Ultrametric integral cryptanalysis

Tim Beyne and Michiel Verbauwhede

COSIC, KU Leuven

Abstract. A systematic method to analyze *divisibility properties* is proposed. In integral cryptanalysis, divisibility properties interpolate between bits that sum to zero (divisibility by two) and saturated bits (divisibility by 2^{n-1} for 2^n inputs). From a theoretical point of view, we construct a new cryptanalytic technique that is a non-Archimedean multiplicative analogue of linear cryptanalysis. It lifts integral cryptanalysis to characteristic zero in the sense that, if all quantities are reduced modulo two, then one recovers the algebraic theory of integral cryptanalysis. The new technique leads to a theory of trails. We develop a tool based on off-the-shelf solvers that automates the analysis of these trails and use it to show that many integral distinguishers on PRESENT and SIMON are stronger than expected.

Keywords: Geometric approach · Integral cryptanalysis · Division property

1 Introduction

Integral cryptanalysis can be approached from two opposing directions. The *structural approach* was formalized by Knudsen and Wagner [24] and stems from the 'Square attack' [14]. It is based on propagating plaintexts with some constant and some saturated parts through a cipher, ultimately resulting in a set of ciphertexts with a saturated part, or some bits that sum to zero. A part of the state is called saturated if all its possible values occur an equal number of times. The *algebraic approach* was introduced by Knudsen [23], based on the observation that the $(d+1)^{\text{st}}$ derivative of a function of degree d is zero. This yields zero sums, but not saturation properties.

Todo [29] partially consolidated the two approaches by introducing the division property, which characterizes structured sets algebraically. More generally, it was shown by Boura and Canteaut at Crypto 2016 [9] that every set has an equivalent parity set representation. The parity set of a set X is the set of all exponents of monomials that sum to one on X.

However, as the division property is based on arithmetic over $\mathbb{F}_2$, it can describe zero sums but not saturation. The gap is significant: the probability that a uniform random Boolean function sums to zero on a set of size 2^n is $1/2$, but it is saturated with probability approximately[1] $2^{-n/2}/\sqrt{\pi}$. A saturation property consequently corresponds to a stronger filter, which is beneficial for the data and time requirements of key-recovery attacks. In spite of this, the difference is sometimes overlooked.

Thus, one might wonder if there can exist a theory of integral cryptanalysis over a field of characteristic zero rather than over $\mathbb{F}_2$, so that both zero sums and

[1] The exact probability is equal to $\binom{2^n}{2^{n-1}}/2^{2^n}$.

saturation properties can be described by it. In practice, zero sums are found by automated analysis of trails – there are several variants including division trails [33], monomial trails [20] and algebraic trails [3]. These concepts are more-or-less similar to trails in linear cryptanalysis, but the analogy is leaky because the 'correlations' are binary. Optimistically, a theory defined in characteristic zero might strengthen the analogy by allowing correlations 'in between' zero and one.

Contribution. We introduce the theory of *ultrametric integral cryptanalysis*, a non-Archimedean multiplicative analogue of linear cryptanalysis. Inspired by the idea that linear cryptanalysis simplifies additions (exclusive or), we construct an analogous theory that simplifies multiplications (bitwise and). Like linear cryptanalysis, it is defined in characteristic zero (over $\mathbb{Q}$), but to obtain a useful theory, we have to change the way distances are measured: we replace the regular (Archimedean) absolute value $|\cdot|$ on $\mathbb{Q}$ with the (non-Archimedean) 2-adic absolute value $|\cdot|_2$. Ultrametric integral cryptanalysis lifts integral cryptanalysis to characteristic zero, in the sense that if all quantities are reduced modulo two, then one obtains the algebraic theory of integral cryptanalysis over $\mathbb{F}_2$ – more precisely, its description using algebraic trails that was recently introduced in ToSC 2023 [3]. Some consequences of the analogy between linear and ultrametric integral cryptanalysis are illustrated in Table 1.

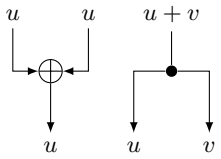
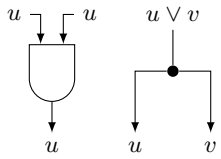
In practical terms, ultrametric integral cryptanalysis provides a systematic way to analyze divisibility properties. For example, one can use it show that the number of times a ciphertext bit equals one, is divisible by 2^ν. In our theory, this can be proven by showing that one or more *correlations* have 2-adic absolute value at most $2^{-\nu}$. Divisibility properties interpolate between zero sums (divisibility by two) and saturation (divisibility by 2^{n-1} for an input space of dimension n). We believe that these properties occur naturally in cryptanalysis, as their existence is essentially an unexplained folklore observation. For example, in Todo's invited talk at FSE 2023, divisibility by four pops up at 43:30[2].

The construction of our theory follows the geometric approach [1], which was introduced at Asiacrypt 2021 as a general description of linear cryptanalysis. In particular, we express the 'pushforward operators' that describe the propagation of states through functions as matrices relative to a carefully chosen basis. The basis is constructed in Section 4, and is uniquely defined by the property that it diagonalizes the matrices corresponding to multiplications $x \mapsto x \wedge k$. This is analogous to linear cryptanalysis, which diagonalizes the matrices corresponding to additions $x \mapsto x+k$. Our choice of basis leads to ultrametric integral transition matrices, which are analogous to correlation matrices in linear cryptanalysis. We show that these matrices are closely related to the numerical normal form of Boolean functions. Like for correlation matrices, composition of functions corresponds to multiplication of ultrametric integral transition matrices.

Section 5 develops the theory of ultrametric integral trails. Properties can be evaluated by summing the correlations of trails, and this can be made practical using dominant trails (Theorem 5.1). Unlike in linear cryptanalysis, the domi-

[2] https://www.youtube.com/watch?v=hgHJu6QrOUs&t=2610s

Table 1: The analogy between linear and ultrametric integral cryptanalysis.

	Linear cryptanalysis	Ultrametric integral cryptanalysis
Field of definition	$\mathbb{Q}$ or $\mathbb{R}$ Archimedean ordinary absolute value $\lvert\cdot\rvert$	$\mathbb{Q}$ or $\mathbb{Q}_2$ non-Archimedean 2-adic absolute value $\lvert\cdot\rvert_2$
Geometric theory	'diagonalizes' additions $x \mapsto x + k$	'diagonalizes' multiplications $x \mapsto x \wedge k$
	additive characters χ^u Fourier transformation $\mathscr{F}$ $C^{\mathsf{F}} = \mathscr{F} T^{\mathsf{F}} \mathscr{F}^{-1}$	multiplicative characters μ^u ultrametric integral change-of-basis $\mathscr{U}$ $A^{\mathsf{F}} = \mathscr{U} T^{\mathsf{F}} \mathscr{U}^{-1}$
Theory of trails	masks $u_1, u_2, \ldots$ correlation $\prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i}$ linear functions linear diffusion, nonlinear confusion	exponents $u_1, u_2, \ldots$ correlation $\prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i}$ multiplicative functions nonlinear diffusion, linear confusion
		

nant trail approximation is not heuristic in the ultrametric setting because the sum of many small numbers in a non-Archimedean field is always small.

Section 6 investigates the properties of ultrametric integral transition matrices. The main result in this section is Theorem 6.1, which characterizes the ultrametric integral transition matrices of low-degree functions. This result implies the Ax-Katz theorem [22] (over $\mathbb{F}_2$), which states that the number of solutions of a system of m equations of degree d in n variables is divisible by $2^{\lceil n/d \rceil - m}$. Interestingly, our proof is cryptanalytic: the result follows by analyzing ultrametric integral trails in a generic function of degree d. We also show that ultrametric integral transition matrices can be computed in time proportional to their size (up to logarithmic factors), and propagation rules for copy and xor operations are derived. Theorem 6.2 relates correlation matrices and ultrametric integral transition matrices, explaining and strengthening a result that was used by Canteaut and Videau [10] and Boura and Canteaut [8] to bound degrees.

Finally, in Sections 7 and 8, we develop an automated tool to analyze ultrametric integral trails using off-the-shelf solvers and apply it to PRESENT and SIMON. Our analysis shows that the distinguishers for reduced-round PRESENT presented by Boura and Canteaut at Crypto 2016 [9] and by Wang *et al.* at Asiacrypt 2019 [32] are stronger than previously believed. For many output bits, we find divisibility by higher powers of two (ranging from 2^2 to 2^9). We also

demonstrate that ultrametric integral cryptanalysis can be used to find zero-correlation linear approximations, and illustrate how divisibility properties are useful to reduce the data-complexity of key-recovery attacks. For SIMON, we reconsider the distinguishers found by Todo [29], Todo and Morii [30] and Xiang *et al.* [33] and prove higher divisibility. In addition, we slightly improve the modelling of SIMON based on the analogy between linear and multiplicative functions. This observation is also applicable to ordinary integral cryptanalysis. The source code of our tool can be found at `https://github.com/MichielVerbauwhede/ultrametric-integral-cryptanalysis`.

Future work. Ultrametric integral cryptanalysis can be extended to all primes p and all commutative inverse monoids, including $\mathbb{F}_q^n$ with multiplication. However, this requires more technical background because the theory must be defined over the p-adic numbers $\mathbb{Q}_p$ when $p \geq 5$. Nevertheless, our results generalize to this setting. In the interest of simplicity, we focus on the case $p = q = 2$ in this paper.

2 Background

The theory of ultrametric integral cryptanalysis is based on the geometric approach, which we present (for the one-dimensional case) in Section 2.1 in slightly modified form. Section 2.2 describes linear cryptanalysis from this point of view, and integral cryptanalysis is discussed in Section 2.3.

2.1 Geometric approach

The geometric approach to symmetric-key cryptanalysis was introduced at Asiacrypt 2021 [1] as an alternative description of linear cryptanalysis. In a subsequent paper at Crypto 2022 [2], the same approach was used to construct a fixed-key theory of differential cryptanalysis. The role of the geometric approach in this paper is similar to that in the latter work: it is used to construct a new cryptanalytic theory, analogous to the theory of linear cryptanalysis.

Let k be a field – in [1,2], k is either $\mathbb{R}$ or $\mathbb{C}$. The free k-vector space on $\mathbb{F}_2^n$ consists of all formal k-linear combinations of elements of $\mathbb{F}_2^n$, with addition defined coordinate-wise. That is, every element a of $k[\mathbb{F}_2^n]$ is of the form

$$a = \sum_{x \in \mathbb{F}_2^n} a_x \, \delta_x \,,$$

where the values a_x are arbitrary elements of k and δ_x is the formal basis vector corresponding to x. Cryptanalytically, a represents an assignment of weights (elements of k) to the elements of $\mathbb{F}_2^n$. For example, a subset $X \subseteq \mathbb{F}_2^n$ corresponds to a vector $\delta_X = \sum_{x \in X} \delta_x$ in $k[\mathbb{F}_2^n]$. Applying a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ to the state transforms the assignment of weights on $\mathbb{F}_2^n$ to an assignment of weights on $\mathbb{F}_2^m$. The relation is given by a linear operator.

Definition 2.1. *Let $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. The pushforward operator of F is the linear map $T^{\mathsf{F}} : k[\mathbb{F}_2^n] \to k[\mathbb{F}_2^m]$ defined by $T^{\mathsf{F}} \, \delta_x = \delta_{\mathsf{F}(x)}$ for all x in $\mathbb{F}_2^n$.*

The matrix representation of T^{F} with respect to the standard basis will be called the *transition matrix* of F. Its rows and columns are indexed by elements of $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$ respectively. Depending on the context, the notation T^{F} either refers to the pushforward operator of F or to its transition matrix.

Transition matrices satisfy several properties, two of which are summarized in Theorem 2.1. In this theorem, $\bigotimes$ denotes the Kronecker product of matrices. That is, $(A \otimes B)_{y_1 \| y_2, x_1 \| x_2} = A_{y_1,x_1} B_{y_2,x_2}$, where $\|$ denotes concatenation.

Theorem 2.1. *For the transition matrix of a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$:*

(1) If $\mathsf{F}(x_1 \| \cdots \| x_l) = \mathsf{F}_1(x_1) \| \cdots \| \mathsf{F}_l(x_l)$, then $T^{\mathsf{F}} = \bigotimes_{i=1}^{l} T^{\mathsf{F}_i}$.

(2) If $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$, then $T^{\mathsf{F}} = T^{\mathsf{F}_r} \cdots T^{\mathsf{F}_2} T^{\mathsf{F}_1}$.

A dual way to assign weights to the elements of $\mathbb{F}_2^n$ is using functions. Let $k^{\mathbb{F}_2^n}$ be the vector space of k-valued functions on $\mathbb{F}_2^n$. Every function in $k^{\mathbb{F}_2^n}$ can be extended to a function on $k[\mathbb{F}_2^n]$ by linearity. Conversely, every linear function on $k[\mathbb{F}_2^n]$ is uniquely determined by its image on the basis vectors δ_x with x in $\mathbb{F}_2^n$. Hence, we identify $k^{\mathbb{F}_2^n}$ with the dual vector space[3] of $k[\mathbb{F}_2^n]$. The functions δ^x with $\delta^x(\delta_x) = \delta^x(x) = 1$ and $\delta^x(\delta_y) = \delta^x(y) = 0$ for $y \neq x$ are a basis for $k^{\mathbb{F}_2^n}$.

A cryptanalytic property of a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a pair (a, b) with a in $k[\mathbb{F}_2^n]$ and b in $k^{\mathbb{F}_2^m}$. The *evaluation* of a property (a, b) is defined as $b(T^{\mathsf{F}} a)$. This is typically a combinatorial quantity of interest, such as the correlation of a linear approximation.

Example 2.1. Let X and Y be subsets of $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively. The evaluation of (δ_X, δ^Y), with $\delta^Y = \sum_{y \in Y} \delta^y$ the indicator function of Y, is equal to

$$\delta^Y \left(T^{\mathsf{F}} \delta_X \right) = \sum_{x \in X} \delta^Y \left(\delta_{\mathsf{F}(x)} \right) = \left| \{ x \in X \mid \mathsf{F}(x) \in Y \} \right| .$$

If F is a permutation, then the property evaluates to $|Y \cap \mathsf{F}(X)|$. ▷

If we apply a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$, then functions on $\mathbb{F}_2^m$ transform to functions on $\mathbb{F}_2^n$. The relation is given by the pullback operator $T^{\mathsf{F}^\vee}$, which is the adjoint[4] of the pushforward operator. That is, $T^{\mathsf{F}^\vee} f = f \circ \mathsf{F}$. Its standard basis matrix representation is the transpose of the transition matrix. Pullback operators also satisfy the properties listed in Theorem 2.1, with the order of multiplication reversed for property (2).

Different cryptanalytic theories are obtained by expressing cryptanalytic properties with respect to different pairs of dual bases for $k[\mathbb{F}_2^n]$ and $k^{\mathbb{F}_2^m}$. A pair of bases for $k[\mathbb{F}_2^n]$ and $k^{\mathbb{F}_2^m}$ consisting of vectors β_u and β^u, labeled by u in $\mathbb{F}_2^n$, is called dual if $\beta^u(\beta_u) = 1$ and $\beta^v(\beta_u) = 0$ for all $u \neq v$.

If $\mathscr{B} : k[\mathbb{F}_2^n] \to k[\mathbb{F}_2^n]$ is the change-of-basis transformation defined by $\mathscr{B}\, \beta_u = \delta_u$, then $\mathscr{B}^{-\vee}\, \beta^v = \delta^v$. That is, $\mathscr{B}^{-\vee}$ is the change-of-basis transformation for

[3] The dual vector space of $k[\mathbb{F}_2^n]$ is the space of all linear functions from $k[\mathbb{F}_2^n]$ to k.

[4] The adjoint of $L : k[\mathbb{F}_2^n] \to k[\mathbb{F}_2^m]$ is a map $L^\vee : k^{\mathbb{F}_2^m} \to k^{\mathbb{F}_2^n}$ s.t. $\left(L^\vee b\right)(a) = b\left(La\right)$.

the dual basis. Let $\mathscr{B}_n$ and $\mathscr{B}_m$ be change-of-basis transformations on $k[\mathbb{F}_2^n]$ and $k[\mathbb{F}_2^m]$ respectively. For a cryptanalytic property (a, b), set $a^\wedge = \mathscr{B}_n\, a$ and $b^\wedge = \mathscr{B}_m^{-\vee}\, b$. The evaluation of (a, b) can then be expressed as

$$b\big(T^{\mathsf{F}}\, a\big) = b^\wedge\Big(\mathscr{B}_m\, T^{\mathsf{F}}\, \mathscr{B}_n^{-1} a^\wedge\Big)\,.$$

Hence, if properties are expressed in the new basis, their propagation is described by the matrix $\mathscr{B}_m\, T^{\mathsf{F}}\, \mathscr{B}_n^{-1}$. Since this matrix is similar to T^{F}, it also satisfies the properties listed in Theorem 2.1.

2.2 Linear cryptanalysis

In linear cryptanalysis, the field k is chosen as $\mathbb{R}$ or $\mathbb{C}$ and one works in a basis of group characters and its dual. The characters of the additive group $\mathbb{F}_2^n$ are the homomorphisms $\chi^u : \mathbb{F}_2^n \to \mathbb{R}$ with $\chi^u(x) = (-1)^{u^\mathsf{T} x}$. The dual basis consists of the vectors χ_u in $\mathbb{R}[\mathbb{F}_2^n]$ with $\delta^x(\chi_u) = \chi^u(x)/2^n$. The corresponding change-of-basis transformation $\mathscr{F}_n : \mathbb{R}[\mathbb{F}_2^n] \to \mathbb{R}[\mathbb{F}_2^n]$ is called the Fourier transformation.

The Fourier transformation simultaneously diagonalizes the transition matrices T^{F} of all translations $\mathsf{F}(x) = x + t$. In fact, as shown in [1, §2.2], this is by construction: the character basis is the only basis with this property. The Fourier transformation of the transition matrix of a function F is its correlation matrix $C^{\mathsf{F}} = \mathscr{F}_m T^{\mathsf{F}} \mathscr{F}_n^{-1}$. These matrices were introduced by Daemen [13], motivated by the fact that the coordinates $C^{\mathsf{F}}_{v,u}$ are the correlations of linear approximations with input mask u and output mask v over F:

$$C^{\mathsf{F}}_{v,u} = \chi^v\big(T^{\mathsf{F}}\, \chi_u\big) = 2 \Pr_{\mathbf{x}}\big[v^\mathsf{T}\mathsf{F}(\mathbf{x}) = u^\mathsf{T}\mathbf{x}\big] - 1\,,$$

with $\mathbf{x}$ uniform random on $\mathbb{F}_2^n$.

The properties listed in Theorem 2.1 carry over to correlation matrices. In particular, if $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$, then $C^{\mathsf{F}} = C^{\mathsf{F}_r} \cdots C^{\mathsf{F}_2} C^{\mathsf{F}_1}$. If one defines a linear trail as a tuple of $r + 1$ masks, then Theorem 2.1 (2) implies that the correlation of a linear approximation is equal to the sum of the correlations of all linear trails with matching input and output masks:

$$C^{\mathsf{F}}_{u_{r+1},u_1} = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i}\,,$$

where the product $\prod_{i=1}^r C^{\mathsf{F}_i}_{u_{i+1},u_i}$ is called the correlation of the trail $(u_1, \ldots, u_{r+1})$. This result is usually used in the form of the principle of dominant trails.

Theorem 2.2 (Dominant trails). *Let $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$. For all subsets Λ of the set Ω of all linear trails from u_1 to u_{r+1},*

$$\left| C^{\mathsf{F}}_{u_{r+1},u_1} - \sum_{u\in\Lambda} \prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i} \right| = \left| \sum_{u\in\Omega\setminus\Lambda} \prod_{i=1}^{r} C^{\mathsf{F}_i}_{u_{i+1},u_i} \right|,$$

where $u = (u_1, u_2, \ldots, u_{r+1})$.

The idea of Theorem 2.2 is that the trails in $\Omega \setminus \Lambda$ contribute little to $C^{\mathsf{F}}_{u_{r+1},u_1}$. In practice, Theorem 2.2 is used heuristically: one assumes that if the absolute values of the correlations of trails in $\Omega \setminus \Lambda$ are small, then so is the absolute value of their sum. This approach is useful for linear approximations (u, v) with large absolute correlation $|C^{\mathsf{F}}_{v,u}|$. Contrary to this, zero-correlation linear cryptanalysis [7] relies on linear approximations with $C^{\mathsf{F}}_{v,u} = 0$. Such approximations can be found using Theorem 2.2, but with $\Lambda = \emptyset$ and by showing that all trails in Ω have correlation zero. Bogdanov *et al.* [6] have shown that zero-correlation linear approximations and saturation properties are closely related. Following Sun *et al.* [28, Corollary 4], if U is a vector space of masks such that $C^{\mathsf{F}}_{v,u} = 0$ for all u in U, then the restriction of $v^{\mathsf{T}}\mathsf{F}$ to a coset of $U^{\perp}$ is a balanced Boolean function. This means that the linear combination of output bits corresponding to the mask v is saturated when the input set is a coset of $U^{\perp}$.

2.3 Integral cryptanalysis

Traditionally, integral cryptanalysis is used to find affine subspaces X such that $\sum_{x \in X} f(x) = 0$ for a coordinate function f of a cryptographic primitive. As mentioned in the introduction, such properties can be approached in two different ways. Wagner and Knudsen [24] describe the propagation of structured sets with some constant and some saturated parts. In earlier work, Knudsen [23] proposed a purely algebraic approach based on higher-order derivatives.

The algebraic point of view is best understood using the algebraic normal form. This is the unique representation of a Boolean function as a polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$. If the algebraic normal form of f does not contain any monomials $x^u = \prod_{i=1}^n x_i^{u_i}$ such that $\sum_{x \in X} x^u = 1$, then f sums to zero on X. The relation with the properties of X and the structural point of view of Wagner and Knudsen was poorly understood before the introduction of the division property by Todo [29]. The division property characterizes X by the set of exponents u such that $\sum_{x \in X} x^u = 1$. This set was called the parity set of X by Boura and Canteaut [9].

A recent paper in ToSC 2023 [3] shows that it is possible to construct a theory of integral cryptanalysis based on the geometric approach. It describes cryptanalytic properties (a, b) over the field $k = \mathbb{F}_2$. If $a = \delta_X$, then the evaluation $b(T^{\mathsf{F}}a)$ of (a, b) is equal to the sum $\sum_{x \in X} f(x)$ with $f = b \circ \mathsf{F}$. Since b is a Boolean function, there exists a change-of-basis transformation $\mathscr{M}_m$ so that $(\mathscr{M}_m b)(u)$ is the coefficient of x^u in the algebraic normal form of b. The transformation $\mathscr{M}_m$ is the binary Möbius transformation. Relative to this change-of-basis, (a, b) evaluates to

$$b\big(T^{\mathsf{F}}a\big) = b^{\wedge}\Big(\mathscr{P}_m T^{\mathsf{F}} \mathscr{P}_n^{-1} a^{\wedge}\Big),$$

with $a^{\wedge} = \mathscr{P}_n a$ and $\mathscr{P}_n = \mathscr{M}_n^{-\vee}$. It was shown in [3] that $\mathscr{P}_n \delta_X = \delta_Y$ with Y the parity set of X.

The matrix $A^{\mathsf{F}} = \mathscr{P}_m T^{\mathsf{F}} \mathscr{P}_n^{-1}$ is called the algebraic transition matrix of F and it satisfies the usual properties from Theorem 2.1. It holds that $A^{\mathsf{F}}_{v,u} = 1$ if and only if x^u occurs in the algebraic normal form of F^v. In particular, if

$\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$, then $A^{\mathsf{F}} = \prod_{i=1}^{r} A^{\mathsf{F}_i}$. This leads to a theory of algebraic trails $(u_1, \ldots, u_{r+1})$ with correlation $\prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i}$ such that

$$A^{\mathsf{F}}_{u_{r+1},u_1} = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i} .$$

This yields an alternative explanation of division trails [33], monomial prediction [20] and the three-subset division property without unknown subset [18].

However, the theory of algebraic trails is not completely satisfactory. The motivation of the division property was to combine the best of the structural and algebraic approaches to integral cryptanalysis, but this was only partially achieved because saturation properties cannot be described over $\mathbb{F}_2$. For example, if zero-correlation linear cryptanalysis shows that the restriction of $f = v^{\mathsf{T}}\mathsf{F}$ to a coset X of $U^{\perp}$ is a balanced Boolean function, then $\sum_{x \in X} f(x) = 0$. However, one actually has the stronger property that $f(x) = 1$ has $|X|/2$ solutions for x in X. Hence, useful information is lost by reducing $|X|/2$ modulo two.

3 Divisibility properties

Suppose that one of the coordinate functions f of a primitive is saturated for an affine input space X of dimension d. This implies that the number of values x in X such that $f(x) = 1$ is divisible by 2^{d-1}. If f sums to zero, then the number of such values is only divisible by two. This raises a natural question: can we find zero sums so that the number of solutions to $f(x) = 1$ in X is actually divisible by a larger power of two?

This turns out to be common. Section 3.1 describes one instance, to be used as a running example. Section 3.2 explains how divisibility properties can be described using the geometric approach.

3.1 Example for PRESENT

In their work introducing parity sets, Boura and Canteaut [9] describe the following integral property for four rounds of the block cipher PRESENT [5]. For a set of 16 plaintexts obtained by saturating the input of the rightmost S-box, every ciphertext bit sums to zero. Using zero-correlation linear cryptanalysis, one can show that first ciphertext bit is saturated, so we focus on the second bit instead.

Figure 1 shows a histogram of the number of times the second output bit is equal to one for different choices of the key. This bit is clearly not saturated, since for some keys the number of ones differs from $8 = 16/2$. The feature of interest to us are the gaps in the histogram. Indeed, the number of ones is always a multiple of four. The analysis of Boura and Canteaut explains the divisibility by two, but integral cryptanalysis cannot prove divisibility by four.

The second bit is not the only one exhibiting divisibility by four or more; some experimental results for the other bits are summarized in Appendix F. In

the remainder of this work, we develop the necessary techniques to systematically find and prove such properties. The observation in Figure 1 will be used as a running example; a complete explanation is given in Section 5.2. Further results on PRESENT are contained in Section 7.

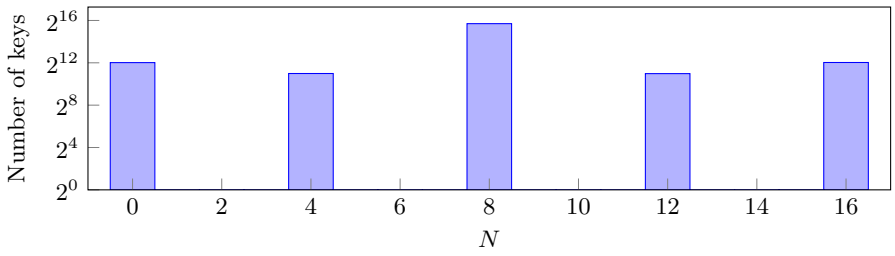


Fig. 1: Number of keys (log scale) so that the second output bit of four-round PRESENT is equal to one N times. The experiment was performed for 2^{16} keys.

3.2 Description using the geometric approach

To describe arbitrary divisibility properties, one should work over the integers rather than over $\mathbb{F}_2$. Since the rational numbers are the smallest field containing the integers, let us apply the geometric approach with $k = \mathbb{Q}$ for now.

Let X be an input set, and set $a = \delta_X$ in $\mathbb{Q}\big[\mathbb{F}_2^n\big]$. Furthermore, let b in $\mathbb{Q}^{\mathbb{F}_2^m}$ be a function that maps the relevant bit (the second, for Figure 1) to its integer value. For a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$, divisibility by 2^ν can be expressed as $b(T^{\mathsf{F}}a) = \sum_{x \in X} b(\mathsf{F}(x)) \equiv 0 \pmod{2^\nu}$.

Alternatively, divisibility by 2^ν is equivalent to $|b(T^{\mathsf{F}}\, a)|_2 \leq 2^{-\nu}$ with $|\cdot|_2$ the 2-adic absolute value on $\mathbb{Q}$. The 2-adic absolute value of a rational number $x = 2^\nu \frac{r}{s}$, with r and s odd integers, is equal to $2^{-\nu}$. One advantage of expressing divisibility using the 2-adic absolute value is that we do not need to worry about whether or not the coordinates of a and b are integers. More importantly, it suggests a strong analogy with linear cryptanalysis. Most of the time, it is not possible to evaluate cryptanalytic properties exactly. Instead, we estimate its evaluation as follows:

$$b\big(T^{\mathsf{F}}a\big) = c + \varepsilon\,,$$

where c is the estimate and ε is an error. In linear cryptanalysis, the estimate is accurate if $|\varepsilon|$ is small. For divisibility properties, the accuracy of the estimate is instead measured by $|\varepsilon|_2$. Although the discussion above focused on the case $c = 0$, there is no reason not to consider $c \neq 0$. Indeed, integral cryptanalysis can also be used to deduce constant sums modulo two and cube attacks.

Despite the analogy, the metric structure on $\mathbb{Q}$ defined by $|\cdot|_2$ is completely different from that defined by $|\cdot|$. This is because $|\cdot|_2$ satisfies the *ultrametric* triangle inequality:

$$|x + y|_2 \leq \max\big\{|x|_2, |y|_2\big\}\,.$$

The fact that this inequality is stronger than the usual triangle inequality $|x + y| \leq |x| + |y|$ plays an essential role in the theory of *ultrametric integral cryptanalysis* that is developed in the next sections. However, this is only one aspect of the theory. Another issue is the choice of basis, and this is addressed in Section 4.

Remark 3.1. As mentioned in Section 2.2, linear cryptanalysis is typically described over $\mathbb{R}$. For most applications $\mathbb{Q}$ is actually sufficient, but the geometry of $\mathbb{R}$ is nicer because it is metrically complete with respect to $|\cdot|$. The metric completion of $\mathbb{Q}$ with respect to $|\cdot|_2$ is the field of 2-adic numbers $\mathbb{Q}_2$. Hence, working with properties defined over $\mathbb{Q}_2$ would be somewhat nicer. However, for simplicity, we continue to work over $\mathbb{Q}$ throughout this paper. ▷

4 Lifting integral cryptanalysis

This section defines a suitable basis to analyze divisibility properties such as the observation from Section 3. Section 4.1 motivates the choice of basis by analogy with linear cryptanalysis. Whereas linear cryptanalysis simplifies addition in $\mathbb{F}_2^n$, the new basis simplifies multiplication *i.e.* bitwise and. The basis and its dual are constructed in Section 4.2. In Section 4.3, we express the pushforward operator of a function relative to the new basis. This leads to an analogue of correlation matrices that we call *ultrametric integral transition matrices*. The algebraic transition matrix of a function turns out to be the reduction of its ultrametric integral transition matrix modulo two. Hence, the theory we construct lifts integral cryptanalysis from $\mathbb{F}_2$ to $\mathbb{Q}$, or more generally $\mathbb{Q}_2$.

4.1 Motivation

From the viewpoint of the geometric approach, linear cryptanalysis is successful because it diagonalizes the transition matrices of translations (including key additions). This is achieved by working relative to the basis of characters of the additive group $\mathbb{F}_2^n$. However, $\mathbb{F}_2^n$ also has multiplicative structure with the bitwise and operation $\wedge$.

Although ciphers rarely use bitwise and with constants, nonlinear layers can often be expressed in terms of a small number of and gates. Hence, choosing a basis that maximally simplifies bitwise and is still of interest. Note, though, that $(\mathbb{F}_2^n, \wedge)$ is a monoid but not a group, because only $11\cdots1$ has an inverse. Nevertheless, the definition of characters can be extended to monoids.

Definition 4.1. *Let k be a field. A character of a monoid M is a homomorphism of monoids $\chi : M \to k$. That is, $\chi(1) = 1$ and $\chi(xy) = \chi(x)\chi(y)$ for all x and y in M.*

For convenience, for m in M, denote the pushforward operator of the function $x \mapsto m \cdot x$ by T^m. Theorem 4.1 shows that, like in the case of groups, the characters of M are eigenvectors of $T^{m^\vee}$. Hence, diagonalizing $T^{m^\vee}$ amounts to finding a basis of characters for the vector space of k-valued functions on M.

Theorem 4.1. *Let χ be a character of a finite monoid M. For all m in M, χ is an eigenvector of $T^{m^\vee}$ with eigenvalue $\chi(m)$.*

Proof. For all x in M, we have $(T^{m^\vee}\chi)(x) = \chi(m \cdot x) = \chi(m)\chi(x)$. That is, $T^{m^\vee}\chi = \chi(m)\,\chi$. Hence, χ is an eigenvector with eigenvalue $\chi(m)$. □

By a theorem of Dedekind [15, §44], characters are linearly independent. The question of whether or not there are enough characters to obtain a basis is answered by representation theory. This is possible for all finite *commutative inverse*[5] monoids, provided that k has characteristic zero and contains enough roots of unity [27, §5.2]. The monoid $(\mathbb{F}_2^n, \wedge)$ is commutative and inverse.

Having found the basis of characters $\chi^1, \ldots, \chi^{|M|}$, we can construct its dual basis $\chi_1, \ldots, \chi_{|M|}$ in $k[M]$. It is not difficult to see that $\chi_1, \ldots, \chi_{|M|}$ are eigenvectors of T^m. Indeed, we have that

$$T^m\chi_j = \sum_{i=1}^{|M|} \chi^i\big(T^m\chi_j\big)\,\chi_i = \sum_{i=1}^{|M|} \underbrace{\big(T^{m^\vee}\chi^i\big)(\chi_j)}_{\chi^i(m)\,\chi^i(\chi_j)}\,\chi_i = \chi^j(m)\,\chi_j\,.$$

In Section 4.2, we explicitly construct the basis of characters and its dual for the monoid $(\mathbb{F}_2^n, \wedge)$ and the field $\mathbb{Q}$.

4.2 Ultrametric integral basis

Theorem 4.2 below shows that the characters of the monoid $(\mathbb{F}_2^n, \wedge)$ are given by the lifted monomial functions $\mu^v : \mathbb{F}_2^n \to \mathbb{Q}$ with $\mu^v(x) = \tau\big(x^v\big)$ for v in $\mathbb{F}_2^n$. Here, $\tau : \mathbb{F}_2 \to \mathbb{Q}$ is the embedding[6] defined by $\tau(0) = 0$ and $\tau(1) = 1$.

Theorem 4.2. *Every character of $(\mathbb{F}_2^n, \wedge)$ is equal to μ^v for some v in $\mathbb{F}_2^n$.*

Proof. The unit of $(\mathbb{F}_2^n, \wedge)$ is equal to $11\cdots1$. From the definition of μ^v, it is clear that $\mu^v(11\cdots1) = 1$ for all v. The multiplicativity of μ^v follows from the multiplicativity of τ and of monomials over $\mathbb{F}_2$. There are no other characters, because the functions μ^v are distinct, the dimension of $\mathbb{Q}^{\mathbb{F}_2^n}$ is 2^n, and characters are linearly independent. Hence, the functions of the form μ^v form a complete set of characters. □

Like in the case of finite groups, the characters of a finite commutative inverse monoid themselves form a monoid under pointwise multiplication [27, Exercise 9.1]. This is called the dual monoid. The dual monoid of $(\mathbb{F}_2^n, \wedge)$ is essentially $(\mathbb{F}_2^n, \vee)$, where $\vee$ denotes bitwise-or. Indeed, $\mu^u\mu^v = \mu^{u\vee v}$.

Following Section 4.1, to find the eigenvectors of the pushforward operators T^m with m in $\mathbb{F}_2^n$, we construct the dual of the character basis. Theorem 4.3 shows that the dual basis consists of the vectors μ_v in $\mathbb{Q}\big[\mathbb{F}_2^n\big]$, with v in $\mathbb{F}_2^n$ and

$$\mu_v = \sum_{x \succcurlyeq v} (-1)^{\mathsf{wt}(x+v)}\,\delta_x\,,$$

[5] A monoid M is inverse if for all x in M, there exists a y such that $xyx = x$.
[6] The symbol τ refers to the fact that $\tau : \mathbb{F}_2 \to \mathbb{Q}_2$ is a Teichmüller character of $\mathbb{F}_2$.

where $\mathsf{wt}(x)$ is the Hamming weight of x and the sum is over $x \succcurlyeq v$ (bitwise order) in $\mathbb{F}_2^n$. The set of vectors μ_v will be called the *ultrametric integral basis*.

Theorem 4.3. *The ultrametric integral basis* $\{\mu_v \mid v \in \mathbb{F}_2^n\}$ *is dual to the character basis* $\{\mu^v \mid v \in \mathbb{F}_2^n\}$*, with in particular* $\mu^v(\mu_v) = 1$*.*

Proof. If $b = \sum_{x \in \mathbb{F}_2^n} b_x \, \delta_x$ is one of the dual basis vectors, then there exists a v in $\mathbb{F}_2^n$ such that $\mu^v(b) = 1$ and $\mu^u(b) = 0$ for all $u \neq v$. By linearity,

$$\mu^u(b) = \sum_{x \in \mathbb{F}_2^n} b_x \, \mu^u(x) = \sum_{x \in \mathbb{F}_2^n} b_x \, \tau(x^u) = \sum_{x \succcurlyeq u} b_x \, .$$

The sum on the right-hand side is over all elements greater than u in the partially ordered set $\mathbb{F}_2^n$. Such sums can be inverted using the Möbius inversion formula [26, Prop. 2], which is just the inclusion-exclusion principle for $\mathbb{F}_2^n$:

$$b_x = \sum_{u \succcurlyeq x} (-1)^{\mathsf{wt}(x+u)} \mu^u(b) = \begin{cases} (-1)^{\mathsf{wt}(x+v)} & \text{if } v \preccurlyeq x \, , \\ 0 & \text{else} \, . \end{cases}$$

It follows that $b = \mu_v$. □

Section 4.3 relies on the change-of-basis transformation $\mathscr{U}_n$ from the standard basis of $\mathbb{Q}\big[\mathbb{F}_2^n\big]$ to the ultrametric integral basis. The subscript n will be dropped when the context resolves the ambiguity. This transformation maps μ_v to δ_v for all v in $\mathbb{F}_2^n$. That is, $\mathscr{U} : \mathbb{Q}\big[\mathbb{F}_2^n\big] \to \mathbb{Q}\big[\mathbb{F}_2^n\big]$ is defined by extending $\mathscr{U}\,\mu_v = \delta_v$ linearly to all of $\mathbb{Q}\big[\mathbb{F}_2^n\big]$. From the definition of μ^v and μ_v, one can see that

$$\mathscr{U}_n = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{\otimes n} \quad \text{and} \quad \mathscr{U}_n^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}^{\otimes n} \, . \tag{1}$$

A similar change-of-basis transformation can be defined on $\mathbb{Q}^{\mathbb{F}_2^n}$ for the character basis, mapping μ^v to δ^v. As explained in Section 2.1, this transformation is equal to $\mathscr{U}^{-\vee}$. Lemma 4.1 gives an analytic expression for $\mathscr{U}$ and its inverse.

Lemma 4.1. *Let* a *in* $\mathbb{Q}\big[\mathbb{F}_2^n\big]$ *be a vector and let* $a^\wedge = \mathscr{U}\,a$*. It holds that*

$$a_v^\wedge = \sum_{x \succcurlyeq v} a_x \qquad \textit{and} \qquad a_x = \sum_{v \succcurlyeq x} (-1)^{\mathsf{wt}(x+v)} \, a_v^\wedge \, .$$

Proof. Immediate from (1). An alternative proof is given in Appendix A.2. □

Similar formulas can be given for the change-of-basis transformation $\mathscr{U}^{-\vee}$ from the standard basis to the basis of monoid characters. For every cryptanalytic property (a, b), we can express a in the ultrametric integral basis and b in the basis of characters. A concrete example is worked out below.

Example 4.1. The indicator of the input set for the experimental property on PRESENT from Section 3.2 is $\delta_{u\wedge\mathbb{F}_2^n}$, with $u\wedge\mathbb{F}_2^n = \{u\wedge x \mid x\in\mathbb{F}_2^n\}$. In particular, $u = 00\cdots01111$. Using Lemma 4.1, we can express $\delta_{u\wedge\mathbb{F}_2^n}$ as a linear combination of the ultrametric integral basis vectors:

$$\left[\mathscr{U}\,\delta_{u\wedge\mathbb{F}_2^n}\right]_v = \sum_{v\preccurlyeq x\preccurlyeq u} 1 = \begin{cases} 2^{\mathsf{wt}(u)-\mathsf{wt}(v)} & \text{if } v\preccurlyeq u\,,\\ 0 & \text{else}\,. \end{cases}$$

Hence,

$$\delta_{u\wedge\mathbb{F}_2^n} = \sum_{v\preccurlyeq u} 2^{\mathsf{wt}(u)-\mathsf{wt}(v)}\,\mu_v\,.$$

Note that $\delta_{u\wedge\mathbb{F}_2^n} \equiv \mu_u \pmod 2$. ▷

The change-of-basis transformation $\mathscr{U}$ is the multiplicative analogue of the Fourier transformation $\mathscr{F}$. However, because $(\mathbb{F}_2^n,\wedge)$ is not a group, there are several important differences. Although the additive characters of $\mathbb{F}_2^n$ are orthogonal, the multiplicative characters μ^v are not. If we identify $\mathbb{R}[\mathbb{F}_2^n]$ and $\mathbb{R}^{\mathbb{F}_2^n}$ using the standard inner product, then orthogonality implies that $\mathscr{F}$ and $\mathscr{F}^{-\vee}$ are the same up to multiplication by 2^n. This fails in the multiplicative case. Since $\mathscr{U}$ and $\mathscr{U}^{-\vee}$ are quite different, identifying $\mathbb{Q}\big[\mathbb{F}_2^n\big]$ and $\mathbb{Q}^{\mathbb{F}_2^n}$ would lead to confusion. Nevertheless, the fact that $\mathscr{F}$ preserves the Euclidean norm does have an analogue in terms of the norm $\|a\|_\infty = \max\left\{|a_x|_2 \mid x\in\mathbb{F}_2^n\right\}$. The proof is given in Appendix A.1.

Theorem 4.4. *The ultrametric integral change-of-basis transformation $\mathscr{U}$ is an isometry with respect to the 2-adic maximum norm $\|\cdot\|_\infty$. That is, for all a in $\mathbb{Q}\big[\mathbb{F}_2^n\big]$, $\|\mathscr{U}\,a\|_\infty = \|a\|_\infty$.*

The transformations $\mathscr{U}$ and $\mathscr{U}^{-\vee}$ are closely related to integral cryptanalysis. Indeed, the characters are monomials when reduced modulo two: $\mu^v(x) \equiv x^v \pmod 2$. Hence, applying $\mathscr{U}^{-\vee} \equiv \mathscr{M} \pmod 2$ to a Boolean function yields a vector containing the coefficients of its algebraic normal form. Furthermore, for a set X, the support of $\mathscr{U}\,\delta_X \pmod 2$ is the parity set of X. Indeed,

$$\left[\mathscr{U}\,\delta_X\right]_v \equiv \sum_{\substack{x\in X\\ x\preccurlyeq v}} 1 \equiv \sum_{x\in X} x^v \pmod 2\,.$$

Hence, $\mathscr{U} \equiv \mathscr{P} \pmod 2$ and $\mathscr{U}\,\delta_X$ generalizes the parity set of X.

4.3 Ultrametric integral transition matrices

The ultrametric integral transition matrix of a function is the matrix representation of the pushforward operator relative to the ultrametric integral basis. Alternatively, one can represent the pullback operator relative to the character basis. This results in the transpose of the ultrametric transition matrix.

Definition 4.2 (Ultrametric integral transition matrix). *For a function* $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$*, let* $A^{\mathsf{F}} = \mathscr{U}_m T^{\mathsf{F}} \mathscr{U}_n^{-1}$*. The ultrametric transition matrix of* F *is the coordinate representation of* A^{F} *with respect to the standard bases of* $\mathbb{Q}\big[\mathbb{F}_2^n\big]$ *and* $\mathbb{Q}\big[\mathbb{F}_2^m\big]$ *respectively.*

Like for correlation matrices, we will use the notation A^{F} for both the operator and its standard basis matrix representation. The notation A^{F} collides with the notation for algebraic transition matrices introduced in Section 2.3, but the following expression shows that this is reasonable. The coordinates of A^{F} are

$$A^{\mathsf{F}}_{v,u} = \delta^v\big(A^{\mathsf{F}}\,\delta_u\big) = \mu^v\big(T^{\mathsf{F}}\mu_u\big) = \sum_{x \preccurlyeq u} (-1)^{\mathsf{wt}(x+u)} \tau(\mathsf{F}^v(x))\,. \tag{2}$$

Row v of A^{F} contains the coefficients of the numerical normal form of the Boolean function F^v [12, §2.2.4]. This is the unique multivariate integer polynomial that interpolates F^v on $\{0,1\}^n \subseteq \mathbb{Z}^n$, and reduces to the algebraic normal form modulo two. This implies that the reduction of A^{F} modulo two is the algebraic transition matrix of F. Indeed, [3, Theorem 6] shows that row v of the algebraic transition matrix of F contains the coefficients of the algebraic normal form of F^v. A more elegant proof is given in Theorem B.1 in Appendix B.1.

Two different extensions of the numerical normal form to vectorial Boolean functions have been proposed in the Boolean functions literature. Carlet [12, §2.2.4] considers the numerical normal form of the indicator function of the graph of F. This is not the right notion for cryptanalysis, as it is not based on a pair of dual bases. Still motivated by interpolation, Dravie *et al.* [16] define *polynomial matrices* by a formula similar to (2). Polynomial matrices are equal to ultrametric integral transition matrices, but it is unclear if this was actually intended. Indeed, [16, Proposition 7] relates the polynomial matrix to the adjacency matrix of the graph of F when $n = m$. However, this result is incorrect and correcting it would require changing the definition of polynomial matrices.

The relation between ultrametric integral transition matrices and the numerical normal form could be of independent interest, as the motivation for the ultrametric change-of-basis is quite different (diagonalization of bitwise and). The interpretation in terms of interpolating polynomials over the integers does not play a role in this paper.

Example 4.2 (Translation). Let $\mathsf{F} : \mathbb{F}_2 \to \mathbb{F}_2$ be defined by $\mathsf{F}(x) = x + k$, for some constant k in $\mathbb{F}_2$. The ultrametric integral transition matrix of F is

$$A^{\mathsf{F}} = \begin{bmatrix} 1 & 0 \\ \tau(k) & (-1)^k \end{bmatrix}$$

If $k = 0$, then this is just the identity matrix. ▷

The following properties are immediate consequences of the properties of transition matrices (Theorem 2.1, as they are invariant under change of basis.

Corollary 4.1. *The ultrametric transition matrix* A^{F} *of* $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *has the following properties:*

(1) If $\mathsf{F}(x_1 \| \cdots \| x_l) = \mathsf{F}_1(x_1) \| \cdots \| \mathsf{F}_l(x_l)$*, then* $A^{\mathsf{F}} = \bigotimes_{i=1}^{l} A^{\mathsf{F}_i}$.

(2) If $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$*, then* $A^{\mathsf{F}} = A^{\mathsf{F}_r} \cdots A^{\mathsf{F}_2} A^{\mathsf{F}_1}$.

Proof. Both of these properties follow from Theorem 2.1. For the proof of property (1), we use the fact that $\mathscr{U}_n = \mathscr{U}_1^{\otimes n}$. Indeed,

$$A^{\mathsf{F}} = \Big(\bigotimes_{i=1}^{l} \mathscr{U} \Big) \Big(\bigotimes_{i=1}^{l} T^{\mathsf{F}_i} \Big) \Big(\bigotimes_{i=1}^{l} \mathscr{U}^{-1} \Big) = \bigotimes_{i=1}^{l} \mathscr{U}\, T^{\mathsf{F}_i}\, \mathscr{U}^{-1} = \bigotimes_{i=1}^{l} A^{\mathsf{F}_i} .$$

For the proof of property (2), we use Theorem 2.1: $T^{\mathsf{F}} = T^{\mathsf{F}_r} \cdots T^{\mathsf{F}_2} T^{\mathsf{F}_1}$. Hence,

$$\mathscr{U} T^{\mathsf{F}} \mathscr{U}^{-1} = \big(\mathscr{U} T^{\mathsf{F}_r} \mathscr{U}^{-1} \big) \cdots \big(\mathscr{U} T^{\mathsf{F}_2} \mathscr{U}^{-1} \big) \big(\mathscr{U} T^{\mathsf{F}_1} \mathscr{U}^{-1} \big) .$$

The result follows by substituting $A^{\mathsf{F}_i} = \mathscr{U} T^{\mathsf{F}_i} \mathscr{U}^{-1}$. □

Example 4.3 (Translation). Let $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $\mathsf{F}(x) = x + k$, for some constant k in $\mathbb{F}_2^n$. If k_i denotes the i^{th} bit of k, then F can be expressed as

$$\mathsf{F}(x_1 \| \cdots \| x_n) = \mathsf{F}_1(x_1) \| \cdots \| \mathsf{F}_n(x_n) ,$$

where $\mathsf{F}_i(x_i) = x_i + k_i$ is the function that was discussed in Example 4.2. Hence, by Corollary 4.1 (1),

$$A^{\mathsf{F}} = \bigotimes_{i=1}^{n} A^{\mathsf{F}_i} = \bigotimes_{i=1}^{n} \begin{bmatrix} 1 & 0 \\ \tau(k_i) & (-1)^{k_i} \end{bmatrix} .$$

More explicitly, A^{F} is a lower-triangular $2^n \times 2^n$ matrix with coordinate in row v and column $u \preccurlyeq v$ equal to $(-1)^{u^{\mathsf{T}} k}\, \tau(k^{u+v})$, and zero elsewhere. ▷

The following properties are specific to ultrametric transition matrices.

Theorem 4.5. *The ultrametric transition matrix* A^{F} *of* $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *has the following properties:*

(1) If F *is a bijection, then* A^{F} *is an isometry.*

(2) If F *is a monoid homomorphism, then* $A^{\mathsf{F}}_{v,u} = 1$ *if* $\mu^v \circ \mathsf{F} = \mu^u$ *and 0 else.*

(3) If $\mathsf{F}(x) = m \wedge x$ *with* m *in* $\mathbb{F}_2^n$*, then* A^{F} *is diagonal with* $A^{\mathsf{F}}_{u,u} = \mu_u(m)$.

Proof. For the first property, note that if F is a bijection, then T^{F} is an isometry. By Lemma 4.1, the ultrametric change-of-basis transformation is an isometry. Since a composition of isometries is again an isometry, A^{F} is an isometry.

If F is a monoid homomorphism, then $\mu^v \circ \mathsf{F}$ is a character of $(\mathbb{F}_2^n, \wedge)$. If $\mu^w = \mu^v \circ \mathsf{F}$, then $A^{\mathsf{F}}_{v,u} = \mu^v(T^{\mathsf{F}} \mu_u) = \mu^w(\mu_u)$. The result follows from the duality between μ_u and μ^w.

The third property is true by construction of the ultrametric change-of-basis transformation, Indeed, $A^{\mathsf{F}}_{v,u} = \mu^v(T^{\mathsf{F}} \mu_u) = \mu_u(m)\, \mu^v(\mu_u)$ since μ_u is an eigenvector of T^{F}. The result follows from the duality between μ_u and μ^v. □

Example 4.4. The function $\mathsf{and} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ defined by $\mathsf{and}(x \| y) = x \wedge y$ is a monoid homomorphism. It follows from Theorem 4.5 (2) that

$$A^{\mathsf{and}}_{w,u\|v} = \begin{cases} 1 & \text{if } w = u = v\,, \\ 0 & \text{else}\,. \end{cases}$$

The fact that only 2^n coordinates of this matrix are non-zero is no coincidence. The expression above is identical to that for the correlation matrix of the xor function. That is, $A^{\mathsf{and}} = C^{\mathsf{xor}}$. This is by construction, since ultrametric integral cryptanalysis is the multiplicative analogue of linear cryptanalysis. ▷

By the results of [3], algebraic transition matrices lead to a theory of trails for integral cryptanalysis (algebraic, division or monomial trails). In Section 5, we show how ultrametric integral transition matrices lead to a similar theory that reduces to ordinary integral cryptanalysis modulo two.

5 Ultrametric integral trails

Let $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. A pair of exponents $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ will be called an *ultrametric integral approximation* for F. The correlation of an ultrametric integral approximation is defined as

$$A^{\mathsf{F}}_{v,u} = \mu^v\big(T^{\mathsf{F}}\,\mu_u\big)\,.$$

In other words, there is a one-to-one correspondence between ultrametric integral approximations (u, v) and properties (μ_u, μ^v) defined by basis vectors. As shown in Section 4.2, the evaluation of every property can in principle be expressed as a linear combination of the evaluations of these properties. Hence, it is sufficient to compute the correlations of ultrametric integral approximations. If F is a composition of functions $\mathsf{F}_1, \ldots, \mathsf{F}_r$ with enough structure so that the coordinates of the matrices $A^{\mathsf{F}_1}, \ldots, A^{\mathsf{F}_r}$ can be determined efficiently, then correlations can be estimated (in the 2-adic sense) using *ultrametric integral trails*.

Definition 5.1. *An ultrametric integral trail for a function* $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$ *is a sequence* $u_1, \ldots, u_{r+1}$ *of exponents. The correlation of this trail is defined as* $\prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i}$.

5.1 Dominant trail approximation

In Corollary 4.1 (2), it was shown that $A^{\mathsf{F}} = A^{\mathsf{F}_r} \cdots A^{\mathsf{F}_2} A^{\mathsf{F}_1}$. Writing out this matrix product in terms of coordinates leads to the expression

$$A^{\mathsf{F}}_{u_{r+1},u_1} = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i}\,.$$

That is, the correlation of the ultrametric integral approximation (u_1, u_{r+1}) is equal to the sum of the correlations of all trails with input and output exponent

u_1 and u_{r+1} respectively. However, this result will not be used in practice because the number of trails is generally too large. Instead, similar to Theorem 2.2 in the case of linear cryptanalysis, we rely on a set of *dominant trails* to estimate the correlation.

Theorem 5.1 (Dominant trails, *cf.* Theorem 2.2). *Let* $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$. *For all subsets* Λ *of the set* Ω *of all trails from* u_1 *to* u_{r+1},

$$\left| A^{\mathsf{F}}_{u_{r+1},u_1} - \sum_{u \in \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i} \right|_2 = \left| \sum_{u \in \Omega \setminus \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i} \right|_2 \leq \max_{u \in \Omega \setminus \Lambda} \left| \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i} \right|_2 ,$$

where $u = (u_1, u_2, \ldots, u_{r+1})$.

Proof. The result follows from the following decomposition:

$$A^{\mathsf{F}}_{u_{r+1},u_1} = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i} = \sum_{u \in \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i} + \sum_{u \in \Omega \setminus \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i} .$$

In particular, the equality follows by rearranging the terms and taking the absolute value of both sides of the equality. The inequality follows from the ultrametric triangle inequality. □

Theorems 2.2 and 5.1 are conceptually the same, but Theorem 5.1 is based on the 2-adic rather than the ordinary absolute value function. This difference has far-reaching implications. In particular, to upper bound the error term in Theorem 5.1, it is sufficient to bound the 2-adic absolute value of the correlation of every trails in $\Omega \setminus \Lambda$. This reflects the fact that, in $\mathbb{Q}_2$, the sum of many small numbers is always small. In contrast, Theorem 2.2 is used heuristically in linear cryptanalysis, because it is difficult to upper bound the error term. Indeed, in $\mathbb{R}$, the sum of many small numbers may be large.

In practice, we will use Theorem 5.1 as follows. If the 2-adic absolute value of the correlations of all trails in $\Omega \setminus \Lambda$ is at most 2^{-t}, then

$$A^{\mathsf{F}}_{u_{r+1},u_1} \equiv \sum_{u \in \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1},u_i} \pmod{2^t} .$$

If $\Lambda = \emptyset$, then this shows that $A^{\mathsf{F}}_{u_{r+1},u_1}$ is divisible by 2^t. This corresponds to an *approximate* zero-correlation approximation.

5.2 Example

As a first example of ultrametric integral trails, we explain and prove the property that we observed in Section 3.1. Throughout the analysis, we ignore the first S-box layer. Indeed, up to constant additions that can be combined with the key addition of the next round, the input set is invariant under the S-box layer. Hence, let F denote three rounds of PRESENT without the final bit-permutation,

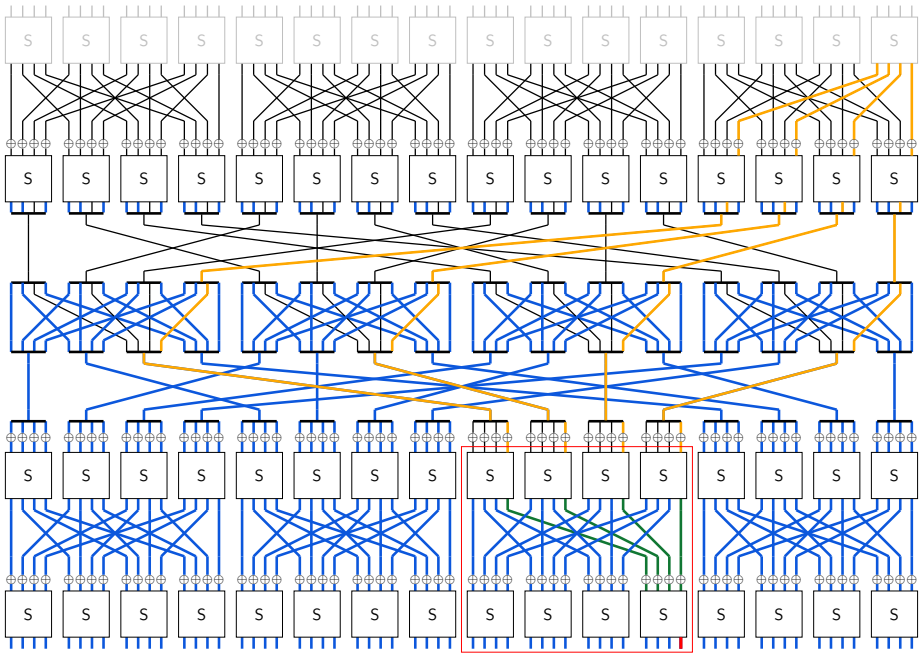


Fig. 2: Miss-in-the-middle using ultrametric integral trails for PRESENT.

as shown in Figure 2. As explained in Section 3.2, the observation corresponds to $\mu^v\big(T^{\mathsf{F}}\,\delta_X\big) \equiv 0 \pmod 4$, where the input set X consists of all values $\mathtt{00}\cdots\mathtt{0}\|x$ with x in $\mathbb{F}_2^4$, and the output exponent v is equal to $\mathtt{0000\ 0000\ 0001\ 0000}$ in hexadecimal notation. Equivalently, $\big|\mu^v\big(T^{\mathsf{F}}\,\delta_X\big)\big|_2 \leq 1/4$.

The vector δ_X is not equal to one of the basis functions μ_u. Nevertheless, the property can be analyzed using ultrametric integral trails by writing δ_X as a linear combination of the ultrametric integral basis functions. In particular, it was shown in Example 4.1 that

$$\delta_X = \sum_{u \in \mathbb{F}_2^4} 2^{4-\mathsf{wt}(u)}\,\mu_{\mathtt{00}\cdots\mathtt{0}\|u}\,.$$

Hence, the evaluation $\mu^v(T^{\mathsf{F}}\delta_X)$ of the property (δ_X, μ^v) is equal to

$$\mu^v\big(T^{\mathsf{F}}\,\delta_X\big) = \sum_{u \in \mathbb{F}_2^4} 2^{4-\mathsf{wt}(u)}\,\mu^v\big(T^{\mathsf{F}}\mu_{\mathtt{00}\cdots\mathtt{0}\|u}\big) = \sum_{u \in \mathbb{F}_2^4} 2^{4-\mathsf{wt}(u)}\,A^{\mathsf{F}}_{v,\mathtt{00}\cdots\mathtt{0}\|u}\,.$$

In particular, the 2-adic absolute value is bounded by

$$\big|\mu^v\big(T^{\mathsf{F}}\,\delta_X\big)\big|_2 \leq \max_{u \in \mathbb{F}_2^4} 2^{\mathsf{wt}(u)-4}\big|A^{\mathsf{F}}_{v,\mathtt{00}\cdots\mathtt{0}\|u}\big|_2\,.$$

Hence, it suffices to show that $A^{\mathsf{F}}_{v,\mathtt{0}\cdots\mathtt{0}\|u}$ is divisible by two if $\mathsf{wt}(u) = 3$ and by four if $\mathsf{wt}(u) = 4$. To prove this, we use Theorem 5.1 with $\Lambda = \emptyset$.

Figure 2 illustrates the structure of ultrametric integral trails with nonzero correlation. As explained below, the colors correspond to conditions on exponent bits.

The blue lines in Figure 2 correspond to exponent bits that are equal to zero. The orange lines correspond to a group of four bits that must have weight equal to $\mathsf{wt}(u)$. The analysis is based on a variant of the miss-in-the-middle principle: we propagate the orange set forward and the blue set backwards, in order to rule out trails with high absolute correlation.

The propagation of exponents through a bit-permutation P is straightforward. Since bit-permutations are monoid homomorphisms, Theorem 4.5 (2) shows that $A^{\mathsf{P}}_{v,u} \neq 0$ if and only if $v = \mathsf{P}(u)$. For $\mathsf{K}(x) = x + k$, it was shown in Example 4.3 that $A^{\mathsf{K}}_{v,u} \neq 0$ for at least one key k if and only if $u \preccurlyeq v$. For the S-box layer, we need Theorem 4.5 (2) and the ultrametric integral transition matrix of the PRESENT S-box:

$$A^{\mathsf{S}} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & -2 & -1 & 2 & 1 & -2 & 0 & 0 & -2 & 4 & 2 & -4 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & -1 & -1 & 1 & 0 & 2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 1 & -1 & 0 & -1 & -1 & 2 & 0 & 0 \\
1 & 0 & 0 & -1 & -1 & 0 & 0 & 2 & -1 & 1 & 1 & -1 & 2 & -1 & -2 & 0 \\
0 & 1 & 0 & -1 & 0 & -1 & 0 & 2 & 0 & -1 & 1 & 0 & 0 & 2 & -1 & -2 \\
0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
1 & -1 & -1 & 2 & 0 & 0 & 1 & -1 & -1 & 2 & 2 & -3 & 0 & -1 & -2 & 2 \\
0 & 0 & 0 & 1 & 1 & -1 & -1 & 1 & 0 & 0 & 1 & -2 & -1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & -2 & 0 & 1 & 1 & -3 & 0 & -1 & -2 & 4 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & -2 & 0 & 0 & -1 & 2 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & 0 & -1 & 2 & 2 & -3 & 1 & -2 & -2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & -1 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -2 & 0 & -1 & -1 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1
\end{bmatrix}.$$

The row that we use in the analysis is indicated in red.

Backward propagation. Since $A^{\mathsf{S}}_{0,w} \neq 0$ if and only if $w = 0$, the bits of the exponent before the last S-box layer are zero except for bits 16 up to 19. Nevertheless, bits 16-19 are not arbitrary. In particular, $|A^{\mathsf{S}}_{1,\mathtt{f}}|_2 = 1/4$ and $|A^{\mathsf{S}}_{1,w}|_2 \leq 1/2$ if $\mathsf{wt}(w) = 3$. In Figure 2, these four bits are indicated in green.

If a bit of the output exponent for the key addition operation is zero, then the corresponding bit of the input exponent must be zero as well. Propagation through the bit-permutation layer is straightforward. Hence, at the input of the third S-box layer, all exponent bits except 16-19 must be zero. Propagating this information through the middle bit-permutation, we find that every nibble of the exponent at the output of the second S-box layer must be 0 or 2.

Forward propagation. Like in the backward direction, propagation through the first bit-permutation is straightforward. For the key-addition layer, for every bit of the input exponent equal to one, the corresponding bit of the output exponent is also equal to one. It was shown above that the output exponents on the S-boxes are either 0 or 2. Hence, since the output exponent must be nonzero if the input exponent is nonzero, the four nonzero output bits of the rightmost superbox must have weight $\mathsf{wt}(u)$. Propagating this information through the bit-permutation is straightforward.

Conclusion. To upper bound the correlation, we focus on the framed superbox in Figure 2. Since the weight of the set of orange-colored exponent bits is $\mathsf{wt}(u)$, at least three of the first layer of four S-boxes are active. If all four S-boxes are active, then the absolute correlation is at most $1/4$. If only three S-boxes are active, then the absolute correlation is at most $1/2$. That is, the correlation is divisible by two if $\mathsf{wt}(u) = 3$ and divisible by four if $\mathsf{wt}(u) = 4$. This is what we set out to prove.

5.3 Trail enumeration

A manual analysis of trails like in Section 5.2 is instructive, but it becomes tedious for larger problems. Hence, like in linear and ordinary integral cryptanalysis, we will use automated methods to find trails. This will be discussed in more detail in Sections 7 and 8.

Theorem 5.1 shows that it is sufficient to upper bound the absolute correlation of every non-dominant trail, but this does not necessarily result in the best possible bound. Indeed, the absolute value of the sum of two correlations can be strictly less than the sum of their absolute values. To take into account these 'cancellations', one can try to enumerate all trails and compute

$$\left| \sum_{u \in \Omega \setminus \Lambda} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1}, u_i} \right|_2 .$$

In practice, this is often infeasible. Nevertheless, in Section 7, we will encounter several properties that we can only explain using trail enumeration.

The distinction between bounding correlations of individual trails and trail enumeration also exists in ordinary integral cryptanalysis. This can be made precise using algebraic trails. As explained in Section 4.3, the algebraic transition matrix of F is the reduction of A^{F} modulo two. Hence, every ultrametric integral trail reduces to an algebraic trail with correlation in $\mathbb{F}_2$. The method of bounding trail correlations then amounts to showing that all algebraic trails in $\Omega \setminus \Lambda$ have correlation zero. Bit-based division property and parity sets both follow this approach. The three-subset division property without unknown subset and monomial prediction additionally take into account the parity of the number of trails with nonzero correlation. This corresponds to trail enumeration. An overview of different methods can be found in [3, §4.1] and in the survey [19].

6 Properties of ultrametric integral transition matrices

The purpose of this section is to introduce additional properties of ultrametric integral transition matrices. Some of these properties are mainly of theoretical interest, others will play an important role in Sections 7 and 8.

6.1 Computation

The ultrametric integral transition matrix of a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be computed in $\mathcal{O}((n+m)2^{n+m})$ time. This is the same time-complexity as for

computing the correlation matrix of F, and the underlying algorithm is analogous. In particular, it exploits the fact that $\mathscr{U}_n = \mathscr{U}_1^{\otimes n}$ – see (1) on page 12. This tensor product structure leads to an $\mathcal{O}(n2^n)$ time algorithm for computing $\mathscr{U}_n\, a$ and $\mathscr{U}_n^{-1}\, a$, for a in $\mathbb{Q}[\mathbb{F}_2^n]$. Since $A^{\mathsf{F}} = \mathscr{U}_n\, T^{\mathsf{F}} \mathscr{U}_n^{-1}$, applying this algorithm to the rows and columns of T^{F} leads to an $\mathcal{O}((n+m)2^{n+m})$ time algorithm for computing A^{F}. A reference implementation is provided in the example in our code repository.

6.2 Linear functions

Since the nonlinear functions used in most primitives only depend on a small number of state bits, it is often the linear functions that pose most difficulties in (ultrametric) integral cryptanalysis.

If the linear layer is a bit-permutation, its ultrametric integral transition matrix is easy to compute. Indeed, bit-permutations are monoid isomorphisms, so Theorem 4.5 (2) can be used. For most other linear functions, there is no simple formula. However, every linear function can be decomposed as a network of forking (or 'copy') and addition (or 'xor') operations. For these two operations, simple exponent propagation rules can be obtained – they are illustrated in Figure 3 and discussed below.

(a) Copy. (b) Xor.

Fig. 3: Propagation rules for copy and xor operations.

Since copy and xor operations are bitwise operations, their ultrametric integral transition matrix can be computed using Corollary 4.1 (1). As the derivation is essentially just a calculation, it is given in Appendix B.2. The copy operation is the function $\mathsf{copy} : \mathbb{F}_2^n \to \mathbb{F}_2^{2n}$ with $\mathsf{copy}(x) = x \| x$. The coordinates of its ultrametric integral transition matrix are

$$A^{\mathsf{copy}}_{u\|v,w} = \begin{cases} 1 & \text{if } w = u \vee v\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

This result implies the following propagation rule: if the output exponent is $u\|v$, then the input exponent must be $u \vee v$. In this case, the correlation is one. This rule is illustrated in Figure 3a.

The xor operation is the function $\mathsf{xor}_n : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ defined by $\mathsf{xor}(x\|y) = x+y$. The coordinates of its ultrametric integral transition matrix are

$$A^{\mathsf{xor}}_{w,u\|v} = \begin{cases} (-2)^{\mathsf{wt}(u\wedge v)} & \text{if } w = u \vee v\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

This result can be summarized as the propagation rule that an input exponent $u \| v$ goes to output exponent $u \vee v$ with correlation $(-2)^{\mathsf{wt}(u \wedge v)}$. This is illustrated in Figure 3b.

It is worth mentioning that there are downsides to decomposing linear functions into copy and xor operations. Copy operations often introduce many high-correlation trails, reducing the accuracy of the principle of dominant trails and making trail enumeration more difficult. Hence, whenever dedicated formulas are available, they are usually preferable.

Finally, the propagation rules in Figure 3 imply an interesting theoretical result: if $\mathsf{L} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a linear function, then $|A^{\mathsf{L}}_{v,u}|_2 \leq 2^{\mathsf{wt}(v)-\mathsf{wt}(u)}$. Every output bit of L can be written as a network of copy and xor operations. For a copy operation, the weight of the output exponent is always greater than the weight of the input exponent. For an xor operation, the output exponent weight *can* be lower than the input exponent weight, but if the weight decreases by Δ then the correlation is $(-2)^{\Delta}$. Hence, the correlation of an approximation (u, v) over L must be divisible by $2^{\mathsf{wt}(u)-\mathsf{wt}(v)}$. In Section 6.3, we generalize this result to nonlinear functions.

6.3 Low-degree functions

Recall from Example 4.4 that the propagation rule for the $\mathsf{and} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ function is identical to that of xor in linear cryptanalysis. This extends to the bitwise and of more than two variables, which is still a monoid homomorphism. Based on this property, the following result shows that the ultrametric integral transition matrix of a function with low algebraic degree is sparse.

Theorem 6.1. *If $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a function with algebraic degree d, then*

$$-\log_2 \left|A^{\mathsf{F}}_{v,u}\right|_2 \geq \left\lceil \frac{\mathsf{wt}(u)}{d} \right\rceil - \mathsf{wt}(v)\,.$$

Equivalently, $\left|A^{\mathsf{F}}_{v,u}\right|_2 \geq 2^{-\nu}$ only if $\mathsf{wt}(v) \geq \lceil \mathsf{wt}(u)/d \rceil - \nu$.

Proof. The result can be proven by a somewhat technical calculation, for example using Equation (2) and splitting up the sum according to the monomials that occur in F^v by using the additive characters of $\mathbb{F}_2$. Instead, we give a more insightful 'cryptanalytic' proof based on ultrametric integral trails.

Every degree d function can be represented as a three-layer circuit, consisting of a layer of copy operations, a layer of and gates with d or fewer inputs each, and a layer of xor operations. This is illustrated in Figure 4.

Figure 4 only depicts one coordinate of F, but in general we have to take into account the coordinate functions corresponding to all $\mathsf{wt}(v)$ nonzero bits in the output exponent v.

If $|A^{\mathsf{F}}_{v,u}|_2 \geq 2^{-\nu}$, then there must exist an ultrametric integral trail with correlation divisible by a power of two less than or equal to 2^{ν}. By the propagation rules for xor operations from Section 6.2, this implies that the weight of the exponent at the output of the and-layer is at most $\mathsf{wt}(v) + \nu$. An and operation

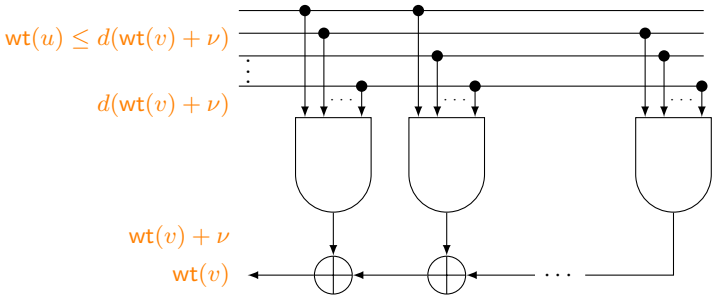


Fig. 4: One of the coordinates of a function of degree d.

with d inputs is a monoid homomorphism from $\mathbb{F}_2^d$ to $\mathbb{F}_2$. By Theorem 4.5 (2), the input exponent is $00\cdots0$ if the output exponent is zero and $11\cdots1$ if it is one. Hence, using the properties of bricklayer maps, the weight of the exponent at the input of the and-layer is at most $d(\mathsf{wt}(v)+\nu)$. As shown in Section 2.2, the weight of the output exponent for a copy is always greater than the weight of its input exponent. Hence,

$$\mathsf{wt}(u) \le d(\mathsf{wt}(v)+\nu)\,.$$

It follows that $\mathsf{wt}(v) \ge \lceil \mathsf{wt}(u)/d \rceil - \nu$. □

The main propagation rule for the word-based division property [29, Proposition 1] is a special case of Theorem 6.1. This rule states that if a multiset X has the division property of order k, then $\mathsf{F}(X)$ has the division property of order $\lceil k/d \rceil$. Indeed, by Theorem 6.1, $|A^{\mathsf{F}}_{v,u}|_2 = 1$ only if $\mathsf{wt}(v) \ge \lceil \mathsf{wt}(u)/d \rceil$. Recall that X has the division property of order k if and only if $[\mathscr{U}\,\delta_X]_u$ is divisible by two for all u with $\mathsf{wt}(u) < k$.

Theorem 6.1 is mostly of theoretical interest. To obtain our results in Sections 7 and 8, more fine-grained models of nonlinear functions are necessary. Nevertheless, Theorem 6.1 has some interesting theoretical applications. For example, it implies the Ax-Katz theorem over $\mathbb{F}_2$.

Corollary 6.1 (Ax-Katz [22]). *The number of solutions of a system of m equations of degree d in n variables is divisible by $2^{\lceil n/d \rceil - m}$.*

Proof. The system of equations can be written as $\mathsf{F}(x) = 11\cdots1$, where $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a function of degree d. That is,

$$\mu^{11\cdots1}\big(T^{\mathsf{F}}\delta_{\mathbb{F}_2^n}\big) = \delta^{11\cdots1}\big(A^{\mathsf{F}}\,\mathscr{U}\,\delta_{\mathbb{F}_2^n}\big) = \sum_{u\in\mathbb{F}_2^n} 2^{n-\mathsf{wt}(u)} A^{\mathsf{F}}_{11\cdots1,u}\,.$$

By Theorem 6.1, the right-hand side is divisible by 2^ν, where

$$\nu \ge \min_{u\in\mathbb{F}_2^n} n - \mathsf{wt}(u) + \left\lceil \frac{\mathsf{wt}(u)}{d} \right\rceil - \mathsf{wt}(11\cdots1) \ge \left\lceil \frac{n}{d} \right\rceil - m\,.$$

For the second inequality, we use that the minimum is reached for $\mathsf{wt}(u) = n$. □

There is a variant of Corollary 6.1 that takes into account the degrees of the individual equations. This result is given in Corollary B.1 of Appendix B. The proof uses a variant of Theorem 6.1.

Finally, it is worth mentioning that Corollary 6.1 implies a well-known weight divisibility property of Reed-Muller codes. McWilliams and Sloane deduce this result from McEliece's theorem [25, Corollary 13].

Corollary 6.2. *The weights of codewords in the Reed-Muller code $\mathscr{R}(d,n)$ are divisible by $2^{\lceil n/d \rceil - 1}$.*

Proof. The codewords in $\mathscr{R}(d,n)$ are truth-tables of Boolean functions of degree d. Hence, the weight of a codeword is the number of solutions of an equation of degree d in n variables. By Corollary 6.1, this is divisible by $2^{\lceil n/d \rceil - 1}$. □

6.4 Relation with correlation matrices

A number of results in the Boolean functions literature relate the algebraic degree of a function to the divisibility of the coordinates of its correlation matrix (equivalently, Walsh-Hadamard transformation). Theorem 6.2 generalizes these results in terms of the ultrametric integral transition matrix. In doing so, we hope to clarify why such results are to be expected.

The correlation matrix C^{F} and the ultrametric integral transition matrix A^{F} of a function are both matrix representations of the pushforward operator T^{F}. In particular, C^{F} can be expressed in terms of A^{F} (and conversely):

$$C^{\mathsf{F}} = \mathscr{F}\, T^{\mathsf{F}} \mathscr{F}^{-1} = \big(\mathscr{F}\, \mathscr{U}^{-1}\big) A^{\mathsf{F}} \big(\mathscr{F}\, \mathscr{U}^{-1}\big)^{-1}.$$

Since the reduction of A^{F} modulo two is the algebraic transition matrix of F, it is not surprising that the divisibility of coordinates of C^{F} can be related to the algebraic degree. However, in general, looking at the divisibility of the coordinates of A^{F} provides finer results. The following results make this precise.

Lemma 6.1. *For the matrix $\mathscr{T} = \mathscr{F}\mathscr{U}^{-1}$ and its inverse $\mathscr{T}^{-1}$, we have*

$$\mathscr{T}_{v,u} = \begin{cases} (-2)^{\mathsf{wt}(u)} & \text{if } u \preccurlyeq v\,, \\ 0 & \text{else}, \end{cases} \quad \text{and} \quad \mathscr{T}^{-1}_{v,u} = \begin{cases} (-1)^{\mathsf{wt}(u)}\, 2^{-\mathsf{wt}(v)} & \text{if } u \preccurlyeq v\,, \\ 0 & \text{else}. \end{cases}$$

Proof. The matrix $\mathscr{T} = \mathscr{F}\mathscr{U}^{-1}$ and its inverse are given by:

$$\mathscr{T} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{\otimes n} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}^{\otimes n} = \begin{bmatrix} 1 & 0 \\ 1 & -2 \end{bmatrix}^{\otimes n} \text{ and } \mathscr{T}^{-1} = \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix}^{\otimes n}.$$

That is, $\mathscr{T}_{v,u}$ is equal to $(-2)^{\mathsf{wt}(u)}$ if $u \preccurlyeq v$ and zero otherwise. For the inverse, note that $\mathscr{T}^{-1}_{v,u}$ is equal to $(-1)^{\mathsf{wt}(u)}\, 2^{-\mathsf{wt}(v)}$ if $u \preccurlyeq v$ and zero otherwise. □

Together with the relation between A^{F} and C^{F}, Lemma 6.1 implies the following two bounds. As shown below, these bounds refine existing results about the divisibility of correlations. A comparable but different result is given for the numerical normal form of the graph indicator of a function by Carlet [12, §2.3].

Theorem 6.2. *Let* $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *be a function with correlation matrix* C^{F} *and ultrametric integral transition matrix* A^{F}*. For all* u *in* $\mathbb{F}_2^n$ *and* v *in* $\mathbb{F}_2^m$*,*

$$\left|C^{\mathsf{F}}_{v,u}\right|_2 \le \max_{\substack{s \succcurlyeq u \\ t \preccurlyeq v}} 2^{\mathsf{wt}(s)-\mathsf{wt}(t)} \left|A^{\mathsf{F}}_{t,s}\right|_2 \quad \textit{and} \quad \left|A^{\mathsf{F}}_{v,u}\right|_2 \le \max_{\substack{s \succcurlyeq u \\ t \preccurlyeq v}} 2^{\mathsf{wt}(v)-\mathsf{wt}(u)} \left|C^{\mathsf{F}}_{t,s}\right|_2 .$$

Proof. For brevity, let $\mathscr{T} = \mathscr{F}\mathscr{U}^{-1}$. By the ultrametric triangle inequality,

$$\left|C^{\mathsf{F}}_{v,u}\right|_2 = \left|\left(\mathscr{T}\, A^{\mathsf{F}}\, \mathscr{T}^{-1}\right)_{v,u}\right|_2 \le \max_{s,t} \left|\mathscr{T}_{v,t}\right|_2 \left|A^{\mathsf{F}}_{t,s}\right|_2 \left|\mathscr{T}^{-1}_{s,u}\right|_2 .$$

The result then follows from Lemma 6.1. Similarly, we have

$$\left|A^{\mathsf{F}}_{v,u}\right|_2 = \left|\left(\mathscr{T}^{-1}\, C^{\mathsf{F}}\, \mathscr{T}\right)_{v,u}\right|_2 \le \max_{s,t} \left|\mathscr{T}^{-1}_{v,t}\right|_2 \left|C^{\mathsf{F}}_{t,s}\right|_2 \left|\mathscr{T}_{s,u}\right|_2 .$$

Again, the result follows from Lemma 6.1. □

Theorem 6.2 implies the well-known result that $\left|C^{\mathsf{F}}_{v,u}\right|_2 \le 2^{n-\lceil n/d \rceil}$ if F is of degree d. The details are worked out in Appendix B.4. More interestingly, Theorem 6.2 also yields the following converse result. A weaker version of Corollary 6.3 (without the condition $\mathsf{wt}(u) \ge d+1$) was proven by Carlet [11, Lemma 3] and used by Canteaut and Videau [10, Proposition 2] at Eurocrypt 2002 and by Boura and Canteaut in 2013 [8] to upper bound the degree of a composition of two functions[7].

Corollary 6.3. *If* $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *is a function with* $\left|C^{\mathsf{F}}_{v,u}\right|_2 \le 2^{d-1}$ *for all* u *and* v *with* $\mathsf{wt}(u) \ge d+1$ *and* $\mathsf{wt}(v) = 1$*, then* F *has algebraic degree at most* d*.*

Proof. To show that F has degree at most d, it suffices to prove that $|A^{\mathsf{F}}_{v,u}|_2 \le 1/2$ for all u and v with $\mathsf{wt}(u) \ge d+1$ and $\mathsf{wt}(v) = 1$. This readily follows from the second inequality of Theorem 6.2:

$$\left|A^{\mathsf{F}}_{v,u}\right|_2 \le 2^{\mathsf{wt}(v)-\mathsf{wt}(u)}\, 2^{d-1} \le 2^d\, 2^{d-1} = 1/2 ,$$

where we have used $\left|C^{\mathsf{F}}_{t,s}\right|_2 \le 2^{d-1}$ for all t and s with $\mathsf{wt}(t) \le \mathsf{wt}(v) = 1$ and $\mathsf{wt}(s) \ge \mathsf{wt}(u) \ge d+1$ □

Another application of Theorem 6.2 is discussed in Section 7.3.

7 Application to PRESENT

In this section, we apply ultrametric integral cryptanalysis to PRESENT. The analysis is automated using off-the-shelf SAT solvers. The choice of PRESENT is didactical. Indeed, integral attacks on PRESENT cover a small number of rounds compared to other methods such as linear cryptanalysis. Nevertheless, PRESENT has often served as a test-case for new ideas in integral cryptanalysis such as the division property [29, §5.3] and parity sets [9, §6].

[7] It is now understood that these bounds can be proven using integral cryptanalysis.

Section 7.1 briefly describes how to automate the analysis of ultrametric integral trails. The distinguishers found by Boura and Canteaut [9] are revisited in Section 7.2. Section 7.3 takes a closer look at the zero-correlation linear cryptanalysis of PRESENT. Finally, Section 7.4 shows that ultrametric integral cryptanalysis can reduce the time- and data-complexity of key-recovery attacks.

7.1 Modelling

To automate the analysis of ultrametric trails, we construct a formula in conjunctive normal form so that each satisfying assignment corresponds to a trail with absolute correlation $2^{-\nu}$. The variables in this formula are the exponents of the ultrametric integral trail, and some bookkeeping variables to keep track of the correlation. Given this formula, a SAT solver can be used to check for the existence of trails, or to enumerate them.

The construction of the conjunctive normal form formula follows from the discussion in Sections 5 and 6. For the S-boxes, a minimal conjunctive normal form representation of the constraints is computed using the implementation from [3], which follows the method proposed by Udovenko [31]. Additional details can be found in Appendix C.1.

The analysis of trails is based on the dominant trail approximation in Theorem 5.1. Initially, an upper bound on the absolute correlation of all trails in $\Omega \setminus \Lambda$ is determined. If additional accuracy (*i.e.* higher divisibility when $\Lambda = \emptyset$) is desired, then trails in $\Omega \setminus \Lambda$ with lower absolute correlation are enumerated as well. However, the properties of interest are often of the form $(\delta_{u_0 \wedge \mathbb{F}_2^n}, \mu^{u_{r+1}})$ rather than $(\mu_{u_1}, \mu^{u_{r+1}})$. One can deal with this discrepancy by expanding $\delta_{u_{r+1} \wedge \mathbb{F}_2^n}$ in the ultrametric integral basis as in Example 4.1. This leads to the following variant of the error term in Theorem 5.1:

$$\left| \sum_{u_1 \preccurlyeq u_0} \sum_{u \in \Omega \setminus \Lambda} 2^{\mathsf{wt}(u_0) - \mathsf{wt}(u_1)} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{u_{i+1}, u_i} \right|_2 .$$

In principle, this can be modelled directly, but doing so introduces spurious trails. For example, if the input of an S-box S in the first round is saturated, then $T^{\mathsf{S}}\, \delta_{\mathbb{F}_2^4} = \delta_{\mathbb{F}_2^4}$. The above approach models this correctly, but it introduces up to 16 redundant trails. A more detailed example is worked out in Appendix C.2.

To reduce the number of spurious trails introduced by handling the input, we automatically propagate the input set through the first few rounds by partial matrix-vector multiplication. The multiplication is done in the ultrametric integral basis, but not using trails. To do this efficiently, the rank-one structure of $\mathscr{U} \delta_{u_0 \wedge \mathbb{F}_2^n}$ in $\mathbb{Q}[\mathbb{F}_2^n] = \bigotimes_{i=1}^{n} \mathbb{Q}[\mathbb{F}_2]$ is exploited. Hence, this optimization is inspired by some of the more general principles of the geometric approach [1]. Additional details and an example are given in Appendix C.2.

Our implementation extends the toolbox for integral cryptanalysis developed in [3]. This makes it easy to construct models for other ciphers. The cardinality constraints we rely on are generated using PySAT [21], and kissat [4] was used as the SAT solver.

7.2 Revisiting the distinguishers of Boura and Canteaut

In this section we revisit the integral distinguishers on PRESENT proposed by Boura and Canteaut [9] at Crypto 2016. They showed that, for the input sets $u \wedge \mathbb{F}_2^{64}$ listed in Table 2 and 4 - 8 rounds of PRESENT, every bit of the state sums to zero in $\mathbb{F}_2$. For the second output bit of four-round PRESENT, we already observed divisibility by four in Section 3.1 and this was proven in Section 5.2.

To validate the efficacy of the model, we compare our results for four and five rounds with experimental results in Appendix F. In most cases, the divisibility predicted by our model without trail enumeration is tight. For a few bits, an additional factor of two or four was gained by enumerating trails. For this reason, trail enumeration was not used to evaluate the 6 - 9 round properties.

Table 2 lists our results for the first 16 output bits for the input sets chosen by Boura and Canteaut. The results for the remaining 48 bits can be found in Appendix D. The first 16 bits give the most interesting results, though the remaining bits are not far off for six rounds and more.

For six rounds, we show that for 48 bits the absolute correlation is at most 1/4, which is stronger than the bound of 1/2 implied by ordinary integral cryptanalysis. The first bit exhibits divisibility by 128. For seven rounds, we improve over divisibility by two for 55 bits and the absolute correlation for the first bit is at most 1/512. For eight rounds, all bits have divisibility by four or more, ranging from 4 to 256. We also consider the eight round input set for nine rounds of PRESENT. It was shown by Wang *et al.* [32] that this results in 28 bits that sum to zero in $\mathbb{F}_2$. Our results show that four of these bits exhibit divisibility by four.

Table 2: Divisibility for the distinguishers of Boura and Canteaut [9] and Wang *et al.* [32], with input set $u \wedge \mathbb{F}_2^{64}$. The i^{th} output bit exhibits divisibility by 2^{ν_i}. Red numbers were obtained using trail enumeration.

rounds	u	$\log_2$(data)	ν_i for bit i															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4	000000000000000f	4	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5	000000000000fff0	12	5	5	5	5	3	2	2	2	3	3	3	3	3	2	2	2
6	00000000ffffffff	32	7	4	4	4	4	1	1	1	4	2	2	2	4	1	1	1
7	ffffffffffff0000	52	9	5	5	5	4	2	2	2	5	2	2	2	4	2	2	2
8	fffffffffffffffe	63	8	5	5	5	5	2	2	2	5	3	3	3	5	2	2	2
9	fffffffffffffffe	63	2	1	1	1	2	0	0	0	2	0	0	0	2	0	0	0

7.3 Finding zero-correlation distinguishers

Traditionally, zero-correlation linear approximations are found by showing that all linear trails have correlation zero. Due to the theoretical links from Section 6.4, the same properties can be analyzed from the point of view of ultrametric integral cryptanalysis. However, the non-existence of linear trails with nonzero correlation does not automatically imply the non-existence of ultrametric integral trails with nonzero correlation (and conversely).

To demonstrate that ultrametric integral cryptanalysis provides an alternative way to find zero-correlation linear approximations, we analyze the zero-correlation distinguishers for five and six rounds of PRESENT given by Hadipour *et al.* [17]. These zero-correlation linear approximations depend on the details of the S-box, so propagating the 'all' property as described by Knudsen and Wagner [24] is not sufficient to explain them. However, they *can* be obtained by propagating the 'all' property at the level of individual bits. Hence, these are properties that one would expect integral cryptanalysis to be able to detect, but most of the result is lost when working over $\mathbb{F}_2$.

Recall from Section 6.4 that $C^{\mathsf{F}} = \mathscr{T} A^{\mathsf{F}} \mathscr{T}^{-1}$, with $\mathscr{T} = \mathscr{F}\mathscr{U}^{-1}$. Using Lemma 6.1, the following variant of Theorem 6.2 is obtained:

$$\left|C^{\mathsf{F}}_{v,u}\right|_2 \leq \max_{t \preccurlyeq v} 2^{-\mathsf{wt}(t)} \left|\delta^t \left(A^{\mathsf{F}} \mathscr{T}^{-1} \delta_u\right)\right|_2 .$$

As explained in Section 7.1, the vector $\mathscr{T}^{-1}\delta_u$ can be propagated using partial matrix-vector multiplication to avoid spurious trails. For the zero-correlation approximations from [17], the input mask u is fixed. Since the bound on the right-hand side also holds for any output mask $s \preccurlyeq v$, multiple output masks can be tested using a single SAT instance.

Using this approach, all $2^{48}-1$ output masks with correlation zero for 5-round PRESENT (corresponding to three active superboxes) reported by Hadipour *et al.* can be found. There is another set of three superboxes leading to $2^{48} - 2^{32}$ additional zero-correlation approximations with the same input mask, which would reduce the data-complexity[8] by a factor of $\sqrt{2}$.

The zero-correlation approximation (u, v) on six rounds of PRESENT in [17, Figure 49d] follows from the five round property. Indeed, the support of the product $A^{\mathsf{F}^\vee} \mathscr{T}^\vee \delta_v$ with F the last round function lies in the set of output exponents that were analyzed for the 5 round property. The same argument can be made using linear cryptanalysis.

7.4 Improving key recovery attacks

Integral distinguishers can be turned into key-recovery attacks using the last-round trick. An important parameter is then the number of incorrect candidate keys that can be filtered out based on a single input set. A single zero-sum bit filters out half of the incorrect candidate keys, but a bit with divisibility by 2^ν provides a filter of (approximately) $2^{-\nu}$. To illustrate this, a key-recovery attack on eight round PRESENT-80 using 2^{12} data and time equivalent to 2^{60} encryptions is worked out below. The time-complexity is not fully optimized and can easily be reduced.

Integral distinguishers on six round PRESENT require at least 2^8 data, for example when the input set is a coset of $\mathtt{0}\cdots\mathtt{0ff0} \wedge \mathbb{F}_2^{64}$. Since this only gives a 1-bit filter, 20 sets would be necessary to append two rounds. However, using

[8] Unlike divisibility by small powers of two, a set of N zero-correlation approximations can be tested statistically using $2^n/\sqrt{N}$ samples.

ultrametric integral cryptanalysis, we find that every coset of $\mathtt{0}\cdots\mathtt{0eff0} \wedge \mathbb{F}_2^{64}$ – eight sets of the minimum-data property – leads to divisibility by four on the first bit. By combining both properties, every set of 2^{11} data provides a 9-bit filter. Using two such sets, one can evaluate the cipher on a coset of $\mathtt{0}\cdots\mathtt{0fff0} \wedge \mathbb{F}_2^{64}$. In this case, one has divisibility by 16, 2, 4 and 2 on the first four ciphertext bits. This results in a $2^{-18-(4-2)-1-2-1} = 2^{-24}$ filter. Hence, a single set of 2^{12} data suffices. Without using ultrametric integral cryptanalysis, one would only have a 19-bit filter. Hence, one would need 2^8 additional plaintexts.

The gain is relatively small in this example, but this is in part because only 20 key bits are guessed. If a stronger filter is required, divisibility properties become more useful.

8 Application to SIMON

Section 7 demonstrates that the ultrametric integral cryptanalysis of substitution-permutation networks such as PRESENT can be automated. The purpose of this section is to show that this also applies to ciphers with a different structure. We use the block cipher family SIMON as an example because, like PRESENT, it has been important in the development of integral cryptanalysis [29,30,33]. As a side result, we propose a small but interesting improvement to the modelling of SIMON's round function. It also applies to ordinary integral cryptanalysis.

8.1 Modelling

The round function of SIMON consists of and, copy and exclusive-or operations. The propagation of ultrametric integral trails though each of these operations was already described in Sections 6.2 and 6.3. The resulting constraints can be converted to conjunctive normal form by hand.

It is worthwhile to take a closer look at the part of the SIMON round function shown in Figure 5, corresponding to $\mathsf{F}(x) = (x \lll 1) \wedge (x \lll 8)$ with $\lll$ a rotation to the left. In previous work on SIMON [29,30,33], propagation through this function has been modeled by decomposing it into a copy and a bitwise and operation. The rotations can be handled by rewiring. The same strategy can be used for ultrametric integral cryptanalysis.

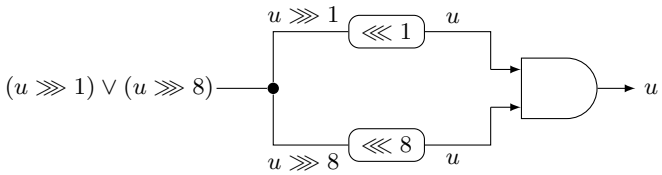


Fig. 5: A part of the round function of SIMON-32.

However, F is actually a monoid homomorphism. Hence, from the point of view of ultrametric integral cryptanalysis, it is no more difficult to handle than

linear functions are in linear cryptanalysis. By Theorem 4.5 (2), the input exponent is uniquely determined by the output exponent. More precisely, if the output exponent is u, then the input exponent is $\mathsf{F}^*(u) = (u \ggg 1) \vee (u \ggg 8)$. The same is clear from Figure 5, which depicts the unique trail with output exponent u. This reduces the number of variables in the model. The function F^* is dual to F in the sense that $\wedge$ is replaced by $\vee$. This is analogous to how, in linear cryptanalysis, the output mask for a linear function $x \mapsto \mathsf{M}\,x$ propagates to the input mask by $u \mapsto \mathsf{M}^\mathsf{T}\,u$.

Finally, two specific technical points should be mentioned. Due to the copy operations, the partial matrix-multiplication method mentioned in Section 7.1 does not work for SIMON. Instead, we decompose the input state as a sum of ultrametric basis vectors. A second point is that the model of SIMON's round function introduce key-independent trails that sum to zero in the end. To deal with this, we enumerate key-independent trails as described in Appendix C.1.

8.2 Results

Our results for SIMON-32 and SIMON-48 are summarized in Table 3, more details and additional results for larger variants are given in Appendix E. The input sets are those proposed by Todo [29] and Todo and Morii [30], as well as Xiang *et al.* [33]. We find divisibility by four and higher for many of the output bits, but not for the maximum number of rounds. This is not unexpected, as previous work has focused on distinguishing a maximal number of rounds with minimal data. This is a natural goal from the point of view of ordinary integral cryptanalysis, but it does not necessarily result in the most useful properties in any given situation (such as for a key-recovery attack).

An interesting conclusion from our results is that using the same input set on a smaller number of rounds, as in Table 3 for 10-13 and 12-15 rounds, does not just yield properties that are universally worse. Indeed, as one would expect, reducing the number of rounds does lead to higher divisibility.

Table 3: Divisibility for SIMON-$\{32, 48\}$ distinguishers with input set $R^{-1}(u \wedge \mathbb{F}_2^{\{32,48\}})$, where R is the round function of SIMON-$\{32, 48\}$ without key-addition.

SIMON-32				SIMON-48			
rounds	u	$\log_2$(data)	$\max_i \nu_i$	rounds	u	$\log_2$(data)	$\max_i \nu_i$
7	0001ffff	17	7	7	00000001ffff	17	10
8	01ffffff	25	7	8	00001fffffff	29	10
9	1fffffff	29	5	9	007fffffffff	39	8
10	7fffffff	31	4	10	0fffffffffff	44	6
11	7fffffff	31	3	11	3fffffffffff	46	5
12	7fffffff	31	2	12	7fffffffffff	47	4
13	7fffffff	31	1	13	7fffffffffff	47	3
14	7fffffff	31	1	14	7fffffffffff	47	2
15	7fffffff	31	1	15	7fffffffffff	47	1
				16	7fffffffffff	47	1

9 Acknowledgments

Tim Beyne is supported by a junior postdoctoral fellowship from the Research Foundation – Flanders (FWO) with reference number 1274724N. This work was partially supported by the Research Council KU Leuven, C16/18/004 through the C1 on New Block Cipher Structures. In addition, this work was supported by CyberSecurity Research Flanders with reference number VR20192203.

References

1. Tim Beyne. A geometric approach to linear cryptanalysis. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 36–66. Springer, Heidelberg, December 2021.
2. Tim Beyne and Vincent Rijmen. Differential cryptanalysis in the fixed-key model. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part III*, volume 13509 of *LNCS*, pages 687–716. Springer, Heidelberg, August 2022.
3. Tim Beyne and Michiel Verbauwhede. Integral cryptanalysis using algebraic transition matrices. *IACR Transactions on Symmetric Cryptology*, 2023(4):244–269, Dec. 2023.
4. Armin Biere and Mathias Fleury. Gimsatul, IsaSAT and Kissat entering the SAT Competition 2022. In Tomas Balyo, Marijn Heule, Markus Iser, Matti Järvisalo, and Martin Suda, editors, *Proc. of SAT Competition 2022 – Solver and Benchmark Descriptions*, volume B-2022-1 of *Department of Computer Science Series of Publications B*, pages 10–11. University of Helsinki, 2022.
5. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, Heidelberg, September 2007.
6. Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang. Integral and multidimensional linear distinguishers with correlation zero. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 244–261. Springer, Heidelberg, December 2012.
7. Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *DCC*, 70(3):369–383, 2014.
8. Christina Boura and Anne Canteaut. On the influence of the algebraic degree of f^{-1} on the algebraic degree of $g \circ f$. *IEEE Transactions on Information Theory*, 59(1):691–702, 2012.
9. Christina Boura and Anne Canteaut. Another view of the division property. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 654–682. Springer, Heidelberg, August 2016.
10. Anne Canteaut and Marion Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 518–533. Springer, Heidelberg, April / May 2002.
11. Claude Carlet. Two new classes of Bent functions. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 77–101. Springer, Heidelberg, May 1994.

12. Claude Carlet. *Boolean functions for cryptography and coding theory*. Cambridge University Press, 2021.
13. Joan Daemen, René Govaerts, and Joos Vandewalle. Correlation matrices. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 275–285. Springer, Heidelberg, December 1995.
14. Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher Square. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 149–165. Springer, Heidelberg, January 1997.
15. Richard Dedekind. Ideale in Normalkörpern. In Robert Fricke, Emmy Noether, and Øystein Ore, editors, *Gesammelte mathematische Werke*. 1930.
16. Brandon Dravie, Jérémy Parriaux, Philippe Guillot, and Gilles Millérioux. Matrix representations of vectorial boolean functions and eigenanalysis. *Cryptography and Communications*, 8:555–577, 2016.
17. Hosein Hadipour, Simon Gerhalter, Sadegh Sadeghi, and Maria Eichlseder. Improved search for integral, impossible-differential and zero-correlation attacks: Application to Ascon, ForkSKINNY, SKINNY, MANTIS, PRESENT and QARMAv2. Cryptology ePrint Archive, Paper 2023/1701, 2023. https://eprint.iacr.org/2023/1701.
18. Yonglin Hao, Gregor Leander, Willi Meier, Yosuke Todo, and Qingju Wang. Modeling for three-subset division property without unknown subset - improved cube attacks against Trivium and Grain-128AEAD. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 466–495. Springer, Heidelberg, May 2020.
19. Phil Hebborn, Gregor Leander, and Aleksei Udovenko. Mathematical aspects of division property. *Cryptography and Communications*, pages 1–44, 2023.
20. Kai Hu, Siwei Sun, Meiqin Wang, and Qingju Wang. An algebraic formulation of the division property: Revisiting degree evaluations, cube attacks, and key-independent sums. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part I*, volume 12491 of *LNCS*, pages 446–476. Springer, Heidelberg, December 2020.
21. Alexey Ignatiev, Antonio Morgado, and Joao Marques-Silva. PySAT: A Python toolkit for prototyping with SAT oracles. In *SAT*, pages 428–437, 2018.
22. Nicholas M. Katz. On a theorem of Ax. *American Journal of Mathematics*, 93(2):485–499, 1971.
23. Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 196–211. Springer, Heidelberg, December 1995.
24. Lars R. Knudsen and David Wagner. Integral cryptanalysis. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 112–127. Springer, Heidelberg, February 2002.
25. Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.
26. Gian Carlo Rota. On the foundations of combinatorial theory I. Theory of Möbius functions. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 2(4):340–368, Jan 1964.
27. Benjamin Steinberg. *Representation theory of finite monoids*. Springer Cham, 2016.
28. Bing Sun, Zhiqiang Liu, Vincent Rijmen, Ruilin Li, Lei Cheng, Qingju Wang, Hoda AlKhzaimi, and Chao Li. Links among impossible differential, integral and zero correlation linear cryptanalysis. In Rosario Gennaro and Matthew J. B. Robshaw,

editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 95–115. Springer, Heidelberg, August 2015.
29. Yosuke Todo. Structural evaluation by generalized integral property. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 287–314. Springer, Heidelberg, April 2015.
30. Yosuke Todo and Masakatu Morii. Bit-based division property and application to simon family. In Thomas Peyrin, editor, *FSE 2016*, volume 9783 of *LNCS*, pages 357–377. Springer, Heidelberg, March 2016.
31. Aleksei Udovenko. Convexity of division property transitions: Theory, algorithms and compact models. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 332–361. Springer, Heidelberg, December 2021.
32. SenPeng Wang, Bin Hu, Jie Guan, Kai Zhang, and Tairong Shi. MILP-aided method of searching division property using three subsets and applications. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 398–427. Springer, Heidelberg, December 2019.
33. Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 648–678. Springer, Heidelberg, December 2016.

A Ultrametric integral basis

A.1 Proof of Theorem 4.4

The result follows from Lemma 4.1 and the ultrametric triangle inequality. In particular, if $a^\wedge = \mathscr{U}\, a$, then

$$\|a^\wedge\|_\infty = \max_{v\in\mathbb{F}_2^n} \left|a_v^\wedge\right|_2 \le \max_{x\in\mathbb{F}_2^n} |a_x|_2 = \|a\|_\infty$$

Furthermore,

$$\|a\|_\infty = \max_{v\in\mathbb{F}_2^n} |a_v|_2 \le \max_{x\in\mathbb{F}_2^n} \left|a_x^\wedge\right|_2 = \|a^\wedge\|_\infty$$

Since $\|a^\wedge\|_\infty \le \|a\|_\infty$ and $\|a\|_\infty \le \|a^\wedge\|_\infty$, we must have $\|a^\wedge\|_\infty = \|a\|_\infty$.

A.2 Alternative proof of Lemma 4.1

The first formula follows from the fact that $a = \sum_{v\in\mathbb{F}_2^n} a_v^\wedge\, \mu_v$. Indeed, by the definition of dual bases, $a_v^\wedge = \mu^v(a)$. Hence,

$$a_v^\wedge = \mu^v(a) = \sum_{x\in\mathbb{F}_2^n} a_x\, \mu^v\big(\delta_x\big) = \sum_{x\in\mathbb{F}_2^n} a_x\, \tau(x^v) = \sum_{x\succcurlyeq v} a_x\,.$$

The inverse formula follows by Möbius inversion.

B Ultrametric integral transition matrices

B.1 Relation to the algebraic normal form

The following result provides an alternative proof of the fact that algebraic transition matrices are the modulo two reductions of ultrametric integral transition matrices.

Theorem B.1. *Let $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. The coordinate $A^{\mathsf{F}}_{v,u}$ is congruent modulo two to the coefficient of x^u in the algebraic normal form of F^v.*

Proof. By the definition of A^{F}, the linear functional $\mu^v \circ \mathsf{F}$ is equal to

$$\mu^v \circ \mathsf{F} = \sum_{u \in \mathbb{F}_2^n} A^{\mathsf{F}}_{v,u}\, \mu^u \,.$$

Evaluating at δ_x and reducing modulo two yields

$$\mathsf{F}^v(x) \equiv \sum_{u \in \mathbb{F}_2^n} A^{\mathsf{F}}_{v,u}\, x^u \pmod 2 \,.$$

Hence, $A^{\mathsf{F}}_{v,u} \bmod 2$ is the coefficient of x^u in the algebraic normal form of F^v. □

B.2 Copy and xor operations

The n-bit copy operation is described by a function $\mathsf{copy}_n : \mathbb{F}_2^n \to \mathbb{F}_2^{2n}$ with $\mathsf{copy}_n(x) = x \| x$. For $n = 1$ one finds that

$$A^{\mathsf{copy}_1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} .$$

Up to postcomposition with a bit-permutation, A^{copy_n} is equal to $(A^{\mathsf{copy}_1})^{\otimes n}$. Furthermore, $A^{\mathsf{copy}_1}_{u\|v,w} = 1$ whenever $w = u \| v$ and zero otherwise. Hence,

$$A^{\mathsf{copy}_n}_{u\|v,w} = \begin{cases} 1 & \text{if } w = u \vee v \,, \\ 0 & \text{otherwise} \,. \end{cases}$$

The n-bit xor operation corresponds to the function $\mathsf{xor}_n : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ defined by $\mathsf{xor}_n(x\|y) = x + y$. Direct computation shows that for $n = 1$,

$$A^{\mathsf{xor}_1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & -2 \end{bmatrix} .$$

Up to precomposition with a bit-permutation, A^{xor_n} is equal to $(A^{\mathsf{xor}_1})^{\otimes n}$. Hence, because $A^{\mathsf{xor}_1}_{w,u\|v} = (-2)^{uv}$ if $w = u \vee v$ and zero elsewhere, it follows that

$$A^{\mathsf{xor}_n}_{w,u\|v} = \begin{cases} (-2)^{\mathsf{wt}(u \wedge v)} & \text{if } w = u \vee v \,, \\ 0 & \text{otherwise} \,. \end{cases}$$

B.3 Refinement of Theorem 6.1 and Corollary 6.1

The following two theorems are refinements of Theorem 6.1 and Corollary 6.1. Let $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. Theorem B.2 uses the following refinement of the algebraic degree:

$$\deg_v \mathsf{F} = \sum_{\substack{i=1 \\ v_i=1}}^{m} \deg \mathsf{F}_i \,.$$

Theorem B.2. *For every function* $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$,

$$-\log_2 \left|A^{\mathsf{F}}_{v,u}\right|_2 \geq \left\lceil \frac{\mathsf{wt}(u) - \deg_v \mathsf{F}}{\deg \mathsf{F}} \right\rceil .$$

Equivalently, $\left|A^{\mathsf{F}}_{v,u}\right|_2 \geq 2^{-\nu}$ *only if* $\deg_v \mathsf{F} \geq \mathsf{wt}(u) - \nu \deg \mathsf{F}$.

Proof. The proof follows that of Theorem 6.1. Assume that $\left|A^{\mathsf{F}}_{v,u}\right|_2 \geq 2^{-\nu}$. For every nonzero bit of the output exponent v, there exists an integer ν_i such that the weight at the output of the and-layer for the coordinate function F_i is at most $\nu_i + 1$. By assumption, we have $\sum_{i=1}^m \nu_i \leq \nu$ with $\nu_i = 0$ if $v_i = 0$. Hence, for the overall function F, the weight at the input of the and-layer is at most

$$\sum_{\substack{i=1 \\ v_i=1}}^{m} (\nu_i + 1) \deg \mathsf{F}_i \leq \nu \deg \mathsf{F} + \sum_{\substack{i=1 \\ v_i=1}}^{m} \deg \mathsf{F}_i = \nu \deg \mathsf{F} + \deg_v \mathsf{F}.$$

Since the weight of the input exponent is $\mathsf{wt}(u)$, we have $\mathsf{wt}(u) \leq \nu + \deg_v \mathsf{F}$ or equivalently $\deg_v \mathsf{F} \geq \mathsf{wt}(u) - \nu \deg \mathsf{F}$. □

Corollary B.1 (Ax-Katz [22]). *The number of solutions of a system of* m *equations of degrees* $d_1, \ldots, d_m$ *in* n *variables is divisible by* 2^ν, *where*

$$\nu \geq \left\lceil \frac{n - \sum_{i=1}^m d_i}{\max_{1 \leq i \leq m} d_i} \right\rceil .$$

Proof. The idea of the proof is the same as for Corollary 6.1, but using Theorem B.2 instead of Theorem 6.1. The system of equations can be written as $\mathsf{F}(x) = 11\cdots1$, so that the number of solutions equals

$$\mu^{11\cdots1}\left(T^{\mathsf{F}} \delta_{\mathbb{F}_2^n}\right) = \sum_{u \in \mathbb{F}_2^n} 2^{n - \mathsf{wt}(u)} A^{\mathsf{F}}_{11\cdots1,u} \,.$$

Using Theorem B.2, one finds that the right-hand side is divisible by

$$\nu \geq \min_{u \in \mathbb{F}_2^n} n - \mathsf{wt}(u) + \left\lceil \frac{\mathsf{wt}(u) - \deg_{11\cdots1} \mathsf{F}}{\deg \mathsf{F}} \right\rceil .$$

The minimum is reached for $\mathsf{wt}(u) = n$. Hence,

$$\nu \geq \left\lceil \frac{n - \deg_{11\cdots1} \mathsf{F}}{\deg \mathsf{F}} \right\rceil .$$

The result follows from $\deg \mathsf{F} = d$ and $\deg_{11\cdots1} \mathsf{F} = \sum_{i=1}^n d_i$. □

B.4 Correlation matrices of low-degree functions

The following result is well-known in the Boolean functions literature as a consequence of the weight divisibility of Reed-Muller codes (Corollary 6.2). Deducing it from Theorem 6.2 provides some additional insight, as it shows that the result follows from the sparsity of the ultrametric integral transition matrix for low-degree functions.

Corollary B.2. *If* $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *is a function with algebraic degree* d*, then* $\left|C^{\mathsf{F}}_{v,u}\right|_2 \leq 2^{n-\lceil n/d \rceil}$ *for all* u *and* v*.*

Proof. By Theorems 6.1 and 6.2, the coordinates of the correlation matrix can be upper bounded as

$$\left|C^{\mathsf{F}}_{v,u}\right|_2 \leq \max_{\substack{s \succcurlyeq u \\ t \preccurlyeq v}} 2^{\mathsf{wt}(s)-\mathsf{wt}(t)}\, 2^{\mathsf{wt}(t)-\lceil \mathsf{wt}(s)/d \rceil} \leq \max_{s \succcurlyeq u} 2^{\mathsf{wt}(s)-\lceil \mathsf{wt}(s)/d \rceil}\,.$$

The maximum is achieved for $\mathsf{wt}(s) = n$. □

C Automating ultrametric integral cryptanalysis

This appendix provides additional details on how to automate the analysis of ultrametric integral trails using off-the-shelf solvers.

C.1 Modelling

Modelling S-boxes. Let $\mathsf{S} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be an S-box. The CNF-formula for the propagation through S is a minimal CNF representation of the Boolean function $f(u, v, c)$, where u in $\mathbb{F}_2^n$ and v in $\mathbb{F}_2^m$ are input and output exponents and c is an additional bitvector used to keep track of the 2-adic absolute value of the correlation.

The function f is one if and only if $A^{\mathsf{S}}_{v,u} \neq 0$, and c is the binary representation of the integer $1/\left|A^{\mathsf{S}}_{v,u}\right|_2 - 1$. This ensures that the Hamming weight of c equals

$$\mathsf{wt}(c) = \mathsf{wt}\left(1/\left|A^{\mathsf{S}}_{v,u}\right|_2 - 1\right) = -\log_2 \left|A^{\mathsf{S}}_{v,u}\right|_2 .$$

This makes it possible to model conditions on the 2-adic absolute value of the correlation with simple cardinality constraints. That is, if r S-boxes are active with corresponding values $c_1, \ldots, c_r$, then the correlation is greater than $2^{-\nu}$ if and only if

$$\sum_{i=1}^{r} \mathsf{wt}(c_i) \leq \nu\,.$$

Modelling key addition. The CNF-formula for the key addition can be derived from Example 4.3. Due to the structure of the ultrametric integral transition matrix, it suffices to add the constraint $(\neg u_i) \vee v_i$ for every bit of u and v and no additional variables are necessary to track the 2-adic absolute value of the trail correlation.

However, in our implementation, we opted to model keys as additional input variables and key additions as xor operations. Although this is not relevant for PRESENT, it is used in the analysis of SIMON to separate key-dependent from key-independent trails.

C.2 Optimized trail enumeration

To enumerate all trails with correlation greater than $2^{-\nu}$ through r rounds of PRESENT with input exponent u and output exponent v, we generate the CNF-formula for these r rounds and add constraints to fix u and v as well as the cardinality constraints to bound the absolute trail correlation.

As discussed in Section 7.1, if the input is of the form $\delta_{u_0 \wedge \mathbb{F}_2^n}$ rather than μ_{u_1}, then a direct decomposition of $\delta_{u_0 \wedge \mathbb{F}_2^n}$ in terms of the ultrametric basis can introduce spurious trails. The following example illustrates this in more detail.

Example C.1 (Spurious trails). Consider the property $(\delta_{\mathbb{F}_2^4}, \mu^1)$ for the PRESENT S-box. Since the S-box is a permutation and the input set corresponds to its whole input space, this property evaluates to 8 – which has 2-adic absolute value 2^{-3}. However, the highest correlation trail has 2-adic absolute value 2^{-2}. In total there are four trails with this absolute correlation:

$$\left|4A^{\mathsf{S}}_{1,6}\right|_2 = \left|2A^{\mathsf{S}}_{1,7}\right|_2 = \left|2A^{\mathsf{S}}_{1,\mathtt{e}}\right|_2 = \left|A^{\mathsf{S}}_{1,\mathtt{f}}\right|_2 = 2^{-2}\,.$$

All of these trails have to be enumerated to compute the correct 2-adic absolute value. As the input sets become larger, the discrepancy between the correct correlation and highest trail correlation – as well as the number of high correlation trails – will only increase further. ▷

To reduce the number of spurious trails introduced by the input set, we propagate $\delta_{u_0 \wedge \mathbb{F}_2^n}$ through the first few rounds by partial matrix-vector multiplication in the ultrametric integral basis.

If the input of one of the S-boxes is saturated, then $T^{\mathsf{S}}\,\delta_{\mathbb{F}_2^4} = \delta_{\mathbb{F}_2^4}$, so also $A^{\mathsf{S}}\mathscr{U}\,\delta_{\mathbb{F}_2^4} = \mathscr{U}\,\delta_{\mathbb{F}_2^4}$. In this case, the matrix-vector product is nothing more than the propagation rule for the 'all' property in the original description of integral cryptanalysis by Knudsen and Wagner [24]. This idea was already used in Section 5.2.

More generally, the optimization leads to replacing the model of every partially saturated component with a model that already takes into account the sum over its saturated inputs. Consider a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ for which the last b input bits are saturated. To model the property $(\mu_u \otimes \delta_{\mathbb{F}_2^b}, \mu^v)$ for all u in $\mathbb{F}_2^{n-b}$ and v in $\mathbb{F}_2^m$, the model for A^{F} is replaced by a model for $\tilde{A}^{\mathsf{F}}$ with

$$\tilde{A}^{\mathsf{F}}_{v,u} = \sum_{w \in \mathbb{F}_2^b} 2^{b - \mathsf{wt}(w)} A^{\mathsf{F}}_{v,u\|w}\,.$$

Example C.2. In the analysis of Section 5.2, the rightmost bit of some of the S-boxes in the second round is saturated. The optimized model uses the following matrix:

$$\tilde{A}^{\mathsf{S}} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 2 & -3 & -1 & 2 \\ 0 & 1 & 0 & -1 & 1 & -1 & 0 & 0 \\ 2 & -1 & -2 & 2 & -1 & 1 & 3 & -4 \\ 1 & -1 & -1 & 2 & -1 & 2 & 2 & -4 \\ 0 & 1 & 0 & -1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & -2 \\ 1 & 0 & 0 & 1 & 0 & 1 & -1 & -2 \\ 0 & 1 & 1 & -1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 2 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}.$$

▷

D Additional results on PRESENT

This appendix provides additional results from the analysis in Section 7.2. Table 4 and Table 5 compare the experimental results on 4- and 5-round PRESENT with the results obtained from modelling without trail enumeration. Table 6 contains the divisibility bounds for every output bit of the 6- to 9-round properties of Boura and Canteaut, and Wang *et al.* [9,32].

Table 4: Divisibility for the integral distinguisher of Boura and Canteaut [9] on 4-round PRESENT, with input set $\mathtt{0}\cdots\mathtt{0f} \wedge \mathbb{F}_2^{64}$. The number of times the i^{th} output bit equals one is divisible by 2^{ν_i}.

	ν_i for bit i															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16 ⋯
experiment	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2 ⋯
theoretical	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2 ⋯

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32 ⋯
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 ⋯
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 ⋯

33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48 ⋯
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 ⋯
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 ⋯

49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 5: Divisibility for the integral distinguisher of Boura and Canteaut [9] on 5-round PRESENT, with input set $\mathtt{0}\cdots\mathtt{0fff0} \wedge \mathbb{F}_2^{64}$. The number of times the i^{th} output bit equals one is divisible by 2^{ν_i}.

	ν_i for bit i																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$\cdots$
experiment	5	5	5	5	3	2	2	2	3	3	3	3	3	2	2	2	$\cdots$
theoretical	5	5	5	5	2	2	2	2	3	3	3	3	2	2	2	2	$\cdots$

	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	$\cdots$
	4	4	4	4	2	1	1	1	2	2	2	2	2	1	1	1	$\cdots$
	4	4	4	4	1	1	1	1	2	2	2	2	1	1	1	1	$\cdots$

	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	$\cdots$
	4	4	4	4	2	2	2	2	2	2	2	2	2	2	2	2	$\cdots$
	4	4	4	4	2	2	2	2	2	2	2	2	2	2	2	2	$\cdots$

	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
	4	4	4	4	2	1	1	1	2	2	2	2	2	1	1	1
	4	4	4	4	1	1	1	1	2	2	2	2	1	1	1	1

Table 6: Divisibility for the integral distinguishers on PRESENT of Boura and Canteaut [9], and Wang *et al.* [32], with input set $u \wedge \mathbb{F}_2^{64}$. The number of times the i^{th} output bit is equal to one is divisible by 2^{ν_i}.

rounds	u	ν_i for bit i															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16 ⋯
6	`00000000ffffffff`	7	4	4	4	4	1	1	1	4	2	2	2	4	1	1	1 ⋯
7	`fffffffffffff000`	9	5	5	5	4	2	2	2	5	2	2	2	4	2	2	2 ⋯
8	`fffffffffffffffe`	8	5	5	5	5	2	2	2	5	3	3	3	5	2	2	2 ⋯
9	`fffffffffffffffe`	2	1	1	1	2	0	0	0	2	0	0	0	2	0	0	0 ⋯

		17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32 ⋯
6	`00000000ffffffff`	7	4	4	4	4	1	1	1	4	2	2	2	4	1	1	1 ⋯
7	`fffffffffffff000`	8	4	4	4	3	1	1	1	4	1	1	1	3	1	1	1 ⋯
8	`fffffffffffffffe`	7	4	5	4	4	2	2	2	5	2	2	2	4	2	2	2 ⋯
9	`fffffffffffffffe`	1	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0 ⋯

		33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48 ⋯
6	`00000000ffffffff`	7	4	4	4	4	1	1	1	4	2	2	2	4	1	1	1 ⋯
7	`fffffffffffff000`	8	4	4	4	5	1	1	1	5	2	2	2	5	1	1	1 ⋯
8	`fffffffffffffffe`	7	4	5	4	5	2	2	2	5	3	3	3	5	2	2	2 ⋯
9	`fffffffffffffffe`	1	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0 ⋯

		49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
6	`00000000ffffffff`	7	4	4	4	4	1	1	1	4	2	2	2	4	1	1	1
7	`fffffffffffff000`	8	4	4	4	3	1	1	1	4	1	1	1	3	1	1	1
8	`fffffffffffffffe`	7	4	5	4	4	2	2	2	5	2	2	2	4	2	2	2
9	`fffffffffffffffe`	1	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0

E Additional results on SIMON

This appendix contains additional results from the analysis of Section 8.2. The bit-wise divisibility for the properties on SIMON-$\{32, 48, 64, 96, 128\}$ can be found in Tables 7 to 11 respectively. The results in Tables 9 to 11 are not complete, because some of these models took too long to evaluate in reasonable time.

Table 7: Divisibility for the integral distinguishers on SIMON-32 of Todo [29], Todo and Morii [30], and Xiang *et al.* [33], with input set $R^{-1}(u \wedge \mathbb{F}_2^{32})$, where R is the round function of SIMON-32 without key addition. The number of times the i^{th} output bit is equal to one is divisible by 2^{ν_i}.

rounds	u	ν_i for bit i																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	⋯
7	`0001ffff`	7	6	7	6	6	6	7	7	7	7	6	6	6	7	7	7	⋯
8	`01ffffff`	6	6	6	7	7	7	6	6	6	6	7	7	7	7	6	5	⋯
9	`1fffffff`	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	⋯
10	`7fffffff`	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	⋯
11	`7fffffff`	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	⋯
12	`7fffffff`	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	⋯
13	`7fffffff`	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	⋯
14	`7fffffff`	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	⋯
15	`7fffffff`	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	⋯

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
3	3	2	2	3	3	3	3	3	2	3	3	2	2	3	3
3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 8: Divisibility for the integral distinguishers on SIMON-48 of Todo [29], and Xiang *et al.* [33], with input set $R^{-1}(u \wedge \mathbb{F}_2^{48})$, where R is the round function of SIMON-48 without key addition. The number of times the i^{th} output bit is equal to one is divisible by 2^{ν_i}.

rounds	u	ν_i for bit i																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	⋯
7	00000001ffff	10	9	9	8	9	9	9	10	9	9	8	8	8	8	7	7	⋯
8	00001fffffff	10	9	9	8	8	8	9	9	9	8	8	7	6	6	7	7	⋯
9	007fffffffff	8	8	8	8	7	7	8	8	8	8	8	7	7	7	7	6	⋯
10	0fffffffffff	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	⋯
11	3fffffffffff	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	⋯
12	7fffffffffff	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	⋯
13	7fffffffffff	3	2	3	3	3	3	3	3	2	3	3	3	2	2	2	2	⋯
14	7fffffffffff	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	⋯
15	7fffffffffff	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	⋯
16	7fffffffffff	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	⋯

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	⋯
7	7	7	6	6	7	8	9	4	4	4	4	4	4	4	5	⋯
8	9	9	8	8	8	8	9	4	4	4	4	3	3	3	4	⋯
7	7	7	7	7	7	7	7	4	4	4	4	4	4	4	4	⋯
6	6	6	6	6	6	6	6	4	4	4	4	4	4	4	4	⋯
5	5	5	5	5	5	5	5	3	3	3	3	3	3	3	3	⋯
4	4	4	4	4	4	4	4	3	2	3	3	3	3	3	3	⋯
3	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	⋯
2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	⋯
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	⋯
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	⋯

33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
5	5	5	4	4	4	4	4	3	3	3	3	3	2	2	3
4	4	3	3	2	2	2	2	3	3	3	3	3	3	3	4
4	4	4	4	4	3	3	3	3	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2	3	3	3	2	2	2	2	3	2	2	2	2	2	3	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 9: Divisibility for some of the integral distinguishers on SIMON-64 of Todo [29], and Xiang *et al.* [33], with input set $R^{-1}(u \wedge \mathbb{F}_2^{64})$, where R is the round function of SIMON-64 without key addition. The number of times the i^{th} output bit is equal to one is divisible by 2^{ν_i}.

rounds	u	ν_i for bit i																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	⋯
7	000000000001ffff	13	13	12	12	13	13	13	13	13	12	12	12	11	10	9	9	⋯
8	00000001ffffffff	12	13	13	13	13	13	13	12	13	12	12	12	12	12	12	13	⋯
17	7fffffffffffffff	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	⋯
18	7fffffffffffffff	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	⋯

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	⋯
8	9	8	7	6	7	8	9	10	9	10	10	11	12	13	13	⋯
12	13	12	12	12	13	13	13	13	12	12	13	13	13	13	13	⋯
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	⋯
0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	⋯

33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	⋯
10	9	10	9	9	9	9	10	9	10	9	9	9	9	8	7	⋯
7	6	7	7	7	7	7	7	7	7	6	6	6	6	6	6	⋯
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	⋯
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	⋯

49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
6	5	5	5	4	3	3	4	4	5	5	5	6	7	8	9
7	6	7	6	6	6	7	7	7	7	6	6	7	7	7	7
0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 10: Divisibility for some of the integral distinguishers on SIMON-96 of Todo [29], and Xiang *et al.* [33], with input set $R^{-1}(u \wedge \mathbb{F}_2^{96})$, where R is the round function of SIMON-96 without key addition. The number of times the i^{th} output bit is equal to one is divisible by 2^{ν_i}.

rounds	u	ν_i for bit i															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16 ⋯
7	000000000000000000001ffff	16	16	16	16	16	16	16	16	16	15	14	13	12	11	10	10 ⋯
8	00000000000000001ffffffff	25	24	25	24	24	24	25	25	24	25	24	24	24	24	23	22 ⋯
21	7fffffffffffffffffffffff	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0 ⋯
22	7fffffffffffffffffffffff	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0 ⋯

		17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32 ⋯
		9	9	8	7	6	7	8	9	10	9	10	10	11	12	13	13 ⋯
		21	20	20	20	19	18	17	17	16	17	16	15	14	14	14	14 ⋯
		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯
		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

		33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48 ⋯
		13	13	13	14	15	15	15	15	15	15	16	16	16	16	16	16 ⋯
		14	13	13	13	13	14	15	16	17	18	19	20	21	22	23	24 ⋯
		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 ⋯
		0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1 ⋯

		49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64 ⋯
		15	14	15	15	15	15	15	15	14	15	14	13	12	11	10	9 ⋯
		17	18	18	18	18	18	18	18	19	18	18	18	18	18	18	18 ⋯
		0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0 ⋯
		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

		65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80 ⋯
		8	7	6	5	4	3	3	4	4	5	5	5	6	7	8	9 ⋯
		17	17	16	16	16	16	15	14	13	12	12	12	11	10	9	9 ⋯
		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯
		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

		81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
		10	9	10	10	11	12	13	13	13	13	13	14	15	15	15	15
		8	9	8	7	7	7	8	9	10	10	11	12	13	14	15	16
		0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1
		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 11: Divisibility for some of the integral distinguishers on SIMON-96 of Todo [29], and Xiang *et al.* [33], with input set $R^{-1}(u \wedge \mathbb{F}_2^{128})$, where R is the round function of SIMON-128 without key addition. The number of times the i^{th} output bit is equal to one is divisible by 2^{ν_i}.

rounds	u	ν_i for bit i															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16 ⋯
7	00000000000000000000000000001ffff	16	16	16	16	16	16	16	16	16	15	14	13	12	11	10	10 ⋯
8	00000000000000000000000001ffffffff	31	30	31	31	31	31	31	31	30	31	30	29	28	27	26	25 ⋯
24	7fffffffffffffffffffffffffffffffff	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0 ⋯
25	7fffffffffffffffffffffffffffffffff	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32 ⋯
	9	9	8	7	6	7	8	9	10	9	10	10	11	12	13	13 ⋯
	24	23	22	21	20	19	18	18	17	17	16	15	14	14	14	14 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48 ⋯
	13	13	13	14	15	15	15	15	15	15	16	16	16	16	16	16 ⋯
	14	13	13	13	13	14	15	16	17	18	19	20	21	22	23	24 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64 ⋯
	16	17	17	17	17	17	17	17	17	17	17	17	17	17	17	17 ⋯
	25	25	26	26	27	28	29	29	29	29	29	30	31	31	31	31 ⋯
	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1 ⋯

	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80 ⋯
	17	16	16	16	16	16	16	16	15	15	14	13	12	11	10	9 ⋯
	29	29	28	28	29	29	29	29	29	28	28	28	27	26	25	24 ⋯
	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96 ⋯
	8	7	6	5	4	3	3	4	4	5	5	5	6	7	8	9 ⋯
	23	23	22	21	20	19	18	17	16	15	14	13	12	11	10	10 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112 ⋯
	10	9	10	10	11	12	13	13	13	13	13	14	15	15	15	15 ⋯
	9	9	8	7	7	7	8	9	10	10	11	12	13	14	15	16 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 ⋯

	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
	15	15	16	16	16	16	16	16	16	17	17	17	17	17	17	17
	17	18	19	20	21	22	23	24	25	25	26	26	27	28	29	29
	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

F Experimental results

All experimental results on 4- and 5-round PRESENT are given in Figures 6 and 7 respectively. Blue indicates the measurement results and red the expected distribution for a random function with the same divisibility as in the measurements. Note that in both experiments, PRESENT behaves significantly different from a random permutation with the same divisibility properties.

Fig. 6: Results of the experiments of Appendix F for every output bit (blue). The divisibility and the expected number of keys based on that divisibility are given in red.

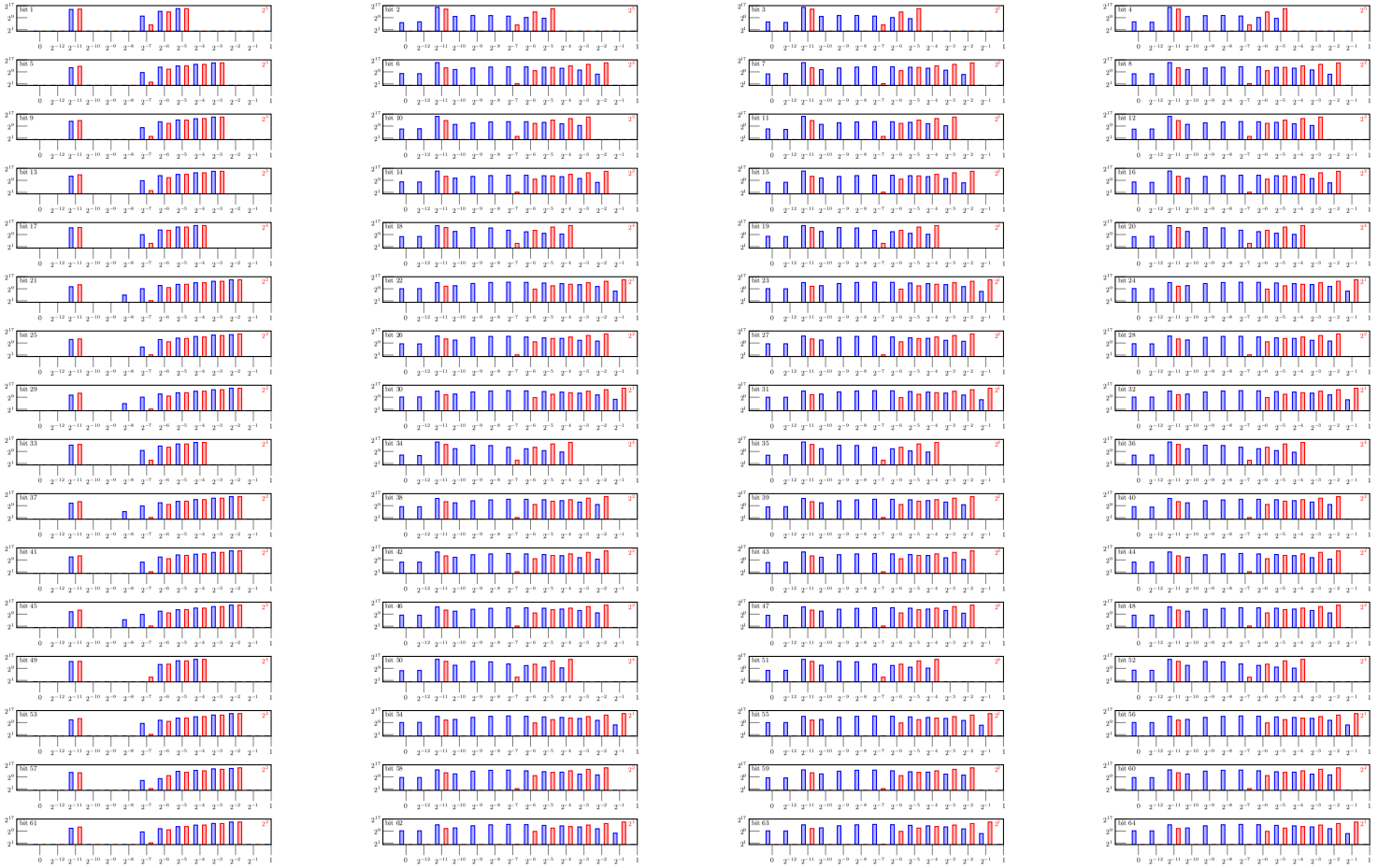


Fig. 7: Results of the experiments on 5 rounds of PRESENT for every output bit (blue, left) and the divisibility and expected number of keys based on that divisibility (red, right). The experiment was performed for 2^{16} keys.