Integral Resistance of Block Ciphers with Key Whitening by Modular Addition

Christof Beierle, Phil Hebborn, Gregor Leander, and Yevhen Perehuda

Faculty of Computer Science, Ruhr University Bochum, Bochum, Germany
firstname.lastname@rub.de

Abstract. Integral attacks exploit structural weaknesses in symmetric cryptographic primitives by analyzing how subsets of inputs propagate to produce outputs with specific algebraic properties. For the case of (XOR) key-alternating block ciphers using (independent) round keys, at ASIACRYPT'21, Hebborn et al. established the first non-trivial lower bounds on the number of rounds required for ensuring integral resistance in a quite general sense. For the case of adding keys by modular addition, no security arguments are known so far. Here, we present a unified framework for analyzing the integral resistance of primitives using (word-wise) modular addition for key whitening, allowing us to not only fill the gap for security arguments, but also to overcome the heavy computational cost inherent in the case of XOR-whitening.

Keywords: Block cipher, Integral attacks, ANF, Modular addition, Inverse cipher

1 Introduction

Symmetric cryptographic primitives play a foundational role in ensuring the confidentiality and integrity of digital communications. The security of these primitives is typically evaluated against well-established cryptanalytic techniques, such as differential [7] and linear attacks [31]. Besides these classical statistical attacks, there is also the important category of structural attacks, which includes *integral cryptanalysis* as the most prominent example. Integral attacks focus on analyzing how subsets of inputs propagate through a cipher to produce outputs with specific algebraic properties. Those properties can then be exploited to distinguish the cipher from a family of random permutations, making them a critical aspect of modern cryptanalysis.

Integral attacks, rooted in the study of high-order differentials, were introduced by Lai [30] and Knudsen [28], then extended by Knudsen and Wagner [29] with the "SQUARE attack". Classically, an integral distinguisher for a block cipher $(E_k \colon \mathbb{F}_2^n \to \mathbb{F}_2^n)_{k \in \mathbb{F}_2^\kappa}$ relies on identifying a subset $M \notin \{\emptyset, \mathbb{F}_2^n\}$ of plaintexts for which the sum of ciphertexts (or internal states if key-recovery rounds are added) $\sum_{x \in M} E_k(x)$ is independent of the secret key k, i.e., for which the map

$$\mathbb{F}_2^\kappa \to \mathbb{F}_2^n, k \mapsto \sum_{x \in M} E_k(x)$$

is constant.

The ability to argue against the existence of such subsets M, a property referred to as *integral resistance* is central to assessing security. A necessary condition for a cipher to be integral resistant is that the encrypted values over any set $M \notin \{\emptyset, \mathbb{F}_2^n\}$ must sum to a value that depends on the key. While arguments for security against classical statistical attacks have been developed over decades, integral attacks present unique difficulties. For many ciphers, integral resistance remains poorly understood, with most existing analyses covering only specific constructions or subsets M with certain properties (e.g., being a linear subspace of $\mathbb{F}_2^n$).

For key-alternating block ciphers, Hebborn et al. [24] provided the first security arguments against integral distinguishers in a more general sense under the assumption of independent round keys. Given a block cipher $(E_k \colon \mathbb{F}_2^n \to \mathbb{F}_2^n)_{k \in \mathbb{F}_2^\kappa}$, their definition of integral resistance was as follows:

For every subset $M \notin \{\emptyset, \mathbb{F}_2^n\}$ of $\mathbb{F}_2^n$ and every non-zero $\beta \in \mathbb{F}_2^n$, the Boolean function

$$\mathbb{F}_2^\kappa \to \mathbb{F}_2, k \mapsto \sum_{x \in M} \langle \beta, E_k(x) \rangle$$

is not constant.

That work established lower bounds on the number of rounds required to guarantee integral resistance in the above sense. Interestingly, when applied to ciphers from the literature, most of these lower bounds coincide with the best-known integral distinguishers, showing the tightness of previously-known cryptanalytic attacks. However, the above definition of integral resistance and the criteria established in [24] for ensuring the resistance necessitate further investigation and generalization, particularly to address limitations and additional scenarios.

Practical Limitations While conceptually nice, the key problem of the approach in [24] is its computational feasibility. In a nutshell, the method required the computation of n^2 monomials in the ANF of the component functions of E_k. While the advances of monomial prediction based on division trails have made the computation of those monomials feasible in many cases, this approach is still far from generic and requires ad-hoc, cipher-specific optimization to terminate in practice. Addressing this computational bottleneck is, therefore, crucial.

Modular Addition of Keys The use of modular addition to mix key material with the state appears throughout ARX-style designs – SPECK [3] and ChaCha [4] employ it in their round functions – and is also used for key whitening in block ciphers, for example, such as Threefish [20] and MARS [13].

Intuitively, and backed up by previous cryptanalytic results, modular addition of the keys enhances the resistance against integral attacks. One of the examples that explores ARX ciphers in the context of integral attacks is the work by Hu and Yap [26], in which monomial prediction is used to find integral distinguishers for ciphers using modular addition for key mixing.

However, when it comes to security arguments, the situation is fundamentally different: The method of [24] is inherently limited to whitening the keys by XOR and thus no formal arguments for the resistance of ciphers with modular key-additions are available to date.

Our Results

In our work, we develop the theory and the results necessary to give the missing security arguments for ciphers with key whitening by modular addition. Intriguingly, as we will see below, our theory also leverages the second drawback, i.e., computational feasibility, as the number of monomials to be considered is drastically reduced for modular addition.

As a second line of research, we investigate the power of chosen ciphertext attacks based on integral properties. That is, we study the integral resistance properties of block cipher inverses, exploring under what conditions the resistance of E implies the resistance of E^{-1}.

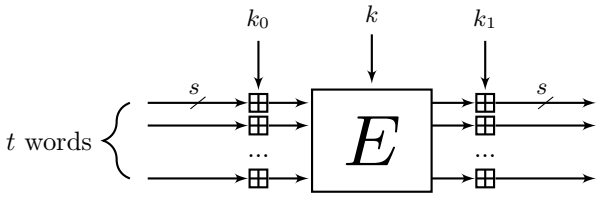
On a bit more technical level, we formulate a generalized notion of integral resistance as follows: A block cipher $E\colon \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n$ is called *d-th order integral resistant* if, for all sets $M_1, \ldots, M_n \subseteq \mathbb{F}_2^n$ with not all $M_i \in \{\emptyset, \mathbb{F}_2^n\}$, the Boolean function

$$\mathbb{F}_2^\kappa \ni k \mapsto \sum_{i=1}^{n} \sum_{x \in M_i} E^{(i)}(x, k)$$

is of algebraic degree at least d. Here $E^{(i)}$ denotes the i-th coordinate of E. As it was already developed in [24], proving (1-st order) integral resistance of E boils down to checking linear independence of a set of $n(2^n-1)+1$ polynomials in the key k, which is infeasible for block ciphers in practice. The main result in [24] was that this complexity can be reduced from $n(2^n-1)$ to only n^2 if we assume that E is an FX-construction.

The generalization to higher degree is, technically and practically, straightforward and for $d \geq 2$ in particular ensures that no linear equations about the key are leaked via integral distinguishers. Of course, also high-degree equations might be helpful for an attack, but an exact definition capturing those cases seems elusive with today's knowledge.

We generalize this result to the case of a t-MAFX (Modular Addition FX) construction depicted below, which adds independent pre- and post-whitening keys by word-wise modular addition, where we assume that n is split into t words, each of length s. Note that the case $s = 1$ coincides with the known case for XORing the key.



The essence of our main result is that for a t-MAFX construction, the above-mentioned complexity is reduced to only t^2. Moreover, we are able to handle the integral resistance of the inverse block cipher as well.

Theorem 1. *Let $E : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n$ be a block cipher with its i-th coordinate $E^{(i)}$ (for $1 \leq i \leq n$) expressed by its algebraic normal form*

$$E^{(i)}(x,k) = \sum_{u \in \mathbb{F}_2^n} p_u^{(i)}(k) x^u,$$

*where each $p_u^{(i)}(k)$ is an ANF polynomial in k. Let $\widetilde{E} : \mathbb{F}_2^n \times \mathbb{F}_2^{\kappa+2n} \to \mathbb{F}_2^n$ be a t-*MAFX *block cipher defined by*

$$(x, k, k_0, k_1) \mapsto E_k(x \boxplus_t k_0) \boxplus_t k_1$$

where $k_0, k_1 \in \mathbb{F}_2^n$.

There is a subset S of t^2 polynomials in $\{p_u^{(i)}(k) \mid u \in \mathbb{F}_2^n, 1 \leq i \leq n\}$ with the following property: If every non-trivial linear combination of S has degree in k at least d, then both $\widetilde{E}$ and its inverse cipher $\widetilde{E}^{-1}$ are d-th order integral resistant.

More precisely, this set S is given as

$$S \coloneqq \{p_{u_{is+1}}^{(js+1)}(k) \mid i, j \in \{0, \ldots, t-1\}\},$$

where u_i is set to the bitwise complement of the i-th unit vector.

In a similar manner as in [24] with the concept of an integral-resistance matrix, we can verify this sufficient condition for d-th order integral resistance. More precisely, let the polynomials $p_u^{(i)}(k)$ be given by

$$p_u^{(i)}(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_{u,v}^{(i)} k^v, \quad \lambda_{u,v}^{(i)} \in \mathbb{F}_2.$$

A *d-th order integral-resistance matrix* for E is defined as

$$\begin{pmatrix} \lambda_{u_1,v_1}^{(1)} & \lambda_{u_1,v_1}^{(s+1)} & \lambda_{u_1,v_1}^{(2s+1)} & \cdots & \lambda_{u_1,v_1}^{((t-1)s+1)} & \lambda_{u_{s+1},v_1}^{(1)} & \lambda_{u_{s+1},v_1}^{(s+1)} & \cdots & \lambda_{u_{(t-1)s+1},v_1}^{((t-1)s+1)} \\ \lambda_{u_1,v_2}^{(1)} & \lambda_{u_1,v_2}^{(s+1)} & \lambda_{u_1,v_2}^{(2s+1)} & \cdots & \lambda_{u_1,v_2}^{((t-1)s+1)} & \lambda_{u_{s+1},v_2}^{(1)} & \lambda_{u_{s+1},v_2}^{(s+1)} & \cdots & \lambda_{u_{(t-1)s+1},v_2}^{((t-1)s+1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & & \vdots \\ \lambda_{u_1,v_p}^{(1)} & \lambda_{u_1,v_p}^{(s+1)} & \lambda_{u_1,v_p}^{(2s+1)} & \cdots & \lambda_{u_1,v_p}^{((t-1)s+1)} & \lambda_{u_{s+1},v_p}^{(1)} & \lambda_{u_{s+1},v_p}^{(s+1)} & \cdots & \lambda_{u_{(t-1)s+1},v_p}^{((t-1)s+1)} \end{pmatrix},$$

where $v_1, \ldots, v_p$ are $p \geq t^2$ elements from $\mathbb{F}_2^\kappa$ of Hamming weight at least d. We get the following corollary.

Corollary 1. *Using the same definitions as in Theorem 1, if there exists a d-th order integral resistance matrix for E of full rank, then both $\widetilde{E}$ and $\widetilde{E}^{-1}$ are d-th order integral resistant.*

Note that the coefficients $\lambda_{u,v}^{(i)}$ are given as the parity of the number of division trails with input pattern u and key pattern v for the i-th output bit. In the case where E is a key-alternating cipher with independent round keys, those can be efficiently computed using mixed-integer linear programming [24] [26]. It is worth highlighting that, in the special case of $t = 1$, i.e., key whitening by a (single-word) modular addition, it is enough to find only a single $v \in \mathbb{F}_2^\kappa$ of Hamming weight at least d such that $\lambda_{u_1,v}^{(1)} = 1$.

Finally, we applied the developed theory to check the bounds on the minimal number of required rounds to prove the integral resistance property of at least 1^{st} order. Specifically, we analyzed well-known ciphers such as `GIFT-64`, `SKINNY-64`, and `PRESENT` in a t-MAFX construction with the assumption of independent and full round key XORing. We showed improved bounds on the number of rounds required to achieve integral resistance compared with bounds in [24], namely from 12-13 rounds to 9-11 rounds. Particularly, some of the new bounds are below the number of rounds that are exploited by the best-known distinguishers on the ciphers. Moreover, we proved in each case at least $18^{\texttt{th}}$ order integral resistance, depending on the cipher. In some cases, the number of rounds coincides with the upper bounds on the algebraic degree [23], demonstrating the tightness of our results. The computational efficiency of the approach is also highlighted, with every result obtained in under 40 minutes, making it a practical tool.

Cipher	Best-known integral distinguisher	IR property in [24] ($t = n$)	IR property for t-word-wise whitening ($t = 1$)	IR property for t-word-wise whitening ($t = 2$)
`GIFT-64`	10 [2]	12	9	10
`PRESENT`	9 [36]	13	10	10
`SKINNY-64`	12 [15]	13	11	11

Note: IR stands for Integral Resistance. The numbers give the number of rounds needed for proving IR. The ciphers assume full and independent round key additions. Note that, as mentioned in [24], the 11-round distinguisher for `SKINNY-64` [15] can be extended to 12 rounds for free due to the absence of a pre-whitening key.

1.1 Related Work

After the foundational works on high-order differentials [30] and the "SQUARE attack" [29], an important research direction became the investigation of the connection between the integral attack and the algebraic degree of a cipher. One of the main results in this area was provided by Boura et al. [9] [11], where the authors established bounds on the algebraic degree of a composition of functions. Hebborn et al. [23] investigated lower bounds on the algebraic degree for various block ciphers, including `PRESENT` and `GIFT-64`. Additionally, the work investigated lower bounds on the minimum algebraic degree and the number of rounds required for every output bit's ANF to include all monomials of maximal degree $n - 1$, as such a property rules out many types of integral distinguishers.

A major breakthrough in integral cryptanalysis came with Todo's work on the *Conventional Division Property* [32]. This technique studies how properties of subsets of messages propagate through different cipher operations. Instead of relying solely on algebraic degree arguments, the division property tracks the change of message structures.

The division property framework was later extended in various ways. For example, Todo et al. introduced the *Bit-based Division Property* and *3-subset Division Property* in 2016 [34] by analyzing bitwise propagation rather than whole-word structures. Hao et al. further refined these techniques by proposing the *3-subset Division Property without Unknown Subset* [22].

Boura et al. [10] provided an alternative perspective on the division property by the theory of *Parity Sets*. Meanwhile, Hu et al. [25] introduced *Monomial Prediction*, an approach that determines integral distinguishers by predicting the appearance of monomials in the polynomial representation of the cipher.

As integral attacks became more sophisticated, researchers began exploring methods for automatizing the search for distinguishers. Hadipour et al. [21] developed a framework for an automated search for identifying integral properties in block ciphers, leveraging constraint-programming techniques. More recently, Beyne et al. [5] introduced the concept of *Algebraic Transition Matrices* and its generalization, *Ultrametric Integral Cryptanalysis* [6]. This latter approach lifts the theory of integral attacks to a field of characteristic zero and is able to describe more general divisibility properties than just divisibility by 2 (as it is used in classical integral cryptanalysis).

Another important branch of research focuses on optimizing key-recovery attacks based on integral distinguishers. Notably, Ferguson et al. [19] used *Partial Sums*, which exploits integral properties to simplify key extraction. In particular, they decreased the complexity of an integral attack on 6-round AES from naive 2^{72} encryptions to 2^{52} S-box lookups. Later, Todo [33] introduced *FFT-based Key-Recovery*. These approaches were further refined by Dunkelman et al. [17], who combined the above-mentioned strategies to improve attack efficiency in many times.

Outline The paper is structured as follows: Section 2 provides the necessary preliminaries, introducing key definitions and notations related to (vectorial) Boolean functions, algebraic normal forms, and word-wise modular addition. Section 3 refines and generalizes the integral resistance criteria established in prior work, addressing limitations in previous definitions. Section 4 analyzes word-wise modular key pre- and post-whitening, demonstrating its strong impact on integral resistance and bridging the gap between full-state modular addition and traditional XOR-key whitening. Section 5 investigates the integral resistance properties of block cipher inverses, exploring under what conditions the resistance of E implies the resistance of E^{-1}.

2 Preliminaries

We provide the basic concepts and notations required to establish the results discussed in this work. These include definitions related to vectorial Boolean functions, their algebraic normal form (ANF), and the necessary theoretical framework for word-wise modular addition.

2.1 Notations on (Vectorial) Boolean Functions

For a positive integer n, we denote by $\mathbb{F}_2$ the finite field with two elements and by $\mathbb{F}_2^n$ the n-dimensional $\mathbb{F}_2$-vector space.

We follow the convention that the *least significant bit* (LSB) of a binary string corresponds to the left-most bit, and indexing starts from 1, meaning that for an n-bit binary vector $x = (x_1, x_2, \ldots, x_n)$, we consider x_1 as the LSB.

A *unit vector* (or *basis vector*) in $\mathbb{F}_2^n$ is a vector e_i where all coordinates are zero except at the i-th position. At the i-th position, its value takes one. We denote by $\mathbf{1}$ the all-one vector $(1, \ldots, 1)$ in $\mathbb{F}_2^n$ and by $\mathbf{0}$ the all-zero vector $(0, \ldots, 0)$ in $\mathbb{F}_2^n$.

A *Boolean function* is a mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Any Boolean function $f(x)$ can be uniquely described by its *algebraic normal form* (ANF) via

$$f(x) = \sum_{u \in \mathbb{F}_2^n} \lambda_u x^u,$$

where input pattern u defines the monomial $x^u \coloneqq \prod_{i=1}^n x_i^{u_i}$ and $\lambda_u \in \mathbb{F}_2$ is the corresponding coefficient. The *algebraic degree* of non-zero f is the maximum degree of the monomials in its ANF, i.e., the maximal Hamming weight of u for which $\lambda_u = 1$.

A *keyed Boolean function* is a Boolean function that depends not only on the input vector $x \in \mathbb{F}_2^n$ but also on a key vector $k \in \mathbb{F}_2^\kappa$, defined by its ANF

$$f_k(x) \coloneqq f(x, k) = \sum_{v \in \mathbb{F}_2^\kappa, u \in \mathbb{F}_2^n} \lambda_{u,v} k^v x^u = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

where $k \in \mathbb{F}_2^\kappa$ is the κ-bit key with corresponding *key-pattern* v (selection of key bits that determine k^v monomial) and $p_u(k) \coloneqq \sum_{v \in \mathbb{F}_2^\kappa} \lambda_{u,v} k^v$ is a polynomial in the key k.

A *vectorial Boolean function* is a mapping $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, where n and m represent the number of input and output bits, respectively. A vectorial Boolean function can be expressed as

$$F(x) = \big(F^{(1)}(x), F^{(2)}(x), \ldots, F^{(m)}(x)\big),$$

where each Boolean function $F^{(i)} : \mathbb{F}_2^n \to \mathbb{F}_2$ is referred to as a *coordinate function* of F. The notion of a *keyed vectorial Boolean function* is analogous.

A Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is said to be *balanced* if for each element $y \in \mathbb{F}_2^m$ there are exactly 2^{n-m} preimages under F.

Any (keyed) vectorial Boolean function F, resp., F_k can be represented in a similar way as the Boolean function with the help of its ANF,

$$F_k(x) = F(x,k) = \sum_{v\in\mathbb{F}_2^\kappa, u\in\mathbb{F}_2^n} \lambda_{u,v} k^v x^u = \sum_{u\in\mathbb{F}_2^n} p_u(k) x^u,$$

with the only difference that $\lambda_{u,v}$ is now an element in $\mathbb{F}_2^m$ and $p_u(k)$ expresses an m-dimensional vector of polynomials. The *algebraic degree* of $F(x)$ is the maximum algebraic degree among all its coordinate functions.

Any non-trivial linear combination of the coordinate functions of a (keyed) vectorial Boolean function F, expressed as

$$\langle \beta, F(x)\rangle \coloneqq \beta_1 F^{(1)}(x) + \beta_2 F^{(2)}(x) + \cdots + \beta_m F^{(m)}(x),$$

where $\beta \in \mathbb{F}_2^m \setminus \{0\}$, is called a *component function* of F.

We define a *block cipher* as keyed vectorial Boolean function $E : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^m$ such that each $E_k \colon x \mapsto E(x,k)$ is balanced. We emphasize that we focus on the most relevant special case of $m = n$, in which the condition of balancedness of E_k is equivalent to E_k being a permutation. In that case, the *inverse* of E is defined by $E^{-1} \colon (x,k) \mapsto E_k^{-1}(x)$.

2.2 Notations on Word-Wise Ordering and Modular Addition

Let x and $y \in \mathbb{F}_2^n$ be partitioned into t equally-sized words, each of dimension $s = n/t$, such that

$$x = \left(x^{(1)}, x^{(2)}, \ldots, x^{(t)}\right) \quad \text{and} \quad y = \left(y^{(1)}, y^{(2)}, \ldots, y^{(t)}\right)$$

with $x^{(j)} = \left(x_1^{(j)}, x_2^{(j)}, \ldots, x_s^{(j)}\right)$ and $y^{(j)} = \left(y_1^{(j)}, y_2^{(j)}, \ldots, y_s^{(j)}\right)$ for $1 \le j \le t$. For each word, the left-most bit corresponds to the LSB and the right-most bit corresponds to the MSB.

We also introduce the ϕ-weight, which provides a flexible framework for assigning weights to vectors based on partitioning the vector into t distinct words. This approach bridges the gap between the *Hamming weight*, which counts the number of non-zero coordinates in a vector, and the *integer weight*, which interprets the vector as a binary representation of an integer and assigns its weight based on its numerical value modulo 2^n.

Firstly, we specify the auxiliary term $\phi_s(x)$, which gives the weight of one particular word. Let be $\phi_s \colon \mathbb{F}_2^s \to \mathbb{Z}$ be the canonical integer representation mapping on vector $x \in \mathbb{F}_2^s$, such that

$$\phi_s(x) = \sum_{i=1}^{s} 2^{i-1} x_i.$$

The *ϕ-weight* of x, denoted $\phi_{t,s}(x)$, is defined as the sum of the weights of each word. Let be $\phi_{t,s} \colon \mathbb{F}_2^{s\times t} \to \mathbb{Z}$ be the mapping on vector $x \in \mathbb{F}_2^n$, such that

$$\phi_{t,s}(x) = \sum_{j=1}^{t} \phi_s(x^{(j)}),$$

where $\phi_s(x^{(j)})$ is the weight assigned to the j-th word.

Again, when $t = n$, the ϕ-weight coincides with the Hamming weight, effectively counting the number of bits set to 1, when $t = 1$ - with the standard integer ordering - the ϕ-weight corresponds to the numerical value between 0 and $2^n - 1$ when interpreting the entire vector as a single binary number.

To illustrate the concept of ϕ-weight, consider the following examples with specific values of n and t:

Example 1. Let $x = (x_1, x_2, x_3, x_4) = (1, 0, 1, 1) \in \mathbb{F}_2^4$ be partitioned into $t = 2$ words, each of dimension $s = n/t = 2$:

$$x = (x^{(1)}, x^{(2)}) = ((x_1, x_2), (x_3, x_4)).$$

Assuming the weight of each word is its integer value modulo 2^s:

$$\begin{aligned}\phi_{2,2}(x) = \phi_2(x^{(1)}) + \phi_2(x^{(2)}) &= (2x_2 + x_1) + (2x_4 + x_3) \\ &= (2 \cdot 0 + 1) + (2 \cdot 1 + 1) = 1 + 3 = 4.\end{aligned}$$

Now, we introduce a partial order for t-partitioned vectors.

Definition 1. *We define the partial order $\preceq_t$ on $\mathbb{F}_2^n$ by*

$$x \preceq_t y \iff \forall j \in \{1, 2, \ldots, t\},\ \phi_s(x^{(j)}) \leq \phi_s(y^{(j)}).$$

An important property of ϕ-weight is its inherent compatibility with the partial order $\preceq_t$. Specifically, if $x \preceq_t y$, then $\phi_{t,s}(x) \leq \phi_{t,s}(y)$. Note that for the case $t = 1$ we write $\leq$ instead of $\leq_1$. If $x \preceq_t y$, we may also write $y \succeq_t x$.

Example 2. It holds that for different values of t:

1. $(0, 0, 1, 1) \leq (1, 0, 1, 1)$
2. $(0, 0, 1, 0) \geq (1, 0, 0, 0)$
3. $((0, 0), (1, 0)) \not\preceq_2 ((1, 0), (0, 0))$
4. $((1, 0), (0, 1)) \succeq_2 ((1, 0), (1, 0))$
5. $((1), (0), (1), (1)) \succeq_4 ((1), (0), (1), (0))$
6. $((1), (0), (0), (1)) \not\preceq_4 ((1), (0), (1), (0))$

Note, when $t = n$, the partial order $\preceq_t$ coincides with the standard componentwise partial order (also known as the predecessor partial order $\preceq$). Conversely, when $t = 1$, then $\preceq_t$ corresponds to the integer (total) ordering $\leq$.

The binary operation $\boxplus_t$ denotes the word-wise modular addition of two vectors x and y in $\mathbb{F}_2^n$. Specifically, each corresponding pair of words from x and y is added modulo 2^s.

Formally,

$$x \boxplus_t y = \left(x^{(1)} \boxplus y^{(1)}, x^{(2)} \boxplus y^{(2)}, \ldots, x^{(t)} \boxplus y^{(t)}\right),$$

where for each $j = 1, 2, \ldots, t$,

$$\phi_s\left(x^{(j)} \boxplus y^{(j)}\right) \equiv \phi_s(x^{(j)}) + \phi_s(y^{(j)}) \bmod 2^s.$$

With this definition, $(\mathbb{F}_2^n, \boxplus_t)$ is an abelian group with neutral element $\mathbf{0}$. We denote the inverse operation by $\boxminus_t$.

The case when $t = n$, each word consists of a single bit ($s = 1$). In this case, the operation $\boxplus_t$ reduces to the bitwise XOR operation since addition modulo 2 is equivalent to XOR. On the other hand, if $t = 1$, the entire vector is treated as a single word of dimension $s = n$. Here, $\boxplus_t$ corresponds to the standard integer addition modulo 2^n, or $\boxplus$.

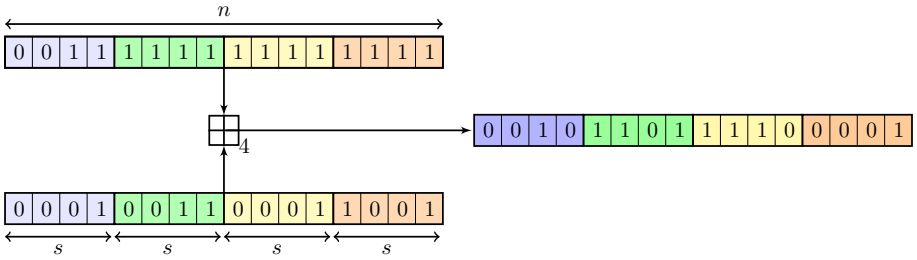


Fig. 1. Example of word-wise modular addition for $t = 4$ and $n = 16$.

Remark 1. Note that our approach can be naturally extended to cases where the partitioning is not restricted to equally-sized words, but instead allows for arbitrary word lengths. All ideas presented here seamlessly adapt to this more general setting. However, for the sake of clarity, we assume throughout our analysis that the full state is partitioned into equally-sized words.

3 On the Definition of Integral Resistance

We recall the formal definition of integral resistance by Hebborn et al. in [24].

Definition 2 (Integral Resistance Property [24]). *Let $E\colon \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^m$ be a block cipher. We say that E is* integral resistant *if, for all sets $M \subseteq \mathbb{F}_2^n$ with $M \notin \{\emptyset, \mathbb{F}_2^n\}$ and all non-zero $\beta \in \mathbb{F}_2^m$, the Boolean function*

$$\mathbb{F}_2^\kappa \to \mathbb{F}_2, k \mapsto \sum_{x \in M} \langle \beta, E(x,k) \rangle$$

is not constant.

In their work, the authors provided security arguments for the integral resistance of a block cipher using XOR pre-whitening and the assumption of independent round keys.

To provide an intuition for how those security arguments work, let us first consider the case of a block cipher with only one output bit, i.e., $f\colon \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2$, and $\beta = 1$. The goal is to prevent the existence of a subset $M \subseteq \mathbb{F}_2^n$ with $M \notin \{\emptyset, \mathbb{F}_2^n\}$ such that

$$\sum_{x \in M} f_k(x) \tag{1}$$

is constant, independently of k.

For a subset $M \subseteq \mathbb{F}_2^n$, we denote its *parity set* [10] by

$$\mathcal{U}(M) := \left\{ u \in \mathbb{F}_2^n \mid \sum_{x \in M} x^u = 1 \right\}.$$

A crucial property used in the following is the fact that there is a one-to-one correspondence between subsets M of $\mathbb{F}_2^n$ and parity sets.

Lemma 1 (Identification of Subsets by Parity Sets [10]). *The mapping $\mathcal{U}\colon M \mapsto \mathcal{U}(M)$ is a bijection on the set of all subsets of $\mathbb{F}_2^n$. We further have*

$$\mathcal{U}(\emptyset) = \emptyset \quad \textit{and} \quad \mathcal{U}(\mathbb{F}_2^n) = \{\mathbf{1}\}.$$

Expressing $f_k(x)$ in its algebraic normal form, we can rewrite (1) as

$$\sum_{x \in M} f_k(x) = \sum_{x \in M} \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u = \sum_{u \in \mathbb{F}_2^n} p_u(k) \sum_{x \in M} x^u = \sum_{u \in \mathcal{U}(M)} p_u(k).$$

Then, following from Lemma 1, the function $k \mapsto \sum_{x \in M} f_k(x)$ is non-constant for all $M \subseteq \mathbb{F}_2^n$ with $M \notin \{\emptyset, \mathbb{F}_2^n\}$ if and only if the polynomial $\sum_{u \in M} p_u(k)$ is non-constant for all non-empty sets $M \subseteq \mathbb{F}_2^n$ with $M \neq \{\mathbf{1}\}$. Because of the fact that $p_{(1,\ldots,1)}(k) = 0$ (because f_k is balanced for all k), this latter statement is equivalent to the statement that every non-trivial linear combination of the set of polynomials $\{p_u(k) \mid u \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}\}$ is non-constant, i.e., has degree at least 1 in the key.

Remark 2. In [24], the authors were missing to include this requirement on the degree in the above characterization of linear independence of polynomials. Indeed, including the bound is necessary for ensuring integral resistance. For example, consider the scenario where $p_{110}(k) = k_1$ and $p_{101}(k) = k_1 + 1$. These are linearly independent, but their sum results in a constant value. The most notable example of exploiting this property is an attack on 12-round SIMON32 [34] using $\mathbb{L}$ set (set of u's s.t. $\sum_{x \in M} x^u = 1$ for defined M) in 3SDP leading to the existence of an integral distinguisher $\sum_{x \in \mathcal{U}(M)} \langle \beta, E(x,k) \rangle = 1$.

It is important to note that, although the incomplete criterion in [24], in their experiments, the authors generated only non-zero key patterns v, i.e., the Hamming weight of v is at least 1. Hence, their bounds on the number of rounds for integral resistance remain valid. This is because they evaluated polynomials only for these key patterns, meaning that if the polynomials are linearly independent in the general sense (without considering bounds on the degree), then the obtained bound corresponds to the minimal weight of key patterns.

So, for the general case of a block cipher E, we can ensure integral resistance if every non-trivial linear combination of the set

$$\bigcup_{i=1}^{n} \{p_u^{(i)}(k) \mid u \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}\} \tag{2}$$

has degree at least 1 in k, where $p_u^{(i)}$ denotes the i-th coordinate of the vector of polynomials p_u.

Remark 3. Ensuring that every non-trivial linear combination of the set in (2) is not constant is actually equivalent to a much stronger property than integral resistance in the sense of Definition 2. Namely, the latter assumes that just a fixed subset of plaintexts M is used when applying a non-zero mask β on the output of the cipher. More generally, each output bit can have its own subset of the input subset. The above-mentioned condition gives more "flexibility", the actual integral resistance outcome is the following statement: for all sets $M_1, \ldots, M_m \subseteq \mathbb{F}_2^n$ with not all of them in $\{\emptyset, \mathbb{F}_2^n\}$, the Boolean function

$$\mathbb{F}_2^\kappa \to \mathbb{F}_2, k \mapsto \sum_{i=1}^{m} \sum_{x \in M_i} E^{(i)}(x, k)$$

is non-constant (or is of algebraic degree at least d, if we use the more general notion, defined below). Note that this notion already covers attacks with a sum over different subsets. Here, we refer, for example, to some of the integral distinguishers on 9-round PRESENT listed in [5]:

$$\sum_{x_{10}=0} E^{(17)}(x) + \sum_{x_{11}=0} E^{(49)}(x) \quad \text{is constant.}$$

Notably, for each $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the number of polynomials $p_u^{(i)}(k)$ grows exponentially with n. Specifically, for each $i \in \{1, \ldots, m\}$, there are $2^n - 1$ such polynomials (since $u \in \mathbb{F}_2^n$ and for a block cipher, we have $p_{(1,\ldots,1)} = 0$), resulting in a total of $m(2^n - 1)$ polynomials. Clearly, this makes direct computation infeasible. This is where the key insight from [24]—Theorem 2 and Corollary 2—becomes crucial. Here, we will state a corrected version of Theorem 2.

Proposition 1 (Theorem 2 in [24]). *Let $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$ be a balanced Boolean function with ANF*

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

and consider a version of f_k with an additional pre-whitening key k_0, i.e.

$$\tilde{f}_{k,k_0}(x) := f_k(x + k_0) = \sum_{v \in \mathbb{F}_2^n} q_v(k, k_0)\, x^v.$$

If any non-trivial linear combination of polynomials $p_u(k)$ for u of Hamming weight $n-1$ is non-constant, then any non-trivial linear combination of polynomials

$$\{q_v(k, k_0) \mid v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}\}$$

is non-constant.

Let us analyze the case of a block cipher E with $m = n$. There are n such monomials for one coordinate function whose input patterns u are of Hamming weight $n-1$ (and n^2 for a permutation $E_k(x)$ as there are n coordinates). Proving that any non-trivial linear combination of just these polynomials p_u's is not constant is enough to guarantee that the block cipher with a whitening key, defined by $E_k(x + k_0)$, achieves integral resistance. In simple words, the linear independence of degree $d = 1$ can be propagated from high-order terms to the full space of monomials in case of using a *pre-whitening key*.

Consequently, the complexity is reduced, involving the computation of values of $p_u(k)$ for n^2 values of the key of Hamming weight at least 1 (i.e., n^2 number of key-patterns v) and proving their linear independence. This technique allowed a robust approach to find the required number of rounds for different ciphers like `SKINNY-64` or `GIFT-64` [24] to ensure resistance against any integral distinguishers.

For that, an integral-resistance matrix $\mathcal{I}(E)$ for the block cipher E is constructed by finding the coefficients $\lambda_{u,v}^{(i)}$ in the algebraic normal form of the cipher, for n input patterns u (of Hamming weight $n-1$), for n output coordinates (i) and $p \geq n^2$ key patterns v (of Hamming weight ≥ 1). Its full rank ensures that every non-trivial linear combination of $p_u(k)$ for u of Hamming weight $n-1$ is non-constant, assuring integral resistance after pre-whitening the cipher.

$$\mathcal{I}(E) = \begin{pmatrix} \lambda_{u_1,v_1}^{(1)} & \lambda_{u_1,v_1}^{(2)} & \cdots & \lambda_{u_1,v_1}^{(n)} & \lambda_{u_2,v_1}^{(1)} & \lambda_{u_2,v_1}^{(2)} & \cdots & \lambda_{u_n,v_1}^{(n)} \\ \lambda_{u_1,v_2}^{(1)} & \lambda_{u_1,v_2}^{(2)} & \cdots & \lambda_{u_1,v_2}^{(n)} & \lambda_{u_2,v_2}^{(1)} & \lambda_{u_2,v_2}^{(2)} & \cdots & \lambda_{u_n,v_2}^{(n)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_{u_1,v_p}^{(1)} & \lambda_{u_1,v_p}^{(2)} & \cdots & \lambda_{u_1,v_p}^{(n)} & \lambda_{u_2,v_p}^{(1)} & \lambda_{u_2,v_p}^{(2)} & \cdots & \lambda_{u_n,v_p}^{(n)} \end{pmatrix}.$$

3.1 A Refinement of the Notion of Integral Resistance

We will refine the notion of integral resistance. Let

$$p_M(k) \coloneqq \sum_{u \in \mathcal{U}(M)} p_u(k),$$

where $p_M(k)$ represents the resulting polynomial in k. Having that $\sum_{x \in M} f_k(x)$ is not constant in k is equivalent to having $\deg_k(p_M(k)) \geq 1$, where $\deg_k(p(k))$ denotes the degree of the polynomial $p(k)$ in k (i.e., the highest degree of any monomial in k that appears with a nonzero coefficient). In other words, $p_M(k)$ must not be a constant polynomial.

For simplicity, we introduce a new concept: *d-independence* of polynomials over $\mathbb{F}_2$. This definition ensures that any non-trivial linear combination of the polynomials in $S = \{p_1(k), p_2(k), \ldots, p_m(k)\}$ retains a degree of at least d.

Definition 3 (d-independence). *Let S be a set of polynomials over $\mathbb{F}_2$. S is called* d-independent *if any non-trivial linear combination of S is a polynomial of degree at least d.*

For integral resistance with respect to the Definition 2, 1-independence is sufficient to ensure that $p_M(k)$ is not constant as a resulting polynomial of a sum of values over any non-empty set $M \subseteq \mathbb{F}_2^n, M \neq \mathbb{F}_2^n$.

Nevertheless, in the light of Remarks 2 and 3, it requires a new more precise definition of integral resistance.

Definition 4 (d-th order Generalized Integral Resistance Property). *Let $E\colon \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^m$ be a block cipher and $d \geq 1$. We say that E is* d-th order integral resistant *if, for all sets $M_1, \ldots, M_m \subseteq \mathbb{F}_2^n$ with not all $M_i \in \{\emptyset, \mathbb{F}_2^n\}$, the Boolean function*

$$\mathbb{F}_2^\kappa \to \mathbb{F}_2, k \mapsto \sum_{i=1}^{m} \sum_{x \in M_i} E^{(i)}(x, k)$$

is of algebraic degree at least d.

In other words, it states that for proving d-th order integral resistance, it is necessary to choose key patterns v for matrix $\mathcal{I}(E)$ only of Hamming weight at least d, similarly to what we briefly discussed in Remark 2.

Intuitively, the higher the order d, the stronger the resistance against integral attacks. However, there are some exceptions to this intuition. Let us define $p_{M_1,\ldots,M_m}(k) \coloneqq \sum_{i=1}^{m} \sum_{u \in \mathcal{U}(M_i)} p_u^{(i)}(k)$. While it may seem reasonable to assume that increasing the degree of $p_{M_1,\ldots,M_m}(k)$ inherently strengthens security, the relationship is more nuanced.

For example, 1st order integral resistance could still imply that the attacker knows a resulting polynomial $p_{M_1,\ldots,M_m}(k)$ of degree 1 for some subsets $M_1, \ldots, M_m$ of $\mathbb{F}_2^n$. Then this is equivalent to revealing one bit of the key. A similar property is exploited by the original cube attack described by Dinur and Shamir [16]. This follows from the fact that solving linear equations over $\mathbb{F}_2$ is trivial. Thus ensuring, for example, that $d \geq 2$ could address such direct key leakage. This is because the analysis of polynomials from degree 2 onwards becomes significantly more complex.

On the other hand, consider the extreme case where some $p_{M_1,\ldots,M_m}(k)$ achieves its maximal degree and $p_{M_1,\ldots,M_m}(k) = k_1 k_2 \cdots k_\kappa$. In this scenario, there is only one key assignment that doesn't satisfy $p_{M_1,\ldots,M_m}(k) = 0$, namely $k_1 = k_2 = k_3 = \cdots = k_m = 1$. Consequently, the integral property holds for almost the entire key space and always evaluates to zero, except for the special case of the "all-one" key. This means that although the resulting polynomial has a high degree, it does not necessarily provide stronger security, as the integral property becomes trivially true for most keys, making the cipher highly predictable in this setting.

So, analyzing the polynomial $p_{M_1,\ldots,M_m}(k)$ provides a way to investigate the existence of weak keys for integral attacks, i.e., keys for which $p_{M_1,\ldots,M_m}(k) = 0$ or $p_{M_1,\ldots,M_m}(k) = 1$. Still, in general, the case analysis becomes significantly more complex for $\deg_k(p_{M_1,\ldots,M_m}(k)) \geq 2$ as already mentioned. Nonetheless, in certain corner cases, we may still be able to derive insights about the size of the kernel $\ker(p_{M_1,\ldots,M_m}(k))$, which represents the set of keys that nullify $p_{M_1,\ldots,M_m}(k)$.

3.2 Does Integral Resistance Exist in Reality?

Let us assume some cipher has a known linear or differential distinguisher, but on only a reduced-round variant and with complexity 2^{n-1}. Does it mean that the full version has no such attack? Of course, no. There still can exist distinguishers. However, we still cannot find them.

In the same manner, things work for integral cryptanalysis. Let us give an example. For simplicity, let us consider an integral attack on one fixed coordinate function $f_k(x)$ and let us assume that the key space and message space are both $\mathbb{F}_2^n$. There are 2^{2^n} subsets M of $\mathbb{F}_2^n$, so we assume to get 2^{2^n} Boolean polynomials in the key of the form $\sum_{x\in M} f_k(x) = p_{\mathcal{U}(M)}(k)$. However, the number of possible unique polynomials is also 2^{2^n}. So, the probability that there will be two subsets M_1 and M_2 of the message space with $\sum_{x\in M_1} f_k(x) = \sum_{x\in M_2} f_k(x) = p(k)$ is almost 1. Hence, if we take the sum of encrypted values over the symmetric difference of M_1 and M_2, i.e., $\sum_{x\in M_1 \Delta M_2} f_k(x)$, where Δ is the symmetric difference, it will be equal to zero (for any key).

For an n-to-n bit block cipher, taking into account that the attacker can use a more sophisticated type of integral attack, for example, exploiting a linear combination of the output bits or different subsets of plaintexts for each output bit, as we discussed in Remark 3, by the pigeonhole principle, the probability of such collision becomes 1. For each $M_1, \ldots, M_n \subseteq \mathbb{F}_2^n$ there are 2^{2^n} possible choices resulting in 2^{n2^n} possible configurations. Then, to at least have a chance that there is no integral attack, this number should be not less than the number of possible resulting polynomials in the key, i.e., 2^{2^κ}. Thus, if the key size κ is below the threshold $n + \log_2 n$, then integral attacks, in the way defined earlier, are certain to exist. Thus, integral distinguishers become almost inevitable unless the key size significantly exceeds $n + \log_2 n$.

It is important to stress that the bounds on the number of rounds for ensuring integral resistance ([24]) use the assumption of independent rounds key and consequently blow up the key space to $\mathbb{F}_2^{rn}$. Therefore, such a collision can be expected to appear with a much smaller probability for such cases. It is important to mention that, in general, the connection between independent keys and the use of an actual key schedule could be an interesting question for future research.

4 Modular Key Addition

Our approach of analyzing the effect of modular key addition for pre- and post-whitening is rooted in Theorem 1 from [12], which states that for a monomial

function $f(x) = x^u$, we have

$$f(x \boxplus k_0) = (x \boxplus k_0)^u = \sum_{v \leq u} k_0^{u \boxminus v} x^v.$$

To illustrate the contrasting effects of XORing the key and performing addition modulo 2^n, we present a simple example of their impact on the function $x^{101} = x^5$.

Example 3.

$$\begin{aligned}(x \boxplus k_0)^5 = (x \boxplus k_0)^{101} &= x^5 + x^4 k_0^1 + x^3 k_0^2 + x^2 k_0^3 + x^1 k_0^4 + k_0^5 \\ &= x^{101} + x^{001} k_0^{100} + x^{110} k_0^{010} + x^{010} k_0^{110} + x^{100} k_0^{001} + k_0^{101} \\ (x + k_0)^5 = (x + k_0)^{101} &= x^{101} + x^{001} k_0^{100} + x^{100} k_0^{001} + k_0^{101}\end{aligned}$$

4.1 Modular Key Pre-Whitening

Note that many ciphers (especially ARX constructions) in their specification use word-wise instead of full-state modular addition. Thus, we generalize the concept of t-word-wise modular addition using the notations given in the preliminaries. Importantly, this framework is independent of the size of the words. When t=1, the lemma and subsequent proposition correspond to the previously discussed case of full-state modular addition. In contrast, when $t = n$, it reduces to the XOR-based case described in "classical" key whitening used in many ciphers.

By bridging these two corner cases—full-state modular addition and XOR-based whitening—this framework provides a unified tool to analyze t-word-wise modular key pre-whitening. This is particularly valuable for more advanced cases where t is neither 1 nor n. To the best of our knowledge, we provide the first explicit security criteria for t-word-wise pre-whitened ciphers, addressing a key gap in the analysis of such constructions.

Firstly, we show how the Boolean function's ANF changes after t-word-wise modular key addition, generalizing Theorem 1 from [12].

Lemma 2. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function with ANF $f(x) = x^u$, where $u \in \mathbb{F}_2^n$. Assume $\tilde{f}_{k_0}(x) \coloneqq f(x \boxplus_t k_0)$. Then we have*

$$\tilde{f}_{k_0}(x) = (x \boxplus_t k_0)^u = \sum_{v \leq_t u} x^v k_0^{u \boxminus_t v} \ .$$

Proof. Let us proceed by induction on t.

– **For $t = 1$.**
This case exactly corresponds to Theorem 1 in [12].

$$\tilde{f}_k(x) = f(x \boxplus k) = (x \boxplus k)^u = \sum_{v \leq u} x^v k^{u \boxminus v}$$

– **For $2 \leq t \leq n$.**

$$\tilde{f}_k(x) = f(x \boxplus_t k) = (x \boxplus_t k)^u$$

Then, we split u as follows:

$$\tilde{f}_k(x) = (x \boxplus_t k)^{\left((u^{(1)},\ldots,u^{(t-1)}),u^{(t)}\right)}$$

By the induction hypothesis, the lemma works for the first $t-1$ words. Then we have

$$\begin{aligned}
\tilde{f}_k(x) &= (x \boxplus_t k)^{\left((u^{(1)},\ldots,u^{(t-1)}),u^{(t)}\right)} \\
&= \left(x^{(u^{(1)},\ldots,u^{(t-1)})} \boxplus_{t-1} k^{(u^{(1)},\ldots,u^{(t-1)})}\right)^{(u^{(1)},\ldots,u^{(t-1)})} \left(x^{u^{(t)}} \boxplus k^{u^{(t)}}\right)^{u^{(t)}} \\
&= \left(\sum_{(v^{(1)},\ldots,v^{(t-1)}) \leq_{t-1} (u^{(1)},\ldots,u^{(t-1)})} x^{(v^{(1)},\ldots,v^{(t-1)})} k^{(u^{(1)},\ldots,u^{(t-1)}) \boxminus_{t-1} (v^{(1)},\ldots,v^{(t-1)})}\right) \\
&\times \sum_{v^{(t)} \leq u^{(t)}} x^{v^{(t)}} k^{u^{(t)} \boxminus v^{(t)}} \\
&= \sum_{(v^{(1)},\ldots,v^{(t-1)}) \leq_{t-1} (u^{(1)},\ldots,u^{(t-1)})} \left(\sum_{v^{(t)} \leq u^{(t)}} x^v k^{u \boxminus_t v}\right) \\
&= \sum_{v \leq_t u} x^v k^{u \boxminus_t v} \ .
\end{aligned}$$

□

Now we consider a keyed Boolean function $f_k(x)$ with the ANF in general form for which a modular word-wise pre-whitening is applied.

Proposition 2. *Let $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function with ANF*

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

and assume $\tilde{f}_{k,k_0}(x) \coloneqq f_k(x \boxplus_t k_0)$ to be expressed by its ANF

$$\tilde{f}_{k,k_0}(x) = f_k\left(x \boxplus_t k_0\right) = \sum_{v \in \mathbb{F}_2^n} q_v\left(k, k_0\right) x^v.$$

Then, for all $v \in \mathbb{F}_2^n$, we have

$$q_v\left(k, k_0\right) = \sum_{u \geq_t v} p_u(k) k_0^{u \boxminus_t v}$$

Proof. We express $q_v\,(k, k_0)$ in terms of p_u. We get

$$\begin{aligned}\tilde{f}_{k,k_0}(x) = f_k\,(x \boxplus_t k_0) &= \sum_{u\in\mathbb{F}_2^n} p_u(k)\,(x \boxplus_t k_0)^u \\ &= \sum_{u\in\mathbb{F}_2^n} p_u(k) \left(\sum_{v\leq_t u} x^v k_0^{u\boxminus_t v}\right) = \sum_{v\in\mathbb{F}_2^n} \left(\sum_{u\geq_t v} p_u(k) k_0^{u\boxminus_t v}\right) x^v.\end{aligned}$$

□

One special case of this proposition corresponds to Corollary 1 from Braeken and Semaev [12], where full-state modular addition is applied, i.e., $\tilde{f}_{k,k_0}(x) = f_k\,(x \boxplus k_0)$. In this case, the expression for $q_v\,(k, k_0)$ simplifies to

$$q_v\,(k, k_0) = \sum_{u\geq v} p_u(k) k_0^{u\boxminus v}.$$

Proposition 2 demonstrates that in the case of $t < n$, the propagation of whitening key monomials $k_0^{u\boxminus_t v}$ and associated polynomials $p_u(k)$ terms under modular addition significantly expands the space of affected terms comparing with XORing whitening. We call it "intra-bit" propagation. This expansion arises due to the existence of a "wider" partial order than the precursor partial order in $\mathbb{F}_2^n$. Consequently, we also need fewer linearly independent $p_u(k)$ to ensure similar linear independence of all $q_v(k, k_0)$, which is shown in Proposition 3. But before proving this, we first introduce a helpful lemma. Note that vectors of weight $t(2^s-1)-1$ correspond to all-ones vectors with one word's LSB set to 0.

Lemma 3. *Let $v, w \in \mathbb{F}_2^n$ be such that $\phi_{t,s}(v) + \phi_{t,s}(w) > t(2^s-1)-1$ and $v \boxplus_t w \geq_t v$. Then, $v \boxplus_t w = \mathbf{1}$.*

Proof. From $v \boxplus_t w \geq_t v$, we have

$$\phi_s(v^{(i)} \boxplus_t w^{(i)}) \geq \phi_s(v^{(i)}) \quad \text{for all } 1 \leq i \leq t.$$

This implies,

$$\phi_s(v^{(i)}) + \phi_s(w^{(i)}) \leq 2^s - 1 \quad \text{for all } 1 \leq i \leq t.$$

Then,

$$\phi_{t,s}(v) + \phi_{t,s}(w) \leq t(2^s-1).$$

Eventually, combined with the initial assumption, we have

$$\phi_{t,s}(v) + \phi_{t,s}(w) = \sum_{i=1}^{t} (\phi_s(v^{(i)}) + \phi_s(w^{(i)})) = t(2^s-1).$$

Then for all $i \in \{1, \ldots, t\}$,

$$\phi_s(v^{(i)}) + \phi_s(w^{(i)}) = 2^s - 1.$$

Thus, $v^{(i)} \boxplus w^{(i)} = (1, \ldots, 1)$ for all i, which implies $v \boxplus_t w = (1, \ldots, 1)$. □

Proposition 3. *Let f_k and $\tilde{f}_{k,k_0}$ be balanced Boolean functions defined by their ANFs as follows*

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \ ,$$
$$\tilde{f}_{k,k_0}(x) \coloneqq f_k(x \boxplus_t k_0) = \sum_{v \in \mathbb{F}_2^n} q_v(k,k_0) x^v \ .$$

Let $\mathcal{U}_t \coloneqq \{\mu \in \mathbb{F}_2^n \mid \phi_{t,s}(\mu) = t(2^s-1)-1\}$. If the set $\{p_\mu(k) \mid \mu \in \mathcal{U}_t\}$ is d-independent, then set of polynomials

$$\{q_v(k,k_0) \mid v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}\}$$

is d-independent.

Proof. Let us assume that there exist coefficients $\alpha_v \in \mathbb{F}_2$ such that

$$\deg_k \left(\sum_{v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}} \alpha_v q_v(k,k_0) \right) < d \ . \tag{3}$$

Note that, by $\deg_k(r(k,k_0))$ for a polynomial r, we mean the degree in k when considering r as a polynomial in k and k_0 (i.e., we do *not* assume k_0 as a constant). We will prove that (3) implies $\alpha_v = 0$ for all v.

$$T = \sum_{v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}} \alpha_v q_v(k,k_0) = \sum_{v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}} \alpha_v \left(\sum_{u \geq_t v} p_u(k) k_0^{u \boxminus_t v} \right)$$
$$= \sum_{v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}} \alpha_v \left(\sum_{\substack{w \in \mathbb{F}_2^n, \\ v \boxplus_t w \geq_t v}} p_{v \boxplus_t w}(k) k_0^w \right) = \sum_{w \in \mathbb{F}_2^n} \left(\sum_{\substack{v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}, \\ v \boxplus_t w \geq_t v}} \alpha_v p_{v \boxplus_t w}(k) \right) k_0^w \ .$$

Assuming,

$$T_w := \sum_{\substack{v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}, \\ v \boxplus_t w \geq_t v}} \alpha_v p_{v \boxplus_t w}(k).$$

Then, $\deg_k(T) < d$ if and only if for all $w \in \mathbb{F}_2^n$ we have

$$\deg_k (T_w) = \deg_k \left(\sum_{\substack{v \in \mathbb{F}_2^n \backslash \{\mathbf{1}\}, \\ v \boxplus_t w \geq_t v}} \alpha_v p_{v \boxplus_t w}(k) \right) < d \ . \tag{4}$$

We show that (4) for all $w \in \mathbb{F}_2^n$ implies $\alpha_v = 0$ for all v by induction on the ϕ-weight of v.

– **For $\phi_{t,s}(v) = 0$.**
If $\phi_{t,s}(v) = 0$ then $v = (0, \dots, 0)$. Let us consider a $w = \mu \in \mathcal{U}_t$. Then, we have

$$T_w = \alpha_{(0,\dots,0)} \cdot p_\mu(k) + \alpha_{(1,\dots,1)\boxminus_t \mu} \cdot p_{(1,\dots,1)}(k)$$

Due to the balancedness of f_k, we have $p_{(1,\dots,1)}(k) = \mathbf{0}$, but $p_\mu(k)$ is non-zero and $\deg_k(p_\mu(k)) \geq d$ by assumption, thus we have necessarily $\alpha_{\mathbf{0}} = 0$.

– **For $\phi_{t,s}(v) = \ell \leq t(2^s - 1) - 1 = \phi_{t,s}(\mu), \mu \in \mathcal{U}_t$.**
Let us consider a vector w of ϕ-weight $\phi_{t,s}(\mu) - \ell$, where $\mu \in \mathcal{U}_t$. Then, we split T_w as follows:

$$T_w = \sum_{\substack{v \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}, \\ \phi_{t,s}(v) > \ell, \\ v \boxplus_t w \geq_t v}} \alpha_v p_{v \boxplus_t w}(k) + \sum_{\substack{v \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}, \\ \phi_{t,s}(v) = \ell, \\ v \boxplus_t w \geq_t v}} \alpha_v p_{v \boxplus_t w}(k) + \sum_{\substack{v \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}, \\ \phi_{t,s}(v) < \ell, \\ v \boxplus_t w \geq_t v}} \alpha_v p_{v \boxplus_t w}(k) \ .$$

The last sum is equal to $\mathbf{0}$ as, by the induction hypothesis, we have $\alpha_v = 0$ for all v such that $\phi_{t,s}(v) < \ell$. Additionally, for the first sum we have $v \boxplus_t w = (1, \dots, 1)$ due to Lemma 3, meaning $p_{v \boxplus_t w}(k) = \mathbf{0}$. Then we have

$$T_w = \sum_{\substack{v \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}, \\ \phi_{t,s}(v) = \ell, \\ v \boxplus_t w \geq_t v}} \alpha_v p_{v \boxplus_t w}(k) = 0 \ ,$$

where $v \boxplus_t w \in \mathcal{U}_t$. By assumption, any non-trivial linear combination of corresponding polynomials $p_{v \boxplus_t w}$ is of degree at least d, so $\deg_k(T_w) < d$ implies $\alpha_v = 0$ for all v of ϕ-weight ℓ such that $v \boxplus_t w \geq_t v$. This implies $\alpha_v = 0$ for all v of ϕ-weight ℓ. This is because for all v with $\phi_{t,s}(v) = \ell$ there exists w with $\phi_{t,s}(w) = t(2^s - 1) - 1 - \ell$ such that $v \boxplus_t w \geq_t v$.

□

It is straightforward to formulate a generalized version of Proposition 3 for vectorial Boolean Functions. That is, if $E_k \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $\widetilde{E}_{k,k_0} \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are balanced, defined by their ANFs as

$$E_k^{(i)}(x) = \sum_{u \in \mathbb{F}_2^n} p_u^{(i)}(k) x^u \ ,$$
$$\widetilde{E}_{k,k_0}^{(i)}(x) \coloneqq E_k^{(i)}(x \boxplus_t k_0) = \sum_{v \in \mathbb{F}_2^n} q_v^{(i)}(k, k_0) x^v \ ,$$

then $\{q_v^{(i)}(k, k_0) \mid v \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}, i = 1, \dots, m\}$ is d-independent if $\{p_\mu^{(i)}(k) \mid \mu \in \mathcal{U}_t, i = 1, \dots, m\}$ is d-independent. The proof works in the same manner, with the difference that we have to consider

$$T_w \coloneqq \sum_{i=1}^{m} \sum_{\substack{v \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}, \\ v \boxplus_t w \geq_t v}} \alpha_v^{(i)} p_{v \boxplus_t w}^{(i)}(k).$$

The vectors $\mu \in \mathcal{U}_t$ have maximal ϕ-weight among all vectors in $\mathbb{F}_2^n$ except the all-one vector. In some sense, $\mathcal{U}_t$ can be considered as a Pareto front dominating all other vectors. In [24], the authors considered the case when $t = n$, and set $\mathcal{U}_t$ corresponds to vectors of Hamming weight $n - 1$.

We can also define $\mathcal{U}_t$ in another convenient way. For this purpose, we denote by u_i the vector in $\mathbb{F}_2^n$ of Hamming weight $n - 1$ such that its i-th position is zero, i.e., u_i is the bitwise complement of the i-th unit vector e_i. Then, the set $\mathcal{U}_t$ can be expressed as:

$$\mathcal{U}_t = \{u_{js+1} \mid j = 0, \ldots, t-1\}.$$

Note, for each t-partition, the corresponding vector in $\mathcal{U}_t$ is unique. Building on this observation, in Proposition 3, we presented a simple general criterion that any non-trivial linear combination of polynomials $q_v(k, k_0)$, generated after applying modular pre-whitening, will be of degree at least d.

Example 4. For $n = 6$ and $t = 2$ (i.e., each word has 3 bits), the set $\mathcal{U}_t$ consists of the vectors 111011 and 011111. These vectors represent the maximal ϕ-weight configuration that dominates all other vectors in the vector space (except for the all-one vector).

A particularly interesting and elegant case of Proposition 3 arises when the whitening key is added to the full state, i.e., $t = 1$ and $\tilde{f}_{k,k_0}(x) = f_k(x \boxplus k_0)$. The reason is that $\mathcal{U}_t$ only contains one element in that case. We formalize this specific case in the following corollary.

Corollary 2. *Let f_k and $\tilde{f}_{k,k_0}$ be balanced Boolean functions defined by their ANFs as follows*

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \ ,$$

$$\tilde{f}_{k,k_0}(x) \coloneqq f_k(x \boxplus k_0) = \sum_{v \in \mathbb{F}_2^n} q_v(k, k_0) x^v \ .$$

If $p_{(0,1,\ldots,1,1)}(k)$ has degree at least d in the key k, then set of polynomials

$$\{q_v(k, k_0) \mid v \in \mathbb{F}_2^n, v \neq \mathbf{1}\}$$

is d-independent.

We established an absolutely simple condition to guarantee the non-existence of integral distinguishes for a single output bit in the case of full-state modular pre-whitening. It suffices to ensure that only *one* of the polynomials $p_u(k)$ ($p_{(0,1,\ldots,1,1)}(k)$ or $p_{u_1}(k)$ in other words) in the ANF representation of the cipher is of degree at least d. Then, after applying the whitening key, $\tilde{f}_{k,k_0}$ is integral-resistant (i.e., all polynomials $q_v(k, k_0)$ and all their non-trivial linear combinations will be of degree at least d). We do not even need to check the linear independence of $p_{(0,1,\ldots,1,1)}(k)$ with other polynomials in the ANF.

4.2 Modular Key Post-Whitening

Typically, papers investigating integral resistance (e.g., [23,24]) use the assumption of pre-whitening keys, as it has already been shown to significantly affect the propagation of linear independence among polynomial coefficients in the ANF of Boolean functions. On the other hand, classical post-whitening using XOR operations does not affect the structure of the ANF for $\widetilde{E}_{k,k_1}(x) = E_k(x) + k_1$, since it only modifies the constant coefficient $p_{(0,\dots,0)}(k)$ without introducing new key dependencies for higher-degree terms. However, this is not the case for modular addition, i.e., $\widetilde{E}_{k,k_1}(x) = E_k(x) \boxplus k_1 = E_k(x) + k_1 + c$, where c is a carry function that introduces significant dependencies across output bits ANFs coefficients via carry bit propagation. We call this "inter-bit" propagation.

Let $x, k \in \mathbb{F}_2^n$ and $F(x,k) \coloneqq x \boxplus k$. Lemma 2 applied to $u = e_i$ yields $F^{(i)}(x,k) = \sum_{\phi_n(v) \leq 2^{i-1}} x^v k^{u \boxminus v}$. In particular, the ANF of $F^{(i)}$ contains the monomial $x_1 \prod_{j=1}^{i-1} k_j$ as a monomial of maximum degree, and this is the only monomial containing $\prod_{j=1}^{i-1} k_j$. For a better understanding, we provide an illustrative example of the values of F after full-state modular addition.

Example 5. The first output bits of F are:

$$\begin{aligned}
F^{(1)} &= \mathbf{x_1} + k_1,\\
F^{(2)} &= x_2 + k_2 + \mathbf{x_1 k_1},\\
F^{(3)} &= x_3 + k_3 + x_2 k_2 + x_1 x_2 k_1 + \mathbf{x_1 k_1 k_2},\\
F^{(4)} &= x_4 + k_4 + x_3 k_3 + x_3 x_2 k_2 + x_3 x_2 x_1 k_1 + x_3 x_1 k_1 k_2 + k_3 x_2 k_2\\
&\quad + k_3 x_2 x_1 k_1 + \mathbf{x_1 k_1 k_2 k_3}.
\end{aligned}$$

The carry bit provides a robust mechanism for propagating integral resistance across the entire state. Specifically, each carry bit part depends recursively on x_1 (the LSB of x) multiplied by unique key monomials. This brings us to proving a simple condition for integral resistance of block cipher E in the case of full-state modular addition post-whitening.

Lemma 4. *Let $E : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n$ be a block cipher and let the block cipher $\tilde{E} : \mathbb{F}_2^n \times \mathbb{F}_2^{\kappa+n} \to \mathbb{F}_2^n$ be defined by*

$$(x, k, k_1) \mapsto E_k(x) \boxplus_t k_1$$

where $k_1 \in \mathbb{F}_2^n$ is a post-whitening key. If $E^{(1)}$ is d-th order integral resistant, then $\widetilde{E}$ is d-th order integral resistant.

Proof. Given the modular post-whitening equation

$$\widetilde{E}_{k,k_1}(x) = E_k(x) \boxplus k_1.$$

Then for each output coordinate we have, due to Lemma 2:

$$\begin{aligned}
\widetilde{E}^{(i)}_{k,k_1}(x) = (E_k(x) \boxplus k_1)^{e_i} &= \sum_{v \leq e_i} E_k^v(x) k_1^{e_i \boxminus v}\\
&= E_k^{e_i}(x) + E_k^{e_i \boxminus e_1}(x) k_1^{e_1} + \dots + E_k^{e_2}(x) k_1^{e_i \boxminus e_2} + E_k^{e_1}(x) k_1^{e_i \boxminus e_1} + k_1^{e_i}.
\end{aligned}$$

Then, we need to prove that the linear combination of output coordinates of $\widetilde{E}$ is of degree at least d for all subsets $M_1, \ldots, M_n \subseteq \mathbb{F}_2^n$ (excluding cases when all of them are in $\{\emptyset, \mathbb{F}_2^n\}$):

$$\sum_{i=1}^{n} \sum_{x \in M_i} \widetilde{E}^{(i)}_{k,k_1}(x) = \sum_{i=1}^{n} \sum_{x \in M_i} (E_k^{e_i}(x) + E_k^{e_i \boxminus e_1}(x) k_1^{e_1} + \ldots + E_k^{e_2}(x) k_1^{e_i \boxminus e_2} + E_k^{e_1}(x) k_1^{e_i \boxminus e_1} + k_1^{e_i})$$

Separating the terms, we obtain:

$$\sum_{i=1}^{n} \sum_{x \in M_i} E^{(i)}_{k,k_1}(x) = \underbrace{\sum_{i=1}^{n} \sum_{x \in M_i} \left(E_k^{e_i}(x) + E_k^{e_i \boxminus e_1}(x) k_1^{e_1} + \ldots + E_k^{e_2}(x) k_1^{e_i \boxminus e_2} \right)}_{\text{Input term}} + \underbrace{\sum_{i=1}^{n} \sum_{x \in M_i} k_1^{e_i}}_{\text{Key addition term}} + \underbrace{\sum_{i=1}^{n} \sum_{x \in M_i} E_k^{e_1}(x) k_1^{e_i \boxminus e_1}}_{\text{Key-dependent term}}.$$

The third term ensures key dependency, as the first two cannot cancel it. The reason is that the third term includes $k_1^{e_i \boxminus e_1}$ of Hamming weight $i-1$, for maximal i such that $M_i \notin \{\emptyset, \mathbb{F}_2^n\}$, and it is the highest weight term in k_1 among other key monomials, Then, in order to prove that the whole sum is of degree at least d it is enough to prove the same for last term

$$\sum_{i=1}^{n} \sum_{x \in M_i} E_k^{e_1}(x) k_1^{e_i \boxminus e_1} = \sum_{i=1}^{n} k_1^{e_i \boxminus e_1} \sum_{x \in M_i} E_k^{(1)}(x).$$

As $k_1^{e_i \boxminus e_1}$ is unique for any $i = 1, \ldots, n$, the above implies that it is sufficient to show for any M_i the sum $\sum_{x \in M_i} E_k^{(1)}(x)$ is of degree at least d. The last statement is equal to proving that $E^{(1)}$ is d-th order integral resistant, which is given by the condition of the lemma. Therefore, $\widetilde{E}$ is d-th integral resistant. □

The same propagation extends naturally to t-word-wise operations, where the state and post-whitening key k_1 are partitioned into t equally-sized words. Modular addition is applied independently within each partition, introducing key dependencies within each word.

Proposition 4. *Let $E : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n$ be a block cipher and let the block cipher $\widetilde{E} : \mathbb{F}_2^n \times \mathbb{F}_2^{\kappa+n} \to \mathbb{F}_2^n$ be defined by*

$$(x, k, k_1) \mapsto E_k(x) \boxplus_t k_1,$$

where $k_1 \in \mathbb{F}_2^n$ is a post-whitening key. If the projection

$$(x, k) \mapsto (E_k^{(1)}(x), E_k^{(s+1)}(x), E_k^{(2s+1)}(x), \ldots, E_k^{((t-1)s+1)}(x))$$

of E is d-th order integral resistant, then $\widetilde{E}$ is d-th order integral resistant.

The proof is trivial and follows directly from the full-state case. Each of the t words is treated independently, with modular addition introducing unique dependence on k_1 in the same manner as described for the full-state key post-whitening. This follows from the fact that the output bit $E_{k,k_1}^{(i)}$ always includes the term $E_k^{(\lfloor \frac{i}{s} \rfloor s+1)} \prod_{l=\lfloor \frac{i}{s} \rfloor s+1}^{i-1} k_1^{(l)}$, where $\lfloor \frac{i}{s} \rfloor \in \{0, \ldots, t-1\}$. Notice that bit $\lfloor \frac{i}{s} \rfloor s + 1$ is the LSB with respect to the word, which also includes i-th bit.

4.3 Modular Key Pre- and Post-Whitening

After introducing intra- and inter-bit propagation, we extend the framework by considering the simultaneous application of modular pre- and post-whitening to the cipher E, i.e., the t-MAFX construction. This construction can be considered in some sense as a generalization of the classical FX construction [27] [1] [8] or of the combination of Addition Even-Mansour (AEM) [18] with a block cipher, depending on the value of t. Specifically, when $t = n$, our setup reduces to the FX construction, and when $t = 1$, it corresponds to AEM compounded with block cipher E. For intermediate values of t, it introduces modular whitening at the granularity of t-words, combining the key dependency and propagation mechanisms in a flexible and scalable manner.

Let E be a block cipher defined as above with ANF

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

and consider $\widetilde{E}$ which adds modular pre- and post-whitening:

$$\widetilde{E}_{k,k_0,k_1}(x) = (E_k(x \boxplus_t k_0)) \boxplus_t k_1,$$

where $k_0 \in \mathbb{F}_2^n$ and $k_1 \in \mathbb{F}_2^n$ are pre- and post-whitening keys, respectively. To ensure the construction is d-th order integral-resistant, we require the following:

1. Due to the post-whitening step, the block cipher with t output coordinates defined by

   $$(x, k, k_0) \mapsto (E_k^{(1)}(x \boxplus_t k_0), E_k^{(s+1)}(x \boxplus_t k_0), \ldots, E_k^{((t-1)s+1)}(x \boxplus_t k_0))$$

   must be d-th order integral resistant (Proposition 4).
2. To ensure 1., due to the pre-whitening step, the set

   $$\{p_\mu^{(js+1)}(k) \mid \mu \in \mathcal{U}_t, j = 0, \ldots, t-1\}$$

   must be d-independent (Proposition 3).

To summarize:

Proposition 5. *Let $E : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n$ be a block cipher and let*

$$\widetilde{E} : \mathbb{F}_2^n \times \mathbb{F}_2^{\kappa+2n} \to \mathbb{F}_2^n, (x, k, k_0, k_1) \mapsto E_k(x \boxplus_t k_0) \boxplus_t k_1,$$

where $k_0, k_1 \in \mathbb{F}_2^n$. If $\{p_\mu^{(js+1)}(k) \mid \mu \in \mathcal{U}_t, 0 \leq j < t\}$ is d-independent, then $\widetilde{E}$ is is d-th order integral resistant.

In a similar manner as in [24] with the help of integral-resistance matrix, we can show the d-independence of the set

$$\{p_\mu^{(js+1)}(k) \mid \mu \in \mathcal{U}_t, j = 0, \ldots, t-1\}.$$

Let the ANFs of the polynomials $p_u^{(i)}(k)$ be given by

$$p_u^{(i)}(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_{u,v}^{(i)} k^v,$$

where $\lambda_{u,v}^{(i)}$ is the parity of the number of division trails with input pattern u and key pattern v for output bit i. A d-th order integral-resistance matrix $\mathcal{I}_d(E)$ is defined as

$$\begin{pmatrix} \lambda_{u_1,v_1}^{(1)} & \lambda_{u_1,v_1}^{(s+1)} & \lambda_{u_1,v_1}^{(2s+1)} & \cdots & \lambda_{u_1,v_1}^{((t-1)s+1)} & \lambda_{u_{s+1},v_1}^{(1)} & \lambda_{u_{s+1},v_1}^{(s+1)} & \cdots & \lambda_{u_{(t-1)s+1},v_1}^{((t-1)s+1)} \\ \lambda_{u_1,v_2}^{(1)} & \lambda_{u_1,v_2}^{(s+1)} & \lambda_{u_1,v_2}^{(2s+1)} & \cdots & \lambda_{u_1,v_2}^{((t-1)s+1)} & \lambda_{u_{s+1},v_2}^{(1)} & \lambda_{u_{s+1},v_2}^{(s+1)} & \cdots & \lambda_{u_{(t-1)s+1},v_2}^{((t-1)s+1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & & \vdots \\ \lambda_{u_1,v_p}^{(1)} & \lambda_{u_1,v_p}^{(s+1)} & \lambda_{u_1,v_p}^{(2s+1)} & \cdots & \lambda_{u_1,v_p}^{((t-1)s+1)} & \lambda_{u_{s+1},v_p}^{(1)} & \lambda_{u_{s+1},v_p}^{(s+1)} & \cdots & \lambda_{u_{(t-1)s+1},v_p}^{((t-1)s+1)} \end{pmatrix},$$

where $v_1, \ldots, v_p \in \mathbb{F}_2^\kappa$ with $p \geq t^2$ are key patterns of Hamming weight at least d. In case where E is a key-alternating cipher with independent round keys, those coefficients can be efficiently constructed using mixed-integer linear programming [24].

For t-MAFX, integral resistance is verified by ensuring the full rank of a $t^2 \times t^2$ matrix $\mathcal{I}_d(E)$. Compared to [24], this significantly reduces complexity, requiring only t^4 instead of n^4 trail computations, where t is the number of words in full-state. This construction allows the analysis to be more practical while maintaining strong security guarantees. Additionally, modular addition enhances resistance to integral distinguishers by enabling broader linear independence propagation than XOR-based constructions, though it lowers the bound on the required number of rounds.

4.4 Application

For computations, we refer in general to the framework developed in [23] and [24], which leverages division trail counting with advanced optimization techniques to derive meaningful lower bounds on the algebraic degree and integral resistance of block ciphers. The most notable method is the use of MILP

and SAT solvers, which provide a systematic way to calculate the propagation of division trails in Boolean functions. In particular, the division property is modeled as a constraint system that traces the propagation of monomials through the cipher's structure. Thus, this framework relies on many optimization techniques for trail counting depending on the cipher design. Note, all our implementations and results are available at: `https://github.com/Eugen17/Integral-Resistance-by-Modular-Addition`

As shown in the table in Section 1, in our analysis of `GIFT-64`, `SKINNY-64`, and `PRESENT` under the t-word-wise pre- and post-whitening assumption for $t = 1$ and $t = 2$, we demonstrated improved bounds on the number of rounds required for integral resistance. The case $t = 1$ corresponds to the full-state modular addition of the key, simplifying the verification process significantly. Here, integral resistance verification reduces to proving just the existence of an odd number of division trails from the input $u_1 = (011\ldots11)$ to the basis vector e_i for at least one non-zero key pattern v. The approach for choosing key patterns follows directly from [23].

For $t = 2$, modular addition operates on two 32-bit words, as all the analyzed ciphers are 64-bit. This configuration balances practical implementation with security guarantees. Implementing ciphers with word sizes other than 32 or 64 bits is impractical, as modern hardware is optimized for these standard word sizes, ensuring efficient execution.

Furthermore, when $t = n$, the modular addition whitening coincides with the classical XOR-based key whitening, making the integral resistance bounds derived in [24] directly applicable.

Our results predictably revealed that modular whitening achieves integral resistance in fewer rounds compared to XOR-based whitening. For example, modular whitening with $t = 1$ and $t = 2$ reduced the number of rounds required to ensure resistance from 12–13 to just 9–11. Moreover, this allows us to address some already existing attacks on `GIFT-64` and `SKINNY-64`. This improvement stems from the stronger intra- and inter-bit key dependency propagation introduced by modular addition, ensuring that all ANF coefficients become linearly independent faster.

Interestingly, some of our results for the number of rounds coincide with the minimal possible values predicted by the upper bounds on the algebraic degree in [23]. For example, for `GIFT-64`, the upper bound on the algebraic degree reaches the maximum of $n-1$ after 9 rounds, which is exactly the same number of rounds we proved for integral resistance when $t = 1$. The same observation holds for `SKINNY-64`, where our results align with the predicted upper bounds.

One of the key advantages of our approach is the significant improvement in computational efficiency. Our results for each cipher were obtained in under 40 minutes on a common PC, with some cases requiring less than a minute (for example, for `GIFT-64`), even without additional optimizations. This is in contrast to the computational costs in [23] and [24], where building matrices could take several hours or even days. In particular, the optimizations used in [24], such as

computing only partial rows of the matrix instead of the full matrix, were not needed in our approach.

A crucial observation in our findings is that the smallest d-th order integral resistance found across all cases for `GIFT-64` was 18. This value is equal to the minimal Hamming weight of all key patterns v used for the calculation of entries in the integral resistance matrices. Similarly, for `PRESENT`, the minimal value of d was 26, and 55 for `SKINNY-64`, across all checked rounds and values of t. It is important to note that, due to the assumption of independent round keys, the key space considered in our analysis was $\mathbb{F}_2^{64r}$, where r denotes the number of rounds.

Remark 4. Despite the improvements in round bounds achieved with modular whitening, it is necessary to note that for $t < n$ (word-wise modular addition), integral resistance is achieved earlier in terms of the number of rounds needed, but does not always extend guarantees to a higher number of rounds. However, for all the analyzed ciphers, these guarantees hold, validating our bounds on more rounds. For example, we are able to say that `PRESENT` is integral resistant beginning from 10^{th} round under pre- and post-whitening by 1- or 2-word-wise modular addition, as it was confirmed that the integral-resistance matrix is full rank for 10 to 12 rounds. This is sufficient since the bounds from [24] guarantee security from the 13^{th} round onward.

5 Integral Resistance of Inverse Ciphers

The connection between a function F and its inverse F^{-1} in the context of integral properties has been previously explored in multiple works. In [9], the authors established that the algebraic degree of F^{-1} imposes constraints on the algebraic degree of the composition $G \circ F$, influencing the propagation of algebraic properties. This insight was further developed in [10] through Lemma 3, which describes conditions for the appearance of monomials x^u in the ANF of S^v for a given permutation S.

Then, it was extended for the division properties in [35], where Proposition 6 generalizes previous findings by stating that if a division trail $u \xrightarrow{S} v$ exists for a permutation S, then there necessarily exists a corresponding division trail for the inverse mapping $\bar{v} \xrightarrow{S^{-1}} \bar{u}$, where $\bar{u}$ and $\bar{v}$ denote the complements of u and v, respectively.

Obviously, there exists some symmetry in integral properties under inversion. Nevertheless, the equivalence of a block cipher E and its inverse E^{-1} from the perspective of integral resistance remains an open question.

5.1 Inequivalence of Integral Resistance of E and E^{-1}

Example 6 gives an integral resistant block cipher $E\colon \mathbb{F}_2^3 \times \mathbb{F}_2^5 \to \mathbb{F}_2^3$, meanwhile its inverse E^{-1} is not. There, E is integral-resistant since all $p_u(k)$ are at least 1-independent and key-dependent, giving full rank for the integral-resistance

matrix $\mathcal{I}(E)$. However, the integral-resistance matrix of E^{-1} is singular, as the $q_u^{(1)}(k)$ depends linearly on other polynomials $q_u(k)$, i.e.,

$$q_{100}^{(1)}(k) = q_{011}^{(1)}(k) + q_{000}^{(1)}(k) + q_{110}^{(1)}(k) + q_{101}^{(2)}(k) + q_{100}^{(2)}(k) + q_{011}^{(2)}(k) + q_{001}^{(2)}(k) + \\ + q_{000}^{(2)}(k) + q_{100}^{(3)}(k) + q_{010}^{(3)}(k) + q_{000}^{(3)}(k).$$

This example clearly demonstrates that the integral resistance of E does not imply the integral resistance of E^{-1} and vice versa.

Example 6. Let $E\colon \mathbb{F}_2^3 \times \mathbb{F}_2^5 \to \mathbb{F}_2^3$ be the block cipher given by the following:

k \ x	0	1	2	3	4	5	6	7
0	5	2	3	6	7	0	4	1
1	1	4	7	2	3	5	0	6
2	0	1	6	3	7	2	4	5
3	6	5	3	1	0	4	2	7
4	6	3	2	5	0	7	1	4
5	3	1	0	2	6	7	4	5
6	4	7	2	3	1	6	5	0
7	6	0	2	3	5	4	7	1
8	7	2	1	5	6	3	4	0
9	5	0	7	1	2	4	6	3
10	6	7	4	0	2	3	1	5
11	4	6	1	0	2	3	5	7
12	0	2	6	1	4	3	7	5
13	2	0	7	5	6	1	4	3
14	1	3	0	7	5	2	6	4
15	5	0	2	7	1	4	3	6
16	6	7	4	5	1	0	3	2
17	2	3	4	6	1	0	5	7
18	6	7	5	3	4	1	0	2
19	0	6	7	1	4	5	3	2
20	7	3	5	0	4	6	2	1
21	0	7	6	4	3	2	5	1
22	5	0	7	4	1	3	2	6
23	6	1	3	7	5	4	0	2
24	4	5	0	7	1	3	2	6
25	7	5	1	6	0	2	3	4
26	4	3	7	0	5	1	2	6
27	3	1	0	5	7	2	4	6
28	5	3	6	7	2	0	1	4
29	4	6	7	0	5	2	1	3
30	3	7	6	5	4	1	0	2
31	5	1	4	2	6	7	0	3

5.2 Equivalence of Integral Resistance of $E_k(x \boxplus_t k_0) \boxplus_t k_1$ and its Inverse

Another important observation is that the sets of key polynomial coefficients $p_u(k)$ of the degree $n-1$ monomials in the ANF of $E_k(x)$ and $E_k^{-1}(x)$ are the same but just permuted. In some sense, it can be seen as an implication of Proposition 6 in [35].

For our proof, we employ the graph indicator technique, following the framework established in [14]. Again, we denote by u_i the bitwise complement of the i-th unit vector e_i.

Lemma 5. *Let $E_k\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation given by its ANF $E_k(x) = \sum_{u\in\mathbb{F}_2^n} p_u(k)x^u$ and let $E_k^{-1}(x) = \sum_{u\in\mathbb{F}_2^n} q_u(k)x^u$ be the ANF of E_k^{-1}. Then, for all $i,j \in \{1,\dots,n\}$:*

$$p_{u_i}^{(j)}(k) = q_{u_j}^{(i)}(k).$$

Proof. We denote the graph of a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ by

$$G(F) \coloneqq \{(x, F(x)) \mid x \in \mathbb{F}_2^n\}.$$

Further, let $\mathbb{I}_S$ be the indicator function of a set S, so that

$$\mathbb{I}_{G(E_k)}(x,y) = \prod_{i=1}^{n} \left(y_i + E_k^{(i)}(x) + 1\right)$$

We can write this as

$$\mathbb{I}_{G(E_k)}(x,y) = \sum_{u\in\mathbb{F}_2^n} y^u \sum_{\substack{v\in\mathbb{F}_2^n \\ \mathrm{Sup}(u)\cap\mathrm{Sup}(v)=\emptyset}} (E_k(x))^v$$

We denote by $\mathrm{Sup}(x)$ the set of non-zero bit positions, that is $\mathrm{Sup}(x) = \{i \mid x_i = 1\}$. It holds that

$$\begin{aligned}
&\mathbb{I}_{G(E_k)}(x,y) = \mathbb{I}_{G\left(E_k^{-1}\right)}(y,x) \\
\Leftrightarrow &\sum_{u\in\mathbb{F}_2^n} y^u \sum_{\substack{v\in\mathbb{F}_2^n \\ \mathrm{Sup}(u)\cap\mathrm{Sup}(v)=\emptyset}} (E_k(x))^v = \sum_{u\in\mathbb{F}_2^n} x^u \sum_{\substack{v\in\mathbb{F}_2^n \\ \mathrm{Sup}(u)\cap\mathrm{Sup}(v)=\emptyset}} \left(E_k^{-1}(y)\right)^v \\
\Leftrightarrow &\sum_{u\in\mathbb{F}_2^n} y^u \sum_{\substack{v\in\mathbb{F}_2^n \\ \mathrm{Sup}(u)\cap\mathrm{Sup}(v)=\emptyset}} \left(\sum_{w\in\mathbb{F}_2^n} p_w(k)x^w\right)^v = \sum_{u\in\mathbb{F}_2^n} x^u \sum_{\substack{v\in\mathbb{F}_2^n \\ \mathrm{Sup}(u)\cap\mathrm{Sup}(v)=\emptyset}} \left(\sum_{w\in\mathbb{F}_2^n} q_w(k)y^w\right)^v.
\end{aligned}$$

Each monomial $x^{u_i}y^{u_j}$ occurs exactly once on both sides of the equation. This leads to the following observation:

$$\forall i \in \{1,\dots,n\}, \forall j \in \{1,\dots,n\} : p_{u_i}^{(j)}(k) = q_{u_j}^{(i)}(k).$$

□

The integral resistance properties of a block cipher E and its inverse E^{-1} are generally inequivalent, as demonstrated in the previous subsection. However, the fact that the sets of high-order polynomial coefficients coincide provides an opportunity to establish equivalence for integral resistance with the help of key whitening. We finally combine everything to prove the main result.

Proof (of Theorem 1). Let S be defined as $\{p_\mu^{(js+1)}(k) \mid \mu \in \mathcal{U}_t, j = 0, \ldots, t-1\}$, which is of size t^2. Let the ANF of E_k^{-1} be given as

$$E_k^{-1}(x) = \sum_{u \in \mathbb{F}_2^n} q_u(k) x^u.$$

If S is d-independent, then, by Proposition 5, $\widetilde{E}$ is d-th order integral resistant. As it was already mentioned before, we have $\mathcal{U}_t = \{u_{is+1} \mid i = 0, \ldots, t-1\}$. Then, the above set S of polynomials is equal to

$$\{p_{u_{is+1}}^{(js+1)}(k) \mid i, j = 0, \ldots, t-1\}.$$

From Lemma 5, $p_{u_{is+1}}^{(js+1)}(k) = q_{u_{js+1}}^{(is+1)}(k)$, so S is equal to

$$\{q_{u_{js+1}}^{(is+1)}(k) \mid j, i = 0, \ldots, t-1\}.$$

Then, any non-trivial linear combination of the $q_{u_{js+1}}^{(is+1)}(k)$'s is also of degree at least d, which is a sufficient condition for d-th order integral resistance with t-word-wise (pre- and post-) whitening by modular addition. Hence, $\widetilde{E}^{-1}$, which can be also defined as $(x, k, k_0, k_1) \mapsto (E_k^{-1}(x \boxminus_t k_1)) \boxminus_t k_0$, where subtraction is equivalent to the addition of complement keys, fulfills integral resistance. □

Acknowledgments. We thank the anonymous reviewers for their helpful comments. This work was (in part) supported by the European Research Council (ERC) project 101097056 (SYMTRUST).

References

1. Alagic, G., Russell, A.: Quantum-secure symmetric-key cryptography based on hidden shifts. In: Coron, J., Nielsen, J.B. (eds.) Advances in Cryptology - EUROCRYPT 2017. LNCS, vol. 10212, pp. 65–93 (2017)
2. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A small present - towards reaching the limit of lightweight encryption. In: Fischer, W., Homma, N. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer (2017)
3. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK lightweight block ciphers. In: Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, June 7-11, 2015. pp. 175:1–175:6. ACM (2015)
4. Bernstein, D.J.: ChaCha, a variant of Salsa20. In: Workshop Record of SASC 2008: The State of the Art of Stream Ciphers. (2008)

5. Beyne, T., Verbauwhede, M.: Integral cryptanalysis using algebraic transition matrices. IACR Trans. Symmetric Cryptol. 2023(4), 244–269 (2023)
6. Beyne, T., Verbauwhede, M.: Ultrametric integral cryptanalysis. In: Chung, K., Sasaki, Y. (eds.) Advances in Cryptology - ASIACRYPT 2024. LNCS, vol. 15490, pp. 392–423. Springer (2024)
7. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. 4(1), 3–72 (1991)
8. Bonnetain, X., Naya-Plasencia, M.: Hidden shift quantum cryptanalysis and implications. In: Peyrin, T., Galbraith, S.D. (eds.) Advances in Cryptology - ASIACRYPT 2018. LNCS, vol. 11272, pp. 560–592. Springer (2018)
9. Boura, C., Canteaut, A.: On the influence of the algebraic degree of F^{-1} on the algebraic degree of $G \circ F$. IEEE Trans. Inf. Theory 59(1), 691–702 (2013)
10. Boura, C., Canteaut, A.: Another view of the division property. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016. LNCS, vol. 9814, pp. 654–682. Springer (2016)
11. Boura, C., Canteaut, A., Cannière, C.D.: Higher-order differential properties of Keccak and *Luffa*. In: Joux, A. (ed.) Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers. LNCS, vol. 6733, pp. 252–269. Springer (2011)
12. Braeken, A., Semaev, I.A.: The ANF of the composition of addition and multiplication mod 2^n with a boolean function. In: Gilbert, H., Handschuh, H. (eds.) Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers. LNCS, vol. 3557, pp. 112–125. Springer (2005)
13. Burwick, C., Coppersmith, D., D'Avignon, E., Gennaro, R., Halevi, S., Jutla, C., Matyas Jr, S.M., O'Connor, L., Peyravian, M., Safford, D., Zunic, N.: Mars - a candidate cipher for AES. NIST AES Proposal (1998)
14. Carlet, C.: Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions. IEEE Trans. Inf. Theory 66(12), 7702–7716 (2020)
15. Derbez, P., Fouque, P.: Increasing precision of division property. IACR Trans. Symmetric Cryptol. 2020(4), 173–194 (2020)
16. Dinur, I., Shamir, A.: Cube attacks on tweakable black box polynomials. In: Joux, A. (ed.) Advances in Cryptology - EUROCRYPT 2009. LNCS, vol. 5479, pp. 278–299. Springer (2009)
17. Dunkelman, O., Ghosh, S., Keller, N., Leurent, G., Marmor, A., Mollimard, V.: Partial sums meet FFT: improved attack on 6-round AES. In: Joye, M., Leander, G. (eds.) Advances in Cryptology - EUROCRYPT 2024. LNCS, vol. 14651, pp. 128–157. Springer (2024)
18. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in cryptography: The Even-Mansour scheme revisited. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology - EUROCRYPT 2012. LNCS, vol. 7237, pp. 336–354. Springer (2012)
19. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D.A., Whiting, D.: Improved cryptanalysis of Rijndael. In: Schneier, B. (ed.) Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings. LNCS, vol. 1978, pp. 213–230. Springer (2000)
20. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The Skein hash function family. Submission to NIST (round 3) (2010)
21. Hadipour, H., Sadeghi, S., Eichlseder, M.: Finding the impossible: Automated search for full impossible-differential, zero-correlation, and integral attacks. In:

Hazay, C., Stam, M. (eds.) Advances in Cryptology - EUROCRYPT 2023. LNCS, vol. 14007, pp. 128–157. Springer (2023)
22. Hao, Y., Leander, G., Meier, W., Todo, Y., Wang, Q.: Modeling for three-subset division property without unknown subset - improved cube attacks against Trivium and Grain-128AEAD. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology - EUROCRYPT 2020. LNCS, vol. 12105, pp. 466–495. Springer (2020)
23. Hebborn, P., Lambin, B., Leander, G., Todo, Y.: Lower bounds on the degree of block ciphers. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2020. LNCS, vol. 12491, pp. 537–566. Springer (2020)
24. Hebborn, P., Lambin, B., Leander, G., Todo, Y.: Strong and tight security guarantees against integral distinguishers. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021. LNCS, vol. 13090, pp. 362–391. Springer (2021)
25. Hu, K., Sun, S., Wang, M., Wang, Q.: An algebraic formulation of the division property: Revisiting degree evaluations, cube attacks, and key-independent sums. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2020. LNCS, vol. 12491, pp. 446–476. Springer (2020)
26. Hu, K., Yap, T.: Perfect monomial prediction for modular addition. IACR Trans. Symmetric Cryptol. 2024(3), 177–199 (2024)
27. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search. In: Koblitz, N. (ed.) Advances in Cryptology - CRYPTO '96. LNCS, vol. 1109, pp. 252–267. Springer (1996)
28. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings. LNCS, vol. 1008, pp. 196–211. Springer (1994)
29. Knudsen, L.R., Wagner, D.A.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers. LNCS, vol. 2365, pp. 112–127. Springer (2002)
30. Lai, X.: Higher order derivatives and differential cryptanalysis. Communications and Cryptography: Two Sides of One Tapestry pp. 227–233 (1994)
31. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) Advances in Cryptology - EUROCRYPT '93. LNCS, vol. 765, pp. 386–397. Springer (1993)
32. Todo, Y.: Structural evaluation by generalized integral property. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology - EUROCRYPT 2015. LNCS, vol. 9056, pp. 287–314. Springer (2015)
33. Todo, Y., Aoki, K.: FFT key recovery for integral attack. In: Gritzalis, D., Kiayias, A., Askoxylakis, I.G. (eds.) Cryptology and Network Security. LNCS, vol. 8813, pp. 64–81. Springer (2014)
34. Todo, Y., Morii, M.: Bit-based division property and application to Simon family. In: Peyrin, T. (ed.) Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers. LNCS, vol. 9783, pp. 357–377. Springer (2016)
35. Udovenko, A.: Convexity of division property transitions: Theory, algorithms and compact models. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021. LNCS, vol. 13090, pp. 332–361. Springer (2021)
36. Xiang, Z., Zhang, W., Bao, Z., Lin, D.: Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology - ASIACRYPT 2016. LNCS, vol. 10031, pp. 648–678 (2016)