij} = 1$ if $(*)$ is satisfied $\delta_{ij} = 0$ otherwise. Then $\mathcal{N}_{perm} = \sum_{i<j} \delta_{ij}$, $E(\mathcal{N}_{perm}) = \sum_{i<j} E(\delta_{ij})$. $E(\delta_{ij}) = Pr_{f \in_R B_{kn}}[S_2(i) = S_2(j) \text{ and } I_2(i) \oplus I_2(j) = S_3(i) \oplus S_3(j)]$
Case 1: $I_2(i) = I_2(j)$. Here $E(\delta_{ij}) = Pr_{f \in_R B_{kn}}[S_2(i) = S_2(j) \text{ and } S_3(i) = S_3(j)]$
$= \frac{2^{(k-2)n}-1}{2^{kn}-1} = \frac{1}{2^{2n}} \times \frac{1-\frac{1}{2^{(k-2)n}}}{1-\frac{1}{2^{kn}}}$
Case 2: $I_2(i) \neq I_2(j)$. Then $E(\delta_{ij}) = Pr_{f \in_R B_{kn}}[S_2(i) = S_2(j) \text{ and } I_2(i) \oplus I_2(j) = S_3(i) \oplus S_3(j)] = \frac{2^{(k-2)n}}{2^{kn}-1} = \frac{1}{2^{2n}} \times \frac{1}{1-\frac{1}{2^{kn}}}$.
Let α be the number of (i,j) such that $I_2(i) = I_2(j)$. Then $E(\mathcal{N}_{perm}) = \alpha\Big(\frac{2^{(k-2)n}-1}{2^{kn}-1}\Big) + \Big(\frac{m(m-1)}{2} - \alpha\Big)\Big(\frac{2^{(k-2)n}}{2^{kn}-1}\Big) = [\frac{m(m-1)}{2 \cdot 2^{2n}} - \frac{\alpha}{2^{kn}}] \times \frac{1}{1-\frac{1}{2^{kn}}}$.
We can assume that $\alpha = \frac{m(m-1)}{2 \cdot 2^n} + 0(\frac{m}{\sqrt{2^n}})$. Then we get

$E(\mathcal{N}_{perm}) = [\frac{m(m-1)}{2\cdot 2^{2n}} - \frac{1}{2^{kn}}\Big(\frac{m(m-1)}{2\cdot 2^n} + 0(\frac{m}{\sqrt{2^n}})\Big)] \times \frac{1}{1-\frac{1}{2^{kn}}} = \frac{m(m-1)}{2\cdot 2^{2n}} \times \frac{1-\frac{1}{2^{(k-1)n}}}{1-\frac{1}{2^{kn}}} + O(\frac{m}{2^{k+\frac{1}{2}}})$. Finally, this gives
$\frac{m(m-1)}{2\cdot 2^{2n}}\Big(1-\frac{1}{2^{(k-1)n}}+\frac{1}{2^{kn}}\Big)+O(\frac{m}{2^{(k+\frac{1}{2})n}}) \leq E(\mathcal{N}_{perm}) \leq \frac{m(m-1)}{2\cdot 2^{2n}}+O(\frac{m}{2^{(k+\frac{1}{2})n}})$. We now gives the main steps in order to compute the standard deviation. We will use the "covariance formula " given in Section 3 in order to compute $V(\mathcal{N}_{perm})$. We have: $V(\delta_{ij}) = E(\delta_{ij}^2) - E(\delta_{ij})^2 = E(\delta_{ij}) - E(\delta_{ij})^2$.

Case 1: $I_2(i) = I_2(j)$. $V(\delta_{ij}) = \frac{1}{2^{2n}} \times \frac{1-\frac{1}{2^{(k-2)n}}}{1-\frac{1}{2^{kn}}} - \Big(\frac{1}{2^{2n}} \times \frac{1-\frac{1}{2^{(k-2)n}}}{1-\frac{1}{2^{kn}}}\Big)^2$. This gives:
$V(\delta_{ij}) = \frac{1}{2^{2n}}\big[1 - \frac{1}{2^{2n}} - \frac{1}{2^{(k-2)n}} + \frac{3}{2^{kn}} - \frac{2}{2^{(k+2)n}} - \frac{2}{2^{(2k-2)n}} + \frac{5}{2^{2kn}} - \frac{3}{2^{(2k+2)n}} - \frac{3}{2^{(3k-2)n}}\Big] + O(\frac{1}{2^{3kn}})$

Case 2: $I_2(i) \neq I_2(j)$. $V(\delta_{ij}) = \frac{1}{2^{2n}} \times \frac{1}{1-\frac{1}{2^{kn}}} - \Big(\frac{1}{2^{2n}} \times \frac{1}{1-\frac{1}{2^{kn}}}\Big)^2$. We obtain
$V(\delta_{ij}) = \frac{1}{2^{2n}}\big[1 - \frac{1}{2^{2n}} + \frac{1}{2^{kn}} - \frac{2}{2^{(k+2)n}} + \frac{1}{2^{2kn}} - \frac{3}{2^{(2k+2)n}}\Big] + O(\frac{1}{2^{3kn}})$.
Since we want to use the covariance formula, we have to evaluate $E(\delta_{ij})E(\delta_{qr})$ and $E(\delta_{ij}\delta_{qr})$. We explain the case where i, j, q, r are pairwise distinct. The case where in $\{i, j, q, r\}$ we have exactly 3 values is similar. The total number of outputs is given by $A = 2^{kn}(2^{kn}-1)(2^{kn}-2)(2^{kn}-3) = 2^{4kn}(1-\frac{6}{2^{kn}}+\frac{11}{2^{2kn}}-\frac{6}{2^{3kn}})$. Then $\frac{1}{A} = \frac{1}{2^{4kn}}\Big(1+\frac{6}{2^{kn}}+\frac{25}{2^{2kn}}+O(\frac{1}{2^{3kn}})\Big)$. We first evaluate $E(\delta_{ij})E(\delta_{qr})$. We have to study several cases:

1. $I_2(i) \neq I_2(j)$ and $I_2(q) \neq I_2(r)$. Then
   $E(\delta_{ij})E(\delta_{qr}) = \frac{1}{2^{4n}}\Big(\frac{1}{1-\frac{1}{2^{kn}}}\Big)^2 = \frac{1}{2^{4n}}(1+\frac{2}{2^{kn}}+\frac{3}{2^{2kn}}+O(\frac{1}{2^{3kn}}))$.
2. ($I_2(i) = I_2(j)$ and $I_2(q) \neq I_2(r)$) or ($I_2(i) \neq I_2(j)$ and $I_2(q) = I_2(r)$). Then
   $E(\delta_{ij})E(\delta_{qr}) = \frac{1}{2^{4n}}\Big(\frac{1-\frac{1}{2^{(k-2)n}}}{(1-\frac{1}{2^{kn}})^2}\Big)$.
   $E(\delta_{ij})E(\delta_{qr}) = \frac{1}{2^{4n}}(1-\frac{1}{2^{(k-2)n}}+\frac{2}{2^{kn}}-\frac{2}{2^{(2k-2)n}}+\frac{3}{2^{2kn}}-\frac{3}{2^{(3k-2)n}}+O(\frac{1}{2^{3kn}}))$.
3. $I_2(i) = I_2(j)$ and $I_2(q) = I_2(r)$. Then $E(\delta_{ij})E(\delta_{qr}) = \frac{1}{2^{4n}} \times \frac{(1-\frac{1}{2^{(k-2)n}})^2}{(1-\frac{1}{2^{kn}})^2}$
   $= \frac{1}{2^{4n}}(1-\frac{2}{2^{(k-2)n}}+\frac{2}{2^{kn}}+\frac{1}{2^{(2k-4)n}}-\frac{4}{2^{(2k-2)n}}+\frac{3}{2^{2kn}}+\frac{2}{2^{(3k-4)n}}-\frac{6}{2^{(3k-2)n}}+O(\frac{1}{2^{3kn}}))$.

We compute $E(\delta_{ij}\delta_{qr})$. Again we have to consider several cases. We give the main case: $I_2(i) \neq I_2(j)$, $I_2(q) \neq I_2(r)$ and $I_2(i) \oplus I_2(j) \oplus I_2(q) \oplus I_2(r) \neq 0$.
In that case, $S_3(j) = I_2(i) \oplus I_2(j) \oplus S_3(i) \neq S_3(i)$. There are 2^{kn} possibilities for $S(i)$. When $S(i)$ is fixed, there are $2^{(k-2)n}$ possibilities for $S(j)$, since $S_2(j)$ and $S_3(j)$ are fixed. Now for $S(q)$ there are 6 possibilities:
1- $S_2(q) \neq S_2(i)$ (we have $S_2(i) = S_2(j)$). Then $S_2(r) = S_2(q) \neq S_2(i)$. Since $S_3(r) = S_3(q) \oplus I_2(q) \oplus I_2(r)$, we have $S_3(q) \neq S_3(r)$. Thus there are $(2^n - 1)2^{(k-1)n}$ possibilities for $S(q)$ and $2^{(k-2)n}$ possibilities for $S(r)$ This gives $(2^n - 1)2^{2k-3)n}$ possibilities for $(S(q), S(r))$.
2- $S_2(q) = S_2(i) = S_2(j)$ and $S_3(q) = S_3(i) \oplus I_2(q) \oplus I_2(r)$.
Then $S_3(r) = S_3(i)$ and $S_2(r) = S_2(q)) = S_2(i)$. There are $2^{(k-2)n}$ possibilities for $S(p)$ and $2^{(k-2)n} - 1$ possibilities for $S(r)$. This gives $2^{2(k-2)n}(2^{2(k-2)n} - 1)$

possibilities for $(S(q), S(r))$.
3- $S_2(q) = S_2(i) = S_2(j)$ and $S_3(q) = S_3(j) \oplus I_2(q) \oplus I_2(r)$.
There are $2^{(k-2)n}$ possibilities for $S(p)$ and $2^{(k-2)n} - 1$ possibilities for $S(r)$. This gives $2^{2(k-2)n}(2^{2(k-2)n} - 1)$ possibilities for $(S(q), S(r))$
4- $S_2(q) = S_2(i) = S_2(j)$ and $S_3(q) = S_3(i)$. This gives $(2^{2(k-2)n} - 1)2^{2(k-2)n}$ possibilities for $(S(q), S(r))$
5- $S_2(q) = S_2(i) = S_2(j)$ and $S_3(q) = S_3(j)$. This gives again $(2^{2(k-2)n} - 1)2^{2(k-2)n}$ possibilities for $(S(q), S(r))$
6- $S_2(q) = S_2(i) = S_2(j)$ and we are not in cases b,c,d, e. This gives $(2^{2(k-2)n} - 4)2^{2(k-2)n}$ possibilities for $(S(q), S(r))$
Finally, the number of possible outputs for $S(i), S(j), S(q), S(r)$ in this case 1 is given by $B = 2^{(4k-4)n}\left(1 - \frac{4}{2^{kn}}\right)$ and $E(\delta_{ij}\delta_{qr}) = \frac{B}{A} = \frac{1}{2^{4n}}\left(1 + \frac{2}{2^{kn}} + \frac{1}{2^{2kn}} + O(\frac{1}{2^{3kn}})\right)$. Thus $E(\delta_{ij})E(\delta_{qr}) - E(\delta_{ij}\delta_{qr}) = \frac{1}{2^{4n}}\left(-\frac{2}{2^{2kn}} + O(\frac{1}{2^{3kn}})\right)$. The term $\frac{-2m^4}{4 \cdot 2^{4n} \cdot 2^{2kn}} \ll \frac{m^2}{2^{2n}}$ since $m \ll 2^{kn}$ The other cases are $I_2(i) = (j)$, $I_2(q) \neq I_2(r)$, $I_2(i) \neq I_2(j)$, $I_2(q) \neq I_2(r)$ and $I_2(i) \oplus I_2(j) \oplus I_2(q) \oplus I_2(r) = 0$ and $I_2(i) = I_2(j)$ and $I_2(q) = I_2(r)$. The study is similar to the main case.
All the computations show that $V(\mathcal{N}_{perm}) = \frac{m(m-1)}{2 \cdot 2^{2n}}(1 - \frac{1}{2^{2n}} + O(\frac{1}{2^{kn}}))$.
Thus $V(\mathcal{N}_{perm}) \simeq E(\mathcal{N}_{perm})$ as claimed.

B Computation of the Mean Value and the Variance for Feistel Type-1 Schemes

Here we suppose that $p = 4$. For any p the computations are similar. We introduce the internal variables:
$X^1 = I_2 \oplus f^1(I_1),\ X^2 = I_3 \oplus f^2(X^1),\ X^3 = I_4 \oplus f^3(X^2) \dots$
$X^{k-1} = I_k \oplus f^{k-1}(X^{k-2}),\ X^k = I_1 \oplus f^3(X^{k-1}),\ X^{k+1} = X^1 \oplus f^{k-1}(X^k) \dots$
$X^{2k-1} = X^{k-1} \oplus f^{2k-1}(X^{2k-2}),\ X^{2k} = X^k \oplus f^{2k}(X^{2k-1}) \dots$
$X^{3k-1} = X^{2k-1} \oplus f^{3k-1}(X^{3k-2}),\ X^{3k} = X^{2k} \oplus f^{3k}(X^{3k-1}) \dots$
$X^{4k-1} = X^{3k-1} \oplus f^{4k-1}(X^{4k-2})$
For $\ell \geq k-1$, X^ℓ depends on all the input variables. Thus we can assume, since the internal functions are randomly chosen, that for $\ell \geq k-1$,the internal variables X^ℓ are completely independent. After $4k-1$ rounds the output is given by: $[S_1, S_2, S_3, \dots, S_k] = [X^{4k-1}, X^{3k}, X^{3k+1}, \dots, X^{4k-2}]$. where $S_3 = I_2 \oplus f^1(I_1) \oplus f^{k+1}(X^k) \oplus f^{2k+1}(X^{2k}) \oplus f^{3k-1}(X^{3k})$. Thus the following conditions:
$(*)$ $\quad S_2(i) = S_2(j)$, and $I_2(i) \oplus I_2(j) = S_3(i) \oplus S_3(j)$ are equivalent to
$(**) X^{3k}(i) = X^{3k}(j)$ and $f^{k+1}(X^k(i)) \oplus f^{2k+1}(X^{2k}(i)) = f^{k+1}(X^k(j))$
$\oplus f^{2k+1}(X^{2k}(j))$
In order to compute $E(\delta_{ij})$, we consider 2 cases.

1. $X^{3k}(i) = X^{3k}(j)$ and $(X^k(i), X^{2k}(i)) = (X^k(j), X^{2k}(j))$. The probability is $\frac{1}{2^{3n}}$.
2. $X^{3k}(i) = X^{3k}(j)$, $(X^k(i), X^{2k}(i)) \neq X^k(j), X^{2k}(j))$ and $f^{k+1}(X^k(i)) \oplus f^{2k+1}(X^{2k}(i)) = f^{k+1}(X^k(j)) \oplus f^{2k+1}(X^{2k}(j))$. The probability is $\frac{1}{2^n}(1 - \frac{1}{2^{2n}})\frac{1}{2^n} = \frac{1}{2^{2n}} - \frac{1}{2^{4n}}$.

Finally $E(\delta_{ij}) = \frac{1}{2^{2n}} + \frac{1}{2^{3n}} - \frac{1}{2^{4n}}$ and $E(\mathcal{N}_{type1}) = \frac{m(m-1)}{2}\Big(\frac{1}{2^{2n}} + \frac{1}{2^{3n}} - \frac{1}{2^{4n}}\Big)$. $V(\delta_{ij}) = E(\delta_{ij}) - (E(\delta_{ij}))^2 = \frac{1}{2^{2n}} + \frac{1}{2^{3n}} - \frac{2}{2^{4n}} - \frac{2}{2^{5n}} + \frac{1}{2^{6n}} + \frac{2}{2^{7n}} - \frac{1}{2^{8n}}$. We will use the covariance formula: $V(\mathcal{N}_{type1}) = V(\sum_{i<j} \delta_{ij}) + \sum_{\substack{1<j \\ q<r \\ (i,j)\neq(q,r)}} [E(\delta_{ij}\delta_{qr}) - E(\delta_{ij})E(\delta_{qr})]$. $E(\delta_{ij})E(\delta_{qr}) = (\frac{1}{2^{2n}} + \frac{1}{2^{3n}} - \frac{1}{2^{4n}})^2 = \frac{1}{2^{4n}} + \frac{2}{2^{5n}} - \frac{1}{2^{6n}} - \frac{2}{2^{7n}} + \frac{1}{2^{8n}}$. We now compute $E(\delta_{ij}\delta_{qr})$. We explain the case where i, j, q, r are pairwise distinct. The case where in $\{i, j, q, r\}$ we have exactly 3 values is similar. When i, j, q, r are pairwise distinct, the conditions $(**)$ are satisfied for the pairs (i, j) and (q, r). Then we have to study several cases.

1. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(r)$, $(X^k(i), X^{2k}(i)) = (X^k(j), X^{2k}(j))$ and $(X^k(q), X^{2k}(q)) = (X^k(r), X^{2k}(r))$. The probability is $\frac{1}{2^{6n}}$.
2. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(r)$, $(X^k(i), X^{2k}(i)) = (X^k(j), X^{2k}(j))$ and $(X^k(q), X^{2k}(q)) \neq (X^k(r), X^{2k}(r))$ and $f^{k+1}(X^k(q)) \oplus f^{2k+1}(X^{2k}(q)) = f^{k+1}(X^k(r)) \oplus f^{2k+1}(X^{2k}(r))$. Then the probability is given by $\frac{1}{2^n} \times \frac{1}{2^n} \times \frac{1}{2^{2n}}(1 - \frac{1}{2^{2n}}) \times \frac{1}{2^n} = \frac{1}{2^{5n}} - \frac{1}{2^{7n}}$.
3. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(r)$, $(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$ and $(X^k(q), X^{2k}(q)) = (X^k(r), X^{2k}(r))$ and $f^{k+1}(X^k(i) \oplus f^{2k+1}(X^{2k}(i)) = f^{k+1}(X^k(j)) \oplus f^{2k+1}(X^{2k}(j))$. As in the previous case, the probability is given by $\frac{1}{2^{5n}} - \frac{1}{2^{7n}}$.
4. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(r)$, $(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$, $(X^k(q), X^{2k}(q)) = (X^k(i), X^{2k}(i))$, $(X^k(r), X^{2k}(r)) = (X^k(j), X^{2k}(j))$ $f^{k+1}(X^k(i) \oplus f^{2k+1}(X^{2k}(i)) = f^{k+1}(X^k(j)) \oplus f^{2k+1}(X^{2k}(j))$. The probability is given by $\frac{1}{2^n} \times \frac{1}{2^n} \times \frac{1}{2^{2n}}(1 - \frac{1}{2^{2n}}) \times \frac{1}{2^{2n}} \times \frac{1}{2^{2n}} \times \frac{1}{2^n} = \frac{1}{2^{7n}} - \frac{1}{2^{9n}}$.
5. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(r)$, $(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$, $(X^k(r), X^{2k}(r)) = (X^k(i), X^{2k}(i))$, $(X^k(q), X^{2k}(q)) = (X^k(j), X^{2k}(j))$, $f^{k+1}(X^k(i) \oplus f^{2k+1}(X^{2k}(i)) = f^{k+1}(X^k(j)) \oplus f^{2k+1}(X^{2k}(j))$. Again the probability is given by $\frac{1}{2^{7n}} - \frac{1}{2^{9n}}$.
6. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(r)$, $(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$ and $(X^k(q), X^{2k}(q)) \neq (X^k(r), X^{2k}(r))$, we are not in cases 4 and 5 and $f^{2k+1}(X^{2k}(i)) = f^{k+1}(X^k(j)) \oplus f^{2k+1}(X^{2k}(j))$ and $f^{k+1}(X^k(q))$ $\oplus f^{2k+1}(X^{2k}(q)) = f^{k+1}(X^k(r)) \oplus f^{2k+1}(X^{2k}(r))$. Then the probability is $\frac{1}{2^n} \times \frac{1}{2^n} \times [(1 - \frac{1}{2^{2n}}) \times (1 - \frac{1}{2^{2n}}) - (1 - \frac{1}{2^{2n}}) \times \frac{1}{2^{2n}} \times \frac{1}{2^{2n}}] \times \frac{1}{2^n} = \frac{1}{2^{4n}} - \frac{2}{2^{6n}}\frac{1}{2^{10n}}$.

Finally we obtain $E(\delta_{ij}\delta_{qr}) = +\frac{2}{2^{5n}} - \frac{1}{2^{6n}}\frac{4}{2^{7n}} - \frac{2}{2^{9n}} + \frac{1}{2^{10n}}$ and $E(\delta_{ij}\delta_{qr}) - E(\delta_{ij})E(\delta_{qr}) = \frac{6}{2^{7n}} - \frac{2}{2^{9n}} + \frac{1}{2^{10n}}$. Thus in $\sum_{\substack{1<j \\ q<r \\ (i,j)\neq(q,r)}} [E(\delta_{ij}\delta_{qr}) - E(\delta_{ij})E(\delta_{qr})]$ the term $\frac{m^4}{2^{7n}} \ll \frac{m^2}{2^{2n}}$ since $m \simeq 2^{2n}$ in our attack.

Our computations show that the CPA-1 on $pk - 1$ rounds with $p \leq k + 2$, we have: $E(\mathcal{N}_{perm}) \simeq \frac{m^2}{2^{2n}}$, $E(\mathcal{N}_{type1}) \simeq \frac{m^2}{2^{2n}} + \frac{m^2}{2^{(p-1)n}}$, $V(\mathcal{N}_{perm}) \simeq \frac{m^2}{2^{2n}}$ and, $\sigma(\mathcal{N}_{perm}) \simeq \frac{m}{2^n}$, $V(\mathcal{N}_{type1}) \simeq \frac{m^2}{2^{2n}}$, and $\sigma(\mathcal{N}_{type1}) \simeq \frac{m}{2^n}$. Thus we can distinguish a permutation obtained by a Type 1 Feistel scheme from a random permutation as soon as $|E(\mathcal{N}_{perm}) - E(\mathcal{N}_{type1})| \geq \sigma(\mathcal{N}_{perm})$, $|E(\mathcal{N}_{perm}) - E(\mathcal{N}_{type1})| \geq \sigma(\mathcal{N}_{type1})$ i.e. as soon as $\frac{m^2}{2^{(p-1)n}} \geq \frac{m}{2^n}$ i.e. $m \geq 2^{(p-2)n}$