Generic attacks on Alternating Unbalanced Feistel Schemes

Valérie Nachef

Department of Mathematics
University of Cergy-Pontoise
CNRS UMR 8088
2, Avenue Adolphe Chauvin
95302 Cergy-Pontoise Cedex
France
valerie.nachef@u-cergy.fr

Abstract. Generic attacks against classical (balanced) Feistel schemes, unbalanced Feistel schemes with contracting functions and unbalanced Feistel schemes with expanding functions have been studied in [12], [4], [15], [16]. In this paper we study schemes where we use alternatively contracting random functions and expanding random functions. We name these schemes "Alternating Unbalanced Feistel Schemes". They allow constructing pseudo-random permutations from kn bits to kn bits where $k \geq 3$. At each round, we use either a random function from n bits to $(k-1)n$ bits or a random function from $(k-1)n$ bits to n bits. We describe the best generic attacks we have found. We present "known plaintext attacks" (KPA) and "non-adaptive chosen plaintext attacks" (CPA-1). Let d be the number of rounds. We show that if $d \leq k$, there are CPA-1 with 2 messages and KPA with m the number of messages about $2^{\frac{(d-1)n}{4}}$. For $d \geq k+1$ we have to distinguish k even and k odd. For k even, we have $m = 2$ in CPA-1 and $m \simeq 2^{\frac{kn}{4}}$ in KPA. When k is odd, we show that there exist CPA-1 for $d \leq 2k-1$ and KPA for $d \leq 2k+3$ with less than 2^{kn} messages and computations. Beyond these values, we give KPA against generators of permutations.

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

1 Introduction

A Feistel scheme from $\{0,1\}^N$ to $\{0,1\}^N$ with d rounds is a permutation built from round functions. When these functions are randomly chosen, we get what we call a "Random Feistel Scheme". "Generic attacks" on these schemes are attacks that are valid for most of the round functions $f_1, \ldots, f_d$. The most classical Feistel schemes are when $N = 2n$ and the f_i functions are from $\{0,1\}^n$ to $\{0,1\}^n$ (i.e. from n bits to n bits). Such schemes are called "balanced" Feistel schemes and they have been studied a lot since the famous paper of M.Luby and C.Rackoff [8] (see [10] for an overview of these results). When the number of rounds is less than 5, there are attacks with less than $2^N (= 2^{2n})$ operations: for 5 rounds, an attack with $O(2^n)$ inputs is given in [12], [13] and there in an attack with $\sqrt{2^n}$ inputs for 3 and 4 rounds in [1] and [11]. When the functions are permutations, attacks for 5 rounds are given in [5] and [6].

When $N = kn$ and the round functions are from $(k-1)n$ bits to n bits, we obtain what we call an Unbalanced Feistel Scheme with Contracting Functions. Some security results on these schemes can be found in [9], [10]. In [15], generic attacks on these schemes are given: when the number of rounds d is less than $2k-1$, there are KPA and CPA-1 with $m < 2^{kn}$ (here m denotes the number of messages) and complexity less than $O(2^{kn})$.

When $N = kn$ and the round functions are from n bits to $(k-1)n$ bits, we obtain what is called an Unbalanced Feistel Scheme with Expanding Functions. These schemes and their attacks are investigated in [4], [16] and [17]. When $d \leq 3k-1$, there exist generic attacks with a complexity and a number of messages less than 2^{kn} [16].

In [2], R.J. Anderson and E. Biham introduced block ciphers that use alternatively expanding and contracting functions: BEAR and LION. In these schemes, the input is divided into two parts of different lengths. Following similar ideas, we introduce here another family of schemes which alternate contracting and expanding functions. Namely the large half of the message is a multiple of the small half of the message and we rotate the register. We define them as "Alternating Unbalanced Feistel Schemes" (a precise definition will be given in Section 2) and we suppose $k \geq 3$. The paper is organized as follows. In section 2 and 3, we give the notation, the definitions and we present an overview of the attacks. In Section 4, we study the case $d \leq k$: we show that there exists CPA-1 with $m = 2$ and if d is odd, we have KPA for d and $d+1$ rounds with $m \simeq 2^{\frac{(d-1)n}{4}}$. In Section 5, we study the case when k is even and $d > k$: we give CPA-1 with $m = 2$ and KPA with $m \simeq 2^{\frac{kn}{4}}$ for any round. In Section 6, we show that when k is odd, $k \geq 5$, there exists CPA-1 with $k < d \leq 2k-1$ and KPA with $k < d \leq 2k+3$, such that $m < 2^{kn}$ and with complexity $O(m) < 2^{kn}$. The results for $k \geq 5$ are summarized in Section 7. Attacks against permutations generators are studied in Appendix A. The generic attacks for $k = 3$ are explained in Appendix B.

2 Notation

Our notation is very similar to [15] and [16]. We describe now one round of an unbalanced Feistel scheme with expanding functions and one round of an unbalanced Feistel scheme with contracting functions.

For an unbalanced Feistel scheme with expanding functions, the input is $[I^1, I^2, \ldots, I^k]$ and $g = (g^1, g^2, \ldots, g^{k-1})$ is a function from n bits to $(k-1)n$ bits. The output is given by $[I^2 \oplus g^1(I^1), I^3 \oplus g^2(I^1), \ldots, I^k \oplus g^{k-1}(I^1), I^1]$.

When we have an unbalanced Feistel Scheme with contracting functions and the input is $[I^1, I^2, \ldots, I^k]$, we use a function f from $(k-1)n$ bits to n bits. Then, the output is given by $[I^2, I^3, \ldots, I^k, I^1 \oplus f(I^2, I^3, \ldots, I^k)]$.

We now describe an alternating unbalanced Feistel scheme (or shortly an alternating scheme) for $k \geq 3$ and d rounds. We will study the case where we begin with an expanding round (the case where we begin with a contracting round is similar; we will only mention the results). Such schemes are denoted by A_k^d. We say that they produce a A_k^d permutation. The input is $[I^1, I^2, \ldots, I^k]$. After one expanding round, we have used a function $g_1 = (g_1^1, \ldots, g_1^{k-1})$, we get the output $[Y^1, Y^2, \ldots, Y^{k-1}, I^1]$ where $Y^i = I^{i+1} \oplus g_1^i(I^1)$ for $1 \leq i \leq k-1$. Then we apply a contracting round with a function f_2 and the output is $[Y^2, Y^3, \ldots, Y^{k-1}, I^1, X^2]$ where $X^2 = Y^1 \oplus f_2(Y^2, \ldots, Y^{k-1}, I^1)$. Figure 1 shows the first two rounds of an alternating scheme when we begin with an expanding round.

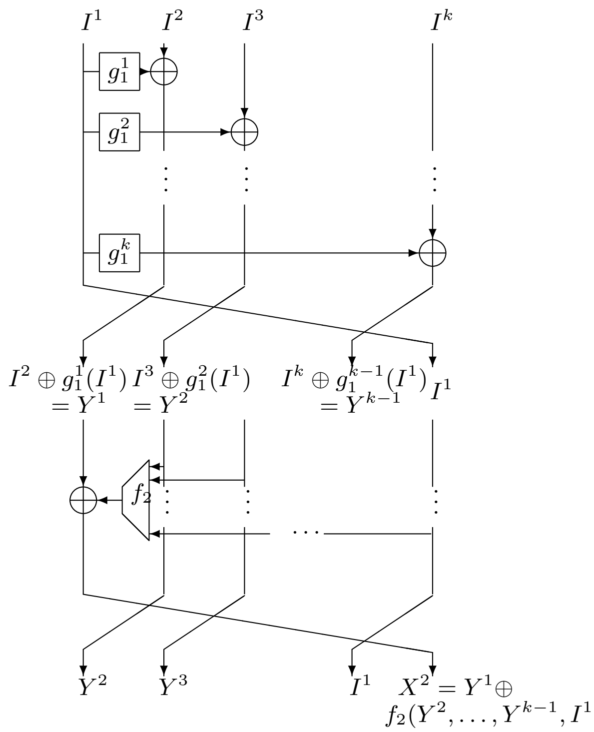

Fig. 1. First two rounds of an alternating scheme

More generally, for $p \geq 1$, we denote by $Y^{p(k-1)+i}$, $1 \leq i \leq k-1$, the internal variables we obtain on the first $k-1$ coordinates of the output after $2p+1$ rounds (this last round is an expanding round). Notice that after $2p+1$ rounds, the last coordinate of the output is $Y^{(p-1)(k-1)+2}$ (i.e. the second coordinate of the output after $2p-1$ rounds). Similarly, X^{2p} denotes the internal variable we get on the last coordinate after $2p$ rounds (here this last round is a contracting round). This means that after $2p+1$ rounds, we can write:

$$\begin{cases} S^i & = Y^{p(k-1)+i} & = Y^{(p-1)(k-1)+i-k+2} \oplus g^i_{2p+1}(Y^{(p-1)(k-1)+2}), i \le k-3 \\ S^{k-2} & = Y^{p(k-1)+k-2} & = Y^{(p-2)(k-1)+2} \oplus g^{k-2}_{2p+1}(Y^{(p-1)(k-1)+2}) \\ S^{k-1} & = Y^{p(k-1)+k-1} & = X^{2p} \oplus g^{k-1}_{2p+1}(Y^{(p-1)(k-1)+2}) \\ S^k & = Y^{(p-1)(k-1)+2} & \end{cases}$$

where $X^{2p} = Y^{(p-1)(k-1)+1} \oplus f_{2p}(Y^{(p-1)(k-1)+2}, \ldots, Y^{(p-1)(k-1)+k-1}, Y^{(p-2)(k-1)+2})$. After $2p+2$ rounds, the output is $[Y^{p(k-1)+2}, \ldots, Y^{p(k-1)+k-1}, Y^{(p-1)(k-1)+2}, X^{2p+2}]$.

Let m denotes the number of messages. For $1 \le i \le m$ and $1 \le t \le k$, I_i^t denotes the coordinate of rank t of the input of the message number i. We use the same notation on the output $[S_i^1, \ldots, S_i^k]$ and on the internal variables.

KPA will mean "known plaintext attacks" and CPA-1 "non-adaptive chosen plaintext attacks".

Remarks:

1.We will not introduce full adaptive attacks or chosen plaintext and chosen ciphertext attacks since we have not found anything significantly better than CPA-1 and KPA on A_k^d.

2.We consider $k \ge 3$, since for $k = 2$, such schemes are not interesting: the I^2 part of the input still remains I^2.

3 Overview of the Attacks

We present attacks that allow us to distinguish a A_k^d permutation 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 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 $\mathcal{N}_{A_k^d}$, the number of such couples we obtain with an alternating scheme, with $\mathcal{N}_{perm}$, the corresponding number for a random permutation. The attack is successful, i.e. we are able to distinguish a A_k^d permutation from a random permutation if the difference $|E(\mathcal{N}_{A_k^d}) - E(\mathcal{N}_{perm})|$ is much larger than both standard deviations σ_{perm} and $\sigma_{A_k^d}$, where E denotes the expectancy function. In order to compute these values, we need to take into account the fact that the structures obtained from the m plaintext/ciphertext t-uples are not independent. However their mutual dependence is very small. To compute σ_{perm} and $\sigma_{A_k^d}$, we will use this well-known formula (see [3], p.97), that we will call the "Covariance Formula": if $x_1, \ldots x_n$ are random variables, then $V(\sum_{i=1}^n x_i) = \sum_{i=1}^n V(x_i) + 2\sum_{i=1}^{n-1}\sum_{j=i+1}^n \big[E(x_i, x_j) - E(x_i)E(x_j)\big]$.

4 Generic Attacks on A_k^d with $d \le k$

In this section, we suppose that $d \le k$ and we describe CPA-1 and KPA. If we have m messages, the input of message number i is denoted by $[I_i^1, I_i^2, \ldots, I_i^k]$.

The output produced by applying either a random permutation or a A_k^d permutation is denoted by $[S_i^1, S_i^2, \ldots, S_i^k]$. We always start with an expanding round. We will perform our attacks on S^k after an odd number of rounds. Then since we apply a contracting round, the same attacks will be valid on S^{k-1} for the next round. After one round, we have $S^k = I^1$ and after 2 rounds, $S^{k-1} = I^1$. This gives an attack with one message. We just check if $S^k = I^1$ (or and after 2 rounds, $S^{k-1} = I^1$). For a random permutation, this happens with probability $\frac{1}{2^n}$ and with an alternating scheme the probability is 1. In order to give the next attacks, we now state the basic property that we need.

The basic Property:
After $2p-1$ rounds and $2p \leq k-2$, the second coordinate of the output is $Y^{(p-1)(k-1)+2} = I^{2p+1} \oplus G_{2p-1}(I^1, I^3, \ldots, I^{2p-1})$ where G_{2p-1} is a function that depends only on $I^1, I^3, \ldots, I^{2p-1}$.

Proof of the basic Property
The proof proceeds by induction in p. It is easy to see that for $p = 1$, we have $Y^2 = I^3 \oplus g_1^2(I^1)$. Also for $p = 2$, we get $Y^{(2-1)(k-1)+2} = Y^{k+1} = I^5 \oplus g_1^4(I^1) \oplus g_3^2(Y^2) = I^5 \oplus G_3(I^1, I^3)$.

More generally, it is easy to check that after $2p-1$ rounds, the second coordinate of the output is given by $Y^{(p-1)(k-1)+2} = I^{2p+1} \oplus g_1^{2p}(I^1) \oplus g_3^{2p-2}(Y^2) \oplus \ldots \oplus g_{2p-1}^2(Y^{(p-2)(k-1)+2})$ and if we apply the induction hypothesis, we can write: $Y^{(p-1)(k-1)+2} = I^{2p+1} \oplus G_{2p-1}(I^1, I^3, \ldots, I^{2p-1})$ as claimed.

The Attacks:
We will use the basic property to give a CPA-1 on A_k^{2p+1} with 2 messages. Here we have: $S^k = Y^{(p-1)(k-1)+2}$. We choose these messages such that $I_1^1 = I_2^1$, $I_1^3 = I_2^3$, $I_1^5 = I_2^5$, …, $I_1^{2p-1} = I_2^{2p-1}$ and we test if $S_1^k \oplus I_1^{2p+1} = S_2^k \oplus I_2^{2p+1}$. This property happens with probability 1 when we are testing a A_k^{2p+1} permutation and with probability about $\frac{1}{2^n}$ with a random permutation. This gives a CPA-1 with only 2 messages. As usual, we can transform this CPA-1 in a KPA. When $m \simeq 2^{\frac{pn}{2}}$, from the birthday paradox, we will get with a good probability $i < j$ satisfying $I_i^1 = I_j^1$, $I_i^3 = I_j^3$, $I_i^5 = I_j^5$, …, $I_i^{2p-1} = I_j^{2p-1}$ and we test again if $S_i^k \oplus I_i^{2p+1} = S_j^k \oplus I_j^{2p+1}$. We obtain a KPA with $O(2^{\frac{pn}{2}})$ messages and complexity. After $2p+2$ rounds, we can perform the same CPA-1 and KPA with S^{k-1} instead of S^k since we apply a contracting round. We perform these attacks until we reach round k. Notice that the attack on A_k^k uses S^{k-1} if k is even and S^k if k is odd. Also $m = 2$ for CPA-1 and $m \simeq 2^{\frac{(k-1)n}{4}}$ for KPA.
Here the internal variable $Y^{(p-1)(k-1)+2}$ is the Xor of several terms whose first one is I^{2p+1}. This leads us to introduce the following definition in order to generalize this fact.

Definition 1 *Let I^i any coordinate of the input. The "chain generated by I^i" is the sequence of internal variables whose expression begins with I^i.*

5 Generic Attacks on A_k^d when $k = 2l$ is even and $d \geq k+1$

After $k+1$ rounds, we have $S^k = Y^{(l-1)(k-1)+2} = I^1 \oplus g_3^{k-2}(Y^2) \oplus g_5^{k-4}(Y^{k+1}) \oplus \ldots \oplus g_{k-1}^2(Y^{(l-2)(k-1)+2})$ and if we apply the basic property, we know that $Y^{(l-2)(k-1)+2} = I^{k-1} \oplus g_1^{k-1}(I^1) \oplus \ldots \oplus g_{k-3}^2(Y^{(l-3)(k-1)+2})$. This shows that $Y^{(l-1)(k-1)+2}$ depends only of $I^1, I^3, \ldots, I^{k-1}$. Again, we have a CPA-1 with 2 messages. We just choose 2 messages such that $I_1^1 = I_2^1$, $I_1^3 = I_2^3$, $I_1^5 = I_2^5$, ..., $I_1^{k-1} = I_2^{k-1}$ and we test if $S_1^k = S_2^k$. With an alternating scheme, this will happen with probability 1 and with a random permutation with probability about $\frac{1}{2^n}$. Then as usual, we obtain a KPA in $O(2^{\frac{ln}{2}}) = O(2^{\frac{kn}{4}})$ messages and complexity. After $k+2$ rounds, the same attacks work on S^{k-1}.

After $k+3$ rounds, we have: $S^k = Y^{l(k-1)+2} = Y^2 \oplus g_5^{k-2}(Y^{k+1}) \oplus g_7^{k-4}(Y^{2k}) \oplus \ldots \oplus g_{k-1}^2(Y^{(l-1)(k-1)+2})$. Again $Y^{l(k-1)+2}$ is a function of $I^1, I^3, \ldots I^{k-1}$ and we have a CPA-1 with 2 messages and a KPA with $O(2^{\frac{kn}{4}})$ messages and complexity.

More generally, by induction it is possible to show that after $k+2p-1$ rounds ($1 \leq p \leq l-1$), the second coordinate of the output is given by $Y^{(l+p-1)(k-1)+2} = Y^{(p-1)(k-1)+2} \oplus g_{2p+3}^{k-2}(Y^{p(k-1)+2}) \oplus g_{2p+5}^{k-4}(Y^{(p+1)(k-1)+2}) \oplus \ldots \oplus g_{k+2p-1}^2(Y^{(l+p-2)(k-1)+2})$ and $Y^{(p-1)(k-1)+2}$ comes from the chain generated by I^{2p+1}. This shows that $Y^{(l+p-1)(k-1)+2}$ depends only on $I^1, I^3, \ldots, I^{k-1}$. Now, after $k+2p+1$ rounds, the value becomes the last coordinate of the output and we can perform similar attacks as previously. This phenomena is k-periodic. This shows that when k is even and $d \geq k+1$, we have a CPA-1 with only 2 messages and a KPA with $O(2^{\frac{kn}{4}})$ messages and complexity whatever the number of rounds is.

Remark: when we begin with a contracting round instead of an expanding round, we attack S^k for even rounds (the same attacks work on S^{k-1} for odd rounds). In the computations, the variables I^2, I^4, ..., I^k appear instead of the variables I^1, I^3, ..., I^{k-1}. If $2d < k$, we have a generic CPA-1 attack with $m = 2$ messages and a generic KPA attack with $m \simeq 2^{\frac{d-1}{2}n}$. If $2d \geq k$, we still have a CPA-1 with two messages and a KPA attack with $m \simeq 2^{\frac{k}{4}n}$ random queries and $O(m)$ computations.

6 Generic Attacks when $k = 2l+1$ is odd, $k \geq 5$ and $d \geq k+1$

We are going to study the case where $k = 2l+1$, $k \geq 5$ and $d \geq k+1$ (the case $k = 3$ is given in Appendix B: it is possible to attack 11 rounds in CPA-1 and 12 rounds in KPA). First we will give the best CPA-1 that we have found. Then we will investigate the KPA. Here the best KPA do not always follow from the CPA-1. Remind that we begin with an expanding round. In order to get the best attacks, we will use two strategies. With the first strategy, we perform the attacks on S^k after an odd number of rounds (this gives the same attack on S^{k-1} after the following round since we apply a contracting round). We already performed these attacks when $d \leq k$. But when k is odd, after $k+3$ rounds, there are too many new internal variables on the last coordinate of the output and this produces too many conditions. For this reason, we have to choose the second strategy: we will use the chain generated by one well chosen coordinate of the input. Moreover, when a chain arrives on the first coordinate of the output after an expanding round, usually we cannot use it anymore because we apply a contracting round to reach the coordinate of rank k and this again produces too many internal variables. Thus we use another chain. For the CPA-1, we will use couples of plaintext/ciphertext pairs and set conditions on some coordinates of the input variables. Then we will test equalities between the input and output variables. With an alternating scheme, these equalities appear at random or due to conditions on the internal variables $Y^{(p-1)(k-1)+i}$. For a random permutation, they appear only at random. As we said in the Section 3, this will allow us to distinguish a A_k^d permutation from a random permutation. For KPA, we will impose equalities between the coordinates of the input variables and also between the input and output variables.

6.1 CPA-1

We have seen in Section 4 that after k rounds, the CPA-1 is on S^k. Thus, the same attack works on S^{k-1} after $k+1$ rounds since we apply a contracting round and $S^{k-1} = Y^{(l-1)(k-1)+2} = I^k \oplus g_1^{k-1}(I^1) \oplus g_3^{k-3}(Y^2) \oplus \ldots \oplus g_{k-2}^2(Y^{(l-2)(k-1)+2})$. Consequently, with only 2 messages, we can distinguish a A_k^{k+1} permutation from a random permutation.

Attacks on A_k^{k+2}, A_k^{k+3}

After $k+2$ rounds, we have:

$$S^k = I^2 \oplus g_1^1(I^1) \oplus f_2(Y^2, Y^3, \ldots, Y^{k-1}, I^1) \oplus g_3^{k-1}(Y^2) \oplus g_5^{k-3}(Y^{k+1}) \oplus \ldots$$
$$\oplus g_k^2(Y^{(l-1)(k-1)+2})$$

and we have: $\forall t,\ 2 \leq t \leq k-1,\ Y^t = I^{t+1} \oplus g_1^t(I^1)$. This gives a CPA-1 with 2 messages. We choose our messages such that $\forall t,\ 1 \leq t \leq k,\ t \neq 2,\ I_1^t = I_2^t$ and we check if $S_1^k \oplus I_1^2 = S_2^k \oplus I_2^2$. With an alternating scheme, this will happen with probability 1 and with a random permutation, the probability is about $\frac{1}{2^n}$. The same attacks works on S^{k-1} instead of S^k after $k+3$ rounds since we apply a contracting round.

Attacks on A_k^{k+4}, A_k^{k+5}

We concentrate the attack on S^{k-2}, i.e. we follow the chain generated by I^2 since the first strategy is no more interesting:

$$S^{k-2} = I^2 \oplus g_1^1(I^1) \oplus f_2(Y^2, Y^3, \ldots, Y^{k-1}, I^1) \oplus g_3^{k-1}(Y^2) \oplus g_5^{k-3}(Y^{k+1}) \oplus$$
$$\ldots \oplus g_k^2(Y^{(l-1)(k-1)+2}) \oplus g_{k+3}^{k-2}(Y^{(l+1)(k-1)+2})$$

and $S^k = Y^{(l+1)(k-1)+2}$. We choose our m messages such that: $\forall i,\ 1 \leq i \leq m,\ \forall t,\ 1 \leq t \leq k,\ t \neq 2,\ I_i^t = 0$. We wait for the collision $i < j$, such that $S_i^k = S_j^k$ and then we test if $S_i^{k-2} \oplus I_i^2 = S_j^{k-2} \oplus I_j^2$. From the birthday paradox, when $m \simeq 2^{\frac{n}{2}}$ such a collision appears with a good probability. With an alternating scheme, the probability that $S_i^{k-2} \oplus I_i^2 = S_j^{k-2} \oplus I_j^2$ is 1 and again with a random permutation, the same probability is about $\frac{1}{2^n}$. Notice that here we can have at most 2^n different messages. After $k+5$ rounds, the same attack can be performed on S^{k-3}. This gives an attack with $O(2^{\frac{n}{2}})$ messages and computations.

Attacks on A_k^{k+6}, A_k^{k+7}

Here

$$S^{k-4} = I^2 \oplus g_1^1(I^1) \oplus f_2(Y^2, Y^3, \ldots, Y^{k-1}, I^1) \oplus g_3^{k-1}(Y^2) \oplus g_5^{k-3}(Y^{k+1}) \oplus \ldots$$

$$\oplus g_k^2(Y^{(l-1)(k-1)+2}) \oplus g_{k+3}^{k-2}(Y^{(l+1)(k-1)+2}) \oplus g_{k+5}^{k-4}(Y^{(l+2)(k-1)+2})$$

and $S^k = Y^{(l+2)(k-1)+2}$. We choose our m messages such that: $\forall i,\ 1 \le i \le m,\ \forall t,\ 1 \le t \le k,\ t \ne 2,\ I_i^t = 0$. Then we count the number of $(i,j),\ i<j$ such that $S_i^k = S_j^k$, and $S_i^{k-4} \oplus I_i^2 = S_j^{k-4} \oplus I_j^2$ **(6.1)**. This number $\mathcal{N}$ is about $\frac{m(m-1)}{2 \cdot 2^{2n}}$ for a random permutation. With a A_d^{k+6} permutation, we have about two times more solution since $Y_i^{(l+1)(k-1)+2} = Y_j^{(l+1)(k-1)+2}$ and $Y_i^{(l+2)(k-1)+2} = Y_j^{(l+2)(k-1)+2}$ imply **(6.1)**. Thus when $\mathcal{N}$ is not 0, i.e. when $m \simeq 2^n$, the attack succeeds. We have the same attack on S^{k-5} instead of S^{k-4} after $k+7$ rounds. Notice that here we have reached the maximal number of possible messages. We will choose another chain.

Attacks on A_k^{k+2p}, A_k^{k+2p+1}, $8 \le 2p < k-1$ and A_k^{2k-1}.

We will follow the chain generated by I^k which gives the best results and concentrate the attack on S^{k-2p}. We have:

$$S^{k-2p} = I^k \oplus g_1^{k-1}(I^1) \oplus \ldots \oplus g_{k-2}^2(Y^{(l-2)(k-1)+2}) \oplus g_{k+2}^{k-2}(Y^{l(k-1)+2}) \oplus$$

$$g_{k+4}^{k-4}(Y^{(l+1)(k-1)+2}) \oplus \ldots \oplus g_{k+2p}^{k-2p}(Y^{(l+p-1)(k-1)+2})$$

where $S^k = Y^{(l+p-1)(k-1)+2}$. We choose m messages such that $\forall i,\ 1 \le i \le m,\ \forall t,\ 0 \le t \le l-1,\ I_i^{2t+1} = 0$. This implies that $m \le 2^{(l+1)n}$. We then count the number of $(i,j), i<i$ such that: $S_i^k = S_j^k$, and $S_i^{k-2p} \oplus I_i^k = S_j^{k-2p} \oplus I_j^k$ **(6.2)**. With a random permutation, we have: $\mathcal{N}_{perm} = \frac{m(m-1)}{2 \cdot 2^{2n}} + O(\frac{m}{2^n})$. We explain this kind of computation in Appendix C. It is shown that the standard deviation is about the square root of the mean value. With an alternating scheme, **(6.2)** is also implied by $\forall s,\ l \le s \le l+p-1, \forall i,\ \forall j,\ Y_i^{s(k-1)+2} = Y_j^{s(k-1)+2}$. Then $\mathcal{N}_{A_k^{k+2p}} \simeq \frac{m(m-1)}{2 \cdot 2^{2n}} + \frac{m(m-1)}{2 \cdot 2^{pn}}$. We explain with an example in Appendix D, how to compute the mean value and the standard deviation which is in $O(\frac{m}{2^n})$. So we can distinguish a A_k^{k+2p} permutation from a random permutation when the difference of the two mean values is greater than both standard deviations. This gives the condition: $\frac{m^2}{2^{pn}} \ge \frac{m}{2^n}$, i.e. $m \simeq 2^{(p-1)n}$. Again the same attack is valid on S^{k-1} after $k+2p+1$ rounds since we apply a contracting round. Then we can perform this kind of attacks until, using the chain generated by I^k, we reach round $2k-1$

where we have: $S^1 = I^k \oplus g_1^{k-1}(I^1) \oplus \ldots \oplus g_{k-2}^2(Y^{(l-2)(k-1)+2}) \oplus g_{k+2}^{k-2}(Y^{l(k-1)+2}) \oplus \ldots \oplus g_{2k-1}^1(Y^{(2l-1)(k-1)+2})$. This gives a CPA-1 with $m \simeq 2^{(l-1)n}$. Then we apply a contracting round and there is no more CPA-1 since this will produce too many equalities between the new internal variables that appear (with all the possible chains).

6.2 KPA

For $k+1$ rounds, the best KPA comes from the CPA-1 on S^{k-1}. This gives a KPA with $m \simeq 2^{\frac{(k-1)n}{4}} = 2^{\frac{ln}{2}}$. After $k+2$ rounds, we will use the chain generated by I^k.

Attacks on A_k^{k+2}, A_k^{k+3}

After $k+2$ rounds, we have:

$$S^{k-2} = I^k \oplus g_1^{k-1}(I^1) \oplus \ldots \oplus g_{k-2}^2(Y^{(l-2)(k-1)+2}) \oplus g_{k+2}^{k-2}(Y^{l(k-1)+2})$$

where $S^k = Y^{l(k-1)+2}$. We wait for collisions $i < j$, such that $\forall t,\ 0 \le t \le l-1,\ I_i^{2t+1} = I_j^{2t+1}$ and $S_i^k = S_j^k$ and we test if $S_i^{k-2} \oplus I_i^k = S_j^{k-2} \oplus I_j^k$. With an alternating scheme this will happen with probability 1 and with a random permutation with probability $\frac{1}{2^n}$. From the birthday paradox, these collisions happen with a good probability when $m \simeq 2^{\frac{(l+1)n}{2}}$ and $O(2^{\frac{(l+1)n}{2}})$ computations. After $k+3$ rounds, we apply the same attack on S^{k-3}.

Attacks on A_k^{k+2p}, A_k^{k+2p+1}, $2p < k-1$ and A_k^{2k-1}

After $k+2p$ rounds with $k-2p > 1$, we have

$$S^{k-2p} = I^k \oplus g_1^{k-1}(I^1) \oplus \ldots \oplus g_{k-2}^2(Y^{(l-2)(k-1)+2}) \oplus g_{k+2}^{k-2}(Y^{l(k-1)+2}) \oplus \ldots$$

$$\oplus g_{k+2p}^{k-2p}(Y^{(l+p-1)(k-1)+2})$$

where $S^k = Y^{(l+p-1)(k-1)+2}$. We will count the number of (i,j), $i<j$ such that

$$\forall t,\ 0 \le t \le l-1,\ I_i^{2t+1} = I_j^{2t+1},\ S_i^k = S_j^k \text{ and } S_i^{k-2p} \oplus I_i^k = S_j^{k-2p} \oplus I_j^k \qquad \mathbf{(6.3)}$$

With a random permutation, we have: $E(\mathcal{N}_{perm}) \simeq \frac{m(m-1)}{2 \cdot 2^{(l+2)n}} + O(\frac{m}{2^{\frac{(l+2)n}{2}}})$. With an alternating scheme, we get: $E(\mathcal{N}_{A_k^{k+2p}}) \simeq \frac{m(m-1)}{2 \cdot 2^{(l+2)n}} + \frac{m(m-1)}{2 \cdot 2^{(l+p)n}}$ since **(6.3)** is also implied by $\forall t,\ 0 \le t \le l-1,\ I_i^{2t+1} = I_j^{2t+1}$, $\forall s,\ l \le s \le l+p-1,\ Y_i^{s(k-1)+2} = Y_j^{s(k-1)+2}$. All the computations are similar to those performed in Appendices C and D. We can distinguish when $\frac{m^2}{2^{(l+p)n}} \ge \frac{m}{2^{\frac{(l+2)n}{2}}}$ i.e. $m \ge 2^{\frac{(l+2p-2)n}{2}}$. The same attack works after $k+2p+1$ rounds since we apply a contracting rounds. After $2k-1$ rounds, we have:

$$S^1 = I^k \oplus g_1^{k-1}(I^1) \oplus \ldots \oplus g_{k-2}^2(Y^{(l-2)(k-1)+2})$$

$$\oplus g_{k+2}^{k-2}(Y^{l(k-1)+2}) \oplus \ldots \oplus g_{k+2p}^{k-2p}(Y^{(l+p-1)(k-1)+2}) \oplus \ldots \oplus g_{2k-1}^1(Y^{(2l-1)(k-1)+2})$$

and we have a KPA with $m \simeq 2^{\frac{(3l-2)n}{2}}$ and $O(2^{\frac{(3l-2)n}{2}})$ computations.

Attacks on A_k^{2k}, A_k^{2k+1}

After $2k$ rounds, since we apply a contracting round, there are two many new internal variables with the chain generated by I^k and this chain does not give any more an interesting KPA. We are using now the chain generated by I^2. Then, after $2k$ rounds, we have:

$$S^2 = I^2 \oplus g_1^1(I^1) \oplus f_2(Y^2, Y^3, \ldots, Y^{k-1}, I^1) \oplus \ldots \oplus g_k^2(Y^{(l-1)(k-1)+2}) \oplus$$
$$g_{k+4}^{k-2}(Y^{(l+1)(k-1)+2}) \oplus \ldots \oplus g_{2k-1}^3(Y^{(2l-1)(k-1)+2})$$

where $S^{k-1} = Y^{(2l-1)(k-1)+2}$ and $\forall t,\ 2 \leq t \leq k-1,\ Y^t = I^{t+1} \oplus g_1^t(I^1)$. We will count the number of (i,j), $i < j$ such that

$$\forall t, 1 \leq t \leq k,\ t \neq 2,\ I_i^t = I_j^t,\ S_i^{k-1} = S_j^{k-1} \text{ and } S_i^2 \oplus I_i^2 = S_j^2 \oplus I_i^2 \quad \textbf{(6.4)}$$

With a random permutation, we have: $E(\mathcal{N}_{perm}) \simeq \frac{m(m-1)}{2 \cdot 2^{(k+1)n}} + O(\frac{m}{2^{\frac{(k+1)n}{2}}})$. With an alternating scheme, **(6.4)** is also implied by

$$\forall t, 1 \leq t \leq k,\ t \neq 2,\ I_i^t = I_j^t \text{ and } \forall s,\ l+1 \leq s \leq 2l-1,\ Y_i^{s(k-1)+2} = Y_j^{s(k-1)+2}$$

This gives about $\frac{m^2}{2^{(k+l-2)n}}$ more solutions. We can distinguish if $\frac{m^2}{2^{(k+l-2)n}} \geq \frac{m}{2^{\frac{(k+1)n}{2}}}$, i.e. when $m \simeq 2^{(2l-2)n}$.

After $2k+1$ rounds, since we apply an expanding round, we introduce a new internal variable $S^k = Y^{(2l)(k-1)+2}$ and we obtain a KPA with $m \simeq 2^{(2l-1)n}$. Notice that this chain is now on the first coordinate of the output.

Attacks on A_k^{2k+2}, A_k^{2k+3}

After $2k+2$ rounds, the chain generated by I^2 is on the coordinate of rank k of the output and we have applied a contracting round. Again, there are too many new internal variables. We now use the chain generated by I^4 and we perform the attack on S^2. Using similar computations, we get $E(\mathcal{N}_{perm}) \simeq \frac{m(m-1)}{2 \cdot 2^{(k)n}} + O(\frac{m}{2^{\frac{kn}{2}}})$. With an alternating scheme, there are about $\frac{m^2}{2^{(k+l-1)n}}$ more solutions. We can distinguish if $\frac{m^2}{2^{(k+l-1)n}} \geq \frac{m}{2^{\frac{kn}{2}}}$, i.e. when $m \simeq 2^{(2l-\frac{1}{2})n}$.

After $2k+3$ rounds, since we apply an expanding round, we introduce a new internal variable $S^k = Y^{(2l+1)(k-1)+2}$ and we obtain a KPA with $m \simeq 2^{(2l+\frac{1}{2})n}$ and $O(m)$ computations. Beyond $2k+3$ rounds, we will attack generators of permutations and not a single permutation. This is done in Appendix A.

Remarks:

1. We can attack the chains beginning by I^2 and I^4 since the internal variables which are taken as inputs for f_2 and f_4 do not depend on all the coordinates of input variables. We have then more conditions on the input variables and less conditions on the internal variables and the attacks succeed.
2. If we begin with a contracting round instead of an expanding round, the computations and the attacks are quite similar, but we can attack only $2k-2$ rounds in CPA-1 and $2k+2$ rounds in KPA as long as we use a single permutation.

7 Summary of the Results for k odd, $d \leq 2k+3$ and $k \geq 5$

All the results for k odd, $d \leq 2k+3$ and $k \geq 5$ are summarized in the following table.

Table 1. Summary of the complexity of the best attacks on A_k^d against one permutation, $k = 2l+1$, $k \geq 5$. After $2k+3$ rounds, we need to attack a generator of permutations and not only a single permutation.

d	KPA	CPA-1	d	KPA	CPA-1
1, 2	1	1	$k+6,\ k+7$	$2^{\frac{(l+4)n}{2}}$	2^n
3, 4	$2^{\frac{n}{2}}$	2	$k+2p,\ k+2p+1$	$2^{\frac{(l+2p-2)n}{2}}$	$2^{(p-1)n}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2p+1,\ 2p+2$	$2^{\frac{pn}{2}}$	2	$2k-1$	$2^{\frac{(3l-2)n}{2}}$	$2^{(l-1)n}$
$\vdots$	$\vdots$	$\vdots$	$2k$	$2^{(2l-2)n)}$	
$k,\ k+1$	$2^{\frac{ln}{2}}$	2	$2k+1$	$2^{(2l-1)n}$	
$k+2,\ k+3$	$2^{\frac{(l+1)n}{2}}$	2	$2k+2$	$2^{(2l-\frac{1}{2})n)}$	
$k+4,\ k+5$	$2^{\frac{(l+2)n}{2}}$	$2^{\frac{n}{2}}$	$2k+3$	$2^{(2l+\frac{1}{2})n)}$	

8 Conclusion

Classical Feistel schemes, unbalanced Feistel schemes with contracting functions, and unbalanced Feistel schemes with expanding functions have been widely studied. In this paper, we focused on less known Feistel schemes, the alternating ones. More particularly, we presented attacks against these schemes. We demonstrated that they are completely unsecure when k is even: it is possible to attack any round with 2 messages in CPA-1 and about $2^{\frac{kn}{4}}$ messages in KPA. When k is odd, we can attack $2k-1$ rounds in CPA-1 and $2k+3$ rounds in KPA with less than 2^{kn} messages and computations. For $k=3$, it is possible to attack more rounds than with expanding (8 rounds) or contracting (6 rounds) functions. When k odd and $k \geq 5$, these schemes for CPA-1, seem to have the same level of security than unbalanced contracting schemes. However with alternating schemes, we need less memory to store the internal functions than with only contracting functions. An open question is the security of these schemes.

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. Paul G.Hoel, Sidney C.Port, and Charles J.Stone. *Introduction to Probability Theory.* Houghton Mifflin Company, 1971.
4. 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.
5. Lars R. Knudsen. DEAL - A 128-bit Block Cipher. Technical Report 151, University of Bergen, Department of Informatics, Norway, february 1998.
6. 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.
7. Michael Luby. *Pseudorandomness and cryptographic applications.* Princeton University Press, 1996.
8. Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
9. Stefan Lucks. Faster Luby-Rackoff Ciphers. In Dieter Gollman, editor, *Fast Software Encryption – FSE '96*, volume 1039 of *Lecture Notes in Computer Science*, pages 189–203. Springer-Verlag, 1996.
10. Moni Naor and Omer Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *J. Cryptology*, 12(1):29–66, 1999.
11. 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.
12. 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.
13. 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.
14. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions. *Cryptology ePrint archive: 2007/449: Listing for 2007.*
15. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 396–411. Springer-Verlag, 2006.
16. 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.
17. 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.

A Attacks with more than 2^{kn} computations

Until now we have studied Alternating Unbalanced Feistel schemes with random functions. In practice, for example in designing block ciphers we need to consider generators of pseudo-random permutations. In this section, we will describe attacks against a generator of permutations (and not only against a single permutation randomly generated by a generator of permutations), i.e. we will be able to study several permutations generated by the generator. This allows more than 2^{kn} computations.

A.1 Attack by the Signature

Using the following theorem, it is easy to see that an alternating permutation has an even signature.

Theorem 1 *Let Ψ be an alternating Feistel permutation from $\{0,1\}^{\alpha+\beta}$ to $\{0,1\}^{\alpha+\beta}$ with round functions from $\{0,1\}^{\beta}$ to $\{0,1\}^{\alpha}$. Then if $\alpha \geq 2$ and $\beta \geq 1$, Ψ has an even signature.*

The proof of this theorem follows from Theorem 1 of the extended version of [16] (see [14]). Let f be a permutation from kn bits to kn bits. Then using $O(2^{kn})$ computations on the 2^{kn} input/output values of f, we can compute the signature of f. To achieve this we just compute all the cycles c_i of f, $f = \prod_{i=1}^{\alpha} c_i$ and use the formula: signature$(f) = \prod_{i=1}^{\alpha} (-1)^{length(c_i)+1}$. The consequence is that it is possible to distinguish a generator of A_k^d from a generator of truly random permutations from kn bits to kn bits after $O(2^{kn})$ computations on $O(2^{kn})$ input/output values.

Remark: to compute the signature of a permutation g we need however to know all the input/outputs of g (or all of them minus one, since the last one can be found from the others if g is a permutation).

A.2 Attacks of A_k^d generators for $k \geq 5$ and odd

After $2k+4$ rounds, we are going to attack generators of permutations. We describe KPA. Let μ be the number of permutations that we will use. We will concentrate the attack on S^2, i.e. we use the chain generated by I^6:
$S^2 = I^6 \oplus g_1^5(I^1) \oplus g_3^3(Y^2) \oplus g_5^1(Y^{k+1}) \oplus f_6(Y^{2k}, Y^{2k+1}, \ldots, Y^{2(k-1)+(k-1)}, Y^{k+1}) \oplus g_7^{k-1}(Y^{2k}) \oplus g_9^{k-3}(Y^{3(k-1)+2}) \oplus \ldots \oplus g_{k+4}^2(Y^{(l+1)(k-1)+2}) \oplus g_{k+8}^{k-2}(Y^{(l+3)(k-1)+2}) \oplus \ldots \oplus g_{2k+3}^3(Y^{(2l+1)(k-1)+2})$ where $S^{k-1} = Y^{(2l+1)(k-1)+2}$.
It is possible to show that $\forall u,\ 2 \leq u \leq k-4,\ Y^{2(k-1)+u}$ depends on I^1, I^3, I^5 and I^t, $7 \leq t \leq k$. Moreover $Y^{2(k-1)+k-3}$, $Y^{2(k-1)+k-3}$, $Y^{2(k-1)+k-1}$ depend to all the input coordinates. The attack proceeds as follow: we count the number of (i,j), $i < j$ such that $I_i^1 = I_j^1,\ I_i^3 = I_j^3,\ I_i^5 = I_j^5,\ \forall t,\ 7 \leq t \leq k,\ I_i^t = I_j^t,\quad S_i^{k-1} = S_j^{k-1}$ and $S_i^2 \oplus I_i^6 = S_j^2 \oplus I_i^6$**(A1)**. When we are testing a random

permutation, we have: $\mathcal{N}_{perm} \simeq \mu\frac{m^2}{2\cdot 2^{2ln}} + O(\sqrt{\mu}\frac{m}{2^{ln}})$. For A_k^d, we have that $I_i^1 = I_j^1,\ I_i^3 = I_j^3,\ I_i^5 = I_j^5,\ \forall t,\ 7 \le t \le k,\ I_i^t = I_j^t$ and $\forall s,\ l \le s \le 2l+1,\ s \ne l+2,\ Y_i^{s(k-1)+2} = Y_j^{s(k-1)+2},\quad \forall u,\ k-3 \le u \le k-1,\ Y_i^{2(k-1)+u} = Y_j^{2(k-1)+u}$ imply **(A1)**. We obtain: $\mathcal{N}_{A_k^d} \simeq \mu\frac{m^2}{2\cdot 2^{2ln}} + \frac{m^2}{2\cdot 2^{(3l+2)n}}$. Thus we can distinguish the two generators when $\frac{m^2}{2^{(3l+2)n}} \ge \sqrt{\mu}\frac{m}{2^{ln}}$, i.e. when $\mu m^2 \ge 2^{(4l+4)n}$. When $m = 2^{kn} = 2^{(2l+1)n}$, this gives $\mu = 2^2$ and the complexity is $\lambda = \mu\cdot m = 2^{(2l+3)n}$. After $2k+5$ rounds, the chain beginning with I^6 is now on the first coordinate of the output, and since we have applied an expanding round we have one more internal variable $S^k = Y^{(2l+2)(k-1)+2}$. A similar attack gives $\mu = 2^4$ and the complexity $\lambda = \mu \cdot m = 2^{(2l+5)n}$.

After $2k+6$ rounds, we cannot keep the attacks on the chain generated by I^6. We have a contracting round and the chain becomes the coordinate of rank k of the output. Then it is easy to check that λ is multiplied by a factor of $2^{(2l-1)n}$. The chain beginning with I^8 which is S^2 will give the best attack. More generally, it is easy to see that for rounds $2k+2p$ and $2k+2p+1$, the chain generated by I^{2p+2} gives the best attacks with $\lambda = 2^{(2l+5p-7)n}$ and $\lambda = 2^{(2l+5p-5)n}$ respectively. Here we have that the internal variables $Y^{(p-1)(k-1)+u}$ that appear at round $2p$ satisfy: $\forall u,\ 2 \le u \le 2l-2p+3,\ Y^{(p-1)(k-1)+u}$ depend on $I^1, I^3, I^5, \ldots, I^t,\ 2p+1 \le t \le k$. Moreover $\forall u,\ 2l-2p+2 \le u \le k-1$, $Y^{(p-1)(k-1)+u}$, depend on all the coordinates of the input.

For rounds $3k-3$ and $3k-2$, we use the chain generated by I^{k-1}. Then $\lambda = 3^{(7l-12)n}$ and $\lambda = 3^{(7l-10)n}$. For rounds $3k-1$ and $3k$, we use the chain generated by I^1 for example (here there are several possibilities) and we obtain: $\lambda = 2^{(7l-8)n}$ and $\lambda = 2^{(7l-6)n}$. Then from round $3k+1$ to round $4k-1$, the chain generated by I^k gives the best attacks. For rounds $4k$ and $4k+1$, we use the chain generated by I^2 and finally for $4k+2$ and $4k+3$, we choose the chain generated by I^4. Then it is $2k$-periodic and we can iterate the choices of the chains. All the values of λ are multiplied by a factor of $2^{(8l-4)n}$ for each period.

For $k \ge 5$ and odd the results are given in table 2.

B Attacks on A_3^d

In this section, we explain briefly how to deal with the case $k = 3$. Here in fact, we can attack more rounds than in the general case: 11 rounds in CPA-1 instead of $2k-1 = 5$ rounds and 12 rounds in KPA instead of $2k+3 = 9$. This comes from the fact that in an expanding round, we only have 2 internal variables. Moreover, in all the attacks we studied, the CPA-1 can be transformed to KPA. Sometimes there exists other KPA, but they do not give a better result.

The attacks are quite similar to those used for $k \ge 5$. Up to round 8, we perform the attacks alternatively on S^3 and S^2. For rounds 9, 10 and 12, we use the chain generated by I^2 and for round 11, we choose the chain generated by I^3. After 13 rounds, we attack generators of permutations and we always take the chain generated by I^2. Then the phenomena is 6-periodic. The results are summarized in the table 3.

Table 2. Summary of the complexity of the best attacks on A_k^d against generators of permutations, $k = 2l + 1$, $k \geq 5$. After $2k + 4$ rounds, it is $2k$-periodic. If we suppose that for d rounds with $2k + 4 \leq d \leq 4k + 3$, the value is 2^{tn}, then for $d + p(2k)$, the value is given by $2^{[t+p(8l-4)]n}$.

d	KPA	d	KPA
$2k+4$	$2^{(2l+3)n}$	$3k$	$2^{(7l-6)n}$
$2k+5$	$2^{(2l+5)n}$	$3k+1$	$2^{(7l-6)n}$
$2k+6$	$2^{(2l+8)n}$	$3k+2,\ 3k+3$	$2^{(7l-5)n}$
$2k+7$	$2^{(2l+10)n}$	$\vdots$	$\vdots$
$2k+2p$	$2^{(2l+5p-7)n}$	$3k+2p,\ k+2p+1$	$2^{(7l-2p-7)n}$
$2k+2p+1$	$2^{(2l+5p-5)n}$	$4k-1$	$2^{(9l-7)n}$
$\vdots$	$\vdots$	$4k$	$2^{(10l-9)n)}$
$3k-3$	$2^{(7l-12)n}$	$4k+1$	$2^{(10l-7)n}$
$3k-2$	$2^{(7l-10)n}$	$4k+2$	$2^{(10l-6)n}$
$3k-1$	$2^{(7l-8)n}$	$4k+3$	$2^{(10l-4)n}$

Table 3. Summary of the complexity of the best attacks on A_3^d against one permutation. After 12 rounds, we need to attack a generator of permutations and not only a single permutation.

d	KPA	CPA-1	d	KPA
1, 2	1	1	$13+6p$	$2^{(3+4p)n}$
3, 4	$2^{\frac{n}{2}}$	2	$14+6p$	$2^{(4+4p)n}$
5, 6	2^n	2	$15+6p$	$2^{(5+4p)n}$
7, 8	$2^{\frac{3n}{2}}$	$2^{\frac{n}{2}}$	$16+6p$	$2^{(5+4p)n}$
9,10	2^{2n}	2^n	$17+6p$	$2^{(6+4p)n}$
11	$2^{\frac{5n}{2}}$	2^{2n}	$18+6p$	$2^{(6+4p)n}$
12	$2^{\frac{5n}{2}}$			

C Computation of the standard deviation for random permutations

In this section, we will explain how to compute $E(\mathcal{N}_{perm})$ and $\sigma(\mathcal{N}_{perm})$ after $k+8$ rounds, where $k = 2l+1$, in CPA-1. For any round, the computations are similar and we obtain that the standard deviation is about the square root of the mean value. The input is $[I^1, \ldots, I^k]$ and the output is $[S^1, \ldots, S^k]$. In the case of random permutations, we consider m messages such that $\forall i,\ 1 \leq i \leq m$, $\forall t,\ 0 \leq t \leq l-1,\ I_i^{2t+1} = 0$ and we suppose that $k \geq 9$ and $m \leq 2^{(l+1)n}$. We want to count the number of (i,j), $i < j$ such that $S_i^k = S_j^k$ and $S_i^{k-8} \oplus I_i^k = S_j^{k-8} \oplus I_j^k$ (**C.1**). We introduce the following random variables:

$$\begin{cases} \delta_{i,j} = 1 \text{ if } S_i^k = S_j^k \text{ and } S_i^{k-8} \oplus I_i^k = S_j^{k-8} \oplus I_j^k \\ \delta_{i,j} = 0 \text{ otherwise} \end{cases}$$

Then $\mathcal{N}_{perm} = \sum_{i<j} \delta_{i,j}$ and $E(\mathcal{N}_{perm}) = \sum_{i<j} E(\delta_{i,j})$. We have: $E(\delta_{i,j}) = Pr_{h\in B_{kn}}\big[S_i^k = S_j^k$ and $S_i^{k-8} \oplus I_i^k = S_j^{k-8} \oplus I_j^k\big]$ where B_{kn} is the set of all permutations from kn bits to kn bits. If $I_i^k = I_j^k$, then $E(\delta_{i,j}) = \frac{2^{(k-2)n}-1}{2^{kn}-1}$ and if $I_i^k \neq I_j^k$, then $E(\delta_{i,j}) = \frac{2^{(k-2)n}}{2^{kn}-1}$. Let α be the number of (i,j) such that $I_i^k = I_j^k$. If we choose $\alpha = \frac{m(m-1)}{2\cdot 2^n} + O(\frac{m}{\sqrt{2^n}})$, we obtain:
$\frac{m(m-1)}{2\cdot 2^{2n}}\big(1 + \frac{1}{2^{kn}} + \frac{1}{2^{2kn}} + O(\frac{1}{2^{3kn}})\big) \leq E(\mathcal{N}_{perm}) \leq \frac{m(m-1)}{2\cdot 2^{2n}} + O(\frac{m}{2^{(k+\frac{1}{2})n}})$. Thus $E(\mathcal{N}_{perm}) \simeq \frac{m(m-1)}{2\cdot 2^{2n}}$. We now compute the standard deviation. $V(\delta_{i,j}) = E(\delta_{i,j}^2) - E(\delta_{i,j})^2 = E(\delta_{i,j}) - E(\delta_{i,j})^2$. When $I_i^k = I_j^k$, we obtain:
$V(\delta_{i,j}) = \frac{1}{2^{2n}}\big(1 - \frac{1}{2^{2n}} + \frac{3}{2^{kn}} - \frac{2}{2^{(k+2)n}} + \frac{5}{2^{2kn}}\big) + O(\frac{1}{2^{(3k+2)n}}) + \frac{1}{2^{kn}} - \frac{2}{2^{kn}} + O(\frac{1}{2^{3kn}})$. This gives: $V(\delta_{i,j}) \simeq \frac{1}{2^{2n}}\big(1 - \frac{1}{2^{2n}}\big)$. When $I_i^k \neq I_j^k$, we have:
$V(\delta_{i,j}) = \frac{1}{2^{2n}}\big(1 - \frac{1}{2^{2n}} + \frac{1}{2^{kn}} - \frac{2}{2^{(k+2)n}} + \frac{1}{2^{2kn}} + \frac{1}{2^{(2k+2)n}}\big) + O(\frac{1}{2^{(3k+2)n}})$. and again $V(\delta_{i,j}) \simeq \frac{1}{2^{2n}}\big(1 - \frac{1}{2^{2n}}\big)$. This implies that $\sum_{i<j} V(\delta_{i,j}) \simeq \frac{m(m-1)}{2\cdot 2^{2n}}\big(1 - \frac{1}{2^{2n}}\big)$.

We now use the formula: $V(\mathcal{N}_{perm}) = V(\sum_{i<j} \delta_{i,j}) = \sum_{i<j} V(\delta_{i,j}) + \sum_{i<j,q<r,(i,j)\neq(q,r)} \big[E(\delta_{i,j}\,\delta_{q,r}) - E(\delta_{i,j})\,E(\delta_{q,r})\big]$.

First, we consider the case where i,j,q,r are pairwise distinct. If $I_i^k \neq I_j^k$ and $I_q^k \neq I_r^k$, we have $E(\delta_{i,j})\,E(\delta_{q,r}) = \frac{1}{2^{4n}}\big(1 + \frac{2}{2^{kn}} + \frac{3}{2^{2kn}} - O(\frac{1}{2^{3kn}})\big)$. If $I_i^k \neq I_j^k$ and $I_q^k = I_r^k$, then $E(\delta_{i,j})\,E(\delta_{q,r}) = \frac{1}{2^{4n}}\big(1 - \frac{1}{2^{(k-2)n}} + \frac{2}{2^{kn}} - \frac{2}{2^{(2k-2)n}} + \frac{3}{2^{2kn}} - \frac{3}{2^{(3k-2)n}} + O(\frac{1}{2^{3kn}})\big)$. If $I_i^k = I_j^k$ and $I_q^k = I_r^k$, we obtain $E(\delta_{i,j})\,E(\delta_{q,r}) = \frac{1}{2^{4n}}\big(1 - \frac{2}{2^{(k-2)n}} + \frac{2}{2^{kn}} + \frac{1}{2^{(2k-4)n}} - \frac{4}{2^{(2k-2)n}} + \frac{3}{2^{2kn}} + \frac{2}{2^{(3k-4)n}} - \frac{6}{2^{(3k-2)n}} + O(\frac{1}{2^{3kn}})\big)$. In order to compute $E(\delta_{i,j}\,\delta_{q,r})$ we have to separate the computations into four cases. We describe the main one: $I_i^k \neq I_j^k$, $I_q^k \neq I_r^k$ and $I_i^k \oplus I_j^k \oplus I_q^k \oplus I_r^k \neq 0$. For the other cases, the computations are similar. We denote by C the total number of possibilities for the output. Then $C = 2^{kn}(2^{kn}-1)(2^{kn}-2)(2^{kn}-3)$. We have now to compute B the number of outputs $[S_i^1,\ldots,S_i^k]$, $[S_j^1,\ldots,S_j^k]$, $[S_q^1,\ldots,S_q^k]$ and $[S_r^1,\ldots,S_r^k]$ that satisfy the above relations (**C.1**). We have 2^{kn} possibilities for $[S_i^1,\ldots,S_i^k]$. When this output is fixed, then we have $2^{(k-2)n}$ possibilities for $[S_j^1,\ldots,S_j^k]$. Then we have to fix the two other outputs. First, we suppose that $S_q^k \neq S_i^k$. Here, there are $(2^n-1)2^{(k-1)n}2^{(k-2)n} = 2^{(2k-3)n}(2^n-1)$ possibilities for $[S_q^1,\ldots,S_q^k]$ and $[S_r^1,\ldots,S_r^k]$. Then we have to consider the case where $S_q^k = S_i^k$. Here, there are five subcases. Cases 1, 2, 3, and 4 are $S_q^{k-8} = S_i^{k-8} \oplus I_q^k \oplus I_r^k$, $S_q^{k-8} = S_j^{k-8} \oplus I_q^k \oplus I_r^k$, $S_q^{k-8} = S_i^{k-8}$ or $S_q^{k-8} = S_j^{k-8}$ and for each of these cases, there are $2^{(k-2)n}(2^{(k-2)n}-1)$ possibilities for $[S_q^1,\ldots,S_q^k]$, $[S_r^1,\ldots,S_r^k]$. The last case is when we have eliminated the previous cases and this gives $(2^n-4)2^{(k-2)n}2^{(k-2)n}$ possibilities for $[S_q^1,\ldots,S_q^k]$, $[S_r^1,\ldots,S_r^k]$. Finally, we obtain $B = 2^{(4k-4)n}\big(1 - \frac{4}{2^{kn}}\big)$ and since $E(\delta_{i,j}\,\delta_{q,r}) = \frac{B}{C}$, we get:
$E(\delta_{i,j}\,\delta_{q,r}) = \frac{1}{2^{4n}}\big(1 + \frac{2}{2^{kn}} + \frac{1}{2^{2kn}} + O(\frac{1}{2^{3kn}})\big)$ and $E(\delta_{i,j}\,\delta_{q,r}) - E(\delta_{i,j})\,E(\delta_{q,r}) = \frac{1}{2^{4n}}\big(-\frac{2}{2^{2kn}} + O(\frac{1}{2^{3kn}})\big)$. The computations in the other cases are similar and we obtain for the case where i,j,q,r are pairwise distinct a term in $O(\frac{m^4}{2^{4n}.2^{(2k-2)n}})$. Then we have to study the case where in $\{i,j,q,r\}$ there are exactly 3 different values. We obtain a term in $O(\frac{m^3}{2^{(k+2)n}})$. Finally, we get $V(\mathcal{N}_{perm}) = \frac{m(m-1)}{2\cdot 2^{2n}} +$

$O(\frac{m^2}{2^{4n}})+O(\frac{m^4}{2^{4n}.2^{(2k-2)n}})+O(\frac{m^3}{2^{(k+2)n}})$. The first two terms correspond to the sum of the variances of $\delta_{i,j}$, the third term corresponds to the covariances of four distinct indices i,j,q,r and the last term to the covariances of 4-tuples of indices with one in common. For $m \geq 2^{2n}$ and $m \leq 2^{(l+1)n}$, we obtain $V(\mathcal{N}_{perm}) \simeq \frac{m(m-1)}{2 \cdot 2^{2n}}$ and the standard deviation is about the square root of the mean value as claimed.

D Computation of the standard deviation for A_k^{k+8}

We still suppose that $k \geq 9$, $k = 2l+1$ and we want to compute $E(\mathcal{N}_{A_k^{k+8}})$ and $\sigma(\mathcal{N}_{A_k^{k+8}})$. The input is $[I^1, \ldots, I^k]$ and the output is $[S^1, \ldots, S^k]$. We have m messages such that $\forall i,\ 1 \leq i \leq m,\ \forall t,\ 0 \leq t \leq l-1,\ I_i^{2t+1} = 0\ (*)$ and we want to compute the number of (i,j), $i<j$ satisfying: $S_i^k = S_j^k$ and $S_i^{k-8} \oplus I_i^k = S_j^{k-8} \oplus I_j^k$ $(\mathbf{D.1})$ where $S^{k-8} = I^k \oplus g_1^{k-1}(I^1) \oplus g_3^{k-3}(Y^2) \oplus \ldots \oplus g_{k-2}^2(Y^{(l-2)(k-1)+2}) \oplus g_{k+2}^{k-2}(Y^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y^{(l+2)(k-1)+2}) \oplus g_{k+8}^{k-8}(Y^{(l+3)(k-1)+2})$ and $S^k = Y^{(l+3)(k-1)+2}$. Since we have condition $(*)$ on the inputs, $(\mathbf{D.1})$ is equivalent to $(\mathbf{D.2})$: $Y_i^{(l+3)(k-1)+2} = Y_j^{(l+3)(k-1)+2}$ and $g_{k+2}^{k-2}(Y_i^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_i^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_i^{(l+2)(k-1)+2}) = g_{k+2}^{k-2}(Y_j^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_j^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_j^{(l+2)(k-1)+2})$. There are two different possibilities:

1. $\forall s,\ l \leq s \leq l+3,\ Y_i^{s(k-1)+2} = Y_j^{s(k-1)+2}$.
2. $Y_i^{(l+3)(k-1)+2} = Y_j^{(l+3)(k-1)+2}$, $(Y_i^{l(k-1)+2}, Y_i^{(l+1)(k-1)+2}, Y_i^{(l+2)(k-1)+2}) \neq (Y_j^{l(k-1)+2}, Y_j^{(l+1)(k-1)+2}, Y_j^{(l+2)(k-1)+2})$ and $g_{k+2}^{k-2}(Y_i^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_i^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_i^{(l+2)(k-1)+2}) = g_{k+2}^{k-2}(Y_j^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_j^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_j^{(l+2)(k-1)+2})$.

If we study $Y^{l(k-1)+2}, Y^{(l+1)(k-1)+2}, Y^{(l+2)(k-1)+2}, Y^{(l+3)(k-1)+2}$, we obtain that these internal variables are uniformly distributed random variables. Thus the probability to obtain Case 1 is $\frac{1}{2^{4n}}$. For Case 2, the probability is given by $\frac{1}{2^n}(1-\frac{1}{2^{3n}})\frac{1}{2^n} = \frac{1}{2^{2n}} - \frac{1}{2^{5n}}$. If the $\delta_{i,j}$ are defined as in Appendix C, we obtain: $E(\delta_{i,j}) = \frac{1}{2^{2n}} + \frac{1}{2^{4n}} - \frac{1}{2^{5n}}$. Since $\mathcal{N}_{A_k^{k+8}} = \sum_{i<j} \delta_{i,j}$, we get: $E(\mathcal{N}_{A_k^{k+8}}) = \frac{m(m-1)}{2}\left(\frac{1}{2^{2n}} + \frac{1}{2^{4n}} - \frac{1}{2^{5n}}\right)$. Now we want to compute the standard deviation:

$V(\delta_{i,j}) = E(\delta_{i,j}^2) - E(\delta_{i,j})^2 = E(\delta_{i,j}) - E(\delta_{i,j})^2$

$V(\delta_{i,j}) = \frac{1}{2^{2n}} - \frac{2}{2^{5n}} - \frac{2}{2^{6n}} + \frac{2}{2^{7n}} + \frac{1}{2^{8n}} - \frac{2}{2^{9n}} + \frac{1}{2^{10n}}$

We will use again the covariance formula. Here we have:

$E(\delta_{i,j})E(\delta_{q,r}) = \frac{1}{2^{4n}} + \frac{2}{2^{6n}} - \frac{2}{2^{7n}} + \frac{1}{2^{8n}} - \frac{2}{2^{9n}} + \frac{1}{2^{10n}}$ and we now have to compute $E(\delta_{i,j}\,\delta_{q,r})$. Again we first consider the case where i,j,q,r are pairwise distinct. We have several cases. The first one is $Y_i^{(l+3)(k-1)+2} = Y_j^{(l+3)(k-1)+2}$, $Y_q^{(l+3)(k-1)+2} = Y_r^{(l+3)(k-1)+2}$ and $(Y_i^{l(k-1)+2}, Y_i^{(l+1)(k-1)+2}, Y_i^{(l+2)(k-1)+2}) = (Y_j^{l(k-1)+2}, Y_j^{(l+1)(k-1)+2}, Y_j^{(l+2)(k-1)+2})$

$(Y_q^{l(k-1)+2}, Y_q^{(l+1)(k-1)+2}, Y_q^{(l+2)(k-1)+2}) = (Y_r^{l(k-1)+2}, Y_r^{(l+1)(k-1)+2}, Y_r^{(l+2)(k-1)+2})$
The probability is $\frac{1}{2^{8n}}$.
The second case is $Y_i^{(l+3)(k-1)+2} = Y_j^{(l+3)(k-1)+2}$, $Y_q^{(l+3)(k-1)+2} = Y_r^{(l+3)(k-1)+2}$ and
$(Y_i^{l(k-1)+2}, Y_i^{(l+1)(k-1)+2}, Y_i^{(l+2)(k-1)+2}) = (Y_j^{l(k-1)+2}, Y_j^{(l+1)(k-1)+2}, Y_j^{(l+2)(k-1)+2})$
$(Y_q^{l(k-1)+2}, Y_q^{(l+1)(k-1)+2}, Y_q^{(l+2)(k-1)+2}) \neq (Y_r^{l(k-1)+2}, Y_r^{(l+1)(k-1)+2}, Y_r^{(l+2)(k-1)+2})$
and
$g_{k+2}^{k-2}(Y_q^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_q^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_q^{(l+2)(k-1)+2}) =$
$g_{k+2}^{k-2}(Y_r^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_r^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_r^{(l+2)(k-1)+2})$. and the similar case when we exchange (i,j) and (q,r). The probability is given by $\frac{1}{2^{6n}} - \frac{1}{2^{9n}}$.
The third case is $Y_i^{(l+3)(k-1)+2} = Y_j^{(l+3)(k-1)+2}$, $Y_q^{(l+3)(k-1)+2} = Y_r^{(l+3)(k-1)+2}$ and
$(Y_i^{l(k-1)+2}, Y_i^{(l+1)(k-1)+2}, Y_i^{(l+2)(k-1)+2}) \neq (Y_j^{l(k-1)+2}, Y_j^{(l+1)(k-1)+2}, Y_j^{(l+2)(k-1)+2})$
$(Y_i^{l(k-1)+2}, Y_i^{(l+1)(k-1)+2}, Y_i^{(l+2)(k-1)+2}) = (Y_q^{l(k-1)+2}, Y_q^{(l+1)(k-1)+2}, Y_q^{(l+2)(k-1)+2})$
$(Y_j^{l(k-1)+2}, Y_j^{(l+1)(k-1)+2}, Y_i^{(l+2)(k-1)+2}) = (Y_r^{l(k-1)+2}, Y_r^{(l+1)(k-1)+2}, Y_r^{(l+2)(k-1)+2})$
and
$g_{k+2}^{k-2}(Y_i^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_i^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_i^{(l+2)(k-1)+2}) =$
$g_{k+2}^{k-2}(Y_j^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_j^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_j^{(l+2)(k-1)+2})$
and the similar case when we exchange (i,j) and (q,r). The probability is given by $\frac{1}{2^{9n}} - \frac{1}{2^{12n}}$.
The last case is $Y_i^{(l+3)(k-1)+2} = Y_j^{(l+3)(k-1)+2}$, $Y_q^{(l+3)(k-1)+2} = Y_r^{(l+3)(k-1)+2}$ and
$(Y_i^{l(k-1)+2}, Y_i^{(l+1)(k-1)+2}, Y_i^{(l+2)(k-1)+2}) \neq (Y_j^{l(k-1)+2}, Y_j^{(l+1)(k-1)+2}, Y_j^{(l+2)(k-1)+2})$
$(Y_q^{l(k-1)+2}, Y_q^{(l+1)(k-1)+2}, Y_q^{(l+2)(k-1)+2}) \neq (Y_r^{l(k-1)+2}, Y_r^{(l+1)(k-1)+2}, Y_r^{(l+2)(k-1)+2})$
and we have eliminated the previous cases and
$g_{k+2}^{k-2}(Y_i^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_i^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_i^{(l+2)(k-1)+2}) =$
$g_{k+2}^{k-2}(Y_j^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_j^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_j^{(l+2)(k-1)+2})$ $g_{k+2}^{k-2}(Y_q^{l(k-1)+2}) \oplus$
$g_{k+4}^{k-4}(Y_q^{(l+1)(k-1)+2}) \oplus g_{k+6}^{k-6}(Y_q^{(l+2)(k-1)+2}) = g_{k+2}^{k-2}(Y_r^{l(k-1)+2}) \oplus g_{k+4}^{k-4}(Y_r^{(l+1)(k-1)+2}) \oplus$
$g_{k+6}^{k-6}(Y_r^{(l+2)(k-1)+2})$. The probability is $\frac{1}{2^{4n}} - \frac{2}{2^{7n}} + \frac{1}{2^{10n}} + \frac{2}{2^{13n}}$. Finally in the case where i,j,q,r are pairwise distinct we obtain $E(\delta_{i,j}\,\delta_{q,r}) - E(\delta_{i,j})\,E(\delta_{q,r}) = \frac{2}{2^{9n}} - \frac{2}{2^{10n}} - \frac{2}{2^{12n}} + \frac{2}{2^{13n}}$. When we have only 3 different values in $\{i,j,q,r\}$ we obtain with similar computations: $E(\delta_{i,j}\,\delta_{q,r}) - E(\delta_{i,j})\,E(\delta_{q,r}) = \frac{1}{2^{6n}} - \frac{1}{2^{7n}} - \frac{1}{2^{9n}} + \frac{1}{2^{10n}}$.
This gives: $V(\mathcal{N}_{A_k^{k+8}}) = \frac{m(m-1)}{2\cdot 2^{2n}}\left(1 - \frac{1}{2^{3n}} - \frac{2}{2^{4n}} + \frac{2}{2^{5n}} - \frac{1}{2^{6n}} + \frac{2}{2^{7n}} - \frac{1}{2^{10n}}\right) + O(\frac{m^4}{2^{9n}}) + O(\frac{m^3}{2^{6n}})$.

E Conclusion on A_k^{k+8}

The computations in Appendices C and D show that when $m \simeq 2^{3n}$, we have: $\sigma(\mathcal{N}_{perm}) \simeq \frac{m}{2^n}$, $\sigma(\mathcal{N}_{A_k^{k+8}}) \simeq \frac{m}{2^n}$ and $|E(\mathcal{N}_{perm}) - E(\mathcal{N}_{A_k^{k+8}})| \simeq \frac{m(m-1)}{2\cdot 2^{4n}}$. This shows that we can distinguish a A_k^{k+8} permutation from a random permutation when $\frac{m(m-1)}{2\cdot 2^{4n}} \geq \frac{m}{2^n}$ i.e. $m \simeq 2^{3n}$ as wanted.