IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2019, No. 1, pp. 264–301. DOI:10.13154/tosc.v2019.i1.264-301

General Diffusion Analysis: How to Find Optimal Permutations for Generalized Type-II Feistel Schemes

Victor Cauchois[1,2], Clément Gomez[1] and Gaël Thomas[1]

[1] Direction générale de l'armement - Maîtrise de l'information (DGA MI), Boîte Postale 7, 35998 Rennes Cedex 9, France
victor.cauchois@m4x.org, clement.gomez@m4x.org, gael.thomas@intradef.gouv.fr

[2] Institut de Recherche Mathématique de Rennes (IRMAR), Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France

Abstract.
Type-II Generalized Feistel Schemes are one of the most popular versions of Generalized Feistel Schemes. Their round function consists in applying a classical Feistel transformation to p sub-blocks of two consecutive words and then shifting the k = 2p words cyclically. The low implementation costs it offers are balanced by a low diffusion, limiting its efficiency. Diffusion of such structures may however be improved by replacing the cyclic shift with a different permutation without any additional implementation cost. In this paper, we study ways to determine permutations with the fastest diffusion called *optimal permutations*.
To do so, two ideas are used. First, we study the natural equivalence classes of permutations that preserve cryptographic properties; second, we use the representation of permutations as coloured trees.
For both heuristic and historical reasons, we focus first on *even-odd permutations*, that is, those permutations for which images of even numbers are odd. We derive from their structure an upper bound on the number of their equivalence classes together with a strategy to perform exhaustive searches on classes. We performed those exhaustive searches for sizes $k \leq 24$, while previous exhaustive searches on all permutations were limited to $k \leq 16$. For sizes beyond the reach of this method, we use tree representations to find permutations with good intermediate diffusion properties. This heuristic leads to an optimal even-odd permutation for $k = 26$ and best-known results for sizes $k = 64$ and $k = 128$.
Finally, we transpose these methods to all permutations. Using a new strategy to exhaust equivalence classes, we perform exhaustive searches on classes for sizes $k \leq 20$ whose results confirmed the initial heuristic: there always exist optimal permutations that are even-odd and furthermore for $k = 18$ all optimal permutations are even-odd permutations.

Keywords: Feistel · Diffusion · Permutations

1 Introduction

Since its first appearance in 1973 with the cipher Lucifer, later evolving into Data Encryption Standard, DES [DES77], the Feistel network has become one of the main flavour of block ciphers. More recently, Camellia [AIK+00] and SIMON [BSS+13] are also examples of Feistel networks. This initial version splits a message into two blocks and consists in iterating a round function: $(m_1, m_2) \mapsto (m_2, m_1 \oplus F(m_2))$ where F is some non-linear

Received: 2018-06-01, Revised: 2018-11-23, Accepted: 2019-01-23, Published: 2019-03-08

application. A natural generalisation of Feistel Networks called Generalized Feistel Structures reproduces these routines, splitting the message into $k \geq 2$ blocks, where k is called the *partition number*. Among those Generalized Feistel Structures, the so-called Type-II Feistel Ciphers introduced in [ZMI89] consist in iterations of a round function of the form:

$$(m_0, \ldots, m_{k-1}) \mapsto (F_0(m_0) \oplus m_1, m_2, F_1(m_2) \oplus m_3, \ldots, F_{(k-2)/2}(m_{k-2}) \oplus m_{k-1}, m_0)$$

where the F_i's are non-linear cryptographic keyed functions. Type-II Feistel Ciphers have another natural description. They may be seen as the successive application of parallel non-linear transformations: $(m_i, m_{i+1}) \mapsto (m_i, m_{i+1} \oplus F_{i/2}(m_i))$ and of a cyclic shift of one block to the left. This very simple description and its induced high parallelism have inspired several block cipher designers for instance with RC6 [RRSY98], HIGHT [HSH+06], or CLEFIA [SSA+07].

While AES [DR02] has become very popular, it was not really designed with small-scale implementations as a main target and Type-II Feistel Ciphers offer an interesting alternative for these implementations. Large partition numbers are considered suitable for this application since the width of the round function, directly connected with the size of implementations, shrinks with growing partition numbers. Moreover, implementation costs for decryption are negligibly small once encryption has been implemented. For small-scale implementations when both encryption and decryption are needed, such constructions are to be considered. They offer interesting trade-offs between efficiency and compactness measured respectively by the number of rounds and the partition number. Recent Generalized Feistel Structures use a small partition number to balance implementation sizes and speed. Such structures come however with a serious drawback, Type-II Feistel Ciphers have a low diffusion: k rounds are needed to ensure that an input difference diffuses to all output blocks. Imperfections in terms of diffusion are a serious threat and may lead to cryptanalysis such as impossible differential attack [BBS99] or saturation attacks [DKR97].

A major breakthrough was made in [SM10] where the diffusion issue was widely addressed. *Diffusion round*, the minimum number of rounds to ensure a full diffusion, is used to compare permutations. Moreover, they observe that low diffusion round is related to good security against impossible differential attacks and saturation attacks. They noticed the good behaviour of even-odd permutations for which images of odd number are even number and conversely. From exhaustive search, they recorded even-odd permutations with the lowest diffusion round for sizes $k \leq 16$. One of those permutations is used in the block cipher TWINE [SMMK12] or the cryptographic permutation Simpira [GM16]. Furthermore, they present a general construction of a permutation with prescribed diffusion round of $2\log_2(k)$ when k is a power of 2.

Our Contribution

Based on heuristics suggested in [SM10], we first focus on even-odd permutations. The analysis of their natural equivalence classes gives rise to an upper bound on the number of such equivalence classes from which we draw a strategy to exhaustively run through them for all sizes $k \leq 24$. Previous works were running exhaustive search on all permutations and were limited to $k \leq 16$. We exhibit next an expected good behaviour for optimal permutations upon which we propose a method to search for optimal permutations of larger sizes. We introduce there a new criterion called *collision-free depth* to highlight reasonable candidates. This idea allowed us to find an optimal even-odd permutation for size $k = 26$. When focusing on sizes that are powers of two, we define a new set of permutations raised from tree colourings containing the coloured de Bruijn graph already introduced by [SM10]. This method, practical until $k = 128$, allows us to find the best permutations in terms of diffusion to the best of our knowledge for sizes $k = 64$ and $k = 128$. Table 1 presents results on the known permutations with the lowest diffusion round. Up to size $k = 26$, these results are optimal: no better even-odd permutation exists.

Finally, we analyse the general case of all permutations. Once again, from natural equivalence classes of permutations, we draw a new strategy to exhaustively run through them for all sizes $k \leq 20$. The results for cases $k = 18$ and $k = 20$ seem to justify our heuristic to focus on even-odd permutations: there are always optimal permutations that are even-odd, and there are *only* even-odd permutations that are optimal for $k = 18$.

Table 1: Diffusion round of the best known permutations

Size	Diffusion Round	Reference	Size	Diffusion Round	Reference
6	5	[SM10]	20	9	Section 4
8	6	[SM10]	22	8	Section 4
10	7	[SM10]	24	9	Section 4
12	8	[SM10]	26	9	Section 5
14	8	[SM10]	32	10	[SM10] and Section 6
16	8	[SM10]	64	11	Section 6
18	8	Section 4	128	13	Section 6

Outline of the Document

Section 2 sets the framework in which our ideas will be developed with few preliminaries. In Section 3, we present a natural equivalence relation on permutations drawn from equivalence classes of Generalized Feistel Schemes that preserve cryptographic properties. As already suggested in [SM10], we focus in Section 4 on the so-called *even-odd permutations* and derive from a rigorous analysis of their equivalence classes an upper bound on the number of such equivalence classes together with a strategy to exhaustively run through all of them which allowed us to record all optimal ones for sizes $k \leq 24$. In Section 5, we associate collections of trees with permutations and derive a criterion called *collision-free depth* which measures the number of rounds satisfying a kind of perfect diffusion, in that every fork/branching in the algorithm contributes toward full diffusion. From this analysis, arises a new way for filtering permutations in order to find some with good diffusion properties. This method allows us to determine an optimal even-odd permutation for $k = 26$ without performing exhaustive search. This criterion is extended to binary graphs in Section 6 to reduce the number of candidates we want to test for sizes up to $k = 128$. We give then an *ad hoc* exhaustive search for a natural family of graphs. This results in the best known permutations in terms of diffusion for sizes $k \in \{64, 128\}$. Finally, in Section 7, we study the general case of all permutations. Inspired by Section 4, we derive a new strategy to exhaustively run through all of the equivalence classes without running through all permutations. This strategy allows us to exhaustively search all optimal permutations for $k = 20$.

2 Preliminaries

Before diving into the core of the subject, we recall here some notions that will be used throughout the paper.

2.1 Block Construction

A Generalized Type-II Feistel Scheme is defined as follows. One round is illustrated on Fig. 1 in the case where the block permutation is the left cyclic shift. This structure generalises to a round function with a different permutation.

Definition 1. A Generalized Type-II Feistel Scheme is defined by an even partition number $k = 2p$, a word size m, a number of rounds r, a permutation π of $\{0, \ldots, k-1\}$ and $r \cdot p$ cryptographic keyed functions F_i. The ciphertext of a message $(X_0, \ldots, X_{k-1})$ of size $n = k \cdot m$ is given by applying the round functions $\Pi \circ \mathcal{I}_i$ successively, where:

$$\begin{array}{lrcl} \mathcal{I}_i: & (X_0, \ldots, X_{k-1}) & \rightarrow & (X_0, F_{0+i\cdot p}(X_0) \oplus X_1, \ldots, X_{k-2}, F_{p-1+i\cdot p}(X_{k-2}) \oplus X_{k-1}) \\ \Pi: & (X_0, \ldots, X_{k-1}) & \rightarrow & (X_{\pi^{-1}(0)}, \ldots, X_{\pi^{-1}(k-1)}). \end{array}$$

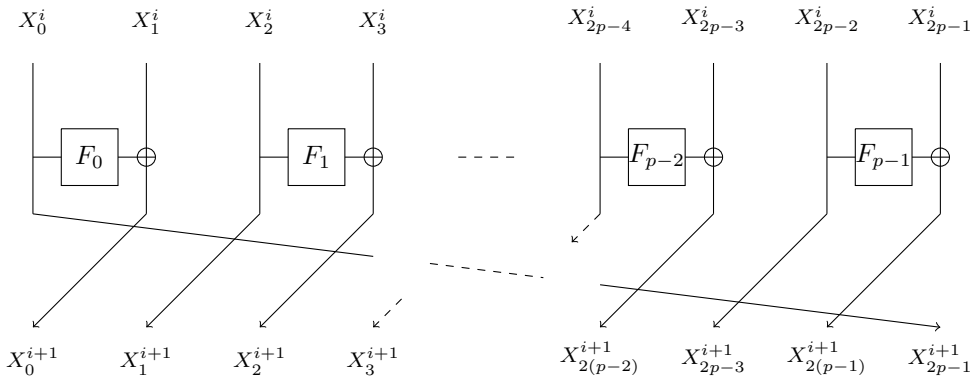

Figure 1: Round function of a Type-II Feistel Scheme

An example of cryptographic keyed function can be given by the XOR of a round key K^i followed by non linear functions, usually called *S-Boxes*. The i-th round is then illustrated on Fig. 2.

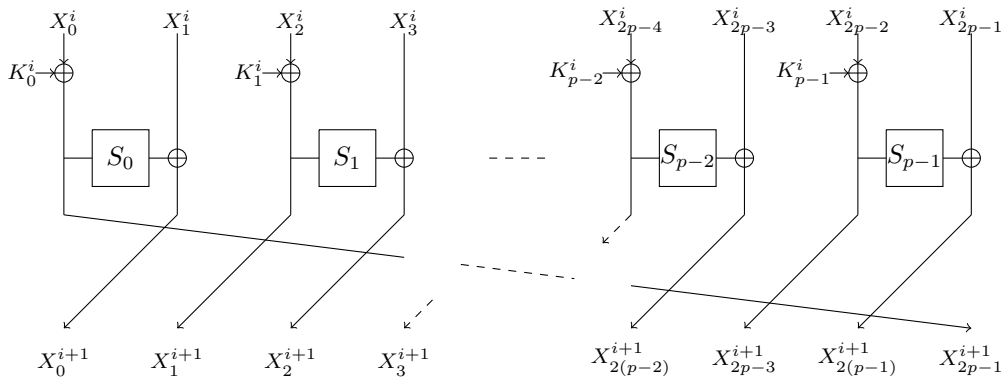

Figure 2: Example of cryptographic keyed functions for a Type-II Feistel Scheme

2.2 Diffusion Round

Designers aim at building *efficient* schemes that are cryptographically resistant. To estimate the cryptographic resistance of their schemes, designers usually make sure it resists to known attacks. Among them and following [SM10], we may cite the differential [BS90] and linear cryptanalysis [Mat93], the saturation attacks [DKR97] or the impossible differential attack [BBS99] against Feistel ciphers.

For a fixed choice of sizes k and m, and a fixed choice of cryptographic keyed functions, a Feistel designer wishes to find a permutation that minimizes r, the number of rounds

needed to ensure security since r dictates the speed of the algorithm. Depending on the choices of k and m, the attacks threatening the maximum number of rounds may either be the classical linear or differential attacks or the more peculiar saturation or impossible differential attacks. In [SM10], the authors show that the number of rounds necessary to achieve resistance against both of the latter attacks is very closely related to a notion they call *diffusion round*, denoted DR. The resistance of the scheme is achieved when r is greater than $2DR + 1$. This notion measures the quality of the diffusion of a round function of a given scheme and reveals to be fundamental in the design of such primitives. Its formalism goes back to Shannon in his seminal paper [Sha49].

This paper discusses ways to find permutations such that the Generalized Type-II Feistel Schemes they build have the best possible diffusion properties and thus offer the best possible resistance against both saturation and impossible differential attacks.

More precisely, diffusion and diffusion round are defined as in the following. If the variable at position i after r_1 rounds, $X_i^{r_1}$, is expressed by a formal equation containing a non-zero term in $X_j^{r_2}$ for $r_2 < r_1$, we say that $X_j^{r_2}$ diffuses to $X_i^{r_1}$ or that $X_i^{r_1}$ is affected by $X_j^{r_2}$. For instance, in Type-II Scheme described in Figure 1, X_0^1 is affected by X_0^0 and X_1^0 whereas X_1^1 is only affected by X_2^0.

Definition 2. For a Generalized Type-II Feistel Scheme built from a permutation π, denote by $DR_i^e(\pi)$ the minimum number of rounds such that the i^{th} input sub-block of the first round, X_i^0, is diffused to all output sub-blocks. The encryption diffusion round denoted by $DR^e(\pi)$ lies in $\{\mathbb{N}, \infty\}$ and is defined by:

$$DR^e(\pi) := \max_{0 \leq i \leq k-1} DR_i^e(\pi).$$

Decryption is made using π^{-1}. We are interested in the maximum between $DR^e(\pi)$ and $DR^e(\pi^{-1})$, hence the following definition:

Definition 3. For Generalized Type-II Feistel Scheme built from a permutation π, denote by $DR(\pi)$ the diffusion round of π defined by:

$$DR(\pi) = \max(DR^e(\pi), DR^e(\pi^{-1})).$$

Definition 4. A permutation of k elements is optimal if its diffusion round is minimal among all permutations of k elements.

The aim of this paper is to present methods to determine optimal permutations.

2.3 Notations on Permutations

In the following, p will be an integer and $k = 2p$ will be the size of the permutations. Permutations we consider will then be permutations of $\{0, \ldots, k-1\}$. We denote by $\mathcal{S}_k$ the set of all those permutations.

Definition 5. Let k be some integer. Let π be a permutation in $\mathcal{S}_k$. A cycle decomposition of π is a decomposition of π as a product of cycles with disjoint supports. If π has n_1 cycles of size t_1,..., and n_n cycles of size t_n, we say that π has decomposition type T_π, written as follows:

$$T_\pi = ((t_1, n_1), \ldots, (t_n, n_n)).$$

Remark 1. Since cycles in the cycle decomposition of a permutation have disjoint supports, they commute with each other. We will then with a slight abuse of notation talk about *the* cycle decomposition of a given permutation even if it is only unique up to the choice of the order of those cycles.

To refer to a permutation π, we may write its cycle decomposition or its value table depending on the context. Example 1 illustrates these notations.

Example 1. $p = 4 \Rightarrow k = 8$. We consider arbitrarily π, the permutation in $\mathcal{S}_8$ defined by:

$$\pi(0) = 3, \pi(1) = 2, \pi(2) = 4, \pi(3) = 6, \pi(4) = 1, \pi(5) = 7, \pi(6) = 0, \text{ and } \pi(7) = 5.$$

- If we are interested in its cycle decomposition, we shall write $\pi = (0, 3, 6)(1, 2, 4)(5, 7)$.
- The decomposition type of π is then $T_\pi = ((3, 2), (2, 1))$.
- Whenever cycle decomposition is not relevant, we shall write $\pi = \{3, 2, 4, 6, 1, 7, 0, 5\}$.

3 Global Considerations on Equivalence Classes

We recall now a notion of equivalence for Generalized Feistel Schemes from which derives a notion of equivalence for permutations. Considerations on the number of those classes, its use and some theoretical aspects are also presented. Note that everything presented in this section is generic and holds for *any* type-II Generalized Feistel Scheme of definition 1, and does not presume anything (such as being even-odd or optimal) about the permutations used in the Generalized Feistel Structures.

3.1 From Equivalence classes of Type-II Generalized Feistel Schemes to Equivalence classes of Permutations

From the definition of diffusion round, it can be seen that diffusion round stays the same regardless of the choice of the cryptographic keyed functions $(F_i)_{i \leq r \cdot p}$. We consider those as indeterminate functions and denote by $\mathcal{I}_i$, the following indeterminate application:

$$\mathcal{I}_i : (X_0, \ldots, X_{k-1}) \to (X_0, F_{0+i \cdot p}(X_0) \oplus X_1, \ldots, X_{k-2}, F_{p-1+i \cdot p}(X_{k-2}) \oplus X_{k-1}).$$

A Type-II Generalized Feistel Structure $\mathcal{F}$ is defined by its round functions $\mathcal{M}_i$ composed of $\mathcal{I}_i$ and Π built from a permutation π in $\mathcal{S}_k$ and by its number of rounds r, denoted by $GFS((\mathcal{I}_i)_{i \in \{1 \cdots r\}}, \pi, r)$:

$$\mathcal{F} = \prod \mathcal{M}_i = \prod (\Pi \circ \mathcal{I}_i).$$

Remark 2. A more formal description of this function is to consider $\mathcal{F}$ as an element of the multivariate polynomial ring $\mathbb{F}_2[Y_1, \ldots, Y_{r \cdot p}][X_0, \ldots, X_{k_1}]$, where the evaluations of the X_i's are made with elements in $\mathbb{F}_{2^m}$ and the evaluations of the Y_i's are made with cryptographic keyed functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$.

Cryptographic properties of a Type-II Generalized Feistel Structure are not modified by any reindexation of blocks. The following definition is a natural consequence of this fact.

Definition 6. Let $\mathcal{F}_1 = \prod \mathcal{M}_{1,i}$ and $\mathcal{F}_2 = \prod \mathcal{M}_{2,i}$ be any two Type-II Generalized Feistel Structure. They are said to be equivalent (up to block reindexation) if there exists a (block reindexing) permutation φ in $\mathcal{S}_k$ such that:

$$\forall i \in \{1, \cdots, r\}, \mathcal{M}_{1,i} = \varphi^{-1} \circ \mathcal{M}_{2,i} \circ \varphi.$$

Remark 3. For any choice of cryptographic keyed functions, two Type-II Generalized Feistel Schemes instantiations of two equivalent Type-II Generalized Feistel Structures have exactly the same cryptographic properties.

The rest of this section is dedicated to showing that any such φ in the previous definition must be of a special type, and that this induces an equivalence relation on the permutations π used in the Π function of a Generalized Feistel Scheme. In order to formalize, we need to define the notion of permutations of pairs:

Definition 7. The set of permutations of pairs $\mathcal{S}_k^p$ is the subset of permutations in $\mathcal{S}_k$ defined as:

$$\mathcal{S}_k^p = \{\varphi \in \mathcal{S}_k |\ \forall i \leq p-1, \varphi(2i) \text{ is even and } \varphi(2i+1) = \varphi(2i)+1\}.$$

We then have the following proposition.

Proposition 1. *Two Type-II Generalized Feistel Structures $\mathcal{F}_1 = GFS((\mathcal{I}_i)_{i\in\{1\cdots r\}}, \pi_1, r)$ and $\mathcal{F}_2 = GFS((\mathcal{I}_i)_{i\in\{1\cdots r\}}, \pi_2, r)$ are equivalent if and only if there exists a permutation of pairs $\varphi \in \mathcal{S}_k^p$ such that:*

$$\pi_1 = \varphi^{-1} \circ \pi_2 \circ \varphi.$$

Proof. Developing the variables $\mathcal{M}_{i,0}$, we have:

$$\pi_1 \circ \mathcal{I}_0 = \varphi^{-1} \circ \pi_2 \circ \mathcal{I}_0 \circ \varphi.$$

Evaluating the indeterminate functions at 0, we get:

$$\pi_1 = \varphi^{-1} \circ \pi_2 \circ \varphi.$$

This equality imposes:

$$\mathcal{I}_0 = \varphi^{-1} \circ \mathcal{I}_0 \circ \varphi.$$

This latest equality is equivalent to φ being a permutation of pairs.

□

Thanks to Proposition 1, we can rephrase Definition 6 using permutations of pairs. Both definitions are equivalent.

Definition 8. Let $\mathcal{F}_1 = \prod \mathcal{M}_{1,i}$ and $\mathcal{F}_2 = \prod \mathcal{M}_{2,i}$ be any two Type-II Generalized Feistel Structure. They are said to be equivalent (up to block reindexation) if there exists a (block reindexing) permutation *of pairs* φ in $\mathcal{S}_k^p$ such that:

$$\forall i \in \{1, \cdots, r\}, \mathcal{M}_{1,i} = \varphi^{-1} \circ \mathcal{M}_{2,i} \circ \varphi.$$

Equivalently, we can then define an equivalence relation on the permutations used to build type-II Generalized Feistel Structures.

Definition 9. Two permutations π_1 and π_2 of $\mathcal{S}_k$ are said to be pair-equivalent if there exists a permutation of pairs φ in $\mathcal{S}_k^p$ such that:

$$\pi_1 = \varphi^{-1} \circ \pi_2 \circ \varphi.$$

3.2 Number of Classes

For small values of k, optimal permutations can be found by exhaustive search. Because of its exponential complexity, $O(k!)$, this method becomes very quickly intractable. However, as permutations in the same pair-equivalence class share the same cryptographic properties, we would like to compute the diffusion round of only one element per class. Table 2 exhibits the fact that the number of classes is a lot smaller than the total number of permutations for small values of k. This heuristic is a first step in reducing the complexity of finding optimal permutations for greater values of k.

The previous table is a good motivation to find a strategy that computes quickly an element per equivalence class. An essential point of our work is to give a strategy that produces at least one permutation of each pair-equivalence class without computing these classes beforehand.

Table 2: Comparison between numbers of classes and total numbers of permutations

Feistel size	Number of pair-equivalence classes of permutations	Number of permutations
4	16	24
6	134	720
8	1796	40320

4 The Even-odd Case

From now on and until Section 7, we will focus on even-odd permutations. This property seems to be quite a natural requirement for optimal permutations since each position diffuses in at least two positions every two rounds. For non even-odd permutations, some positions do not diffuse in more than one position before three rounds. Intuitively we may think that such permutations should not diffuse as much as even-odd ones. Focusing on those even-odd permutations significantly decreases the complexity of exhaustive searches. The general case will be discussed in Section 7.

4.1 Even-odd Permutations

Following [SM10], we recall the definition:

Definition 10. Let k be an even number. A permutation π in $\mathcal{S}_k$ is called an even-odd permutation when the image by π of even elements are odd elements and conversely. The set of even-odd permutations of k elements is denoted by $\mathcal{S}_k^{eo}$.

For low values of k, optimal even-odd permutations together with their diffusion round can be determined through exhaustive search. For higher values of k, beyond the reach of practical exhaustive searches, we can compute from their structure a lower bound on the minimal diffusion round of even-odd permutations.

Denote by $(Fib(n))_{n\in\mathbb{N}}$ the Fibonacci sequence defined by:

$$\begin{cases} Fib(0) = 0 \\ Fib(1) = 1 \\ Fib(n+2) \quad = \quad Fib(n+1) + Fib(n) \text{ for } n \in \mathbb{N} \end{cases}$$

Proposition 2. *Let π be an even-odd permutation. Then,*

$$2 \cdot Fib(DR(\pi)) \geq k.$$

Proof. The proof from [SM10] is rewritten here both for the sake of completeness and mainly as an introduction to the search techniques discussed in the next sections. Let $\mathcal{F}$ be a Generalized Feistel Scheme built from an even-odd permutation π. Let i be an odd number in $\{0, \ldots, k-1\}$.

- After one round, X_i^0 has diffused to only one even position: $X^1_{\pi(i)}$.
- After two rounds, X_i^0 has diffused to one even position and one odd position: $X^2_{\pi^2(i)}$ and $X^2_{\pi(\pi(i)+1)}$.
- After r rounds, under the assumption that for all $\ell < r$, when X^ℓ_{2i} is affected by X^0_i, X^ℓ_{2i+1} is not, which maximizes the number of positions impacted, X_i^0 has diffused to $Fib(r-1)$ odd positions and $Fib(r)$ even positions.

Reproducing the same arguments for i even number in $\{0,\ldots,k-1\}$ ensures that X_i^0 diffuses to at most $Fib(r)$ odd positions and $Fib(r+1)$ even positions after r rounds. Full diffusion is obtained when X_i^0 have diffused to both p odd positions and p even positions for all $i \in \{0,\ldots,k-1\}$. This implies $2 \cdot Fib(DR(\pi)) \geq k$.

□

4.2 Number of Pair-equivalence Classes of Even-odd Permutations

We compute here an upper bound $\mathcal{U}_k^{eo}$ of the number of pair-equivalence classes for even-odd permutations and then give a strategy to build a set of $\mathcal{U}_k^{eo}$ even-odd permutations such that all pair-equivalence classes have at least a representative in this set.

Proposition 3. *For $k = 2p$, the cardinal of the set $\mathcal{S}_k^{eo}$ is given by $(p!)^2$.*

Proof. There are p possible matches for the images of 0 and 1, corresponding respectively to the number of odd and even elements. Then, there are $p-1$ remaining possible matches for the images of 2 and 3 and so on until $k-2$ and $k-1$.

□

Focusing on even-odd permutations drastically decreases the search space from $k!$ elements to $(p!)^2$ (recall $k = 2p$). In [SM10], exhaustive searches through even-odd permutations are performed up to $k = 16$ which requires 2^{30} tests whereas general exhaustive searches for $k = 16$ was beyond reach, requiring 2^{44} tests. Nevertheless, even exhaustive search through even-odd permutations becomes quickly intractable because of the exponential growth of $(p!)^2$ and the case $k = 22$ with its 2^{50} even-odd permutations is already beyond reach. Table 3 compares the number of classes and the number of even-odd permutations for small values of k:

Table 3: Number of pair-equivalence classes of even-odd permutations

Feistel size	Number of pair-equivalence classes of even-odd permutations	Number of even-odd permutations
4	4	4
6	11	36
8	43	576
10	161	14400
12	901	518400
14	5579	25401600

Denote by N_p the number of distinct cycle decompositions of permutations in $\mathcal{S}_p$.

Theorem 1. *Let $k = 2p$, and N_p be the number of distinct cycle decompositions of permutations in $\mathcal{S}_p$. The number of pair-equivalence classes of even-odd permutations in $\mathcal{S}_k$ is upper bounded by:*

$$\mathcal{U}_k^{eo} = N_p \cdot p!.$$

Proof. There are two natural bijections Ψ_1 and Ψ_2 given by:

$$\Psi_1 : \left\{ \begin{array}{ccc} \mathcal{S}_k^p & \to & \mathcal{S}_p \\ \varphi & \mapsto & \overline{\varphi} \text{ s.t. } \overline{\varphi}(i) = \frac{\varphi(2i)}{2}. \end{array} \right.$$

and

$$\Psi_2 : \left\{ \begin{array}{ccc|l} \mathcal{S}_p \times \mathcal{S}_p & \to & \mathcal{S}_k^{eo} & \\ (\varphi_1, \varphi_2) & \mapsto & \varphi \text{ s.t.} & \begin{array}{l} \varphi(2i) = 2\varphi_1(i) + 1 \\ \varphi(2i+1) = 2\varphi_2(i) \end{array} \end{array} \right.$$

with :

$$\Psi_2^{-1} : \left\{ \begin{array}{ccc} \mathcal{S}_k^{eo} & \rightarrow & \mathcal{S}_p \times \mathcal{S}_p \\ \varphi & \mapsto & (\varphi_1, \varphi_2) \text{ s.t. } \left| \begin{array}{l} \varphi_1(i) = \frac{\varphi(2i)-1}{2} \\ \varphi_2(i) = \frac{\varphi(2i+1)}{2} \end{array} \right. \end{array} \right.$$

Let $\{\varphi_j\}_{1 \leq j \leq N_p}$ be a set of permutations such that for any existing decomposition type t of elements in $\mathcal{S}_p$ there exists φ_ℓ in that set such that φ_ℓ is of type t, i.e. $T_{\varphi_\ell} = t$ (recall definition 5). We show now that any pair-equivalence class of even-odd permutations owns at least one element of the following set:

$$\{\Psi_2(\varphi_j, \pi), j \in \{1, \ldots, N_p\}, \pi \in \mathcal{S}_p\}.$$

Indeed, let π be an even-odd permutation and $(\pi_1, \pi_2) = \Psi_2^{-1}(\pi)$. Let $j \in \{1, \ldots, N_p\}$ such that $T_{\varphi_j} = T_{\pi_1}$ and let $\phi \in \mathcal{S}_p$ such that:

$$\phi^{-1} \circ \pi_1 \circ \phi = \varphi_j.$$

Then, for some $\psi \in \mathcal{S}_p$, we have:

$$\Psi_2^{-1}(\Psi_1^{-1}(\phi^{-1}) \circ \pi \circ \Psi_1^{-1}(\phi)) = (\varphi_j, \psi)$$

□

Remark 4. Computing the value of N_k is a well-known problem in partition theory. As a consequence of the Euler pentagonal number theorem, the numbers N_k can be computed recursively:

$$\left\{ \begin{array}{lcl} N_k & = & 0 \text{ if } k < 0 \\ N_0 & = & 1 \\ N_k & = & \sum_{i>0} (-1)^{i+1} \cdot (N_{k - \frac{i \cdot (3i+1)}{2}} + N_{k - \frac{i \cdot (3i-1)}{2}}) \end{array} \right.$$

The complexity reduction Theorem 1 induces is significant since $N_p \sim \frac{e^{\pi \cdot \sqrt{\frac{2 \cdot p}{3}}}}{4 \cdot \sqrt{3} \cdot p}$, which is negligible compared to $p!$.

Together with the proof of Theorem 1 comes a strategy to produce at least one even-odd permutation in each pair-equivalence class by constructing $N_p \cdot p!$ permutations.

Strategy 1 (Even-odd Pair-equivalence Class Exhaustive Search)**.**

1. *For all decomposition types t of size p, fix an arbitrary permutation ψ_t that satisfies this decomposition type.*

2. *For all permutation ϕ of p elements, construct the permutation $\pi_{\psi_t, \phi}$ given by:*

$$\left\{ \begin{array}{lcl} \pi_{\psi_t,\phi}(2j+1) & = & 2\psi_t(j) \\ \pi_{\psi_t,\phi}(2j) & = & 2\phi(j) + 1. \end{array} \right.$$

3. *The set $\mathcal{E}_k = \{\pi_{\psi_t,\phi}\}_{t,\phi}$ is then a set such that for any permutation φ in $\mathcal{S}_k$, there exists ϕ in $\mathcal{E}$ such that φ and ϕ are in the same pair-equivalent class.*

Example 2 illustrates the design of a permutation in $\mathcal{S}_k$ from a decomposition type of size p and a permutation in $\mathcal{S}_p$.

Example 2. Let $p = 7$. Consider the decomposition type $t = ((4, 1), (3, 1))$. Construct the permutation $\psi_t = (0, 1, 2, 3)(4, 5, 6)$. Let Id be the identity of $\{1, \ldots, 7\}$, the permutation $\pi_{\psi_t, Id}$ is given by:

$$\{1, 2, 3, 4, 5, 6, 7, 0, 9, 8, 11, 10, 13, 12\}.$$

Table 4: Comparisons between $\mathcal{U}_k^{eo}$ and $|\mathcal{S}_k^{eo}|$

k	N_p	$\log_2(\mathcal{U}_k^{eo})$	$\log_2(\lvert\mathcal{S}_k^{eo}\rvert)$
6	3	4.2	5.2
8	5	6.9	9.2
10	7	9.7	13.8
12	11	13.0	19.0
14	15	16.2	24.6
16	22	19.8	30.6
18	30	23.4	36.9
20	42	27.2	43.6
22	56	31.1	50.5
24	77	35.1	57.7
26	101	39.2	65.1
28	135	43.4	72.7
30	176	47.7	80.5
32	231	52.1	88.5

Table 5: Fibonacci lower bounds and optimal even-odd diffusion rounds

k	lower bound	$\min_{\pi\in\mathcal{S}_k^{eo}}(DR(\pi))$	Number of classes
6	5	5	1
8	6	6	2
10	6	7	3
12	7	8	32
14	7	8	23
16	7	8	13
18	8	8	2
20	8	9	2133
22	8	8	4
24	8	9	56

Table 4 compares the upper bound we found with the total number of even-odd permutations.

Remark 5. The upper bound $\mathcal{U}_k^{eo}$ is quite satisfying since $p!$ is a lower bound on the number of pair-equivalence classes. It is indeed the cardinal of the even-odd permutations divided by the cardinal of permutations of pairs. We have finally:

$$p! \leq \text{Number of classes } \leq N_p \cdot p!$$

4.3 Exhaustive Search on Even-odd Permutations

Computations in [SM10] were limited to $k \leq 16$. Applying Strategy 1 to produce $\mathcal{E}_k$ for $k \leq 24$ and testing all permutations built leads to the results shown in Table 5.

Representatives for pair-equivalence classes reaching optimal even-odd diffusion rounds are given in the appendix. Optimal even-odd diffusion rounds surprisingly do not grow uniformly with k. Two particularly interesting cases arise from previous results:

- Case $k = 18$: only two optimal even-odd pair-equivalence classes exist.
- Case $k = 20$: no even-odd permutation with diffusion round 8 exists.

5 Designing Permutations with Good Diffusion Rounds

When $k > 24$, even Strategy 1 becomes computationally intractable. This section introduces new strategies to find even-odd permutations with good diffusion rounds. We present now a search algorithm which aims at finding optimal even-odd permutations: **Collision-free**

Exhaustive Search. It builds first a subset of even-odd permutations designed to ensure a perfect diffusion until a given round before computing actual diffusion rounds of those permutations.

5.1 Collision-free Depths

As stipulated in [SM10], as can also be seen from the proof of Proposition 2, the number of collisions between consecutive even and odd positions (X^r_{2j} and X^r_{2j+1} affected by some X^0_i) seems to play an important part in the value of diffusion rounds. The following definitions are direct consequences of this remark.

From a permutation π in $\mathcal{S}_k$, from any integer $i \in \{0, \ldots, k-1\}$, we can recursively construct trees $\mathcal{T}(\pi, i, r)$ which illustrate the diffusion of an input position X^0_i after $n \leq r$ rounds. A tree is here recursively defined by an integer, the root of the tree, and by a set of trees, the children of the root. Nodes of depth n of $\mathcal{T}(\pi, i, r)$ are the set of position affected by i after n rounds.

Precise definition of $\mathcal{T}(\pi, i, r)$ is given by:

$$\begin{cases} \mathcal{T}(\pi, i, 0) & = & \{i, \emptyset\} \\ \mathcal{T}(\pi, 2 \cdot i, n) & = & \{2 \cdot i, \mathcal{T}(\pi, \pi(2 \cdot i), n-1), \mathcal{T}(\pi, \pi(2 \cdot i + 1), n-1)\} \\ \mathcal{T}(\pi, 2 \cdot i + 1, n) & = & \{2 \cdot i + 1, \mathcal{T}(\pi, \pi(2 \cdot i + 1), n-1)\} \end{cases}$$

The following definition aims to catch the number of rounds without collisions when considering diffusion from an input position.

Definition 11. A permutation π is said to be collision-free of depth r from i if the leaves of its associated trees $\mathcal{T}(\pi, i, n)$ are distinct for any $n < r$ and leaves of $\mathcal{T}(\pi, i, r)$ are not. We denote this depth by $CD(\pi, i)$.

We are then able to compute the minimum of those collision-free depths from input positions in order to catch the number of rounds without collisions from any input.

Definition 12. The collision-free depth of π, $CD(\pi)$, is the minimum of collision-free depths from each possible root:

$$CD(\pi) = \min_i(CD(\pi, i)).$$

A high collision-free depth denotes a very structured permutation.

Examples 3 and 4 should clarify these definitions:

Example 3. Let $\pi_1 = \{3, 0, 5, 2, 1, 4\}$. Figure 3 illustrates that $CD(\pi_1, 0) = 2$.

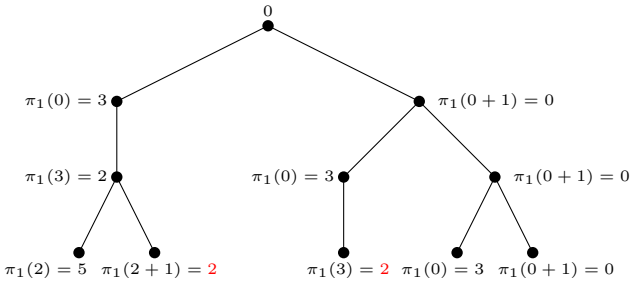

Figure 3: $\mathcal{T}(\pi_1, 0, 3)$

Let $\pi_2 = \{3, 0, 5, 4, 1, 2\}$. Figure 4 illustrates that $CD(\pi_2, 0) = 3$.

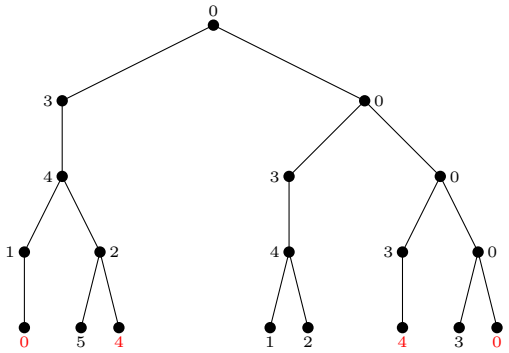

Figure 4: $\mathcal{T}(\pi_2, 0, 4)$

Remark 6. In the case of even-odd permutations, we do not need to study collision-free depths from odd roots since when i is odd, $CD(\pi, i) = 1 + CD(\pi, \pi(i))$ with $\pi(i)$ even. Collision-free depth of an even-odd permutation π is then:

$$CD(\pi) = \min_{i \text{ even}} (CD(\pi, i)).$$

We believe permutations with greater collision-free depths are more likely to have smaller diffusion rounds than other ones. This belief comes from the fact that when the Fibonacci bound is tight (for $k = 16$ or $k = 26$), this bound can only be reached by permutations whose odd positions X_i^0 diffuse without collisions of consecutive positions (X_{2j}^r and X_{2j+1}^r affected by X_i^0) when r is lower than the theoretical bound. Table 6 reinforces this hope by exhibiting Collision-free depths of known optimal even-odd permutations from [SM10] and subsection 4.3. Despite our heuristic, we notice however that some of the optimal permutations can also suffer from quite low collision-free depths.

Table 6: Collision-free depths of optimal even-odd permutations

k	16		18	20				22	24		
CD	3	4	3	2	3	4	5	5	3	4	5
♯ optimal classes	9	4	2	165	1624	340	4	4	19	32	5

Remark 7. It is clear that collision-free depths are pair-equivalence invariants. We have therefore focused once again our study on pair-equivalence classes.

5.2 Collision-free Search Algorithm

The Collision-free Search Algorithm, given in Algorithm 1, constructs a representative of each class of permutations that has a given collision-free depth. It works using a depth-first search with backtracking to avoid going through all permutations. More precisely, the algorithm works iteratively. From a partial permutation, we try to construct the image of the next element such that the new image doesn't lead to a collision. In case of impossibility, we perform backtracking in the search tree to consider another possibility for the previous choice of images.

It seems hard to give a theoretical value of its complexity and we only measure its efficiency empirically. Modifying parameters of Algorithm 1 leads to the following behaviour: low values of collision-free depth return many permutations whereas high values of collision-free depth impose many constraints and may return very few permutations.

The speed of Algorithm 1 comes from the fact that it gets rid of many classes at once. For instance, for all permutations π with $\pi(0) = 1$ and $\pi(1) = 0$, the algorithm does not find any further images for odd entries which yield a permutation with a collision-free depth greater than 3 and then it excludes all of these possibilities at once.

Results

- For $k \in \{16, 18\}$ with $CD(\pi) \geq 3$, optimal permutations are found almost instantaneously.
- For $k = 26$ with $CD(\pi) \geq 4$, many permutations with diffusion round 10 are found and none with diffusion round 9.

This result is quite surprising since the lower bound allows the hope to find permutations with diffusion round 9 or even 8. However, since $Fib(8) = 13 = \frac{26}{2}$, 8 was a tight bound of optimal diffusion round for $k = 26$ that could only be reached by even-odd permutations with collision-free depth of 7. The result of the algorithm shows that optimal permutations must have either 9 or 10 for their diffusion round.

Non-deterministic analogues

Algorithm 1 can also be used in a non-deterministic version. For large values of k, even exhaustive searches of permutations with fixed collision-free depth is beyond reach. In order to find permutations with low diffusion rounds, we choose random values for a given subset of entries and we construct all permutations with these fixed images and with a chosen collision-free depth. Such permutations are likely to have low diffusion round and even to be optimal. This strategy applied on $k = 26$ together with a collision-free depth of 3 raised permutations with diffusion round of 9. From the previous analysis, we know these permutations to be optimal which is a great validation of both this heuristic and this method. An example is given in the appendix.

6 From Collision-Free Permutations to Collision-Free Block Trees

To compute permutations with high collision-free depths, we introduced trees associated with a permutation and ensured that any root from 0 to $k-1$ yields a tree with no colliding nodes before collision-free depth. Considering only even-odd permutations, the number of leaves of those trees is given by the Fibonacci sequence, complexifying their structures. From an higher perspective, we would like to construct permutations whose associated trees respect this collision-free property without enumerating all of them. The notions developed in this section are not specific to even-odd permutations, and apply to any permutation. However, following our heuristic, the actual applications of the technique described here is restricted to even-odd permutations for which algorithms can be optimized.

6.1 Binary Trees

To simplify this analysis, we focus now on blocks rather than single positions. By block, we mean a pair of adjacent positions $(2i, 2i + 1)$. The two positions of a block diffuse in the two blocks that contain $\pi(2i)$ and $\pi(2i + 1)$. We can grow trees of blocks $\mathcal{T}_B(\pi, i, n)$ associated with some permutation π recursively, as we did before with single positions:

$$\begin{cases} \mathcal{T}_B(\pi, i, 0) &= \{i, \emptyset\} \\ \mathcal{T}_B(\pi, i, n) &= \{i, \mathcal{T}_B(\pi, \lfloor \frac{\pi(2 \cdot i)}{2} \rfloor, n-1), \mathcal{T}_B(\pi, \lfloor \frac{\pi(2 \cdot i+1)}{2} \rfloor, n-1)\} \end{cases}$$

Algorithm 1 Collision-free Search Algorithm

Input: An integer p such that $2p$ is the size. An integer r, the minimal collision-free depth.

Output: A list of even-odd permutations $\mathcal{P} \subset \mathcal{S}_k$ such that if π is a permutation with collision-free depth at least r, there exists $\varphi \in \mathcal{P}$ in the pair-equivalence class of π.

$\mathcal{P} \leftarrow \{\}$
for all decomposition types t of size p **do**
  Choose arbitrarily ψ_t such that $T_{\psi_t} = t$
  for $i = 0$ **to** $p - 1$ **do**
    $\varphi(2 \cdot i) = 2 \cdot \psi_t(i) + 1$
  end for
  for $i_0 = 0$ **to** $p - 1$ **do**
    $\varphi(1) = 2 \cdot i_0$
    if φ has no collision up to depth r **then**
      for $i_1 = 0$ **to** $p - 1$, $i_1 \neq i_0$ **do**
        $\varphi(3) = 2 \cdot i_1$
        $\ddots$
        if φ has no collision up to depth r **then**
          $\varphi(2 \cdot p - 1) = 2 \cdot i_{p-1}$
          if φ has no collision up to depth r **then**
            $\mathcal{P} \leftarrow \mathcal{P} \cup \{\varphi\}$
          end if
        end if
        $\iddots$
      end for
    end if
  end for
end for
return $\mathcal{P}$

The following equality may happen: $\lfloor \frac{\pi(2\cdot i)}{2} \rfloor = \lfloor \frac{\pi(2\cdot i+1)}{2} \rfloor$. Such a node i has then twin children trees. Definitions of collision-free depths translate immediately to these trees. Beside, a tree of blocks of collision-free depth r, associated with some permutation π, ensures π to have a collision-free depth at least r from the positions given by the roots of the trees. The main advantage of this representation is that its structure, binary trees, is easier to build, study and manipulate.

Example 4. An example of this association is given in Figure 5 for the cycle π_1 defined by:

$$\pi_1 = (0, 1, 2, 5, 4, 3, 6, 9, 8, 7).$$

Several permutations are associated with the same collection of trees of blocks. Conversely, constructing a permutation from such a tree consists in choosing images of each

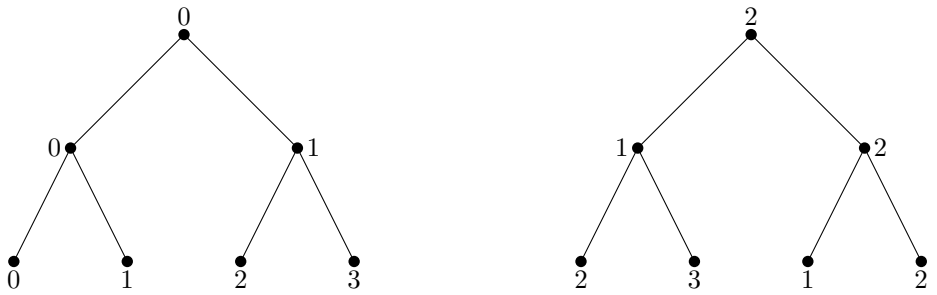

Figure 5: $\mathcal{T}_B(\pi, 0, 2)$ and $\mathcal{T}(\pi, 2, 2)$

position compatible with the constraints of blocks fixed by the tree. For instance, if a node i has two children c_1 and c_2, an even-odd permutation π compatible with this tree can only satisfy one of the two possibilities:

$$\begin{cases} \pi(2i) &= 2c_1 + 1 \\ \pi(2i+1) &= 2c_2 \end{cases} \quad \text{or} \quad \begin{cases} \pi(2i) &= 2c_2 + 1 \\ \pi(2i+1) &= 2c_1 \end{cases}$$

Such a construction of a permutation from a collection of trees is called a *colouring*.

Example 5 gives a construction for $k = 8$ of a collection of trees with collision-free depth of 3:

Example 5. This construction consists simply in addressing children to nodes according to the ascending order: $0 \mapsto \{0, 1\}$, $1 \mapsto \{2, 3\}$, $2 \mapsto \{0, 1\}$ and $3 \mapsto \{2, 3\}$.

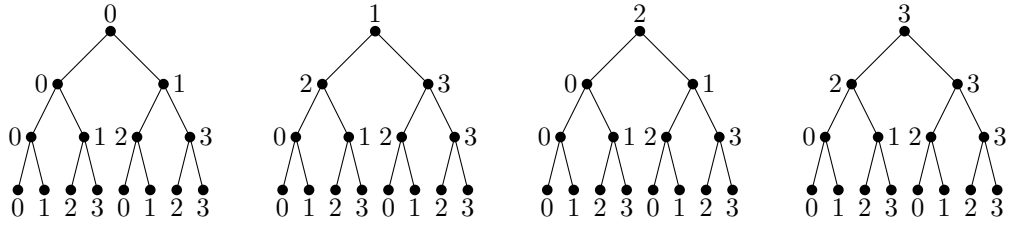

Figure 6: A collection of trees with collision-free depth of 3

This construction generalises obviously for 2^ℓ with $\ell \in \mathbb{N}$. We denote these collections of trees $\mathbf{T}_\ell$. Any permutation of size $2^{\ell+1}$ compatible with such a collection of trees is then of prescribed collision-free depth greater than ℓ. In the same way as collision free depth for a permutation, we may introduce the notion of collision free depth for a collection of compatible trees (compatible means that all nodes with the same index have the same indexes as children).

Definition 13. The collision-free depth of a collection of compatible trees $\mathbf{T}$, is the minimum of the collision-free depths of all its trees, denoted by $CD(\mathbf{T})$. A collection $\mathbf{T}$ with the highest collision-free depth is called a collision-free collection of trees.

Remark 8. For a collection of trees $\mathbf{T}$ of size p, the collection free depth satisfies:

$$CD(\mathbf{T}) \leq \lfloor \log_2(p) \rfloor.$$

As in the previous section, permutations arising form collection-free collections of trees have by construction a high collision-free depth and are likely to be optimal permutations. Furthermore, given a collection of trees with ℓ nodes (permutations of sizes 2ℓ), they are only 2^ℓ colourings which can be tested exhaustively even for larger values of ℓ.

Example 5 is then a collection-free collection of trees. Such a collection of binary trees is however not unique even up to positions reindexing:

Example 6. The two following constraints yield two collision-free collections of trees that cannot be obtained from each other with a reindexing of blocks:

- $0 \mapsto \{0,1\}$, $1 \mapsto \{2,3\}$, $2 \mapsto \{4,5\}$, $3 \mapsto \{6,7\}$, $4 \mapsto \{0,1\}$, $5 \mapsto \{2,3\}$, $6 \mapsto \{4,5\}$, $7 \mapsto \{6,7\}$.
- $0 \mapsto \{0,1\}$, $1 \mapsto \{2,3\}$, $2 \mapsto \{4,5\}$, $3 \mapsto \{6,7\}$, $4 \mapsto \{0,3\}$, $5 \mapsto \{1,2\}$, $6 \mapsto \{4,5\}$, $7 \mapsto \{6,7\}$.

6.2 Colouring Trees Algorithm

Algorithm 2 realizes the exhaustive even-odd colorations of the family of collision-free collections of trees $\mathbf{T}_\ell$.

Algorithm 2 Colouring-$\mathbf{T}_\ell$

Input: an integer ℓ, such that 4ℓ is the size of the permutations ($\ell = log_2(l) - 1$).
Output: $\mathcal{P}$, the list of even-odd permutations associated with $\mathbf{T}_\ell$ with lowest diffusion round.

$\mathcal{P} \leftarrow \{\}$
$min \leftarrow 4\ell$

for $i_1 = 0$ **to** 1 **do**
  $\pi(0) = 2i_1 + 1 \qquad \pi(1) = 2(1 - i_1),$
  $\pi(p) = 2(1 - i_1) + 1 \qquad \pi(p + 1) = 2i_1$
    $\ddots$
  for $i_\ell = 0$ **to** 1 **do**
    $\pi(2(\ell-1)) = 2 \cdot (2(\ell-1) + i_\ell) + 1, \qquad \pi(2(\ell-1)+1) = 2 \cdot (2(\ell-1) + 1 - i_\ell)$
    $\pi(2(\ell-1)+p) = 2 \cdot (2(\ell-1) + 1 - i_\ell) + 1 \qquad \pi(2(\ell-1)+p+1) = 2 \cdot (2(\ell-1) + i_\ell)$
    if $DR(\pi) \leq min$ **then**
      if $DR(\pi) < min$ **then**
        $min \leftarrow DR(\pi)$
        $\mathcal{P} \leftarrow \{\pi\}$
      else
        $\mathcal{P} \leftarrow \mathcal{P} \cup \{\pi\}$
      end if
    end if
  end for
  $\ddots$
end for

return $\mathcal{P}$

Compared to previous methods, this algorithm with its complexity of $O(2^{\frac{k}{4}})$ is rather fast and computes permutations in $\mathcal{S}_k$ likely to hide among them optimal permutations. For sizes that are powers of 2, this heuristic leads to the best known even-odd permutations, as illustrated by table 7. Complete optimal results are shown in appendix A.

Table 7: Some even-odd permutations associated with $\mathbf{T}_l$ graphs

k	π	$DR(\pi)$
32	{ 1, 2, 5, 6, 9, 10, 13, 14, 19, 16, 23, 20, 27, 24, 31, 28, 3, 0, 7, 4, 11, 8, 15, 12, 17, 18, 21, 22, 25, 26, 29, 30 }	10
64	{ 1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30, 35, 32, 39, 36, 41, 42, 45, 46, 49, 50, 53, 54, 59, 56, 63, 60, 3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28, 33, 34, 37, 38, 43, 40, 47, 44, 51, 48, 55, 52, 57, 58, 61, 62 }	11
128	{ 1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30, 35, 32, 39, 36, 41, 42, 45, 46, 49, 50, 53, 54, 59, 56, 63, 60, 67, 64, 71, 68, 73, 74, 77, 78, 81, 82, 85, 86, 91, 88, 95, 92, 97, 98, 101, 102, 107, 104, 111, 108, 115, 112, 119, 116, 121, 122, 125, 126, 3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28, 33, 34, 37, 38, 43, 40, 47, 44, 51, 48, 55, 52, 57, 58, 61, 62, 65, 66, 69, 70, 75, 72, 79, 76, 83, 80, 87, 84, 89, 90, 93, 94, 99, 96, 103, 100, 105, 106, 109, 110, 113, 114, 117, 118, 123, 120, 127, 124 }	13

6.3 From trees to graphs

Surprisingly, this construction is a new perspective on the construction coming from the de Brujin graphs in [SM10]. To be consistent with those, we give a graph description of our collections of trees. With a permutation, we can associate a graph recording connections between blocks of two consecutive positions.

Definition 14. Let $k = 2p$ be an even number and π be a permutation in $\mathcal{S}_k$. The graph associated with π, denoted by $\mathbf{G}_\pi$ is a directed graph of order p whose vertices are labelled with $\{0, \dots, p-1\}$ and whose directed edges are (i, j) for all $i, j \in \{1, \dots, p-1\}$ such that $\pi(2i) \in \{2j, 2j+1\}$ or $\pi(2i+1) \in \{2j, 2j+1\}$.

Graphs associated with permutations have clearly in- and out-degrees of 2. In our representations, vertices will be doubled to offer a better understanding of edges. Vertices at the top of the figures will correspond to inputs of edges while vertices at the bottom of the figures will correspond to output of edges. From our directed binary graphs, we grow conversely an associated collection of binary trees defined recursively:

$$\begin{cases} \mathcal{T}(\mathbf{G}, i, 0) &= \{i, \emptyset\} \\ \mathcal{T}(\mathbf{G}, i, n) &= \{i, \mathcal{T}(\mathbf{G}, j_1, n-1), \mathcal{T}(\mathbf{G}, j_2, n-1)\} \end{cases}$$

where (i, j_1) and (i, j_2) are edges of $\mathbf{G}$.

Example 7. Figure 7 gives an example for $p = 8$. The careful reader may notice that it is a de Bruijn binary graph and yield also the first collection of trees of Example 6.

Let π be some permutation in $\mathcal{S}_k$ and $\mathbf{G}_\pi$ be its associated graph. If $\mathbf{G}_\pi$ is of collision-free depth d, we know that for any $a \in \{0, \dots, k-1\}$, and any $i \in \{0, \dots, d\}$, $\mathcal{T}(\pi, a, i)$ has distinct leaves. This implies $CD(\mathbf{G}_\pi) \leq CD(\pi)$. It seems then natural to search optimal permutations among those whose associated graph has a high collision-free depth. This last sentence explains why the de Brujin graphs exhibited in [SM10] allow to build permutations with high diffusion rounds.

Remark 9. Equivalence classes of invertible symmetric binary graphs may be built as before by reindexing vertices. From Example 6, we know the equivalence classes of collision-free graphs not to be unique. The results we get from our natural construction might then be improved by considering other collision-free graphs.

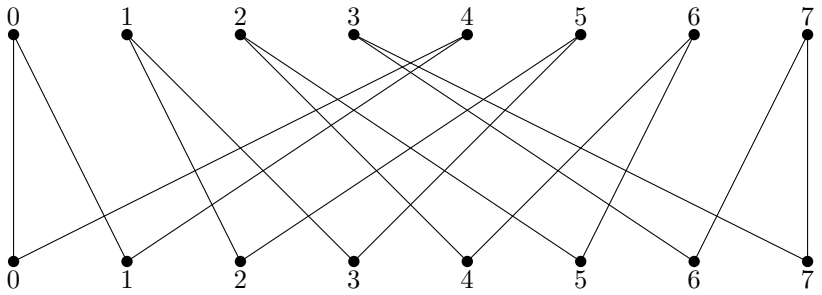

Figure 7: A collision-free graph

The colorations requirement for the trees can be rephrased in term of graphs, which is the definition given in [SM10]:

Definition 15. We call a correct 2-colouring of a binary directed graph a colouring of the edges such that any vertex is the input of two edges with different colors and is also the output of two edges with different colors.

From a correct 2-colouring of a binary directed graph of size p, we have a corresponding even-odd permutation in $\mathcal{S}_{2p}$, constructed as follows:

- If (i, j_1) is blue then $\pi(2i) = 2j_1 + 1$.
- If (i, j_2) is red then $\pi(2i + 1) = 2j_2$.

Remark 10. When k is a power of 2, $k = 2^s$, we notice that the coloured de Bruijn graph used in [SM10] to construct even-odd permutations of diffusion round less than $2\log_2(k)$ may be seen as a colouring of the graphs $\mathbf{CG}_3$.

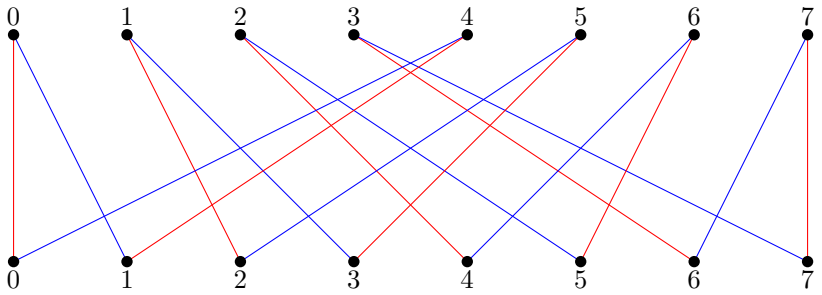

Figure 8: Coloured de Bruijn graph for $s = 3$

When [SM10] exhibits one graph with one particular colouring, we propose a tree representation that explains why de Brujin graphs are likely to produce high diffusion rounds permutations. We searched among all colorations the ones that produced the lowest diffusion round. This latest search allowed us to find a permutation with the lowest diffusion round in the literature. Furthermore, collision-free collections of trees are not unique even up to reindexation as Example 6 shows. Testing colorations for other collision-free collection of trees could be a new way to find new permutations with low diffusion round.

7 General Case

Until this point, we have restricted our study to even-odd permutations. This restriction had three reasons: first, even-odd permutations are the closest generalisation of the usual Feistel structure. Secondly, instinctively and heuristically for small sizes of k, they are the ones that are more likely to be optimal. Finally, they were easier to study. In this section, we try to analyse the general case. Results from section 4.3 onward have raised two points of special interest:

- For $k = 18$, only two optimal pair-equivalence classes, which are inverse of one another, exist; do non even-odd optimal permutations exist?
- For $k = 20$, optimal even-odd permutations have diffusion round 9. This appears surprising since for $k = 18$ and $k = 22$, even-odd permutations with diffusion round 8 exist. Can we find a non even-odd permutation with diffusion round 8?

  Answering these two questions will either justify or contradict the intuition on focusing on even-odd permutations.

Before going into the details, example 8 gives a family of non even-odd permutations reaching a diffusion round of $2\log_2(k)$ when k is a power of 2 and $k \leq 512$. Higher values of k have not been considered but the statement for all powers of 2 seems easy to prove. This permutation is highly non even-odd but it still achieve the same diffusion round as the best permutations known for high values of k and its existence justifies our interest in the general case.

Example 8. For $k = 2^s$, we define $\pi_k = \{1, 3, 5, \ldots, 2^s - 1, 0, 2, \ldots, 2^s - 2\}$.

7.1 Towards a Theoretical Lower Bound

Proposition 2 gives a theoretical lower bound on diffusion rounds for even-odd permutations. It ensures that even-odd permutations reaching it are optimal among even-odd permutations. The proof relies deeply on the even-odd property. Such a bound has not been found for the general case. Nevertheless, here are some insights that explain why even-odd permutations are more likely to be optimal.

The proof of Proposition 2 studies diffusion from each point independently. For the general case, let φ be an arbitrary permutation. We consider all the points together, and together with the collection of trees they yield.

- Roots of those trees are then the set $(i)_{i\in\{0,\ldots,k-1\}}$.

- Nodes at depth 1 are $(\varphi(i))_{i\in\{0,\ldots,k-1\}} \cup (\varphi(i))_{i \text{ odd}} = (i)_{i\in\{0,\ldots,k-1\}} \cup (\varphi(i))_{i \text{ odd}}$ counted with multiplicity. Recall for instance that for even-odd permutations, the second set are the set of even numbers.

- Reproducing this counting until the depth corresponding to the diffusion round of φ, each position appears at least k times in the set of leaves, at least one time in each tree.

Conversely, the diffusion round can only be reached when all the numbers appear at least k times in the set of leaves. Recall for instance that for even-odd permutations, at round r, odd numbers appear $Fib(r)$ times and even numbers appear $Fib(r+1)$ accordingly to lower bound given by Proposition 2.

In general, multiplicities of positions at depth r in such collection of trees are not known. Even the number of nodes at a fixed depth seems difficult to determine. Permutations do not all behave in the same way for this general diffusion. For instance, the identity permutation raises a collection of trees with $k + r \cdot p$ nodes at depth r and not $Fib(r+1)$. Notice however that the number of nodes at depth $r+1$ depends directly on the number of nodes at depth r and on the number of even nodes at this depth since it is their sum. Notice also that in order to maximize the number of nodes at depth 2, one should maximize the number of even nodes at depth 1. To achieve it, a permutation shall send all odd nodes that have only one child to even ones. Even-odd permutations maximize then the total number of nodes at depth 2. Analogous arguments may be invoked to prove that even-odd permutations maximize the number of nodes until depth 4. This is evidence that the heuristic focusing on even-odd permutations is well-founded. Unfortunately, we could not extend this argument for any depth, which would have given an even better motivation together with a general lower bound on diffusion rounds.

7.2 Number of Pair-equivalence Classes of Permutations

Theorem 1 gives an upper bound on the number of pair-equivalence classes of even-odd permutations. Such an upper bound exists for the general case:

Theorem 2. *Let $k = 2p$ and N_k be the number of decomposition types of size k. The number of pair-equivalence classes of permutations in $\mathcal{S}_k$ is upper bounded by:*

$$\mathcal{U}_k = N_k \cdot \frac{k!}{p!}.$$

The proof of Theorem 2 is a direct consequence of the following proposition.

Proposition 4. *Let $\{g_i\}_{1 \leq i \leq N_k}$ and $\{\phi_j\}_{1 \leq j \leq \frac{k!}{p!}}$ be sets of permutations such that:*

$$\begin{array}{ll} \forall g \in \mathcal{S}_k, & \exists i \in \{1, \ldots, N_k\} \text{ and } \varphi \in \mathcal{S}_k | \quad \varphi \circ g_i \circ \varphi^{-1} = g, \\ \forall g \in \mathcal{S}_k, & \exists j \in \{1, \ldots, \frac{k!}{p!}\} \text{ and } h \in \mathcal{S}_k^p | \quad \phi_j \circ h = g. \end{array}$$

Then for all g in $\mathcal{S}_k$, there exist $i \in \{1, \ldots, N_k\}$ and $j \in \{1, \ldots, \frac{k!}{p!}\}$ such that g and $\phi_j^{-1} \circ g_i \circ \phi_j$ are in the same pair-equivalence class.

Proof. We first prove the existence of such sets $\{g_i\}_{1 \leq i \leq N_k}$ and $\{\phi_j\}_{1 \leq j \leq \frac{k!}{p!}}$:

- The first one is a direct consequence of the fact that if ψ_1 and ψ_2 are two permutations with the same decomposition cycle, there exists φ such that $\varphi \circ \psi_1 \circ \varphi^{-1} = \psi_2$.
- The second set is just a set of right representatives of $\mathcal{S}_k$ modulo $\mathcal{S}_k^p$.

Let g be an element of $\mathcal{S}_k$. By construction, there exist $i \in \{1, \ldots, N_k\}$ and $\varphi \in \mathcal{S}_k$ such that:

$$g = \varphi^{-1} \circ g_i \circ \varphi.$$

By construction, there exist also $j \in \{1, \ldots, \frac{k!}{p!}\}$ and $h \in \mathcal{S}_k^p$ such that:

$$\varphi = \phi_j \circ h.$$

Then

$$g = h^{-1} \circ \phi_j^{-1} \circ g_i \circ \phi_j \circ h$$

g is thus in the same pair-equivalence class as $\phi_j^{-1} \circ g_i \circ \phi_j$.

□

Remark 11. For a permutation ϕ, the set $\{\phi^{-1}(i) |$ i is odd$\}$ remains invariant by any left or right composition by a permutation of pairs. Furthermore, denoting this set $\{x_1, \ldots, x_p\}$ where $x_i < x_j$ when $i < j$, there exists a permutation of pairs φ such that $\phi \circ \varphi(x_i) = 2 \cdot i + 1$. This allows to construct easily a set of representatives $\{\phi_j\}_{1 \leq j \leq \frac{k!}{p!}}$.

7.3 Exhaustive Search, Collision-Free Trees and Colouring

Similarly to Strategy 1, we use Proposition 4 to construct at least one permutation in each pair-equivalence class without computing explicitly all classes beforehand. Moreover, in our search for optimal permutations, some classes can be directly excluded. Let π be a permutation with a fixed point i, $\pi(i) = i$. Then, $DR(\pi) = \infty$ and π cannot be optimal. Indeed:

- If i is even, X_i^r is not affected by X_j for all r and all j different to i.
- If i is odd, X_j^r is not affected by X_i for all r and all j different to i.

Denote by N_k^0 the number of decomposition types with no fixed point. The search space reduces to:

$$\mathcal{U}_k^0 = N_k^0 \cdot \frac{n!}{p!}.$$

Table 8 illustrates how this might affect complexities when searching for optimal diffusion rounds.

Table 8: Comparison between $\mathcal{U}_k^0$ and $|\mathcal{S}_k|$

k	N_k^0	$\log_2(\mathcal{U}_k^0)$	$\log_2(\lvert\mathcal{S}_k\rvert)$
6	4	8.9	9.5
8	7	12.6	15.3
10	12	18.5	21.8
12	21	23.7	28.8
14	34	29.1	36.3

k	N_k^0	$\log_2(\mathcal{U}_k^0)$	$\log_2(\lvert\mathcal{S}_k\rvert)$
16	55	34.7	44.2
18	88	40.5	52.5
20	137	46.4	61.1
22	210	52.3	69.9
24	320	58.5	79.0

Strategy 2 (Pair-equivalence Class Exhaustive Search)**.**

1. *For each decomposition type t of size k that doesn't have any fixed point, fix an arbitrary permutation g_t compatible with t.*
2. *For each choice $\{x_1, \ldots, x_p\}$ of p elements among k assumed sorted, fix an arbitrary permutation φ_j such that:*
$$\varphi_j(x_i) = 2 \cdot i + 1.$$
3. *For all permutations ϕ of p elements, construct the permutation Φ of k elements such that:*
$$\Phi(2 \cdot i + 1) = 2 \cdot i + 1 \text{ and } \Phi(2 \cdot i) = 2 \cdot \phi(i).$$

Table 9: Fibonacci lower bounds and optimal diffusion rounds

k	lower bound	$\min_{\pi \in \mathcal{S}_k}(DR(\pi))$	Number of classes
16	7	8	33
18	8	8	2
20	8	9	Not computed

4. Compute the diffusion round of the permutation $(\Phi \circ \varphi_j)^{-1} \circ g_t \circ (\Phi \circ \varphi_j)$

Strategy 2 allowed us to compute optimal permutations for $k \leq 18$. For $k = 20$, strategy 2 costs $2^{46.4}$ tests of diffusion rounds. Because of this huge complexity, we used a supercomputer and we limited our search to permutation diffusion round 8 to take advantage of fast exponentiation. In the latter case, results were negative in the sense that all permutations have diffusion round strictly greater than 8. Results are summarized in table 9.

Representatives for optimal pair-equivalence classes are given in the appendix.

Refined methods to construct good candidates for low diffusion rounds with collision-free trees or graphs colouring applies directly to the general case. The serious drawback for the general case remains the exponential growth of the number of permutations. All these strategies, even improving the search complexity, are still quickly bounded by practical capacities.

- Algorithm 1 translates to all permutations.
- Associations between permutations, collection of binary trees or binary graphs may be deduced from Section 6. For instance $k = 2^{\ell+1}$, there exist though 2^k possible colorations of $\mathbf{T}_\ell$ whereas there is only $2^{\frac{k}{4}}$ even-odd colorations.

8 Security Analysis

We evaluated the resistance against classical attacks of every type-II Generalized Feistel Structure that we found, even-odd or not. Individual results can be found next to each permutation in Appendix. The presentation of the attacks and the discussion concerning the resistance of Feistel structures are done in the following.

8.1 Differential and Linear Cryptanalysis

Differential [BS90] and Linear [Mat93] cryptanalysis count as the most famous attacks on ciphers. Usually, to estimate the resistance against such attacks, the minimal number of S-boxes with a non-zero difference/mask (called active S-boxes) crossed by differential and linear characteristics is counted. Let P be the maximal differential or linear probability of an S-box, and N be the minimal number of active S-boxes. Then the best differential or linear attack against the cipher has a complexity of about $1/P^N$ operations. Thus, a cipher is supposed to be secure against differential and linear cryptanalysis as soon as the quantities $1/P^N$ for differential and linear characteristics are greater than the entire codebook.

To count the minimal number of actives S-boxes, we used the method described in [MWGP11], based on Mixed-Integer Linear Programming (MILP). Following the study of [SM10], we evaluated the minimal number of differentially and linearly active S-boxes across 20 rounds for every permutation we found. Here we assume that each function F_i in the Feistel Structure counts as a single S-box.

From the results, we can draw the following conclusion. Suzaki and Minematsu [SM10] have already observed that the minimal number of active S-boxes varies widely among the permutations with optimal diffusion round. We confirm and extend this results by looking at non-even-odd permutation for up to $k = 20$ blocks, and for even-odd permutation with $k \in \{22, 24, 26, 32, 64, 128\}$, sometimes to less than an average of a single active S-box per round. Besides non-even-odd permutations are in general worse than even-odd permutation, despite some non-even-odd permutations being as good as the best even-odds in certain cases.

This tends to confirm the heuristic to search for even-odd permutations when building a block cipher, yet does not replace careful security evaluation.

8.2 Impossible Differential Cryptanalysis

Impossible differential attacks [Knu98, BBS99] are a type of cryptanalysis that exploits differentials appearing with probability zero in some middle round of the cipher. It is then possible to rule out wrong key candidates if the aforementioned differential holds for some plaintext/ciphertext pair.

Impossible differentials are usually found using a "miss-in-the-middle" technique: find two differential characteristics, one forward $\alpha \to \alpha'$ over r_α rounds and the other backward $\beta \to \beta'$ over r_β rounds, that both hold with probability one, but such that the middle differences α' and β' cannot both happen. The differential $\alpha \to \beta$ is then an impossible differential over $r_\alpha + r_\beta$ rounds.

The $\mathcal{U}$-method [KHS+03, KHL10] is a classical tool for finding truncated word-wise or block-wise impossible differentials. They are thus particularly effective against any generalized Feistel structure since they naturally come with a notion of (sub)block.

In the $\mathcal{U}$-method, each truncated block-wise difference lies within the set $\{0, \gamma, \delta, \gamma \oplus \delta, ?\}^k$ where 0 denotes a zero difference, γ a non-zero fixed difference (denoted γ), δ a non-zero unfixed difference, $\gamma \oplus \delta$ the exclusive-or of a non-zero fixed and a non-zero unfixed difference, and finally ? an unfixed difference. Assuming the functions used in the Feistel structure are bijective, such differences evolve across rounds in a natural way. Input differences α and β only contain 0 and γ. An impossible differential can be found when the middle differences α' and β' have at least one common block with incompatible type, such as 0 vs γ or δ, or γ vs $\gamma \oplus \delta$.

The $\mathcal{U}$-method was later improved to the UID-method [LWLG09, LLWG14], that can also track equality of differences. Both methods were generalized further in [WW12] to deal with more complex linear diffusion layers. In the case of type-II GFS with unspecified functions however, all three methods yield the same results, thus we only implemented the $\mathcal{U}$-method.

Another approach to impossible differentials is MILP-based techniques [ST17]. In a nutshell, the idea is to search for differential paths. If the MILP solver does not find any solution, this yields an impossible differential. Contrary to previous methods, this makes the search very versatile, as one can for example specify which differential transitions are impossible through the S-box. Besides, it can detect any differential contradiction and not just block-wise ones. This comes however at the cost of an increase in complexity.

For even-odd type-II GFS, the authors of [SM10] generically proved that impossible differential attacks happen for at most $2DR(\pi) + 1$ rounds, and exhaustively showed that for any even-odd type-II GFS with $k \leq 16$ branches, the precise number of rounds for impossible differentials was either $2DR(\pi) - 2$, $2DR(\pi) - 1$, or $2DR(\pi) + 1$.

We implemented the $\mathcal{U}$-method and computed the maximum number of rounds with an impossible differential attack, for every permutation we found. The results can be summed up as follows. The precise number of rounds for impossible differentials lies within the range $2DR(\pi) - 3$ to $2DR(\pi) + 1$. This is a slight improvement over previous results, whose best figure was $2DR(\pi) - 2$. However, the new bound is only reached for two non-even-odd

permutations for $k = 12$, and it comes at a cost of a very low number of active S-boxes, and so is probably not a good choice from a designer's perspective. Otherwise, non-even-odd permutations always have a resistance at most as good as even-odd permutations. On average however, even-odd permutations tend to take about one round fewer to resist impossible differentials.

8.3 Integral Cryptanalysis

Integral cryptanalysis [DKR97, KW02] is an attack where one is given 2^n plaintext/ciphertext pairs that "saturate" an n-bit word, i.e. on a given n-bit word, the plaintexts take all possibles values on that n-bit word, while all being equal to some constant elsewhere. The goal of this attack is to predict the value of the sum (a.k.a. the integral) of (parts of) the ciphertexts after some rounds of encryption. Such attack is called a first order integral. It can be generalized to an m-th order integral. This time, one is given 2^{nm} plaintexts that are all different on m words. Again, the goal is to predict the sum of such messages after some encryption rounds.

Just like for impossible differentials, the propagations of some block-wise properties across rounds is studied. For integral cryptanalysis, the block-wise properties are: A (for All) when all texts are different, C (for Constant) when all texts are equal, B (for Balanced) when the sum of all texts is zero for that particular block, or ? when the sum cannot be predicted. An integral characteristic $\alpha \to \beta$ is then such that $\alpha \in \{A, C\}^k$ with at least one A, and $\beta \in \{A, C, B, ?\}^k$ with at least one block not equal to ?.

In order to find an integral, we follow the method of [BS01]: we first build a first-order integral $\alpha \to \beta$ with α containing only one A. This integral characteristic is then extended into an m-th order characteristic by adding rounds at the beginning $\alpha' \to \alpha \to \beta$, as long as α' is not made of A only (i.e. is not the full codebook).

For even-odd type-II GFS, the authors of [SM10] generically proved that integral attacks happen for at most $2DR(\pi)$ rounds, and exhaustively showed that for any even-odd type-II GFS with $k \leq 16$ branches, the precise number of rounds for integrals was either $2DR(\pi) - 2$, $2DR(\pi) - 1$, or $2DR(\pi)$.

We implemented the above method and computed the maximum number of rounds with an integral attack, for every permutation we found. The results are summed up here. The precise number of rounds for integrals lies within the range $2DR(\pi) - 2$ to $2DR(\pi) + 1$. There is no improvement over previous results here, we even observe worse results with non-even-odd permutations reaching $2DR(\pi) + 1$ rounds; no even-odd permutation goes beyond $2DR$ though. As for impossible differentials, we observe that non-even-odd permutations can perform as well as even-odd, but on average lie one round behind.

9 Conclusion and Perspectives

The resistance of Generalized Type-II Feistel Schemes against both integral and impossible differential attacks are related with their diffusion round, number of rounds which ensures a total diffusion of inputs. This diffusion round is completely determined by the permutation used to define this structure. In this paper, we have first analysed even-odd permutations accordingly to the heuristic proposed in [SM10] and then the general case of permutations.

In this analysis, we define pair-equivalence classes of even-odd permutations, for which diffusion rounds are class invariant. We determine a lower bound on the number of classes together with a strategy to run over them all. We performed exhaustive search of pair-equivalence classes of even-odd permutations for $k \leq 24$ while previous exhaustive searches on permutations stopped at $k \leq 16$.

In order to find optimally diffusing permutations, we pursued the following heuristic: permutations which present no lack of intermediate diffusion are likely to have low diffusion

rounds. We give several algorithms which exploit these considerations. It allowed us to find optimal even-odd permutations for $k = 26$ without the test of all pair-equivalence classes which is computationally consuming. Introducing new structures: trees, collections of trees and graphs, we were able to develop new strategies which allowed us to find even-odd permutations with the lowest known diffusion round for sizes $k \in \{64, 128\}$, parameters beyond reach of exhaustive searches.

This analysis we made on even-odd permutations is not fully restricted to their structure. We transposed some results to general permutations and benefit from a strategy which allowed us to compute exhaustive search of pair-equivalence classes of permutations for $k \leq 20$. The heuristic to focus on even-odd permutations to determine permutations with the best possible diffusion round seems to be confirmed by general results for $k = 18$ and $k = 20$.

We also conducted a security analysis of our results with respect to differential and linear cryptanalysis, as well as impossible differentials and integrals attacks. This showed that the previous results for even-odd permutations still hold for $k > 16$: resistance to the latter two attacks is closely linked to the diffusion rounds, while resistance to the former two can vary widely and requires special attention from the designer. For non-even-odd permutations, results vary from as good as even-odd but not better, up to absolutely bad. Thus, from this perspective, it seems a good intuition to search for even-odd permutations, yet it does solve every problem.

Some interrogations remain and some of our results are surprising. For instance, optimal diffusion round for $k = 20$ is greater than the optimal diffusion round for $k = 22$. Despite our insight on what could favour or threaten good diffusion, it seems combinatorics is so important that unexpected behaviours happen. Some theoretical results remain also challenging. The most meaningful result would certainly be to benefit from the same lower bound on diffusion round given by the Fibonacci sequence or at least to determine a similar result.

References

[AIK+00] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In Douglas R. Stinson and Stafford E. Tavares, editors, *Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 14-15, 2000, Proceedings*, volume 2012 of *Lecture Notes in Computer Science*, pages 39–56. Springer, 2000.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 12–23. Springer, 1999.

[BS90] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

[BS01] Alex Biryukov and Adi Shamir. Structural Cryptanalysis of SASAS. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001, Interna-*

tional Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding, volume 2045 of *Lecture Notes in Computer Science*, pages 394–405. Springer, 2001.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. *IACR Cryptology ePrint Archive*, 2013:404, 2013.

[DES77] DES. Data Encryption Standard. In *In FIPS PUB 46, Federal Information Processing Standards Publication*, pages 46–2, 1977.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The Block Cipher Square. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael - AES – The Advanced Encryption Standard*. Springer-Verlag, 2002.

[GM16] Shay Gueron and Nicky Mouha. Simpira v2: A Family of Efficient Permutations Using the AES Round Function. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 95–125. Springer, 2016.

[HSH+06] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee. HIGHT: A New Block Cipher Suitable for Low-Resource Device. In Louis Goubin and Mitsuru Matsui, editors, *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, volume 4249 of *Lecture Notes in Computer Science*, pages 46–59. Springer, 2006.

[KHL10] Jongsung Kim, Seokhie Hong, and Jongin Lim. Impossible differential cryptanalysis using matrix method. *Discrete Mathematics*, 310(5):988–1002, 2010.

[KHS+03] Jongsung Kim, Seokhie Hong, Jaechul Sung, Changhoon Lee, and Sangjin Lee. Impossible Differential Cryptanalysis for Block Cipher Structures. In Thomas Johansson and Subhamoy Maitra, editors, *Progress in Cryptology - INDOCRYPT 2003, 4th International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003, Proceedings*, volume 2904 of *Lecture Notes in Computer Science*, pages 82–96. Springer, 2003.

[Knu98] Lars R. Knudsen. DEAL - A 128-bit Block Cipher. In *NIST AES Proposal*, 1998.

[KW02] Lars R. Knudsen and David A. Wagner. Integral Cryptanalysis. In Joan Daemen and Vincent Rijmen, editors, *Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers*, volume 2365 of *Lecture Notes in Computer Science*, pages 112–127. Springer, 2002.

[LLWG14] Yiyuan Luo, Xuejia Lai, Zhongming Wu, and Guang Gong. A unified method for finding impossible differentials of block cipher structures. *Inf. Sci.*, 263:211–220, 2014.

[LWLG09] Yiyuan Luo, Zhongming Wu, Xuejia Lai, and Guang Gong. A Unified Method for Finding Impossible Differentials of Block Cipher Structures. *IACR Cryptology ePrint Archive*, 2009:627, 2009.

[Mat93] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

[MWGP11] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming. In Chuankun Wu, Moti Yung, and Dongdai Lin, editors, *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*, volume 7537 of *Lecture Notes in Computer Science*, pages 57–76. Springer, 2011.

[RRSY98] Ronald L. Rivest, Matthew J. B. Robshaw, Ray Sidney, and Yiqun Lisa Yin. The RC6$^{\text{TM}}$ block cipher. In *First Advanced Encryption Standard (AES) conference*, page 16, 1998.

[Sha49] Claude Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal, Vol 28, pp. 656–715*, October 1949.

[SM10] Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the Generalized Feistel. In Seokhie Hong and Tetsu Iwata, editors, *Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers*, volume 6147 of *Lecture Notes in Computer Science*, pages 19–39. Springer, 2010.

[SMMK12] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A Lightweight Block Cipher for Multiple Platforms. In Lars R. Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, volume 7707 of *Lecture Notes in Computer Science*, pages 339–354. Springer, 2012.

[SSA+07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In Alex Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.

[ST17] Yu Sasaki and Yosuke Todo. New Impossible Differential Search Tool from Design and Cryptanalysis Aspects - Revealing Structural Properties of Several Ciphers. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 185–215. Springer, 2017.

[WW12] Shengbao Wu and Mingsheng Wang. Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers. In Steven D. Galbraith and Mridul Nandi, editors, *Progress in Cryptology - INDOCRYPT 2012, 13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012. Proceedings*, volume 7668 of *Lecture Notes in Computer Science*, pages 283–302. Springer, 2012.

[ZMI89] 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, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 461–480. Springer, 1989.

A Optimal Permutations Found

For the sake of compactness, it is common to introduce extended pair-equivalence class of permutations. By definition, we know the inverse of an optimal permutation to be also an optimal permutation. Pair-equivalence classes generalises naturally to extended pair-equivalence classes where two permutations φ_1 and φ_2 are in the same extended pair-equivalence class if and only if either φ_1 and φ_2 are pair-equivalent or φ_1 and φ_2^{-1} are pair-equivalent.

The following tables exhibit a representative for each extended class of optimal permutations and their security evaluation. Here, Imp. stands for impossible differential characteristic, Intg. stands for Integral characteristic, Diff. and Lin. for Differentially and Linearly actives S-boxes across 20 rounds. When $k \leq 18$, even-odd permutations are indicated by an "eo" superscript. When $k > 18$, all permutations given are even-odd. For $k = 64$ and 128, we were not able to compute the minimal number of actives S-boxes across 20 rounds, hence only resistance against impossible differentials and integrals are given.

Table 10: Optimal permutations for $k = 6$ up to extended pair-equivalence

Optimal Permutations $k = 6$, $DR(\pi) = 5$	Imp.	Intg.	Diff.	Lin.
$\{1, 2, 5, 0, 3, 4\}^{eo}$	9	10	25	25

Table 11: Optimal permutations for $k = 8$ up to extended pair-equivalence

Optimal Permutations $k = 8$, $DR(\pi) = 6$	Imp.	Intg.	Diff.	Lin.
$\{7, 0, 3, 4, 1, 6, 5, 2\}^{eo}$	10	11	26	26
$\{3, 4, 1, 2, 7, 0, 5, 6\}^{eo}$	11	11	30	30
$\{6, 0, 3, 5, 7, 1, 2, 4\}$	11	12	16	16
$\{7, 0, 1, 6, 5, 3, 4, 2\}$	11	13/12	28	28
$\{1, 2, 6, 0, 7, 3, 5, 4\}$	11	13	24	24

Table 12: Optimal permutations for $k = 10$ up to extended pair-equivalence

Optimal Permutations $k = 10$, $DR(\pi) = 7$	Imp.	Intg.	Diff.	Lin.
$\{1, 2, 7, 8, 3, 4, 9, 0, 5, 6\}^{eo}$	12	13	35	35
$\{9, 0, 5, 6, 3, 4, 1, 8, 7, 2\}^{eo}$	12	13	34	34
$\{5, 6, 3, 4, 1, 2, 9, 0, 7, 8\}^{eo}$	13	13	33	33
$\{8, 0, 3, 5, 7, 1, 9, 4, 2, 6\}$	13	14	18	18
$\{9, 4, 0, 2, 6, 8, 7, 1, 5, 3\}$	14	14	24	24

Table 13: Optimal permutations for $k = 12$ up to extended pair-equivalence

Optimal Permutations $k = 12$, $DR(\pi) = 8$	Imp.	Intg.	Diff.	Lin.
$\{1, 2, 6, 10, 9, 4, 5, 8, 7, 11, 3, 0\}$	13	15	20	20
$\{1, 10, 9, 7, 3, 4, 2, 0, 5, 11, 8, 6\}$	13	15	20	20
$\{3, 4, 5, 2, 11, 6, 7, 8, 1, 10, 9, 0\}^{eo}$	14	14	36	34
$\{7, 4, 11, 2, 5, 6, 3, 8, 1, 10, 9, 0\}^{eo}$	14	14/15	34	36
$\{1, 8, 11, 6, 9, 4, 5, 2, 7, 10, 3, 0\}^{eo}$	14	15/14	28	28
$\{5, 8, 11, 6, 9, 4, 7, 2, 1, 10, 3, 0\}^{eo}$	14	15	37	37
$\{5, 8, 11, 2, 9, 6, 7, 4, 1, 10, 3, 0\}^{eo}$	14	15	37	37
$\{7, 8, 9, 4, 5, 6, 11, 2, 1, 10, 3, 0\}^{eo}$	14	15	36	36
$\{5, 8, 9, 2, 1, 4, 11, 6, 7, 10, 3, 0\}^{eo}$	14	15	36	36
$\{9, 4, 5, 6, 11, 2, 7, 8, 1, 10, 3, 0\}^{eo}$	14	15	35	35
$\{5, 6, 7, 2, 11, 4, 3, 8, 1, 10, 9, 0\}^{eo}$	14	15	35	35
$\{9, 4, 7, 8, 5, 6, 11, 2, 1, 10, 3, 0\}^{eo}$	14	15	35	35
$\{5, 2, 3, 4, 11, 6, 7, 8, 1, 10, 9, 0\}^{eo}$	14	15	35	35
$\{3, 6, 11, 4, 5, 2, 7, 8, 1, 10, 9, 0\}^{eo}$	14	15	35	35
$\{11, 4, 9, 2, 5, 6, 1, 8, 7, 10, 3, 0\}^{eo}$	14	15	35	35
$\{7, 2, 11, 4, 5, 6, 3, 8, 1, 10, 9, 0\}^{eo}$	14	15	35	34
$\{7, 4, 5, 2, 11, 6, 3, 8, 1, 10, 9, 0\}^{eo}$	14	15	34	35
$\{9, 4, 11, 6, 5, 8, 1, 2, 7, 10, 3, 0\}^{eo}$	14	15	34	34
$\{1, 8, 9, 6, 7, 2, 3, 0, 5, 11, 4, 10\}$	14	15	34	34
$\{5, 2, 3, 6, 7, 4, 11, 8, 1, 10, 9, 0\}^{eo}$	14	15	34	34
$\{9, 4, 7, 2, 11, 6, 5, 8, 1, 10, 3, 0\}^{eo}$	14	15	34	33
$\{7, 8, 5, 2, 9, 6, 11, 4, 1, 10, 3, 0\}^{eo}$	14	15	34	33
$\{7, 8, 9, 6, 11, 4, 5, 2, 1, 10, 3, 0\}^{eo}$	14	15	33	34
$\{1, 4, 9, 2, 11, 6, 5, 8, 7, 10, 3, 0\}^{eo}$	14	15	33	33
$\{8, 6, 5, 1, 3, 10, 9, 0, 7, 11, 2, 4\}$	14	15	32	32
$\{8, 2, 5, 0, 3, 1, 9, 10, 7, 11, 4, 6\}$	14	15	32	32
$\{9, 2, 7, 4, 3, 0, 1, 8, 5, 11, 6, 10\}$	14	15	30	30
$\{5, 10, 1, 8, 6, 4, 9, 2, 7, 11, 3, 0\}$	14	15	18	31
$\{5, 3, 4, 6, 1, 7, 8, 2, 9, 11, 0, 10\}$	14	15	13	20
$\{4, 2, 8, 0, 9, 3, 7, 1, 5, 11, 6, 10\}$	14	15	20	13
$\{9, 0, 3, 7, 2, 6, 1, 10, 5, 11, 8, 4\}$	14	15/16	32	31
$\{9, 10, 3, 1, 7, 4, 2, 0, 5, 11, 8, 6\}$	14	16/15	31	32
$\{1, 3, 9, 10, 7, 4, 2, 0, 5, 11, 8, 6\}$	14	16/15	29	20
$\{7, 2, 5, 8, 1, 4, 9, 10, 6, 11, 3, 0\}$	14	16	35	35
$\{9, 2, 3, 8, 7, 0, 1, 4, 5, 11, 6, 10\}$	14	16	33	32
$\{6, 10, 1, 2, 5, 8, 9, 4, 7, 11, 3, 0\}$	14	16	32	32
$\{3, 8, 9, 6, 1, 2, 7, 0, 5, 11, 4, 10\}$	15	14/16	34	34
$\{1, 10, 7, 8, 5, 6, 3, 4, 11, 2, 9, 0\}^{eo}$	15	15	37	37
$\{5, 6, 11, 2, 7, 4, 3, 8, 1, 10, 9, 0\}^{eo}$	15	15	35	35
$\{1, 2, 5, 8, 9, 4, 11, 6, 7, 10, 3, 0\}^{eo}$	15	15	35	35
$\{9, 2, 1, 8, 3, 6, 7, 0, 5, 11, 4, 10\}$	15	15	34	34
$\{7, 8, 11, 2, 9, 4, 5, 6, 1, 10, 3, 0\}^{eo}$	15	15	34	34
$\{1, 2, 9, 4, 3, 10, 8, 0, 5, 11, 7, 6\}$	15	15	33	35
$\{9, 6, 7, 8, 11, 4, 5, 2, 1, 10, 3, 0\}^{eo}$	15	15	33	34
$\{9, 4, 1, 2, 11, 6, 5, 8, 7, 10, 3, 0\}^{eo}$	15	15	33	33
$\{5, 6, 9, 4, 1, 2, 10, 8, 7, 11, 3, 0\}$	15	15	33	33
$\{9, 6, 7, 8, 1, 2, 3, 0, 5, 11, 4, 10\}$	15	15	33	33
$\{5, 6, 9, 2, 7, 4, 11, 8, 1, 10, 3, 0\}^{eo}$	15	15	33	33
$\{4, 2, 8, 10, 9, 6, 5, 1, 7, 11, 3, 0\}$	15	15	33	33
$\{1, 8, 7, 4, 9, 10, 5, 2, 6, 11, 3, 0\}$	15	15	32	33
$\{3, 8, 7, 0, 9, 2, 1, 4, 5, 11, 6, 10\}$	15	15	32	33
$\{7, 0, 9, 2, 3, 8, 1, 4, 5, 11, 6, 10\}$	15	15	32	33
$\{7, 8, 1, 2, 9, 4, 3, 0, 5, 11, 6, 10\}$	15	15	33	32
$\{6, 8, 1, 2, 5, 10, 9, 4, 7, 11, 3, 0\}$	15	15	33	32
$\{9, 4, 7, 8, 1, 2, 3, 0, 5, 11, 6, 10\}$	15	15	33	32
$\{3, 6, 10, 4, 1, 2, 7, 8, 5, 11, 9, 0\}$	15	15	33	32
$\{2, 10, 9, 1, 3, 4, 7, 0, 5, 11, 8, 6\}$	15	15	32	32
$\{1, 8, 3, 7, 2, 6, 9, 0, 5, 11, 4, 10\}$	15	15	30	31
$\{2, 6, 5, 10, 7, 8, 3, 4, 9, 11, 1, 0\}$	15	15	30	31
$\{1, 2, 6, 8, 3, 0, 7, 9, 5, 11, 4, 10\}$	15	15	31	30
$\{9, 6, 7, 2, 11, 4, 5, 8, 1, 10, 3, 0\}^{eo}$	15	15	30	30
$\{3, 4, 9, 0, 7, 2, 1, 8, 5, 11, 6, 10\}$	15	15	28	28
$\{9, 8, 3, 1, 7, 6, 2, 0, 5, 11, 4, 10\}$	15	15	27	27
$\{9, 10, 7, 4, 1, 2, 3, 0, 5, 11, 8, 6\}$	15	15	27	27

Table 14: Optimal permutations for $k = 12$ up to extended pair-equivalence (continued)

Optimal Permutations $k = 12$, $DR(\pi) = 8$	Imp.	Intg.	Diff.	Lin.
$\{4, 8, 3, 9, 7, 1, 2, 0, 5, 11, 6, 10\}$	15	15	20	20
$\{6, 10, 1, 4, 7, 8, 5, 2, 9, 11, 3, 0\}$	15	15	31	18
$\{1, 3, 5, 2, 8, 10, 9, 0, 7, 11, 6, 4\}$	15	15	22	13
$\{8, 10, 4, 2, 5, 6, 9, 1, 7, 11, 3, 0\}$	15	15	13	22
$\{2, 6, 5, 10, 9, 1, 4, 8, 7, 11, 3, 0\}$	15	15	20	13
$\{1, 8, 9, 4, 7, 2, 3, 0, 5, 11, 6, 10\}$	15	15/16	34	34
$\{7, 8, 1, 4, 5, 2, 9, 10, 6, 11, 3, 0\}$	15	15/16	34	32
$\{5, 6, 1, 4, 10, 8, 7, 0, 3, 11, 9, 2\}$	15	15/16	32	34
$\{6, 4, 1, 2, 5, 8, 9, 10, 7, 11, 3, 0\}$	15	15/16	32	33
$\{1, 2, 9, 4, 7, 8, 3, 0, 5, 11, 6, 10\}$	15	15/16	32	33
$\{9, 0, 7, 2, 3, 6, 1, 8, 5, 11, 4, 10\}$	15	15/16	32	32
$\{4, 9, 7, 8, 1, 2, 3, 0, 5, 11, 6, 10\}$	15	15/16	31	32
$\{3, 8, 7, 1, 9, 2, 0, 4, 5, 11, 6, 10\}$	15	15/16	32	31
$\{3, 8, 0, 7, 1, 2, 9, 4, 5, 11, 6, 10\}$	15	15/16	26	30
$\{5, 4, 1, 10, 6, 3, 9, 8, 7, 11, 0, 2\}$	15	15/16	29	26
$\{10, 2, 6, 0, 1, 3, 9, 8, 7, 11, 5, 4\}$	15	15/16	26	29
$\{2, 0, 7, 8, 3, 1, 9, 4, 5, 11, 6, 10\}$	15	15/16	26	26
$\{1, 3, 5, 10, 6, 4, 9, 8, 7, 11, 0, 2\}$	15	15/17	32	32
$\{1, 10, 9, 6, 8, 2, 3, 0, 7, 11, 5, 4\}$	15	16/15	35	33
$\{1, 8, 9, 2, 6, 10, 3, 0, 7, 11, 5, 4\}$	15	16/15	33	33
$\{3, 8, 11, 2, 5, 6, 9, 4, 7, 10, 1, 0\}^{eo}$	15	16/15	33	33
$\{10, 6, 5, 8, 1, 4, 9, 2, 7, 11, 3, 0\}$	15	16/15	32	33
$\{1, 4, 9, 6, 10, 2, 5, 8, 7, 11, 3, 0\}$	15	16/15	33	32
$\{8, 6, 3, 7, 9, 2, 1, 0, 5, 11, 4, 10\}$	15	16/15	32	32
$\{7, 8, 9, 6, 1, 2, 3, 0, 5, 11, 4, 10\}$	15	16/15	32	32
$\{1, 2, 9, 4, 3, 10, 0, 8, 5, 11, 7, 6\}$	15	16/15	31	30
$\{9, 10, 3, 1, 5, 8, 2, 0, 7, 11, 4, 6\}$	15	16/15	29	32
$\{9, 4, 7, 10, 1, 2, 3, 0, 5, 11, 8, 6\}$	15	16/15	27	27
$\{2, 0, 9, 10, 5, 8, 3, 1, 7, 11, 4, 6\}$	15	16/15	26	27
$\{2, 4, 9, 1, 5, 8, 10, 6, 7, 11, 3, 0\}$	15	16/15	20	29
$\{7, 4, 1, 2, 3, 6, 10, 8, 5, 11, 9, 0\}$	15	16	35	35
$\{8, 0, 3, 5, 6, 10, 9, 1, 7, 11, 2, 4\}$	15	16	34	34
$\{5, 8, 7, 2, 9, 4, 11, 6, 1, 10, 3, 0\}^{eo}$	15	16	33	33
$\{7, 2, 9, 4, 1, 8, 3, 0, 5, 11, 6, 10\}$	15	16	33	33
$\{1, 3, 9, 10, 0, 2, 5, 8, 7, 11, 6, 4\}$	15	16	33	33
$\{9, 4, 3, 7, 1, 6, 2, 0, 5, 11, 8, 10\}$	15	16	33	33
$\{3, 10, 9, 0, 5, 2, 1, 8, 7, 11, 6, 4\}$	15	16	32	32
$\{5, 2, 3, 10, 9, 0, 1, 8, 7, 11, 6, 4\}$	15	16	32	32
$\{7, 2, 0, 8, 3, 1, 9, 4, 5, 11, 6, 10\}$	15	16	26	31
$\{3, 8, 9, 4, 1, 7, 5, 0, 6, 11, 2, 10\}$	15	16	30	26
$\{1, 3, 7, 9, 0, 2, 4, 8, 5, 11, 6, 10\}$	15	16	26	26
$\{7, 4, 9, 10, 1, 2, 3, 0, 5, 11, 8, 6\}$	15	16	24	24
$\{4, 10, 9, 7, 3, 1, 2, 0, 5, 11, 8, 6\}$	15	16	20	20
$\{8, 0, 6, 2, 7, 3, 9, 1, 5, 11, 4, 10\}$	15	16	20	20
$\{6, 10, 1, 5, 2, 8, 9, 4, 7, 11, 3, 0\}$	15	16	20	20
$\{9, 5, 10, 2, 0, 3, 7, 1, 6, 11, 8, 4\}$	15	16	20	20
$\{2, 0, 6, 10, 5, 9, 4, 8, 7, 11, 3, 1\}$	15	16	20	20
$\{1, 5, 8, 4, 10, 2, 9, 0, 7, 11, 6, 3\}$	15	16	29	18
$\{7, 9, 3, 1, 2, 8, 4, 0, 5, 11, 6, 10\}$	15	16	18	18
$\{1, 10, 9, 4, 3, 8, 2, 0, 5, 11, 7, 6\}$	15	16/17	33	33
$\{1, 3, 6, 8, 7, 2, 9, 0, 5, 11, 4, 10\}$	15	16/17	27	26
$\{7, 4, 9, 10, 0, 2, 3, 1, 5, 11, 8, 6\}$	15	16/17	20	20
$\{4, 6, 1, 2, 7, 8, 5, 10, 9, 11, 3, 0\}$	15	17/15	32	29
$\{3, 4, 7, 8, 2, 1, 9, 0, 5, 11, 6, 10\}$	15	17/16	31	26
$\{2, 8, 9, 1, 6, 10, 3, 0, 7, 11, 5, 4\}$	15	17/16	23	23
$\{8, 3, 4, 10, 5, 6, 9, 1, 7, 11, 0, 2\}$	15	17/16	18	29
$\{7, 10, 9, 4, 3, 1, 2, 0, 5, 11, 8, 6\}$	15	17	20	20
$\{8, 4, 9, 10, 2, 6, 5, 1, 7, 11, 3, 0\}$	15	17	13	20
$\{9, 4, 7, 2, 1, 6, 3, 0, 5, 11, 8, 10\}$	16	16/15	33	33
$\{9, 0, 5, 2, 3, 10, 1, 8, 7, 11, 6, 4\}$	16	16	31	31
$\{9, 3, 7, 2, 1, 6, 0, 8, 5, 11, 4, 10\}$	16	16	32	29
$\{4, 6, 1, 2, 5, 8, 9, 10, 7, 11, 3, 0\}$	16	16	29	32
$\{3, 2, 1, 6, 7, 0, 9, 10, 5, 11, 8, 4\}$	16	16	24	24
$\{9, 2, 5, 6, 7, 4, 11, 8, 1, 10, 3, 0\}^{eo}$	17	16/15	35	35

Table 15: Optimal permutations for $k = 14$ up to extended pair-equivalence

Optimal Permutations $k = 14$, $DR(\pi) = 8$	Imp.	Intg.	Diff.	Lin.
$\{9, 2, 1, 4, 11, 0, 5, 6, 3, 10, 7, 12, 13, 8\}^{eo}$	14	15	41	41
$\{11, 4, 1, 6, 5, 2, 9, 10, 3, 0, 7, 12, 13, 8\}^{eo}$	14	15	40	40
$\{1, 2, 5, 10, 11, 0, 9, 4, 3, 6, 7, 12, 13, 8\}^{eo}$	14	15	40	40
$\{11, 6, 7, 4, 13, 2, 1, 8, 3, 10, 9, 12, 5, 0\}^{eo}$	14	15	40	40
$\{1, 4, 5, 0, 11, 6, 9, 2, 3, 10, 7, 12, 13, 8\}^{eo}$	14	15	39	39
$\{11, 4, 1, 2, 9, 10, 5, 6, 3, 0, 7, 12, 13, 8\}^{eo}$	14	15	40	38
$\{5, 2, 3, 4, 9, 10, 1, 6, 11, 0, 7, 12, 13, 8\}^{eo}$	14	15	38	40
$\{9, 10, 5, 6, 1, 4, 11, 2, 3, 0, 7, 12, 13, 8\}^{eo}$	14	15	38	38
$\{5, 6, 11, 2, 9, 10, 1, 4, 3, 0, 7, 12, 13, 8\}^{eo}$	14	15	33	33
$\{3, 4, 11, 6, 1, 8, 5, 2, 10, 0, 7, 12, 13, 9\}$	14	16/17	33	27
$\{1, 4, 5, 6, 11, 2, 9, 10, 3, 0, 7, 12, 13, 8\}^{eo}$	15	15	39	39
$\{9, 2, 11, 4, 1, 10, 5, 6, 3, 0, 7, 12, 13, 8\}^{eo}$	15	15	39	39
$\{1, 10, 11, 4, 9, 6, 5, 2, 3, 0, 7, 12, 13, 8\}^{eo}$	15	15	39	39
$\{11, 6, 1, 4, 5, 2, 9, 10, 3, 0, 7, 12, 13, 8\}^{eo}$	15	15	38	38
$\{3, 4, 11, 6, 1, 2, 5, 8, 9, 0, 7, 12, 13, 10\}^{eo}$	15	15	38	38
$\{1, 2, 5, 6, 11, 4, 9, 10, 3, 0, 7, 12, 13, 8\}^{eo}$	15	15	37	39
$\{1, 10, 5, 2, 11, 0, 9, 4, 3, 6, 7, 12, 13, 8\}^{eo}$	15	15	39	37
$\{5, 3, 4, 2, 9, 6, 1, 10, 11, 0, 7, 12, 13, 8\}$	15	15	37	37
$\{3, 6, 9, 4, 7, 10, 13, 8, 11, 2, 1, 12, 5, 0\}^{eo}$	15	15	37	37
$\{11, 8, 5, 12, 1, 2, 7, 10, 3, 0, 9, 13, 6, 4\}$	15	15	27	33
$\{5, 2, 11, 6, 9, 4, 1, 10, 3, 0, 7, 12, 13, 8\}^{eo}$	15	15/16	39	39
$\{9, 4, 1, 6, 5, 10, 11, 2, 3, 0, 7, 13, 8, 12\}$	15	15/16	38	37
$\{11, 2, 9, 4, 3, 6, 13, 8, 7, 10, 1, 12, 5, 0\}^{eo}$	15	15/16	37	37
$\{1, 6, 11, 4, 9, 2, 5, 10, 3, 0, 7, 12, 13, 8\}^{eo}$	15	16/15	39	39
$\{9, 6, 1, 10, 2, 4, 3, 5, 11, 0, 7, 12, 13, 8\}$	15	16/15	37	37
$\{1, 10, 5, 6, 11, 2, 9, 4, 3, 0, 7, 13, 8, 12\}$	15	16/15	37	37
$\{11, 2, 9, 6, 5, 1, 3, 8, 4, 0, 7, 12, 13, 10\}$	15	16/15	37	36
$\{13, 2, 11, 4, 9, 6, 3, 8, 7, 10, 1, 12, 5, 0\}^{eo}$	15	16	39	39
$\{11, 4, 1, 2, 5, 6, 9, 10, 3, 0, 7, 12, 13, 8\}^{eo}$	15	16	39	39
$\{1, 10, 11, 4, 5, 6, 9, 2, 3, 0, 7, 13, 8, 12\}$	15	16	37	38
$\{9, 5, 1, 6, 10, 4, 11, 2, 3, 0, 7, 12, 13, 8\}$	15	16	37	38
$\{1, 10, 11, 6, 5, 2, 9, 4, 3, 0, 7, 13, 8, 12\}$	15	16	38	37
$\{5, 10, 1, 6, 7, 2, 8, 12, 11, 0, 9, 13, 3, 4\}$	15	16	37	37
$\{3, 6, 11, 8, 5, 1, 9, 2, 4, 0, 7, 12, 13, 10\}$	15	16	37	37
$\{7, 5, 1, 2, 10, 12, 3, 8, 11, 0, 9, 13, 6, 4\}$	15	16	37	37
$\{2, 8, 3, 4, 11, 1, 5, 6, 10, 0, 7, 12, 13, 9\}$	15	16	37	37
$\{11, 2, 1, 6, 5, 9, 4, 8, 3, 0, 7, 12, 13, 10\}$	15	16	36	37
$\{11, 6, 4, 10, 5, 9, 1, 2, 3, 0, 7, 13, 8, 12\}$	15	16	36	37
$\{9, 4, 1, 2, 11, 8, 5, 10, 3, 0, 7, 12, 13, 6\}^{eo}$	15	16	36	36
$\{10, 0, 11, 4, 9, 6, 5, 2, 3, 1, 7, 13, 8, 12\}$	15	16	36	36
$\{7, 10, 3, 4, 1, 12, 5, 2, 11, 0, 9, 13, 8, 6\}$	15	16	36	36
$\{9, 12, 1, 4, 11, 6, 5, 2, 3, 0, 7, 13, 10, 8\}$	15	16	35	35
$\{5, 10, 1, 2, 11, 4, 8, 12, 3, 0, 9, 13, 7, 6\}$	15	16	32	32
$\{11, 3, 10, 7, 5, 1, 12, 6, 4, 0, 9, 13, 8, 2\}$	15	16	27	27
$\{4, 8, 0, 2, 6, 10, 7, 11, 5, 12, 9, 13, 1, 3\}$	15	16	26	26
$\{4, 10, 11, 1, 5, 2, 8, 12, 3, 0, 9, 13, 7, 6\}$	15	16	23	32
$\{7, 2, 8, 12, 11, 6, 1, 4, 5, 10, 9, 13, 3, 0\}$	15	16	20	20
$\{3, 12, 1, 6, 11, 9, 5, 2, 4, 0, 7, 13, 10, 8\}$	15	16	20	20
$\{11, 8, 5, 12, 3, 1, 7, 10, 2, 0, 9, 13, 6, 4\}$	15	16/17	20	33
$\{5, 3, 11, 6, 1, 8, 4, 2, 10, 0, 7, 12, 13, 9\}$	15	16/17	33	20
$\{11, 2, 1, 6, 5, 9, 4, 0, 3, 10, 7, 13, 8, 12\}$	15	17/15	37	36
$\{7, 8, 11, 12, 1, 2, 5, 10, 3, 0, 9, 13, 6, 4\}$	15	17/16	36	36
$\{2, 10, 11, 4, 5, 1, 8, 12, 3, 0, 9, 13, 7, 6\}$	15	17/16	32	23
$\{11, 2, 5, 8, 1, 12, 7, 10, 3, 0, 9, 13, 6, 4\}$	16	15/16	37	37
$\{5, 8, 11, 4, 3, 6, 1, 2, 10, 0, 7, 12, 13, 9\}$	16	16	37	37
$\{4, 6, 5, 1, 11, 2, 9, 0, 3, 10, 7, 12, 13, 8\}$	16	16	36	36
$\{3, 5, 8, 12, 7, 2, 10, 6, 11, 0, 9, 13, 1, 4\}$	16	16	33	33
$\{9, 6, 7, 4, 11, 2, 3, 12, 5, 1, 8, 13, 0, 10\}$	16	16	24	32
$\{4, 10, 8, 12, 11, 6, 7, 3, 5, 0, 9, 13, 1, 2\}$	16	17	33	33
$\{12, 2, 7, 8, 11, 6, 3, 4, 10, 1, 9, 13, 5, 0\}$	16	17	32	24

Table 16: Optimal permutations for $k = 16$ up to extended pair-equivalence

Optimal Permutations $k = 16$, $DR(\pi) = 8$	Imp.	Intg.	Diff.	Lin.
$\{7, 4, 15, 8, 3, 0, 11, 12, 5, 6, 13, 10, 1, 2, 9, 14\}^{eo}$	14	15	44	44
$\{13, 6, 7, 10, 15, 2, 3, 12, 1, 8, 5, 0, 9, 4, 11, 14\}^{eo}$	14	15	41	41
$\{11, 2, 3, 14, 7, 12, 15, 8, 9, 10, 13, 0, 1, 4, 5, 6\}^{eo}$	14	15	40	40
$\{15, 2, 3, 14, 7, 4, 11, 12, 13, 6, 1, 10, 9, 0, 5, 8\}^{eo}$	15	15	38	38
$\{15, 2, 3, 14, 7, 4, 13, 8, 9, 12, 1, 10, 11, 0, 5, 6\}^{eo}$	15	15	35	35
$\{15, 8, 9, 14, 1, 10, 13, 2, 3, 12, 7, 4, 11, 0, 5, 6\}^{eo}$	15	15	35	35
$\{5, 10, 15, 0, 9, 12, 13, 4, 11, 8, 3, 6, 7, 2, 1, 14\}^{eo}$	15	15	26	39
$\{13, 8, 9, 12, 7, 4, 11, 2, 3, 6, 15, 0, 5, 10, 1, 14\}^{eo}$	15	15	39	26
$\{15, 2, 3, 14, 1, 10, 13, 8, 9, 12, 7, 4, 11, 0, 5, 6\}^{eo}$	15	15	26	26
$\{13, 10, 11, 14, 1, 4, 15, 12, 7, 2, 3, 8, 9, 6, 5, 0\}^{eo}$	15	15/16	42	42
$\{7, 8, 5, 2, 13, 0, 15, 12, 3, 10, 11, 4, 9, 14, 1, 6\}^{eo}$	15	16	42	42
$\{11, 12, 9, 4, 5, 8, 15, 2, 7, 0, 13, 10, 3, 14, 1, 6\}^{eo}$	15	16	39	39
$\{6, 12, 13, 0, 11, 8, 5, 1, 7, 4, 15, 2, 3, 14, 9, 10\}$	15	16	38	38
$\{15, 10, 7, 4, 1, 2, 9, 12, 11, 8, 3, 6, 5, 0, 13, 14\}^{eo}$	15	16	38	38
$\{14, 0, 12, 2, 10, 6, 8, 4, 15, 1, 13, 3, 9, 5, 11, 7\}$	15	16	30	30
$\{14, 0, 10, 6, 8, 2, 12, 4, 15, 1, 9, 3, 13, 5, 11, 7\}$	15	16	26	26
$\{14, 0, 12, 2, 8, 6, 10, 4, 13, 1, 15, 3, 9, 5, 11, 7\}$	15	16	20	20
$\{1, 7, 13, 9, 15, 11, 5, 3, 12, 8, 4, 2, 14, 10, 0, 6\}$	15	16	18	18
$\{14, 0, 9, 6, 15, 1, 5, 2, 3, 12, 13, 8, 11, 4, 7, 10\}$	16	16	41	41
$\{10, 12, 5, 2, 6, 0, 15, 8, 9, 14, 7, 1, 3, 4, 11, 13\}$	16	17	38	38

Table 17: Optimal permutations for $k = 18$ up to extended pair-equivalence

Optimal Permutations $k = 18$, $DR(\pi) = 8$	Imp.	Intg.	Diff.	Lin.
$\{3, 8, 5, 12, 7, 0, 9, 14, 11, 2, 13, 10, 15, 4, 1, 16, 17, 6\}^{eo}$	15	16	40	40

Table 18: Some optimal permutations for $k = 20$ up to extended pair-equivalence

Optimal Permutations $k = 20$, $DR(\pi) = 9$	Imp.	Intg.	Diff.	Lin.
$\{3, 12, 5, 10, 7, 8, 9, 6, 11, 0, 13, 16, 15, 4, 1, 18, 19, 2, 17, 14\}$	16	17/16	42	42
$\{3, 14, 5, 16, 7, 0, 9, 10, 11, 12, 1, 18, 15, 8, 13, 4, 19, 2, 17, 6\}$	16	17	51	51
$\{3, 10, 5, 14, 7, 12, 9, 6, 11, 2, 13, 16, 15, 8, 17, 18, 1, 4, 19, 0\}$	16	17	51	51
$\{3, 8, 5, 2, 7, 0, 9, 14, 11, 12, 13, 16, 15, 4, 1, 18, 17, 10, 19, 6\}$	16	17	51	51
$\{3, 12, 5, 8, 7, 4, 9, 0, 11, 14, 13, 16, 15, 6, 1, 18, 19, 10, 17, 2\}$	16	17/18	52	49
$\{3, 8, 5, 6, 7, 14, 9, 2, 1, 16, 13, 10, 15, 4, 11, 18, 19, 0, 17, 12\}$	17	17	51	51
$\{3, 10, 5, 16, 7, 4, 9, 12, 11, 0, 13, 8, 15, 2, 17, 18, 19, 14, 1, 6\}$	17	17	51	51
$\{3, 10, 5, 12, 7, 4, 9, 0, 11, 16, 1, 14, 15, 8, 17, 18, 13, 2, 19, 6\}$	17	17	51	51
$\{3, 14, 5, 12, 7, 18, 9, 2, 11, 6, 13, 16, 1, 10, 17, 4, 15, 8, 19, 0\}$	17	17/18	51	51
$\{3, 4, 5, 2, 7, 16, 1, 12, 11, 8, 13, 14, 15, 6, 9, 18, 19, 0, 17, 10\}$	17	17/18	51	51
$\{3, 12, 5, 6, 7, 16, 9, 10, 11, 4, 13, 2, 15, 0, 1, 18, 19, 8, 17, 14\}$	17	18	51	51
$\{3, 6, 5, 12, 7, 2, 9, 14, 11, 8, 13, 0, 15, 4, 17, 18, 19, 10, 1, 16\}$	17	18	51	51
$\{3, 12, 5, 6, 7, 2, 9, 16, 11, 14, 13, 0, 1, 4, 17, 18, 19, 10, 15, 8\}$	17	18	51	51
$\{3, 6, 5, 18, 7, 12, 9, 4, 11, 0, 13, 16, 15, 8, 17, 2, 19, 14, 1, 10\}$	16	17	26	26
$\{3, 16, 5, 8, 7, 12, 9, 4, 11, 0, 13, 6, 15, 18, 17, 2, 19, 14, 1, 10\}$	16	17	26	26
$\{3, 8, 5, 2, 7, 12, 9, 16, 11, 4, 13, 14, 15, 6, 17, 18, 1, 10, 19, 0\}$	16	17	26	26
$\{3, 18, 5, 10, 7, 16, 9, 2, 11, 14, 13, 8, 15, 0, 17, 6, 19, 12, 1, 4\}$	16	17	26	26
$\{3, 4, 5, 10, 7, 16, 9, 14, 11, 2, 13, 6, 15, 12, 17, 18, 1, 8, 19, 0\}$	16	17	26	26
$\{3, 16, 5, 0, 7, 12, 9, 18, 11, 14, 13, 6, 15, 10, 17, 2, 19, 8, 1, 4\}$	16	17	26	26
$\{3, 4, 5, 0, 7, 10, 9, 14, 1, 12, 13, 2, 15, 8, 17, 18, 11, 6, 19, 16\}$	16	17	49	26
$\{3, 12, 5, 16, 7, 14, 9, 10, 11, 8, 13, 4, 15, 0, 17, 18, 1, 6, 19, 2\}$	16	17	51	39
$\{3, 10, 5, 0, 7, 14, 9, 2, 11, 8, 13, 4, 1, 16, 17, 18, 15, 12, 19, 6\}$	16	17/18	50	40
$\{3, 12, 5, 2, 7, 16, 9, 10, 11, 8, 13, 14, 15, 4, 1, 18, 19, 6, 17, 0\}$	17	17/16	39	48
$\{3, 6, 5, 0, 7, 12, 9, 18, 11, 14, 13, 16, 15, 10, 17, 2, 19, 8, 1, 4\}$	17	17	26	26
$\{3, 6, 5, 8, 7, 12, 9, 4, 11, 0, 13, 16, 15, 18, 17, 2, 19, 14, 1, 10\}$	17	17	26	26
$\{3, 10, 5, 8, 7, 0, 9, 12, 1, 6, 13, 16, 15, 18, 17, 4, 19, 14, 11, 2\}$	17	17	26	26
$\{3, 16, 5, 0, 7, 12, 9, 18, 1, 14, 13, 6, 15, 10, 17, 2, 19, 8, 11, 4\}$	17	17	26	26
$\{3, 8, 5, 16, 7, 12, 9, 6, 11, 2, 1, 14, 15, 18, 17, 4, 19, 0, 13, 10\}$	17	17	50	26
$\{3, 0, 5, 18, 7, 8, 9, 12, 11, 14, 13, 6, 1, 10, 17, 2, 19, 16, 15, 4\}$	17	17	52	40
$\{3, 4, 5, 14, 7, 2, 9, 0, 11, 16, 13, 10, 15, 6, 17, 18, 19, 12, 1, 8\}$	17	17/18	39	26
$\{3, 10, 5, 16, 7, 8, 9, 6, 11, 14, 13, 4, 15, 12, 17, 18, 1, 2, 19, 0\}$	17	17/18	39	26
$\{3, 16, 5, 2, 7, 10, 9, 18, 11, 6, 13, 0, 15, 8, 17, 4, 19, 14, 1, 12\}$	17	18/17	47	26
$\{3, 16, 5, 6, 7, 0, 9, 14, 11, 12, 13, 4, 1, 10, 17, 2, 19, 8, 15, 18\}$	17	17/18	52	48
$\{3, 14, 5, 10, 7, 4, 9, 18, 1, 6, 13, 0, 15, 8, 17, 2, 11, 12, 19, 16\}$	17	18	26	26
$\{3, 12, 5, 10, 7, 2, 9, 6, 1, 16, 13, 14, 15, 8, 17, 18, 11, 0, 19, 4\}$	17	18	26	26
$\{3, 6, 5, 10, 7, 8, 9, 16, 1, 12, 13, 4, 15, 2, 11, 14, 19, 0, 17, 18\}$	17	18	46	26
$\{3, 16, 5, 12, 7, 8, 9, 6, 11, 2, 13, 14, 1, 10, 17, 18, 15, 0, 19, 4\}$	17	18	51	39
$\{3, 4, 5, 14, 7, 16, 9, 12, 11, 0, 13, 6, 15, 10, 1, 18, 17, 8, 19, 2\}$	17	17/18	46	50
$\{3, 4, 5, 0, 7, 8, 9, 10, 11, 14, 13, 16, 15, 6, 1, 18, 17, 12, 19, 2\}$	17	18/17	50	40
$\{3, 10, 5, 14, 7, 8, 9, 0, 11, 16, 1, 18, 15, 12, 17, 4, 13, 2, 19, 6\}$	17	17	40	49
$\{3, 14, 5, 12, 7, 18, 9, 6, 11, 0, 1, 16, 15, 10, 17, 4, 13, 2, 19, 8\}$	17	17	48	45
$\{3, 8, 5, 14, 7, 2, 9, 0, 11, 4, 13, 16, 15, 10, 17, 18, 19, 6, 1, 12\}$	17	18	44	46
$\{3, 0, 5, 8, 7, 12, 9, 6, 11, 14, 13, 4, 15, 10, 17, 18, 1, 2, 19, 16\}$	17	17	36	40
$\{3, 10, 5, 16, 7, 12, 9, 6, 11, 14, 13, 8, 15, 2, 17, 18, 1, 4, 19, 0\}$	16	17	40	47
$\{3, 0, 5, 14, 7, 16, 9, 6, 11, 12, 1, 8, 15, 10, 13, 18, 19, 2, 17, 4\}$	17	17/18	40	40
$\{3, 14, 5, 0, 7, 4, 9, 16, 11, 6, 13, 10, 15, 2, 17, 18, 19, 8, 1, 12\}$	16	17	40	40
$\{3, 0, 5, 16, 7, 14, 9, 12, 11, 4, 13, 8, 15, 6, 1, 18, 19, 10, 17, 2\}$	16	17	49	45
$\{3, 4, 5, 0, 7, 16, 9, 12, 11, 6, 13, 14, 1, 18, 17, 2, 19, 10, 15, 8\}$	17	17	47	50
$\{3, 6, 5, 16, 7, 14, 9, 12, 11, 0, 13, 4, 15, 8, 1, 18, 17, 2, 19, 10\}$	16	17	40	51
$\{3, 6, 5, 0, 7, 14, 9, 10, 11, 12, 1, 18, 15, 16, 17, 4, 13, 8, 19, 2\}$	17	17	49	40
$\{3, 16, 5, 8, 7, 4, 9, 12, 11, 6, 13, 14, 15, 0, 17, 18, 1, 2, 19, 10\}$	17	17/18	40	48
$\{3, 0, 5, 12, 7, 2, 9, 10, 11, 4, 13, 16, 15, 6, 17, 18, 1, 14, 19, 8\}$	16	17	40	40
$\{3, 4, 5, 12, 7, 18, 9, 10, 11, 0, 13, 8, 1, 14, 17, 2, 15, 16, 19, 6\}$	17	17	49	49
$\{3, 6, 5, 16, 7, 10, 9, 14, 11, 8, 13, 2, 15, 12, 1, 18, 19, 0, 17, 4\}$	17	18/17	50	41
$\{3, 14, 5, 2, 7, 16, 9, 12, 11, 6, 13, 10, 15, 4, 1, 18, 19, 8, 17, 0\}$	16	17	32	40
$\{3, 8, 5, 14, 7, 12, 9, 10, 11, 4, 13, 2, 15, 6, 17, 18, 1, 16, 19, 0\}$	16	17	50	40
$\{3, 12, 5, 6, 7, 2, 9, 14, 11, 0, 13, 4, 15, 8, 17, 18, 1, 16, 19, 10\}$	17	18/17	49	49
$\{3, 6, 5, 12, 7, 4, 9, 10, 11, 2, 13, 16, 15, 8, 17, 18, 1, 14, 19, 0\}$	17	17/18	40	51
$\{3, 8, 5, 0, 7, 14, 9, 2, 11, 4, 13, 10, 15, 6, 17, 18, 1, 12, 19, 16\}$	17	17	26	39
$\{3, 12, 5, 6, 7, 2, 9, 0, 11, 16, 13, 14, 15, 10, 1, 18, 19, 8, 17, 4\}$	17	18/17	39	39
$\{3, 0, 5, 16, 7, 4, 9, 12, 1, 6, 13, 14, 15, 8, 11, 18, 19, 10, 17, 2\}$	16	17	40	40
$\{3, 14, 5, 6, 7, 12, 9, 16, 11, 2, 13, 0, 15, 4, 1, 18, 17, 8, 19, 10\}$	17	17	40	48
$\{3, 12, 5, 8, 7, 0, 9, 16, 11, 14, 1, 4, 15, 10, 13, 18, 17, 6, 19, 2\}$	17	17/18	48	48
$\{3, 12, 5, 10, 7, 0, 9, 16, 1, 6, 13, 8, 15, 4, 17, 18, 19, 2, 11, 14\}$	16	17	47	45
$\{3, 0, 5, 8, 7, 12, 9, 16, 11, 14, 13, 6, 15, 2, 1, 18, 17, 10, 19, 4\}$	17	18	48	51
$\{3, 0, 5, 12, 7, 10, 9, 6, 11, 2, 13, 16, 15, 4, 17, 18, 1, 14, 19, 8\}$	16	17	40	40
$\{3, 14, 5, 8, 7, 18, 1, 6, 11, 2, 13, 16, 9, 10, 17, 4, 15, 12, 19, 0\}$	16	17	50	50
$\{3, 0, 5, 14, 7, 12, 9, 10, 11, 8, 13, 16, 15, 2, 17, 18, 1, 4, 19, 6\}$	16	18/17	49	40
$\{3, 8, 5, 14, 7, 0, 9, 12, 11, 18, 13, 4, 1, 16, 17, 2, 15, 6, 19, 10\}$	17	17/18	46	46
$\{3, 10, 5, 8, 7, 12, 9, 0, 11, 14, 13, 6, 15, 4, 17, 18, 1, 16, 19, 2\}$	17	17/18	48	50
$\{3, 6, 5, 10, 7, 14, 9, 0, 11, 16, 13, 2, 1, 8, 17, 18, 15, 12, 19, 4\}$	16	17	48	48
$\{3, 12, 5, 10, 7, 14, 9, 4, 11, 8, 13, 2, 15, 16, 1, 18, 17, 6, 19, 0\}$	17	17	26	39
$\{3, 6, 5, 14, 7, 10, 9, 16, 1, 12, 13, 0, 15, 8, 17, 18, 19, 4, 11, 2\}$	17	17	49	32
$\{3, 14, 5, 12, 7, 2, 9, 16, 11, 8, 13, 0, 15, 6, 17, 18, 1, 4, 19, 10\}$	16	17	48	48

Table 19: Optimal even-odd permutations for $k = 22$ up to extended pair-equivalence

Optimal Permutations $k = 22$, $DR(\pi) = 8$	Imp.	Intg.	Diff.	Lin.
$\{3, 0, 5, 14, 7, 10, 9, 2, 11, 12, 13, 18, 15, 6, 17, 4, 19, 20, 1, 16, 21, 8\}$	15	16	40	40
$\{3, 18, 5, 8, 7, 14, 9, 0, 1, 12, 13, 10, 15, 4, 17, 2, 19, 20, 11, 16, 21, 6\}$	15	16	40	40

Table 20: Optimal even-odd permutations for $k = 24$ up to extended pair-equivalence

Optimal Permutations $k = 24$, $DR(\pi) = 9$	Imp.	Intg.	Diff.	Lin.
$\{3, 4, 5, 0, 7, 22, 9, 6, 11, 18, 1, 16, 15, 20, 17, 12, 13, 10, 21, 2, 19, 14, 23, 8\}$	16	17	34	34
$\{3, 0, 5, 20, 7, 12, 9, 22, 11, 8, 13, 16, 15, 4, 1, 18, 19, 14, 17, 2, 23, 6, 21, 10\}$	16	17	52	30
$\{3, 8, 5, 20, 7, 4, 9, 22, 11, 0, 13, 16, 15, 12, 1, 18, 19, 14, 17, 2, 23, 6, 21, 10\}$	16	17	30	52
$\{3, 20, 5, 6, 7, 4, 9, 22, 11, 12, 1, 16, 15, 18, 17, 0, 13, 10, 21, 2, 19, 14, 23, 8\}$	16	17	40	26
$\{3, 20, 5, 14, 7, 12, 9, 22, 11, 0, 1, 10, 15, 4, 17, 18, 13, 6, 21, 2, 19, 16, 23, 8\}$	16	17	26	40
$\{3, 8, 5, 14, 7, 0, 9, 6, 11, 20, 13, 18, 15, 4, 17, 10, 19, 16, 1, 22, 23, 12, 21, 2\}$	16	17	38	26
$\{3, 16, 5, 10, 7, 4, 9, 18, 11, 20, 13, 6, 15, 0, 17, 14, 19, 8, 1, 22, 23, 12, 21, 2\}$	16	17	26	38
$\{3, 22, 5, 12, 7, 16, 9, 18, 11, 0, 1, 20, 15, 4, 17, 14, 13, 6, 21, 2, 19, 10, 23, 8\}$	17	17	53	53
$\{3, 12, 5, 6, 7, 0, 9, 16, 11, 14, 13, 8, 15, 2, 17, 18, 19, 4, 21, 22, 1, 20, 23, 10\}$	17	17	51	40
$\{3, 4, 5, 12, 7, 16, 9, 2, 11, 8, 13, 14, 15, 0, 17, 20, 19, 6, 21, 22, 1, 18, 23, 10\}$	17	17	40	51
$\{3, 10, 5, 6, 7, 12, 9, 0, 11, 18, 1, 22, 15, 20, 17, 14, 19, 8, 21, 4, 13, 16, 23, 2\}$	17	17	40	40
$\{3, 16, 5, 6, 7, 14, 9, 18, 11, 4, 1, 8, 15, 2, 17, 0, 19, 10, 21, 22, 13, 20, 23, 12\}$	17	17	40	40
$\{3, 22, 5, 0, 7, 4, 9, 18, 11, 6, 1, 16, 15, 20, 17, 12, 13, 10, 21, 2, 19, 14, 23, 8\}$	17	17	40	40
$\{3, 10, 5, 16, 7, 8, 9, 14, 11, 18, 13, 6, 15, 4, 17, 2, 19, 0, 21, 22, 1, 20, 23, 12\}$	17	17	42	32
$\{3, 18, 5, 14, 7, 10, 9, 16, 11, 20, 13, 8, 15, 4, 17, 0, 19, 6, 1, 22, 21, 12, 23, 2\}$	17	17	38	26
$\{3, 18, 5, 14, 7, 0, 9, 16, 11, 20, 13, 8, 15, 4, 17, 10, 19, 6, 1, 22, 21, 2, 23, 12\}$	17	17	38	26
$\{3, 6, 5, 0, 7, 14, 9, 18, 11, 20, 13, 16, 15, 10, 17, 4, 19, 8, 1, 22, 21, 12, 23, 2\}$	17	17	26	38
$\{3, 18, 5, 8, 7, 2, 9, 20, 11, 4, 13, 16, 15, 10, 17, 14, 19, 6, 21, 22, 1, 12, 23, 0\}$	17	17/18	56	40
$\{3, 0, 5, 14, 7, 12, 9, 10, 11, 8, 13, 2, 15, 18, 17, 20, 19, 4, 1, 22, 23, 6, 21, 16\}$	17	17/18	32	48
$\{3, 4, 5, 20, 7, 18, 9, 16, 11, 14, 13, 10, 15, 0, 17, 6, 19, 2, 21, 22, 1, 8, 23, 12\}$	17	17/18	32	42
$\{3, 22, 5, 14, 7, 16, 9, 12, 11, 18, 1, 20, 15, 8, 13, 0, 19, 10, 17, 6, 21, 4, 23, 2\}$	17	18/17	59	59
$\{3, 12, 5, 10, 7, 8, 9, 6, 11, 20, 13, 18, 15, 4, 17, 14, 19, 2, 1, 22, 23, 0, 21, 16\}$	17	18/17	48	32
$\{3, 0, 5, 14, 7, 12, 9, 4, 11, 8, 13, 2, 15, 18, 17, 20, 19, 10, 1, 22, 23, 6, 21, 16\}$	17	18/17	30	40
$\{3, 12, 5, 10, 7, 18, 9, 6, 11, 20, 13, 8, 15, 4, 17, 14, 19, 2, 1, 22, 23, 0, 21, 16\}$	17	18/17	40	30
$\{3, 18, 5, 6, 7, 20, 1, 2, 11, 8, 13, 16, 15, 12, 9, 22, 19, 14, 17, 4, 23, 0, 21, 10\}$	17	18	58	58
$\{3, 0, 5, 8, 7, 16, 9, 14, 11, 20, 13, 4, 15, 18, 17, 6, 19, 10, 1, 22, 23, 12, 21, 2\}$	17	18	56	56
$\{3, 22, 5, 12, 7, 10, 9, 16, 11, 0, 13, 18, 15, 6, 1, 4, 19, 14, 21, 2, 17, 20, 23, 8\}$	17	18	55	55
$\{3, 18, 5, 8, 7, 4, 9, 20, 11, 6, 13, 16, 15, 2, 17, 10, 19, 14, 21, 22, 1, 12, 23, 0\}$	17	18	40	56
$\{3, 16, 5, 20, 7, 14, 9, 10, 11, 8, 13, 22, 15, 0, 1, 6, 19, 4, 21, 2, 17, 18, 23, 12\}$	17	18	40	30
$\{3, 16, 5, 20, 7, 8, 9, 0, 11, 22, 13, 14, 15, 12, 1, 6, 19, 4, 21, 2, 17, 18, 23, 10\}$	17	18	30	40
$\{3, 16, 5, 0, 7, 14, 9, 18, 11, 20, 13, 6, 15, 10, 17, 4, 19, 8, 1, 22, 21, 2, 23, 12\}$	17	18	26	38

Table 21: One optimal even-odd permutation for $k = 26$

One even-odd optimal Permutation $k = 26$, $DR(\pi) = 9$	Imp.	Intg.	Diff.	Lin.
$\{3, 20, 5, 6, 7, 12, 9, 24, 11, 18, 1, 16, 15,$ $10, 17, 22, 19, 4, 13, 0, 23, 14, 25, 8, 21, 2\}$	17	18	44	44

Table 22: Best known permutations $k = 32$

Best known Permutations $k = 32$, $DR(\pi) = 10$	Imp.	Intg.	Diff.	Lin.
$\{1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30,$ $3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28\}$	18	19	70	70
$\{1, 2, 7, 4, 11, 8, 13, 14, 17, 18, 23, 20, 27, 24, 29, 30,$ $3, 0, 5, 6, 9, 10, 15, 12, 19, 16, 21, 22, 25, 26, 31, 28\}$	18	19	70	70
$\{3, 0, 5, 6, 9, 10, 15, 12, 19, 16, 21, 22, 25, 26, 31, 28,$ $1, 2, 7, 4, 11, 8, 13, 14, 17, 18, 23, 20, 27, 24, 29, 30\}$	18	19	70	70
$\{3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28,$ $1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30\}$	18	19	70	70
$\{1, 2, 7, 4, 11, 8, 13, 14, 19, 16, 21, 22, 25, 26, 31, 28,$ $3, 0, 5, 6, 9, 10, 15, 12, 17, 18, 23, 20, 27, 24, 29, 30\}$	18	19	65	65
$\{3, 0, 5, 6, 9, 10, 15, 12, 17, 18, 23, 20, 27, 24, 29, 30,$ $1, 2, 7, 4, 11, 8, 13, 14, 19, 16, 21, 22, 25, 26, 31, 28\}$	18	19	65	65
$\{1, 2, 5, 6, 9, 10, 13, 14, 19, 16, 23, 20, 27, 24, 31, 28,$ $3, 0, 7, 4, 11, 8, 15, 12, 17, 18, 21, 22, 25, 26, 29, 30\}$	19	20	71	71
$\{1, 2, 7, 4, 9, 10, 15, 12, 17, 18, 23, 20, 25, 26, 31, 28,$ $3, 0, 5, 6, 11, 8, 13, 14, 19, 16, 21, 22, 27, 24, 29, 30\}$	19	20	71	71
$\{3, 0, 5, 6, 11, 8, 13, 14, 19, 16, 21, 22, 27, 24, 29, 30,$ $1, 2, 7, 4, 9, 10, 15, 12, 17, 18, 23, 20, 25, 26, 31, 28\}$	19	20	71	71
$\{3, 0, 7, 4, 11, 8, 15, 12, 17, 18, 21, 22, 25, 26, 29, 30,$ $1, 2, 5, 6, 9, 10, 13, 14, 19, 16, 23, 20, 27, 24, 31, 28\}$	19	20	71	71
$\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31,$ $0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30\}$	19	20	23	23
$\{2, 0, 6, 4, 10, 8, 14, 12, 18, 16, 22, 20, 26, 24, 30, 28,$ $3, 1, 7, 5, 11, 9, 15, 13, 19, 17, 23, 21, 27, 25, 31, 29\}$	19	20	23	23

Table 23: Best known permutations $k = 64$

Best known Permutations $k = 64$, $DR(\pi) = 11$	Imp.	Intg.
$\{1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30,$ $35, 32, 39, 36, 41, 42, 45, 46, 49, 50, 53, 54, 59, 56, 63, 60,$ $3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28,$ $33, 34, 37, 38, 43, 40, 47, 44, 51, 48, 55, 52, 57, 58, 61, 62\}$	21	21/22
$\{3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28,$ $33, 34, 37, 38, 43, 40, 47, 44, 51, 48, 55, 52, 57, 58, 61,$ $62, 1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29,$ $30, 35, 32, 39, 36, 41, 42, 45, 46, 49, 50, 53, 54, 59, 56, 63, 60\}$	21	21/22
$\{1, 2, 7, 4, 11, 8, 13, 14, 19, 16, 21, 22, 25, 26, 31, 28,$ $33, 34, 39, 36, 43, 40, 45, 46, 51, 48, 53, 54, 57, 58, 63,$ $60, 3, 0, 5, 6, 9, 10, 15, 12, 17, 18, 23, 20, 27, 24, 29,$ $30, 35, 32, 37, 38, 41, 42, 47, 44, 49, 50, 55, 52, 59, 56, 61, 62\}$	21	22/21
$\{3, 0, 5, 6, 9, 10, 15, 12, 17, 18, 23, 20, 27, 24, 29, 30,$ $35, 32, 37, 38, 41, 42, 47, 44, 49, 50, 55, 52, 59, 56, 61,$ $62, 1, 2, 7, 4, 11, 8, 13, 14, 19, 16, 21, 22, 25, 26, 31,$ $28, 33, 34, 39, 36, 43, 40, 45, 46, 51, 48, 53, 54, 57, 58, 63, 60\}$	21	22/21

Table 24: Best known permutations $k = 128$

Best known Permutations $k = 128$, $DR(\pi) = 13$	Imp.	Intg.
$\{1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30, 35, 32, 39, 36, 41, 42, 45, 46,$ $49, 50, 53, 54, 59, 56, 63, 60, 67, 64, 71, 68, 73, 74, 77, 78, 81, 82, 85, 86, 91, 88, 95, 92,$ $97, 98, 101, 102, 107, 104, 111, 108, 115, 112, 119, 116, 121, 122, 125, 126, 3, 0, 7, 4,$ $9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28, 33, 34, 37, 38, 43, 40, 47, 44, 51, 48, 55, 52,$ $57, 58, 61, 62, 65, 66, 69, 70, 75, 72, 79, 76, 83, 80, 87, 84, 89, 90, 93, 94, 99, 96, 103, 100,$ $105, 106, 109, 110, 113, 114, 117, 118, 123, 120, 127, 124\}$	24	25
$\{3, 0, 5, 6, 9, 10, 15, 12, 17, 18, 23, 20, 27, 24, 29, 30, 33, 34, 39, 36, 43, 40, 45, 46,$ $51, 48, 53, 54, 57, 58, 63, 60, 67, 64, 69, 70, 73, 74, 79, 76, 81, 82, 87, 84, 91, 88, 93, 94,$ $97, 98, 103, 100, 107, 104, 109, 110, 115, 112, 117, 118, 121, 122, 127, 124, 1, 2, 7, 4,$ $11, 8, 13, 14, 19, 16, 21, 22, 25, 26, 31, 28, 35, 32, 37, 38, 41, 42, 47, 44, 49, 50, 55, 52,$ $59, 56, 61, 62, 65, 66, 71, 68, 75, 72, 77, 78, 83, 80, 85, 86, 89, 90, 95, 92, 99, 96, 101, 102,$ $105, 106, 111, 108, 113, 114, 119, 116, 123, 120, 125, 126\}$	24	25
$\{3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28, 33, 34, 37, 38, 43, 40, 47, 44,$ $51, 48, 55, 52, 57, 58, 61, 62, 65, 66, 69, 70, 75, 72, 79, 76, 83, 80, 87, 84, 89, 90, 93, 94,$ $99, 96, 103, 100, 105, 106, 109, 110, 113, 114, 117, 118, 123, 120, 127, 124, 1, 2, 5, 6,$ $11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30, 35, 32, 39, 36, 41, 42, 45, 46, 49, 50, 53, 54,$ $59, 56, 63, 60, 67, 64, 71, 68, 73, 74, 77, 78, 81, 82, 85, 86, 91, 88, 95, 92, 97, 98, 101, 102,$ $107, 104, 111, 108, 115, 112, 119, 116, 121, 122, 125, 126\}$	24	25
$\{1, 2, 7, 4, 11, 8, 13, 14, 17, 18, 23, 20, 27, 24, 29, 30, 35, 32, 37, 38, 41, 42, 47, 44,$ $51, 48, 53, 54, 57, 58, 63, 60, 67, 64, 69, 70, 73, 74, 79, 76, 83, 80, 85, 86, 89, 90, 95, 92,$ $97, 98, 103, 100, 107, 104, 109, 110, 113, 114, 119, 116, 123, 120, 125, 126, 3, 0, 5, 6,$ $9, 10, 15, 12, 19, 16, 21, 22, 25, 26, 31, 28, 33, 34, 39, 36, 43, 40, 45, 46, 49, 50, 55, 52,$ $59, 56, 61, 62, 65, 66, 71, 68, 75, 72, 77, 78, 81, 82, 87, 84, 91, 88, 93, 94, 99, 96, 101, 102,$ $105, 106, 111, 108, 115, 112, 117, 118, 121, 122, 127, 124\}$	24	25
$\{1, 2, 7, 4, 11, 8, 13, 14, 19, 16, 21, 22, 25, 26, 31, 28, 35, 32, 37, 38, 41, 42, 47, 44,$ $49, 50, 55, 52, 59, 56, 61, 62, 65, 66, 71, 68, 75, 72, 77, 78, 83, 80, 85, 86, 89, 90, 95, 92,$ $99, 96, 101, 102, 105, 106, 111, 108, 113, 114, 119, 116, 123, 120, 125, 126, 3, 0, 5, 6,$ $9, 10, 15, 12, 17, 18, 23, 20, 27, 24, 29, 30, 33, 34, 39, 36, 43, 40, 45, 46, 51, 48, 53, 54,$ $57, 58, 63, 60, 67, 64, 69, 70, 73, 74, 79, 76, 81, 82, 87, 84, 91, 88, 93, 94, 97, 98, 103, 100,$ $107, 104, 109, 110, 115, 112, 117, 118, 121, 122, 127, 124\}$	24	25
$\{3, 0, 5, 6, 9, 10, 15, 12, 19, 16, 21, 22, 25, 26, 31, 28, 33, 34, 39, 36, 43, 40, 45, 46,$ $49, 50, 55, 52, 59, 56, 61, 62, 65, 66, 71, 68, 75, 72, 77, 78, 81, 82, 87, 84, 91, 88, 93, 94,$ $99, 96, 101, 102, 105, 106, 111, 108, 115, 112, 117, 118, 121, 122, 127, 124, 1, 2, 7, 4,$ $11, 8, 13, 14, 17, 18, 23, 20, 27, 24, 29, 30, 35, 32, 37, 38, 41, 42, 47, 44, 51, 48, 53, 54,$ $57, 58, 63, 60, 67, 64, 69, 70, 73, 74, 79, 76, 83, 80, 85, 86, 89, 90, 95, 92, 97, 98, 103, 100,$ $107, 104, 109, 110, 113, 114, 119, 116, 123, 120, 125, 126\}$	24	25
$\{3, 0, 5, 6, 11, 8, 13, 14, 17, 18, 23, 20, 25, 26, 31, 28, 35, 32, 37, 38, 43, 40, 45, 46,$ $49, 50, 55, 52, 57, 58, 63, 60, 65, 66, 71, 68, 73, 74, 79, 76, 83, 80, 85, 86, 91, 88, 93, 94,$ $97, 98, 103, 100, 105, 106, 111, 108, 115, 112, 117, 118, 123, 120, 125, 126, 1, 2, 7, 4,$ $9, 10, 15, 12, 19, 16, 21, 22, 27, 24, 29, 30, 33, 34, 39, 36, 41, 42, 47, 44, 51, 48, 53, 54,$ $59, 56, 61, 62, 67, 64, 69, 70, 75, 72, 77, 78, 81, 82, 87, 84, 89, 90, 95, 92, 99, 96, 101, 102,$ $107, 104, 109, 110, 113, 114, 119, 116, 121, 122, 127, 124\}$	25	25
$\{1, 2, 7, 4, 9, 10, 15, 12, 19, 16, 21, 22, 27, 24, 29, 30, 33, 34, 39, 36, 41, 42, 47, 44,$ $51, 48, 53, 54, 59, 56, 61, 62, 67, 64, 69, 70, 75, 72, 77, 78, 81, 82, 87, 84, 89, 90, 95, 92,$ $99, 96, 101, 102, 107, 104, 109, 110, 113, 114, 119, 116, 121, 122, 127, 124, 3, 0, 5, 6,$ $11, 8, 13, 14, 17, 18, 23, 20, 25, 26, 31, 28, 35, 32, 37, 38, 43, 40, 45, 46, 49, 50, 55, 52,$ $57, 58, 63, 60, 65, 66, 71, 68, 73, 74, 79, 76, 83, 80, 85, 86, 91, 88, 93, 94, 97, 98, 103, 100,$ $105, 106, 111, 108, 115, 112, 117, 118, 123, 120, 125, 126\}$	25	25
$\{3, 0, 7, 4, 11, 8, 15, 12, 19, 16, 23, 20, 27, 24, 31, 28, 33, 34, 37, 38, 41, 42, 45, 46,$ $49, 50, 53, 54, 57, 58, 61, 62, 65, 66, 69, 70, 73, 74, 77, 78, 81, 82, 85, 86, 89, 90, 93, 94,$ $99, 96, 103, 100, 107, 104, 111, 108, 115, 112, 119, 116, 123, 120, 127, 124, 1, 2, 5, 6,$ $9, 10, 13, 14, 17, 18, 21, 22, 25, 26, 29, 30, 35, 32, 39, 36, 43, 40, 47, 44, 51, 48, 55, 52,$ $59, 56, 63, 60, 67, 64, 71, 68, 75, 72, 79, 76, 83, 80, 87, 84, 91, 88, 95, 92, 97, 98, 101, 102,$ $105, 106, 109, 110, 113, 114, 117, 118, 121, 122, 125, 126\}$	25	25/26
$\{1, 2, 5, 6, 9, 10, 13, 14, 17, 18, 21, 22, 25, 26, 29, 30, 35, 32, 39, 36, 43, 40, 47, 44,$ $51, 48, 55, 52, 59, 56, 63, 60, 67, 64, 71, 68, 75, 72, 79, 76, 83, 80, 87, 84, 91, 88, 95, 92,$ $97, 98, 101, 102, 105, 106, 109, 110, 113, 114, 117, 118, 121, 122, 125, 126, 3, 0, 7, 4,$ $11, 8, 15, 12, 19, 16, 23, 20, 27, 24, 31, 28, 33, 34, 37, 38, 41, 42, 45, 46, 49, 50, 53, 54,$ $57, 58, 61, 62, 65, 66, 69, 70, 73, 74, 77, 78, 81, 82, 85, 86, 89, 90, 93, 94, 99, 96, 103, 100,$ $107, 104, 111, 108, 115, 112, 119, 116, 123, 120, 127, 124\}$	25	25/26
$\{1, 2, 7, 4, 9, 10, 15, 12, 17, 18, 23, 20, 25, 26, 31, 28, 35, 32, 37, 38, 43, 40, 45, 46,$ $51, 48, 53, 54, 59, 56, 61, 62, 65, 66, 71, 68, 73, 74, 79, 76, 81, 82, 87, 84, 89, 90, 95, 92,$ $99, 96, 101, 102, 107, 104, 109, 110, 115, 112, 117, 118, 123, 120, 125, 126, 3, 0, 5, 6,$ $11, 8, 13, 14, 19, 16, 21, 22, 27, 24, 29, 30, 33, 34, 39, 36, 41, 42, 47, 44, 49, 50, 55, 52,$ $57, 58, 63, 60, 67, 64, 69, 70, 75, 72, 77, 78, 83, 80, 85, 86, 91, 88, 93, 94, 97, 98, 103, 100,$ $105, 106, 111, 108, 113, 114, 119, 116, 121, 122, 127, 124\}$	25	25/26

Table 25: Best known permutations $k = 128$ (continued)

Best known Permutations $k = 128$, $DR(\pi) = 13$	Imp.	Intg.
$\{3, 0, 5, 6, 11, 8, 13, 14, 19, 16, 21, 22, 27, 24, 29, 30, 33, 34, 39, 36, 41, 42, 47, 44, 49, 50, 55, 52, 57, 58, 63, 60, 67, 64, 69, 70, 75, 72, 77, 78, 83, 80, 85, 86, 91, 88, 93, 94, 97, 98, 103, 100, 105, 106, 111, 108, 113, 114, 119, 116, 121, 122, 127, 124, 1, 2, 7, 4, 9, 10, 15, 12, 17, 18, 23, 20, 25, 26, 31, 28, 35, 32, 37, 38, 43, 40, 45, 46, 51, 48, 53, 54, 59, 56, 61, 62, 65, 66, 71, 68, 73, 74, 79, 76, 81, 82, 87, 84, 89, 90, 95, 92, 99, 96, 101, 102, 107, 104, 109, 110, 115, 112, 117, 118, 123, 120, 125, 126\}$	25	25/26
$\{3, 0, 7, 4, 9, 10, 13, 14, 19, 16, 23, 20, 25, 26, 29, 30, 35, 32, 39, 36, 41, 42, 45, 46, 51, 48, 55, 52, 57, 58, 61, 62, 65, 66, 69, 70, 75, 72, 79, 76, 81, 82, 85, 86, 91, 88, 95, 92, 97, 98, 101, 102, 107, 104, 111, 108, 113, 114, 117, 118, 123, 120, 127, 124, 1, 2, 5, 6, 11, 8, 15, 12, 17, 18, 21, 22, 27, 24, 31, 28, 33, 34, 37, 38, 43, 40, 47, 44, 49, 50, 53, 54, 59, 56, 63, 60, 67, 64, 71, 68, 73, 74, 77, 78, 83, 80, 87, 84, 89, 90, 93, 94, 99, 96, 103, 100, 105, 106, 109, 110, 115, 112, 119, 116, 121, 122, 125, 126\}$	25	26/25
$\{3, 0, 5, 6, 9, 10, 15, 12, 19, 16, 21, 22, 25, 26, 31, 28, 35, 32, 37, 38, 41, 42, 47, 44, 51, 48, 53, 54, 57, 58, 63, 60, 67, 64, 69, 70, 73, 74, 79, 76, 83, 80, 85, 86, 89, 90, 95, 92, 99, 96, 101, 102, 105, 106, 111, 108, 115, 112, 117, 118, 121, 122, 127, 124, 1, 2, 7, 4, 11, 8, 13, 14, 17, 18, 23, 20, 27, 24, 29, 30, 33, 34, 39, 36, 43, 40, 45, 46, 49, 50, 55, 52, 59, 56, 61, 62, 65, 66, 71, 68, 75, 72, 77, 78, 81, 82, 87, 84, 91, 88, 93, 94, 97, 98, 103, 100, 107, 104, 109, 110, 113, 114, 119, 116, 123, 120, 125, 126\}$	25	26/25
$\{1, 2, 7, 4, 11, 8, 13, 14, 17, 18, 23, 20, 27, 24, 29, 30, 33, 34, 39, 36, 43, 40, 45, 46, 49, 50, 55, 52, 59, 56, 61, 62, 65, 66, 69, 70, 73, 74, 79, 76, 83, 80, 85, 86, 89, 90, 95, 92, 99, 96, 101, 102, 105, 106, 111, 108, 115, 112, 117, 118, 121, 122, 127, 124, 3, 0, 5, 6, 9, 10, 15, 12, 19, 16, 21, 22, 25, 26, 31, 28, 35, 32, 37, 38, 41, 42, 47, 44, 51, 48, 53, 54, 57, 58, 63, 60, 67, 64, 69, 70, 73, 74, 79, 76, 83, 80, 85, 86, 89, 90, 95, 92, 99, 96, 101, 102, 105, 106, 111, 108, 115, 112, 117, 118, 121, 122, 127, 124\}$	25	26/25
$\{1, 2, 5, 6, 11, 8, 15, 12, 17, 18, 21, 22, 27, 24, 31, 28, 33, 34, 37, 38, 43, 40, 47, 44, 49, 50, 53, 54, 59, 56, 63, 60, 67, 64, 71, 68, 73, 74, 77, 78, 83, 80, 87, 84, 89, 90, 93, 94, 99, 96, 103, 100, 105, 106, 109, 110, 115, 112, 119, 116, 121, 122, 125, 126, 3, 0, 7, 4, 9, 10, 13, 14, 19, 16, 23, 20, 25, 26, 29, 30, 35, 32, 39, 36, 41, 42, 45, 46, 51, 48, 55, 52, 57, 58, 61, 62, 65, 66, 69, 70, 75, 72, 79, 76, 81, 82, 85, 86, 91, 88, 95, 92, 97, 98, 101, 102, 107, 104, 111, 108, 113, 114, 117, 118, 123, 120, 127, 124\}$	25	26/25
$\{3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28, 33, 34, 37, 38, 43, 40, 47, 44, 51, 48, 55, 52, 57, 58, 61, 62, 67, 64, 71, 68, 73, 74, 77, 78, 81, 82, 85, 86, 91, 88, 95, 92, 97, 98, 101, 102, 107, 104, 111, 108, 115, 112, 119, 116, 121, 122, 125, 126, 1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30, 35, 32, 39, 36, 41, 42, 45, 46, 49, 50, 53, 54, 59, 56, 63, 60, 65, 66, 69, 70, 75, 72, 79, 76, 83, 80, 87, 84, 89, 90, 93, 94, 99, 96, 103, 100, 105, 106, 109, 110, 113, 114, 117, 118, 123, 120, 127, 124\}$	25	26
$\{1, 2, 5, 6, 11, 8, 15, 12, 19, 16, 23, 20, 25, 26, 29, 30, 35, 32, 39, 36, 41, 42, 45, 46, 49, 50, 53, 54, 59, 56, 63, 60, 65, 66, 69, 70, 75, 72, 79, 76, 83, 80, 87, 84, 89, 90, 93, 94, 99, 96, 103, 100, 105, 106, 109, 110, 113, 114, 117, 118, 123, 120, 127, 124, 3, 0, 7, 4, 9, 10, 13, 14, 17, 18, 21, 22, 27, 24, 31, 28, 33, 34, 37, 38, 43, 40, 47, 44, 51, 48, 55, 52, 57, 58, 61, 62, 67, 64, 71, 68, 73, 74, 77, 78, 81, 82, 85, 86, 91, 88, 95, 92, 97, 98, 101, 102, 107, 104, 111, 108, 115, 112, 119, 116, 121, 122, 125, 126\}$	25	26