Differential Attacks on Generalized Feistel Schemes

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

[1] Department of Mathematics, University of Cergy-Pontoise, CNRS UMR 8088
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
[2] PRISM, University of Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
valerie.nachef@u-cergy.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 [8], have not been systematically investigated. These generalized Feistel schemes are used in 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}.In this paper, we give our best Known Plaintext Attacks and non-adaptive Chosen Plaintext Attacks on these schemes. We determine the maximal number of rounds that we can attack when we want to distinguish a permutation produced by the scheme from a permutation chosen randomly in the set of permutations.

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 [14]. These schemes allow to construct permutations from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$ by using round functions from n bits to n bits (DES is an example of a classical Feistel scheme). For 3 and 4 rounds, there are attacks with $\sqrt{2^n}$ inputs in [1] and [18]. For 5 rounds, an attack with $O(2^n)$ inputs is given in [19, 20]. When the round functions are permutations, attacks are studied in [12, 13, 25]. Security results on classical Feistel schemes are given in [8, 20, 17].

We define generalized Feistel schemes 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 round 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 [22]. 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 [10, 23, 24, 26]. Alternating Feistel schemes alternate contracting and expanding rounds. 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 [9, 29]). These schemes are used respectively in the block ciphers CAST-256, RC6 and MARS. In [4], the authors provide 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]. Impossible differential attacks on generalized Feistel schemes are studied in [5] when there is no condition on the round functions, and in [6, 13, 27] when the round functions are permutations.

Security results have been obtained for most of these schemes. For classical Feistel schemes the different results are given in [8, 20, 17]. Unbalanced Feistel schemes with contracting functions have been studied in [8, 15, 17, 28] and for unbalanced Feistel schemes with expanding functions, alternating, type-1, type-2 and type-3 Feistel schemes, the results are in [8].

This paper is devoted to the study of generic attacks on type-1, type-2, type-3 and alternating generalized Feistel schemes. Our attacks are distinguishers that allow to distinguish a permutation produced by a scheme from a permutation chosen randomly in the set of permutations. The round functions are chosen at random and are not known to the adversary. Moreover, we assume that the round functions are independent of each other.

Our attacks will use differential characteristics. We provide Known Plaintext Attacks (KPA) and non-adaptive Chosen Plaintext Attacks (CPA-1). For each kind of scheme, we will give the maximal number of rounds that we can attack in KPA and CPA-1 and we will describe our best attacks up to the maximal number of rounds. Table 1 gives the maximal number of rounds attacked by either KPA, CPA-1 that we have obtained and the comparison with impossible differential attacks for type-1, type-2 and type-3 Feistel schemes when the round functions are bijective or not. In this table, we consider that we want to distinguish permutations kn bits to kn bits either produced by the scheme or chosen randomly from the set of permutations.

Table 1. Maximal number of rounds reached by our attacks and impossible differential attacks

Structure	KPA	CPA-1	Impossible Differential	
			bijective	any
Type-1	$2k^2+2k-2$ (Sec. 4.1)	$2k^2+k-1$ (Sec. 4.1)	k^2+2 [6, 27]	k^2 [4]
Type-2	$2k+2$ (Sec. 4.2)	$2k+1$ (Sec. 4.2)	$2k+1$ [27]	N/A
Type-3	$k+\lfloor\frac{k}{2}\rfloor+1$ (Sec. 4.3)	$k+1$ (Sec. 4.3)	$2k+3$ [27]	$2k$ [4]
Alternating	$3k$ (Sec. 4.4)	$3k$ (Sec. 4.4)	N/A	N/A

The paper is organized as follows. In Section 2, we give the notations 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 the results of our simulations. In the Appendices, we give examples of computations of the variances, needed to get the complexity of our attacks.

2 Notations - Definitions of the schemes

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 as well. We use differential attacks, i.e. attacks where we study how differences on pairs of input variables will propagate following a differential characteristic, and give relations between pairs of input/output variables. The number of rounds is denoted by r. 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. After one round, the output is given by $[I_2 \oplus F_1^1(I_1), I_3, I_4 \oplus F_2^1(I_3), \ldots, I_k \oplus F_{\frac{k}{2}}^1(I_{k-1}), I_1]$ where each F_s^1, $1 \leq s \leq \frac{k}{2}$ is a function from n bits to n bits.
3. *Type-3 Feistel schemes (Fig. 2)*
   After one round, the output is given by $[I_2 \oplus F_1^1(I_1), I_3 \oplus F_2^1(I_2), I_4 \oplus F_3^1(I_3), \ldots, I_k \oplus F_{k-1}^1(I_{k-1}), I_1]$ where each F_s^1, $1 \leq s \leq k-1$ 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 function F^1 from $(k-1)n$ bits to n. Let $X^1 = I_1 \oplus F^1([I_2, \ldots, I_k])$. After one round, the output is given by $[X^1, I_2, \ldots, I_k]$ and X^1 is called an internal variable. For the second round, we apply an expanding function $G^2 = (G_1^2, G_2^2, \ldots, G_k^2)$ where each G_s^2 is a function from n bits to n bits. The output after the second round is given by $[X^1, I_2 \oplus G_1^2(X^1), \ldots, I_k \oplus G_k^2(X^1)]$. Then we alternate contracting 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, the notation $[\mathbf{0}, \mathbf{0}, \Delta_3^0, \Delta_4^0, \ldots, \Delta_k^0]$ means that the pair of messages (i,j) satisfies $I_1(i) = I_1(j)$, $I_2(i) = I_2(j)$, and $I_s(i) \oplus I_s(j) = \Delta_s^0$, $3 \leq s \leq k$. In CPA-1, the notation $[\underline{\mathbf{0}}, \underline{\mathbf{0}}, \Delta_3^0, \Delta_4^0, \ldots, \Delta_k^0]$ means that we choose I_1 and I_2 to be constants. The differential of the outputs i and j after round r is denoted by $[\Delta_1^r, \Delta_2^r, \ldots, \Delta_k^r]$. At each round, internal variables are defined by the structure of the scheme. In our attacks, we determine

Fig. 1. First round for type-1 and type-2 Feistel schemes

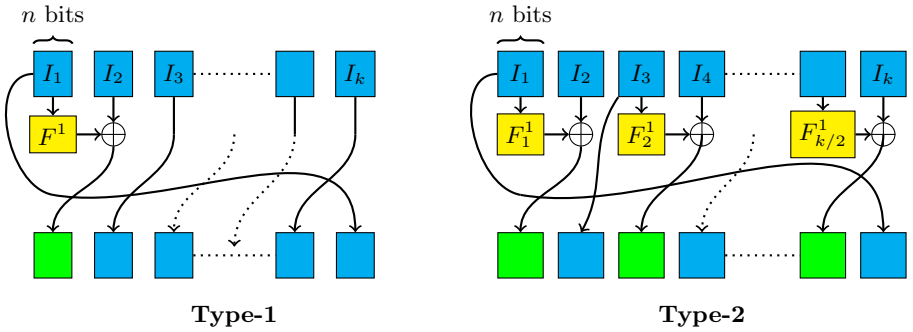
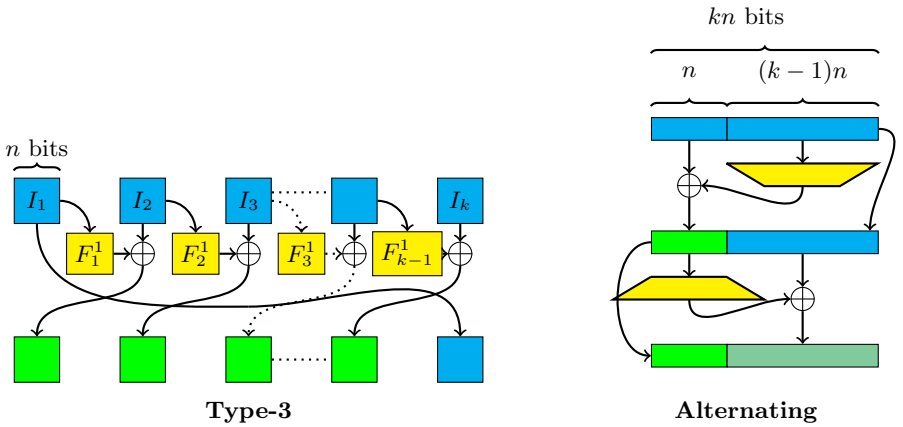


Fig. 2. First round for type-3 Feistel scheme and first two rounds of alternating Feistel scheme



conditions that have to be satisfied by the outputs. When we have a scheme, these conditions are satisfied either at random or because the internal variables verify some equalities. Thus, we will impose conditions on the internal variables on some chosen rounds. When we impose conditions on the internal variables in order to get a differential characteristic, 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. 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 of 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 [7], 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 $V(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} V(x_i) + 2\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\big[E(x_i\, x_j) - E(x_i)E(x_j)\big]$. Similar computation are also performed in [22].
As we will see in our computations, in this paper, we will always have $\sigma(\mathcal{N}_{perm}) \simeq \sqrt{E(\mathcal{N}_{perm})}$ and $\sigma(\mathcal{N}_{scheme}) \simeq \sqrt{E(\mathcal{N}_{scheme})} \simeq \sqrt{E(\mathcal{N}_{perm})}$. In Appendices A and B, this is explained on an example.

4 Description of our 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 maximal number of rounds. We always assume that $k \geq 3$.

4.1 Type-1 Feistel schemes

For 1 to $k-1$ rounds, one message is enough, since after r rounds, $1 \leq r \leq k-1$, we have $S_{k-r+1} = I_1$. 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.
We now consider KPA for $r \geq k$. In Table 2 (left part), we give the general pattern of the differential characteristics used in our KPA.

Table 2. Differential characteristic used in our attacks on type-1 Feistel schemes

round	Δ_1^0	Δ_2^0	Δ_3^0	...	Δ_{k-1}^0	Δ_k^0
1				...		Δ_1^0
2				...	Δ_1^0	
$\vdots$						
$k-1$	$\boxed{0}$	Δ_1^0		...		
k	Δ_1^0			...		0
$k+1$				...		Δ_1^0
$\vdots$						
$rk-2$		0	Δ_1^0	...		
$rk-1$	$\boxed{0}$	Δ_1^0		...		
rk	Δ_1^0			...		0
$\vdots$						
$(r+1)k-2$		0	Δ_1^0	...		

KPA

round	$\underline{\mathbf{0}}$	Δ_2^0	Δ_3^0	...	Δ_{k-1}^0	Δ_k^0
1	Δ_2^0	Δ_3^0		...		0
2				...	0	Δ_2^0
$\vdots$						
$k-1$		0	Δ_2^0	...		
k	$\boxed{0}$	Δ_2^0		...		
$k+1$	Δ_2^0				...	0
$k+2$				...	0	Δ_2^0
$\vdots$						
$rk-1$		0	Δ_2^0	...		
rk	$\boxed{0}$	Δ_2^0		...		
$\vdots$						
$(r+1)k-1$		0	Δ_2^0	...		

CPA-1

The conditions after $rk-2$ rounds ($r \geq 3$) are given by

$$\begin{cases} S_2(i) = S_2(j) \\ I_1(i) \oplus I_1(j) = S_3(i) \oplus S_3(j) \end{cases} \tag{1}$$

We count the number of indices (i, j) such that these conditions are satisfied. Let $\mathcal{N}_{perm}$ be the number obtained when we have permutation chosen randomly and uniformly from the set of permutations from kn bits to kn bits. Similarly, $\mathcal{N}_{scheme}$ represents the number obtained with a permutation produced by the scheme. For $\mathcal{N}_{perm}$, the conditions appear at random and we obtain $E(\mathcal{N}_{perm}) \simeq \frac{m^2}{2.2^{2n}}$. For $\mathcal{N}_{scheme}$, the conditions appear at random or because some conditions are satisfied by the internal variables and we get $E(\mathcal{N}_{scheme}) \simeq \frac{m^2}{2.2^{2n}} + O(\frac{m^2}{2^{(r-1)n}})$. The O function comes from the conditions $\boxed{0}$ that we impose on the differential characteristic. In Appendix B, we will explain on an example how to estimate this O function. Both 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 $r \geq 4$. This means that we can distinguish between a random permutation and a type-1 Feistel scheme as soon as $\frac{m^2}{2^{(r-1)n}} \geq \frac{m}{2^n}$. This gives the condition $m \geq 2^{(r-2)n}$. Since the maximal number of messages is 2^{kn}, these attacks work for $r - 2 \leq k$ and then with $r = k + 2$, we can attack up to $(k + 2)k - 2 = k^2 + 2k - 2$ rounds.

The analysis of all the attacks will be very similar. We first choose the differential characteristics. Then, we compute $E(\mathcal{N}_{perm})$, $E(\mathcal{N}_{scheme})$, $\sigma(\mathcal{N}_{perm})$

and $\sigma(\mathcal{N}_{scheme})$ as define previously. Again, $E(\mathcal{N}_{perm})$ will be greater than $E(\mathcal{N}_{scheme})$ because there are conditions on the internal variables that will imply conditions on the outputs. Moreover, we have $\sigma(\mathcal{N}_{perm}) \simeq \sqrt{E(\mathcal{N}_{perm})}$ and $\sigma(\mathcal{N}_{scheme}) \simeq \sqrt{E(\mathcal{N}_{scheme})} \simeq \sqrt{E(\mathcal{N}_{perm})}$. Then, we compare the difference of the mean values with the standard deviation and we obtain the number of messages needed for the attack. The previous attack is summarized by the Table 3, where σ denotes either $\sigma(\mathcal{N}_{perm})$ or $\sigma(\mathcal{N}_{scheme})$.

Table 3. Type-1 Feistel scheme: KPA on $rk-2$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_2^{rk-2}=0$ $\Delta_3^{rk-2}=\Delta_1^0$	$\frac{m^2}{2.2^{2n}}$	$\frac{m^2}{2.2^{2n}}+O(\frac{m^2}{2^{(r-1)n}})$	$\frac{m}{\sqrt{2}2^n}$	$2^{(r-2)n}$

We study CPA-1 for $r \geq k$. 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, at round r ($k \leq r \leq 2k-1$), with a type-1 Feistel scheme, we obtain with probability 1 that $S_{2k-r}(1) \oplus S_{2k-r}(2) = I_k(1) \oplus I_k(2)$. If we are not dealing with a type-1 Feistel scheme, the probability to obtain this equality is $\frac{1}{2^n}$.
On round r (with $r \geq 2k$), we will have to consider different conditions on the input variables. We explain now a CPA-1 on $rk-1$ rounds (with $r \geq 3$) in Table 2 (right part) and Table 4, where we choose the messages such that I_1 takes only one value for all messages. Here, we have $m \geq 2^{(r-2)n}$. Since the maximal number

Table 4. Type-1 Feistel scheme: CPA-1 on $rk-1$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_2^{rk-2}=0$ $\Delta_3^{rk-2}=\Delta_2^0$	$\frac{m^2}{2.2^{2n}}$	$\frac{m^2}{2.2^{2n}}+O(\frac{m^2}{2^{(r-1)n}})$	$\frac{m}{\sqrt{2}2^n}$	$2^{(r-2)n}$

of messages is $2^{(k-1)n}$, these attacks work as long as $r-2 \leq k-1$. Thus with $r = k+1$, we can attack up to $(k+1)k-1 = k^2+k-1$ rounds.
Table 6 summarizes the complexities for type-1 Feistel schemes. We also give the results of our simulations in Table 5.

4.2 Type-2 Feistel schemes

For type-2 Feistel schemes, k is always even. Table 7 and Table 8 represent a KPA on $2k+2$ rounds.

Table 5. Experimental results for CPA-1 against type-1 Feistel scheme with k^2+k-1 rounds

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

Table 6. Complexities of the attacks on type-1 Feistel schemes

r rounds	KPA
$1 \to k-1$	1
$k \to 2k-1$	$2^{n/2}$
$2k \to 3k-2$	2^n
$\vdots$	
$rk-2$	$2^{(r-2)n}$
$rk-1$	$2^{(r-3/2)n}$
rk	
$\vdots$	$2^{(r-1)n}$
$(r+1)k-2$	
$\vdots$	
k^2+2k-2	2^{kn}

r rounds	CPA-1	r	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+1	
$\vdots$	2^n	$\vdots$	$2^{(k-1)n}$
$4k-3$		k^2+k-1	

Table 7. Differential characteristic used in our attacks on type-2 Feistel schemes (KPA)

round	**0**	Δ_2^0	Δ_3^0	Δ_4^0	...	Δ_{k-3}^0	Δ_{k-2}^0	Δ_{2k-1}^0	Δ_k^0
1	Δ_2^0				...				0
2					...			$\boxed{0}$	Δ_2^0
3					...		0	Δ_2^0	
$\vdots$									
$k-1$		0	Δ_2^0		...				
k	$\boxed{0}$	Δ_2^0			...				
$k+1$	Δ_2^0				...				0
$k+2$					...			$\boxed{0}$	Δ_2^0
$\vdots$									
$2k-1$		0	Δ_2^0		...				
$2k$	$\boxed{0}$	Δ_2^0			...				
$2k+1$	Δ_2^0				...				0
$2k+2$					...				Δ_2^0

Table 8. Type-2 Feistel scheme: KPA on $2k+2$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	m
$\Delta_1^0 = 0$ $\Delta_k^k = \Delta_2^0$	$\frac{m^2}{2.2^{2n}}$	$\frac{m^2}{2.2^{2n}} + O(\frac{m^2}{2^{(k+1)n}})$	2^{kn}

We explain how to get attacks on intermediate rounds. After $2r$ rounds, $r \geq 1$, we have in Table 9:

Table 9. Type-2 Feistel scheme: KPA on $2r$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_1^0 = 0$ $\Delta_s^{2r} = \Delta_2^0$	$\frac{m^2}{2.2^{2n}}$	$\frac{m^2}{2.2^{2n}} + O(\frac{m^2}{2^{rn}})$	$\frac{m}{\sqrt{2}2^n}$	$2^{(r-1)n}$

where $1 \leq s \leq k$ and $s \equiv 2 - 2r \pmod{k}$.
In this attack, $m = 2^{(r-1)n}$. Thus, for $r = k+1$, we have reached the maximal number of rounds with $2^{(k-1)n}$ messages.

After $2r+1$ rounds, $r \geq 1$, the attack is represented in Table 10:

Table 10. Type-2 Feistel scheme: KPA on $2r+1$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_1^0 = 0$ $\Delta_t^{2r+1} = \Delta_2^0$ $\Delta_{t-1}^{2r+1} = 0$	$\frac{m^2}{2.2^{3n}}$	$\frac{m^2}{2.2^{3n}} + O(\frac{m^2}{2^{(r+1)n}})$	$\frac{m}{\sqrt{2}2^n}$	$2^{(r-\frac{1}{2})n}$

where $1 \leq t \leq k$ and $t \equiv 1 - 2r \pmod{k}$.

For CPA-1, we can impose conditions on a given number of input variables. We give in Table 11 and Table 12 an example of an attack on $2k-1$ rounds for which we consider messages where I_1, I_2, I_3 are given constant values. Then we will generalize.

For round $2k-2$, the attack is represented in Table 13.

More generally, if we suppose that for the input variables, we have $I_1, \ldots, I_r$ are constants ($r \leq k-1$), we can perform the same kind of attacks. It is easy to check that we can attack up to $2k-r+2$ rounds and we need exactly $2^{(k-r)n}$ messages. 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 values, then we will have $I_1, \ldots I_{k-2}$ constants, and so on.

Table 14 summarizes the complexities for type-2 Feistel schemes.

Table 11. Differential characteristic used in our attacks on type-2 Feistel schemes (CPA-1)

round	$\underline{\mathbf{0}}$	$\underline{\mathbf{0}}$	$\underline{\mathbf{0}}$	Δ_4^0	Δ_5^0	Δ_6^0	...	Δ_{k-3}^0	Δ_{k-2}^0	Δ_{k-1}^0	Δ_k^0
1	0	0	Δ_4^0				...				0
2	0	Δ_4^0					...				0
3	Δ_4^0						...				0
4							...			$\boxed{0}$	Δ_4^0
5							...		0	Δ_4^0	
$\vdots$											
k			$\boxed{0}$	Δ_4^0			...				
$k+1$		0	Δ_4^0				...				
$k+2$	$\boxed{0}$	Δ_4^0					...				
$k+3$	Δ_4^0						...				0
$\vdots$											
$2k-2$					$\boxed{0}$	Δ_4^0	...				
$2k-1$				0	Δ_2^0		...				

Table 12. Type-2 Feistel scheme: CPA-1 on $2k-1$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_4^{2k-1}=0$ $\Delta_5^{2k-1}=\Delta_4^0$	$\frac{m^2}{2.2^{2n}}$	$\frac{m^2}{2.2^{2n}}+O(\frac{m^2}{2^{(k-2)n}})$	$\frac{m}{\sqrt{2}2^n}$	$2^{(k-3)n}$

Table 13. Type-2 Feistel scheme: CPA-1 on $r=2k-2$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_6^{2k-2}=0$	$\frac{m^2}{2.2^n}$	$\frac{m^2}{2.2^n}+O(\frac{m^2}{2^{(k-3)n}})$	$\frac{m}{\sqrt{2}2^{\frac{n}{2}}}$	$2^{(k-\frac{7}{2})n}$

Table 14. Complexities of the attacks on type-2 Feistel schemes

r	KPA	CPA-1
1	1	1
2	$2^{n/2}$	2
$3 \le r \le k$	$2^{\frac{r-2}{2}n}$	2
$k+1$	$2^{(k-1/2)n}$	$2^{n/2}$
$k+1$	$2^{\frac{k}{2}n}$	$2^{n/2}$
$k+3 \le r \le 2k+2$	$2^{\frac{r-2}{2}n}$	$2^{(r-k-2)n}$

4.3 Type-3 Feistel schemes

We will present our attacks when k is even. For k odd, the computations are similar. The results are summarized in Table 18. We begin with KPA. For one round, we need one message, we just have to check if $I_1 = S_k$. With a random permutation, this happens with probability $\frac{1}{2^n}$ and with a scheme with proba-

bility one. Suppose we want to attack r rounds with $2 \leq r \leq k$. We wait until we have 2 messages such that $I_1(1) = I_1(2), \ldots, I_{r-1}(1) = I_{r-1}(2)$. Then we test if $I_{r-1}(1) \oplus I_{r-1}(2) = S_k(1) \oplus S_k(2)$. 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 $2^{\frac{(r-1)n}{2}}$ messages, we get 2 messages with the given conditions with a high probability. We give in Table 15 (left part) a KPA on $k+4$ rounds, where we suppose that $4 \leq \frac{k}{2} + 1$.

Table 15. Differential characteristics used in our attacks on type-3 Feistel schemes

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

KPA

round	$\underline{\mathbf{0}}$	$\underline{\mathbf{0}}$	...	$\underline{\mathbf{0}}$	$\underline{\mathbf{0}}$	$\underline{\mathbf{0}}$	$\underline{\mathbf{0}}$	Δ_k^0
1	0	0	...	0	0	0	Δ_k^0	0
2	0	0	..	0	0	Δ_k^0		0
3	0	0	..	0	Δ_k^0			0
$\vdots$								
$k-1$	Δ_k^0		...					0
k			...				$\boxed{0}$	Δ_k^0
$k+1$			...				Δ_k^0	

CPA-1

For this KPA on $k+4$ rounds, we have in Table 16:

Table 16. Type-3 Feistel scheme: KPA on $r = k+4$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_1^0 = 0$ $\Delta_2^0 = 0$ $\vdots$ $\Delta_{k-1}^0 = 0$ $\Delta_k^0 = \Delta_{k-5}^{k+4}$	$\frac{m^2}{2.2^{kn}}$	$\frac{m^2}{2.2^{kn}} + O(\frac{m^2}{2^{(k+3)n}})$	$\frac{m}{\sqrt{2}2^{\frac{kn}{2}}}$	$2^{(\frac{k}{2}+3)n}$

Since $m = 2^{(\frac{k}{2}+3)n}$, we can perform the same kind of attack for $k+r$ rounds, with $r \leq \frac{k}{2} + 1$. We can attack up to $k + \frac{k}{2} + 1$ rounds. For $k + \frac{k}{2} + 1$, we need the maximal 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 r rounds with $r \leq k$, 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 choose m messages such that $I_1, I_2, \ldots, I_{k-1}$ have a constant value. We have the following CPA-1 described in Table 15 (right part) and Table 17:

Table 17. Type-3 Feistel scheme: CPA-1 on $k+1$ rounds

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_{k-1}^{k+1} = \Delta_k^0$	$\frac{m^2}{2.2^n}$	$\frac{m^2}{2.2^n} + O(\frac{m^2}{2^n})$	$\frac{m}{\sqrt{2}2^{\frac{n}{2}}}$	$2^{\frac{n}{2}}$

Table 18 gives KPA and CPA-1 complexities.

Table 18. Complexities of the attacks on type-3 Feistel schemes

r	KPA	CPA-1
1	1	1
2	$2^{n/2}$	2
3	2^n	2
$\vdots$		
k	$2^{(k-1)n/2}$	2
$k+1$	$2^{\frac{k}{2}n}$	$2^{n/2}$
$k+2 \leq r \leq k+\lfloor \frac{k}{2} \rfloor + 1$	$2^{(r-\lfloor \frac{k}{2} \rfloor - 1)n}$	$2^{(r-\lfloor \frac{k}{2} \rfloor - 1)n}$

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 now show. We have the following KPA on $2r$ ($r \leq k$) rounds, described in Table 19 and Table 20, where Δ^0 denotes $[\Delta_2^0, \Delta_3^0, \Delta_4^0, \ldots, \Delta_k^0]$.

Table 19. Differential characteristic of our attacks on alternating Feistel schemes (KPA)

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

Table 20. Alternating Feistel scheme: KPA on $2r$ rounds $r \leq k$

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	m
$\Delta_1^0 = 0$ $\Delta^{2r} = \Delta^0$	$\frac{m^2}{2.2^{kn}}$	$\frac{m^2}{2.2^{kn}} + O(\frac{m^2}{2^{rn}})$	$2^{\frac{r}{2}n}$

Here we obtain, $m = 2^{\frac{r}{2}}$, since when $r \leq k$, $E(\mathcal{N}_{perm})$ is greater than or equal to twice $E(\mathcal{N}_{scheme})$ and we can distinguish when $m = 2^{\frac{r}{2}}$. Notice that in this case, we do not need to use the standard deviation. Thus, after 2 rounds we get a KPA with $2^{\frac{n}{2}}$ messages (notice that the CPA-1 complexity of the previous attack was better). After 2 rounds, KPA are the best attacks. We do not have better attack if we fix some part on the inputs.
After $2r$ rounds with $r > k$, in KPA, we keep the same differential characteristics and the attack is given in Table 21.

Table 21. Alternating Feistel scheme: KPA on $2r$ rounds $r > k$

Differential	$E(\mathcal{N}_{perm})$	$E(\mathcal{N}_{scheme})$	σ	m
$\Delta_1^0 = 0$ $\Delta^{2r} = \Delta^0$	$\frac{m^2}{2.2^{kn}}$	$\frac{m^2}{2.2^{kn}} + O(\frac{m^2}{2^{rn}})$	$\frac{m}{\sqrt{2}2^{\frac{kn}{2}}}$	$2^{(r-\frac{k}{2})n}$

Here since $r > k$, we need to compute the standard deviation and we get $m = 2^{(r-\frac{k}{2})n}$. Since the number of messages cannot exceed 2^{kn}, we obtain the condition $r \leq 3k/2$. Here we have given the complexity for even rounds. If we want to attack the odd round $2r+1$, we will only impose $\Delta^{2r+1} = \Delta^0$. We can attack up to $3k$ rounds. The complexities are summarized in Table 22.

Table 22. Complexities of the attacks on alternating Feistel schemes

r rounds	KPA
1	1
2	$2^{n/2}$
3	$2^{n/2}$
$\vdots$	
$3 \leq r \leq 2k+1$	$2^{(\frac{\lfloor \frac{r}{2} \rfloor}{2})n}$
$\vdots$	
$2k+1$	$2^{\frac{kn}{2}}$
$\vdots$	
$2k+1 \leq r \leq 3k$	$2^{(\frac{(r-k)}{2})n}$
$\vdots$	
$3k$	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: type-1, type-2, type-3 and alternating Feistel schemes. Since these schemes are used in well known block ciphers, it is interesting to find the maximal 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 maximal number of possible messages to perform the attack. A way to overcome this problem is to attack permutation generators instead of a single permutation. Impossible differential attacks are better on type-3 Feistel schemes. For type-2 Feistel schemes, we can attack the same number of rounds as impossible attacks but here the internal functions are not necessarily bijective. For type-1 Feistel schemes, our attacks can reach more rounds as impossible differential attacks.

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 Dunkelman, Gaetan Leurent, 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. Charles Bouillaguet, Orr Dunkelman, Gaetan Leurent, and Pierre-Alain Fouque. New Insights on Impossible Differential Cryptanalysis. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptographyl – SAC '11*, volume 7118 of *Lecture Notes in Computer Science*, pages 243–259. Springer-Verlag, 2011.
6. Jiali Choy and Huihui Yap. Impossible Boomerang Attack for Block Cipher Structures. In Tsuyoshi Takagi and Masahiro Mambo, editors, *Advances in Information and Computer Security*, volume 5824 of *Lecture Notes in Computer Science*, pages 22–37. Springer Berlin Heidelberg, 2009.
7. Paul G.Hoel, Sidney C.Port, and Charles J.Stone. *Introduction to Probability Theory.* Houghton Mifflin Company, 1971.
8. 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.
9. Subariah Ibrahim and f Mohd Aizaini Mararof. Diffusion Analysis of Scalable Feistel Networks. *World Academy of Science, Engineering and Technology*, 5:98–101, 2005.
10. 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.
11. Jongsung Kim, Seokhie Hong, and Jongin Lim. Impossible Differential Cryptanalysis Using Matrix Method . *Discrete Mathematics*, 310(5):988 – 1002, 2010.
12. Lars R. Knudsen. DEAL - A 128-bit Block Cipher. Technical Report 151, University of Bergen, Department of Informatics, Norway, february 1998.
13. 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.
14. Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
15. Moni Naor and Omer Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *J. Cryptology*, 12(1):29–66, 1999.
16. Jacques Patarin. Generic Attacks on Feistel Schemes - Extended version. *Cryptology ePrint archive: 2008/036: Listing for 2008.*
17. Jacques Patarin. Security of balanced and unbalanced Feistel schemes with linear non equalities. *Cryptology ePrint archive: 2010/293: Listing for 2010.*
18. 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.
19. 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.
20. 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.
21. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions - Extended version. *Cryptology ePrint archive: 2007/449: Listing for 2007.*
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. Xuejia Lai Yiyuan Luo, Zhongming Wu and Guang Gong. A Unified Method for Finding Impossible Differentials of Block Cipher Structures. 2009. http://eprint.iacr.org/.
28. Aaram Yun, Je Hong Park, and Jooyoung Lee. Lai-Massey Scheme and Quasi-Feistel Networks. *Cryptology ePrint archive: 2007/347: Listing for 2007.*
29. Yuliang Zheng, Tsutomu Matsumoto, and Hideki 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 Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 461–480. Springer New York, 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. This is an attack on $pk - 1$ rounds with $3 \leq p \leq k + 1$ 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 (2) is satisfied $\quad \delta_{ij} = 0$ otherwise. Then $\mathcal{N}_{perm} = \sum_{i<j} \delta_{ij}$,
$E(\mathcal{N}_{perm}) = \sum_{i<j} E(\delta_{ij})$ and
$E(\delta_{ij}) = Pr[S_2(i) = S_2(j)$ and $I_2(i) \oplus I_2(j) = S_3(i) \oplus S_3(j)]$
Case 1: $I_2(i) = I_2(j)$.
$E(\delta_{ij}) = Pr[S_2(i) = S_2(j)$ and $S_3(i) = S_3(j)] = \frac{2^{(k-2)n}-1}{2^{kn}-1} = (\frac{1}{2^{2n}})(\frac{1-\frac{1}{2^{(k-2)n}}}{1-\frac{1}{2^{kn}}})$
Case 2: $I_2(i) \neq I_2(j)$.
$E(\delta_{ij}) = Pr[S_2(i) = S_2(j)$ and $I_2(i) \oplus I_2(j) = S_3(i) \oplus S_3(j)] = \frac{2^{(k-2)n}}{2^{kn}-1} = (\frac{1}{2^{2n}})(\frac{1}{1-\frac{1}{2^{kn}}})$.
Let α be the number of (i,j) such that $I_2(i) = I_2(j)$. Then
$E(\mathcal{N}_{perm}) = \alpha\Big(\frac{2^{(k-2)n}-1}{2^{kn}-1}\Big) + \Big(\frac{m(m-1)}{2} - \alpha\Big)\Big(\frac{2^{(k-2)n}}{2^{kn}-1}\Big) = [\frac{m(m-1)}{2\cdot 2^{2n}} - \frac{\alpha}{2^{kn}}](\frac{1}{1-\frac{1}{2^{kn}}})$.
We can assume that $\alpha = \frac{m(m-1)}{2\cdot 2^n} + O(\frac{m}{\sqrt{2^n}})$. Then we get
$E(\mathcal{N}_{perm}) = [\frac{m(m-1)}{2\cdot 2^{2n}} - \frac{1}{2^{kn}}\Big(\frac{m(m-1)}{2\cdot 2^n} + 0(\frac{m}{\sqrt{2^n}})\Big)](\frac{1}{1-\frac{1}{2^{kn}}}) =$
$(\frac{m(m-1)}{2\cdot 2^{2n}}) \times (\frac{1-\frac{1}{2^{(k-1)n}}}{1-\frac{1}{2^{kn}}}) + O(\frac{m}{2^{k+\frac{1}{2}}})$.
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 $E(\delta_{ij})E(\delta_{qv})$ and $E(\delta_{ij}\delta_{qv})$. We explain the case where i,j,q,v are pairwise distinct. The case where in $\{i,j,q,v\}$ 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 $E(\delta_{ij})E(\delta_{qv})$. We have to study several cases:

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

We compute $E(\delta_{ij}\delta_{qv})$. Again we have to consider several cases. We give the main case: $I_2(i) \neq I_2(j)$, $I_2(q) \neq I_2(v)$ and $I_2(i) \oplus I_2(j) \oplus I_2(q) \oplus I_2(v) \neq 0$.
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 $S_2(v) = S_2(q) \neq S_2(i)$. Since $S_3(v) = S_3(q) \oplus I_2(q) \oplus I_2(v)$, we have $S_3(q) \neq S_3(v)$. Thus there are
$(2^n - 1)2^{(k-1)n}$ possibilities for $S(q)$ and $2^{(k-2)n}$ possibilities for $S(v)$ This gives $(2^n - 1)2^{(2k-3)n}$ possibilities for $(S(q), S(v))$.
2) $S_2(q) = S_2(i) = S_2(j)$ and $S_3(q) = S_3(i) \oplus I_2(q) \oplus I_2(v)$.
Then $S_3(v) = S_3(i)$ and $S_2(v) = S_2(q)) = S_2(i)$. There are $2^{(k-2)n}$ possibilities for $S(p)$ and $(2^{(k-2)n} - 1)$ possibilities for $S(v)$. This gives $2^{2(k-2)n}(2^{2(k-2)n} - 1)$ possibilities for $(S(q), S(v))$.
3) $S_2(q) = S_2(i) = S_2(j)$ and $S_3(q) = S_3(j) \oplus I_2(q) \oplus I_2(v)$.
There are $2^{(k-2)n}$ possibilities for $S(p)$ and $2^{(k-2)n} - 1$ possibilities for $S(v)$. This gives $2^{2(k-2)n}(2^{2(k-2)n} - 1)$ possibilities for $(S(q), S(v))$
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 $(S(q), S(v))$
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 $(S(q), S(v))$
6) $S_2(q) = S_2(i) = S_2(j)$ and we are not in cases 2), 3), 4), 5). This gives $(2^{2(k-2)n} - 4)2^{2(k-2)n}$ possibilities for $(S(q), S(v))$
Finally, the number of possible outputs for $S(i), S(j), S(q), S(v)$ in this case 1 is given by $B = 2^{(4k-4)n}\Big(1 - \frac{4}{2^{kn}}\Big)$ and $E(\delta_{ij}\delta_{qv}) = \frac{B}{A} = \frac{1}{2^{4n}}\Big(1 + \frac{2}{2^{kn}} + \frac{1}{2^{2kn}} + O(\frac{1}{2^{3kn}})\Big)$. Thus $E(\delta_{ij})E(\delta_{qv}) - E(\delta_{ij}\delta_{qv}) = \frac{1}{2^{4n}}\Big(-\frac{2}{2^{2kn}} + O(\frac{1}{2^{3kn}})\Big)$. 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 $I_2(i) = (j)$, $I_2(q) \neq I_2(v)$, $I_2(i) \neq I_2(j)$, $I_2(q) \neq I_2(v)$ and $I_2(i) \oplus I_2(j) \oplus I_2(q) \oplus I_2(v) = 0$ and $I_2(i) = I_2(j)$ and $I_2(q) = I_2(v)$. 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^i where X^i is the first block of the output after round i.
After $4k-1$ rounds the output is given by:

$$[S_1, S_2, S_3, \ldots, S_k] = [X^{4k-1}, X^{3k}, X^{3k+1}, \ldots, X^{4k-2}]$$

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 $(X^k(i), X^{2k}(i)) = (X^k(j), X^{2k}(j))$.
2. $X^{3k}(i) = X^{3k}(j)$, $(X^k(i), X^{2k}(i)) \neq X^k(j), X^{2k}(j))$ and $F^{k+1}(X^k(i)) \oplus F^{2k+1}(X^{2k}(i)) = F^{k+1}(X^k(j)) \oplus F^{2k+1}(X^{2k}(j))$.

Let

$$p_1 = Pr[X^{3k}(i) = X^{3k}(j)/(X^k(i), X^{2k}(i)) = (X^k(j), X^{2k}(j))$$
$$p_1' = Pr[X^{3k}(i) = X^{3k}(j)/(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$$
$$p_2 = Pr[(X^k(i), X^{2k}(i)) = (X^k(j), X^{2k}(j))$$

The the probability of the first case is $p_1 p_2$ and the probability of the second case is $\frac{1}{2^n} p_1'(1-p_2)$. Finally $E(\delta_{ij}) = p_1 p_2 + \frac{1}{2^n} p_1'(1-p_2)$, and $E(\mathcal{N}_{type1}) = \frac{m(m-1)}{2}\Big(p_1 p_2 + \frac{1}{2^n} p_1'(1-p_2)\Big)$. We have $p_1' \simeq \frac{1}{2^n}$. In p_2 the dominant term is in $O(\frac{1}{2^{2n}})$. Indeed, according to Lemma 24 of [8], we have $\frac{1}{2^n} \leq Pr[X^k(i) = X^k(j)] \leq \frac{k-1}{2^n}$. Using the same arguments, we obtain $\frac{1}{2^{2n}} \leq p_2 \leq \frac{(k-1)^2}{2^{2n}}$ and $\frac{1}{2^n} \leq p_1 \leq \frac{k-1}{2^n}$.
We want to show that the variance behaves like the mean value. For this, we will use the covariance formula:

$$V(\mathcal{N}_{type1}) = \sum_{i<j} V(\delta_{ij}) + \sum_{\substack{1<j \\ q<v \\ (i,j)\neq(q,v)}} [E(\delta_{ij}\delta_{qv}) - E(\delta_{ij})E(\delta_{qv})]$$

We now compute $E(\delta_{ij}\delta_{qv})$. We explain the case where i, j, q, v are pairwise distinct. The case where in $\{i, j, q, v\}$ we have exactly 3 values is similar.
When i, j, q, v are pairwise distinct, the conditions $(**)$ are satisfied for the pairs (i, j) and (q, v). Then we have to study several cases.

1. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(v)$, $(X^k(i), X^{2k}(i)) = (X^k(j), X^{2k}(j))$ and $(X^k(q), X^{2k}(q)) = (X^k(v), X^{2k}(v))$. The probability is $(p_1 p_2)^2$.

2. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(v)$, $(X^k(i), X^{2k}(i)) = (X^k(j), X^{2k}(j))$ and $(X^k(q), X^{2k}(q)) \neq (X^k(v), X^{2k}(v))$ and $F^{k+1}(X^k(q)) \oplus F^{2k+1}(X^{2k}(q)) = F^{k+1}(X^k(v)) \oplus F^{2k+1}(X^{2k}(v))$. Then the probability is given by $\frac{1}{2^n} p_1 p_1' p_2 (1 - p_2)$.
3. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(v)$, $(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$ and $(X^k(q), X^{2k}(q)) = (X^k(v), X^{2k}(v))$ 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 $\frac{1}{2^n} p_1 p_1' p_2 (1 - p_2)$.
4. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(v)$, $(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$, $(X^k(q), X^{2k}(q)) = (X^k(i), X^{2k}(i))$, $(X^k(v), X^{2k}(v)) = (X^k(j), X^{2k}(j))$ $F^{k+1}(X^k(i) \oplus F^{2k+1}(X^{2k}(i)) = F^{k+1}(X^k(j)) \oplus F^{2k+1}(X^{2k}(j))$. The probability is given by $\frac{1}{2^n} (p_1')^2 p_2^2 (1 - p_2)$.
5. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(v)$, $(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$, $(X^k(v), X^{2k}(v)) = (X^k(i), X^{2k}(i))$, $(X^k(q), X^{2k}(q)) = (X^k(j), X^{2k}(j))$, $F^{k+1}(X^k(i) \oplus F^{2k+1}(X^{2k}(i)) = F^{k+1}(X^k(j)) \oplus F^{2k+1}(X^{2k}(j))$. Again the probability is given by $\frac{1}{2^n} (p_1')^2 p_2^2 (1 - p_2)$.
6. $X^{3k}(i) = X^{3k}(j)$, $X^{3k}(q) = X^{3k}(v)$, $(X^k(i), X^{2k}(i)) \neq (X^k(j), X^{2k}(j))$ and $(X^k(q), X^{2k}(q)) \neq (X^k(v), X^{2k}(v))$, 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 $F^{k+1}(X^k(q))$ $\oplus F^{2k+1}(X^{2k}(q)) = F^{k+1}(X^k(v)) \oplus F^{2k+1}(X^{2k}(v))$. Then the probability is $\frac{1}{2^{2n}} (p_1')^2 [(1 - p_2)^2 - 2(1 - p_2) p_2^2]$.

Finally we obtain when i, j, q, v are pairwise distinct

$$E(\delta_{ij}\delta_{qv}) - E(\delta_{ij})E(\delta_{qv}) = 2\frac{1}{2^n}(p_1')^2 p_2^2 (1 - p_2) - 2\frac{1}{2^{2n}}(p_1')^2 p_2^2 (1 - p_2)$$

Using the dominant term in p_1' and p_2, we get that the dominant term in $\sum_{\substack{1<j \\ q<v \\ (i,j)\neq(q,v)}} [E(\delta_{ij}\delta_{qv}) - E(\delta_{ij})E(\delta_{qv})]$ is in $O(\frac{m^4}{2^{7n}})$ and $\frac{m^4}{2^{7n}} \ll \frac{m^2}{2^{2n}}$ since $m \simeq 2^{2n}$ in our attack.
Similarly, in the case where we have exactly 3 values in $\{i, j, q, v\}$, the dominant term in $\sum_{\substack{1<j \\ q<v \\ (i,j)\neq(q,v)}} [E(\delta_{ij}\delta_{qv}) - E(\delta_{ij})E(\delta_{qv})]$ is in $O(\frac{m^3}{2^{5n}})$ and $\frac{m^3}{2^{5n}} \ll \frac{m^2}{2^{2n}}$ since $m \simeq 2^{2n}$ in our attack.
Thus the dominant term in the $V(\mathcal{N}_{type1})$ is in $O(\frac{m^2}{2^{2n}})$.

More generally, our computations show that the CPA-1 on $pk - 1$ rounds with $p \leq k + 2$, we have: $E(\mathcal{N}_{perm}) \simeq \frac{m^2}{2.2^{2n}}$, $E(\mathcal{N}_{type1}) \simeq \frac{m^2}{2.2^{2n}} + O(\frac{m^2}{2^{(p-1)n}})$, $V(\mathcal{N}_{perm}) \simeq \frac{m^2}{2^{2n}}$ 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. $m \geq 2^{(p-2)n}$.