Zero-Sum Distinguishers for Iterated Permutations and Application to Keccak-f and Hamsi-256

Christina Boura, Anne Canteaut

Zero-Sum Distinguishers for Iterated Permutations and Application to KECCAK-f and Hamsi-256*

Christina Boura[1,2] and Anne Canteaut[1]

[1] SECRET Project-Team - INRIA Paris-Rocquencourt - B.P. 105
78153 Le Chesnay Cedex - France
[2] Gemalto - 6, rue de la Verrerie - 92447 Meudon sur Seine - France
{Christina.Boura, Anne.Canteaut}@inria.fr

Abstract. The zero-sum distinguishers introduced by Aumasson and Meier are investigated. First, the minimal size of a zero-sum is established. Then, we analyze the impacts of the linear and the nonlinear layers in an iterated permutation on the construction of zero-sum partitions. Finally, these techniques are applied to the KECCAK-f permutation and to Hamsi-256. We exhibit several zero-sum partitions for 20 rounds (out of 24) of KECCAK-f and some zero-sum partitions of size 2^{19} and 2^{10} for the finalization permutation in Hamsi-256.

Keywords. Hash functions, integral properties, zero-sums, SHA-3.

1 Introduction

The existence of zero-sum structures is a new distinguishing property which has been recently investigated by Aumasson and Meier [2], and by Knudsen and Rijmen [14]. For a given function F, a *zero-sum* is a set of inputs which sum to zero, and whose images by F also sum to zero. Such zero-sum properties can be seen as a generalization of multiset properties (a.k.a. integral properties) [10,15]. Classical integral attacks for block ciphers include higher-order differential attacks and saturation attacks. Similarly, zero-sum structures may exploit either the fact that the permutation or its inverse after a certain number of rounds has a low degree, or some saturation properties due to a low diffusion. The keypoint is that the first type of weakness arises from the nonlinear part of the function whereas the second type arises from its linear part. The first direction has been investigated in [2] for three SHA-3 candidates, Luffa, Hamsi and KECCAK. Here, we show that, when the nonlinear part of the round transformation consists of several parallel applications of a smaller Sbox, an improved bound on the degree of the iterated function can be deduced, leading to zero-sums with a smaller size. Moreover, we investigate the impact of the linear part of the inner round permutation on the construction of zero-sums. Then, combining both types of properties enables us to find zero-sum partitions for the inner permutations of two SHA-3 Round-2 candidates, KECCAK [4] and Hamsi-256 [16]. More precisely, we exhibit several zero-sum partitions up to 20 (out of 24) rounds of the inner permutation in KECCAK and we improve the zero-sum partitions found in [1] for the finalization permutation of Hamsi-256. Even if our results do not seem to affect the security of KECCAK and Hamsi-256, they point out that the involved inner permutation of Hamsi-256 and 20 rounds of the inner permutation of KECCAK do not have an ideal behavior.

The rest of the paper is organized as follows. Section 2 defines the notions of zero-sum and of zero-sum partition, and it also establishes the minimal size for a zero-sum. Section 3 analyzes how a low degree of the nonlinear part of the round transformation and of its inverse can be exploited for constructing zero-sum partitions. It also applies a result from [8], and shows that the size of the previously obtained zero-sum partitions can be improved when the nonlinear layer in the round transformation consists of several applications of a small Sbox. The role of the linear layer in the construction of zero-sum partitions is investigated in Section 4. Finally some applications to the inner permutation of KECCAK and to the finalization permutation of Hamsi-256 are presented in Sections 5 and 6.

* Partially supported by the French Agence Nationale de la Recherche through the SAPHIR2 project under Contract ANR-08-VERS-014.

2 Zero-sum structures and distinguishing properties

In the whole paper, the addition in $\mathbb{F}_2^n$, *i.e.* the bitwise exclusive-or will be denoted by $+$, while $\oplus$ will be used for denoting the direct sum of subspaces of $\mathbb{F}_2^n$.

Zero-sum distinguishers were firstly introduced by J.-P. Aumasson and W. Meier in [2].

Definition 1. *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. A* zero-sum *for F of size K is a subset $\{x_1, \ldots, x_K\} \subset \mathbb{F}_2^n$ of elements which sum to zero and for which the corresponding images by F also sum to zero,* i.e.*,*

$$\sum_{i=1}^{K} x_i = \sum_{i=1}^{K} F(x_i) = 0 \, .$$

2.1 Zero-sums and codewords in a linear code

We use standard notation of the algebraic coding theory (see [18]). A binary linear code of length n and dimension k, denoted by $[n, k]$, is a k-dimensional subspace of $\mathbb{F}_2^n$. It can then be defined by a $k \times n$ binary matrix G, named generator matrix for $\mathcal{C}$: $\mathcal{C} = \{xG, x \in \mathbb{F}_2^k\}$. Any $[n, k]$-linear code $\mathcal{C}$ is associated with its dual $[n, n-k]$-code, denoted by $\mathcal{C}^\perp$ and defined by $\mathcal{C}^\perp = \{x \in \mathbb{F}_2^n, \;\; x \cdot c = 0 \;\text{ for all } c \in \mathcal{C}\}$.

Let $(x_i, 0 \leq i < 2^n)$ denote the set of all elements in $\mathbb{F}_2^n$. To any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we associate the linear code $\mathcal{C}_F$ of length 2^n and dimension $n + m$ defined by the generator matrix

$$G_F = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & \ldots & x_{2^n-1} \\ F(x_0) & F(x_1) & F(x_2) & F(x_3) & \ldots & F(x_{2^n-1}) \end{pmatrix} \, ,$$

where each entry is viewed as a binary column vector. Then, we get the following result.

Proposition 1. *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$.*
The set of inputs $\{x_{i_1}, \ldots, x_{i_K}\} \subset \mathbb{F}_2^n$ is a zero-sum *for F if and only if the codeword of Hamming weight K with support $\{i_1, \ldots, i_K\}$ belongs to the dual code $\mathcal{C}_F^\perp$. Most notably, when $m = n$, we deduce that*

- *there exists at least one zero-sum of size 5 for F;*
- *F has no zero-sum of size less than or equal to 4 if and only if F is an almost perfect nonlinear permutation,* i.e., *if $\max_{a,b \neq 0} \#\{x \in \mathbb{F}_2^n, \; F(x+a) + F(x) = b\} = 2$.*

Proof. Clearly, a binary vector $(c_0, \ldots, c_{2^n-1})$ belongs to $\mathcal{C}_F^\perp$ if and only if

$$\sum_{i=0}^{2^n-1} c_i x_i = 0 \text{ and } \sum_{i=0}^{2^n-1} c_i F(x_i) = 0 \, .$$

This equivalently means that the support of c, *i.e.*, $\{i, c_i = 1\}$, defines a zero-sum for F. Moreover, the size of the zero-sum corresponds to the Hamming weight of the codeword. For $m = n$, $\mathcal{C}_F^\perp$ is a linear code of length 2^n and dimension $2^n - 2n$. It is known that the minimum distance for such a linear code with these parameters cannot exceed 5 [6,11], implying that F has some zero-sums of size 5. The correspondence between the APN property and the fact that $\mathcal{C}_F^\perp$ has minimum distance 5 has been established in [9]. Since the smallest possible size for a non-trivial zero-sum is 3, F has some zero-sums of size 3 or 4 if and only if F is not APN. □

When F is a randomly chosen function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$, it is clear that any subset of size K is a zero-sum with probability 2^{-2n}. Therefore, random functions have many zero-sums of size $K \geq 5$ and there exist efficient generic algorithms for finding zero-sums. For instance, the generalized birthday algorithm [19] finds a zero-sum of size 2^κ with complexity

$$\mathcal{O}\left(2^{\frac{2n}{\kappa+1}+\kappa}\right),$$

which corresponds to the $2^{\frac{2n}{\kappa+1}+\kappa}$ evaluations of F required for building the 2^κ initial lists of size $2^{\frac{2n}{\kappa+1}}$. When the size of the zero-sum, K, is larger than $2n$, the previous generic algorithm can be improved by the XHASH attack [3], as pointed out in [5,1]: the complexity of this improved algorithm essentially corresponds to K evaluations of F, while the generalized birthday algorithm behaves similarly only for $K \geq 2^{\sqrt{2n}}$. It is worth noticing that the information set decoding algorithm (and its variants [7]) can also be used for solving this problem and improve the previous algorithm when the size of the zero-sum is very small [12], but all these methods take as input a generator matrix for the code and then require a complete evaluation of F.

There is a trivial case where zero-sums can be easily found: any affine subspace of dimension $\deg(F)+1$ is a zero-sum for F, leading to a distinguishing property when $\deg(F) \leq n-1$ (resp. $\deg(F) \leq n-2$ if F is a permutation)[3]. These zero-sums exactly correspond to the minimum-weight codewords of $R(n, n-\deg(F)-1) \subset \mathcal{C}_F^\perp$, where $R(n,r)$ denotes the Reed-Muller code of length 2^n and order r, *i.e.*, the set of all Boolean functions of n variables and degree at most r. This is because $\mathcal{C}_F \subset R(n, \deg(F))$ and the dual of $R(n,r)$ is $R(n, n-r-1)$.

2.2 Zero-sum partitions

However, in the case where F is a permutation over $\mathbb{F}_2^n$, the minimum-weight codewords of $R(n, n-\deg(F)-1)$ correspond to zero-sums with an additional property: any coset of such a zero-sum is still a zero-sum. This leads to a much stronger property, named *zero-sum partition*.

Definition 2. *Let P be a permutation from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. A* zero-sum partition *for P of size $K = 2^k$ is a collection of 2^{n-k} disjoint zero-sums $X_i = \{x_{i,1}, \ldots, x_{i,2^k}\} \subset \mathbb{F}_2^n$,* i.e.,

$$\bigcup_{i=1}^{2^{n-k}} X_i = \mathbb{F}_2^n \text{ and } \sum_{j=1}^{2^k} x_{i,j} = \sum_{j=1}^{2^k} P(x_{i,j}) = 0, \ \forall 1 \leq i \leq 2^{n-k} \ .$$

A generic algorithm for finding a zero-sum partition of size 2^κ, with $2^\kappa \geq 2n$, consists in iteratively applying the XHASH attack as follows: we first apply this method for finding a zero-sum of size 2^{n-1}, which defines a zero-sum partition of $\mathbb{F}_2^n$. Then, within both resulting sets of size 2^{n-1}, the same technique is applied for finding a zero-sum of size 2^{n-2}. And the algorithm is iterated until a decomposition into zero-sums of size 2^κ is found. With this algorithm, we need to evaluate the permutation at all points except the last $2^\kappa - 2n$ points. Besides these evaluations of the permutation, the complexity of the algorithm can be approximated by $\big((2n)^3(2^{n-\kappa}-1)\big)$, leading to an overall complexity of roughly $\big(2^n + 2^{n-\kappa}(2n)^3 - 2^\kappa\big)$.

It clearly appears that, for a randomly chosen permutation, the description of the zero-sums found by such a generic algorithm requires the evaluation of the permutation at almost all points since the searching technique is not deterministic. This makes a huge difference with zero-sum partitions coming from a structural property of the permutation, which can be described by means of some close formula. Note that, structural zero-sums like those described in this paper can be used for proving that some given permutations do not satisfy the expected property, and this may only require the evaluation of the permutation on a few sets X_i.

3 Exploiting the degree of the nonlinear part

In the rest of the paper we focus on the search for zero-sum partitions coming from structural properties of the permutation P, when P is an iterated permutation of the form

$$P = R_r \circ \ldots \circ R_1,$$

where all R_i are simpler permutations over $\mathbb{F}_2^n$, named the *round permutations*. In most practical cases, all R_i are derived from a unique keyed permutation for r different choices of the parameter. The first weakness which has been exploited in [2] for constructing zero-sum partitions for some iterated permutations is the low algebraic degrees of the round permutation and of its inverse.

[3] In this paper, the *degree* of a Boolean function corresponds to the degree of its algebraic normal form. Moreover, the *degree* of a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is defined as the highest degree of its coordinates.

3.1 Zero-sum partitions from higher-order derivatives

As previously mentioned, the algebraic degree of a permutation F provides some particular zero-sums, which correspond to all affine subspaces of $\mathbb{F}_2^n$ with dimension $(\deg(F)+1)$. This result comes from the following property of higher-order derivatives of a function.

Definition 3. *[17] Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. For any $a \in \mathbb{F}_2^n$ the* derivative *of F with respect to a is the function $D_aF(x) = F(x+a) + F(x)$. For any k-dimensional subspace V of $\mathbb{F}_2^n$, the k-th order derivative of F with respect to V is the function defined by*

$$D_VF(x) = D_{a_1}D_{a_2}\dots D_{a_k}F(x) = \sum_{v\in V} F(x+v), \forall x \in \mathbb{F}_2^n \ .$$

It is well-known that the degree of any first-order derivative of a function is strictly less than the degree of the function. This simple remark, which is also exploited in higher-order differential attacks [13], implies that for every subspace V of dimension $(\deg F + 1)$,

$$D_VF(x) = \sum_{v\in V} F(x+v) = 0, \quad \text{for every} \quad x \in \mathbb{F}_2^n.$$

The fact that the permutation used in a hash function does not depend on any secret parameter allows to exploit the previous property starting from the middle, *i.e.*, from an intermediate internal state. This property was used by Aumasson and Meier [2] and also by Knudsen and Rijmen in the case of a known-key property of a block cipher [14]. The only information needed for finding such zero-sums on the iterated permutation using this first approach is an upper bound on the algebraic degrees of both the round transformation and its inverse.

More precisely, we consider $P = R_r \circ \dots \circ R_1$, and we choose some integer t, $1 \le t \le r$. We define the following functions involved in the decomposition of P: F_{r-t} consists of the last $(r-t)$ round transformations, *i.e.*, $F_{r-t} = R_r \circ \dots \circ R_{t+1}$ and G_t consists of the inverse of the first t round transformations, *i.e.*, $G_t = R_1^{-1} \circ \dots \circ R_t^{-1}$. Then, we can find many zero-sum partitions for P by the technique introduced in [2] and described in the following proposition.

Proposition 2. *Let d_1 and d_2 be such that $\deg(F_{r-t}) \le d_1$ and $\deg(G_t) \le d_2$. Let V be any subspace of $\mathbb{F}_2^n$ of dimension $d+1$ where $d = \max(d_1, d_2)$, and let W denote the complement of V,* i.e., *$V \oplus W = \mathbb{F}_2^n$. Then, the sets*

$$X_a = \{G_t(a+z),\ z \in V\}, \quad a \in W$$

form a zero-sum partition of $\mathbb{F}_2^n$ of size 2^{d+1} for the r-round permutation P.

Proof. Let a be any element in W. First, we prove that all input states $x \in X_a$ sum to zero:

$$\sum_{x\in X_a} x = \sum_{z\in V} G_t(a+z) = D_VG_t(a)$$

which is the value of a derivative of order $(d+1)$ of a function with degree $d_2 \le d$ and thus it vanishes. Now, the images of these input states under P correspond to the images of the intermediate states z under F_{r-t}. Similarly, we have

$$\sum_{x\in X_a} P(x) = \sum_{z\in V} F_{r-t}(a+z) = D_VF_{r-t}(a)$$

which is the value of a derivative of order $(d+1)$ of a function of degree less than d. Thus, this sum vanishes, implying that each X_a is a zero-sum. Since all X_a are the images of disjoint sets by the permutation G_t, they are all disjoint and then they form a partition of $\mathbb{F}_2^n$. □

The permutations studied in [2] consist in iterating a low-degree round transformation. Then, the zero-sum partitions described in [2] are obtained by choosing for V a subspace spanned by $(d+1)$ elements of the canonical basis, where $d = \max(\deg(F_{r-t}), \deg(G_t))$.

3.2 An improved bound on the degree based on the Walsh spectrum

It clearly appears from the description of the previous method that we are interested in estimating the degree of a composed permutation and of its inverse. If F and G are two mappings from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$, we can bound the degree of the composition $G \circ F$ by $\deg(G \circ F) \leq \deg(G)\deg(F)$. Though, this trivial bound is often very little representative of the real degree of the permutation, in particular if we are trying to estimate the degree after a high number of rounds. In some special cases, exploring the spectral properties of the permutation can lead to a better upper bound. In particular, it was shown by Canteaut and Videau [8] that the trivial bound can be improved when the values occurring in the Walsh spectrum of F are divisible by a high power of 2.

The Walsh spectrum of a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ consists of the Walsh spectra of all nonzero linear combinations of its coordinates:

$$\left\{ \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x}, b \in \mathbb{F}_2^n \setminus \{0\}, a \in \mathbb{F}_2^n \right\},$$

where $x \cdot y$ denotes the dot product between two vectors x and y. The divisibility by a large power of 2 of all elements in the Walsh spectrum of F may provide an upper bound on the degree of $G \circ F$.

Theorem 1. *[8] Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ such that all values in its Walsh spectrum are divisible by 2^ℓ, for some integer ℓ. Then, for any $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$, we have*

$$\deg(G \circ F) \leq n - \ell + \deg(G).$$

From now on, we focus on a very common case where the Walsh spectrum of the round permutation is divisible by a large power of 2 and when its nonlinear part, denoted by χ, consists of n/n_0 parallel applications of a small permutation χ_0 over $\mathbb{F}_2^{n_0}$. In this situation, any n-bit vector is seen as a collection of $n_r = n/n_0$ rows, where each row is an element in $\mathbb{F}_2^{n_0}$. Then, χ applies on each row separately. For implementation reasons, this situation occurs for many iterated permutations used in cryptography. Then, since the Walsh spectrum is invariant under composition with a linear transformation, for any $\alpha \in \mathbb{F}_2^n$, there exists some β such that

$$\mathcal{F}(R + \varphi_\alpha) = \mathcal{F}(\chi + \varphi_\beta) = \prod_{i=1}^{n_r} \mathcal{F}(\chi_0 + \varphi_{\beta_i}) \,. \tag{1}$$

Then, if all elements in the Walsh spectrum of χ_0 are divisible by 2^{ℓ_0}, we deduce that the Walsh spectrum of the round transformation is divisible by $2^{n_r \ell_0}$.

4 Exploiting the structure of the diffusion part

Besides the degree of the round transformation, a second element can be exploited for constructing zero-sum partitions, similarly to the techniques used for mounting saturation attacks. Indeed, the fact that χ consists of many parallel applications of a smaller function can be used for extending the previously described zero-sum partitions to one additional round. Moreover, we can also exploit the fact that a few iterations of the round permutation R are not enough for providing full diffusion. This leads to some *multiset* properties for a small number of rounds.

In the following, we denote by B_i, $0 \leq i < n_r$, the n_0-dimensional subspaces corresponding to the rows, *i.e.*,

$$B_i = \langle e_{n_0 i}, \ldots, e_{n_0 i + n_0 - 1} \rangle$$

where $e_0, \ldots, e_{n-1}$ denotes the canonical basis of $\mathbb{F}_2^n$ and where the positions of the n bits in the internal state are numbered such that the n_0-bit rows correspond to n_0 consecutive bits.

4.1 One-round multiset property

First, we show how to extend a number of zero-sum partitions that have been found for t rounds, to $t+1$ rounds, without increasing the complexity. The idea is the following: the zero-sum partition described in Proposition 2 is obtained from a set of intermediate states after t rounds, which is a coset of a $(d+1)$-dimensional subspace V. Moreover, such a zero-sum partition is obtained for any choice of V. However, we now focus on those subspaces V which correspond to a collection of any $\lceil (d+1)/n_0 \rceil$ rows: $V = \bigoplus_{i \in \mathcal{I}} B_i$, for some set $\mathcal{I} \subset \{0, \ldots, n_r\}$ of size $\lceil (d+1)/n_0 \rceil$. Since χ applies to the rows separately, variables from different rows are not mixed after the application of χ. This implies that $\chi(a+V) = b+V$, for some b. Then, we can find some zero-sum partitions of size 2^{d+1} for the r-round permutation P as follows.

Proposition 3. *Let d_1 and d_2 be such that $\deg(F_{r-t-1}) \leq d_1$ and $\deg(G_t) \leq d_2$. Let us decompose the round transformation after t rounds into $R_{t+1} = A_2 \circ \chi \circ A_1$ where both A_1 and A_2 have degree 1. Let $\mathcal{I}$ be any subset of $\{0, \ldots, n_r - 1\}$ of size $\lceil (d+1)/n_0 \rceil$,*

$$V = \bigoplus_{i \in \mathcal{I}} B_i$$

and W be its complement. Then, the sets

$$X_a = \{(G_t \circ A_1^{-1})(a+z),\ z \in V\}, \quad a \in W$$

form a zero-sum partition of $\mathbb{F}_2^n$ of size 2^k, with $k = n_0 \lceil \frac{d+1}{n_0} \rceil$, for the r-round permutation P.

Proof. For any a, the sum of all input states in X_a is given by

$$\sum_{x \in X_a} x = \sum_{z \in V} G_t \circ A_1^{-1}(a+z) = D_V(G_t \circ A_1^{-1})(a) = 0$$

since $\deg(G_t \circ A_1^{-1}) = \deg(G_t) \leq d$. Using that $\chi(a+V) = b+V$, we obtain that the sum of the corresponding outputs satisfies

$$\begin{aligned} \sum_{x \in X_a} P(x) = \sum_{z \in V} F_{r-t-1} \circ A_2 \circ \chi(a+z) &= \sum_{z \in V} F_{r-t-1} \circ A_2(b+z) \\ &= D_V(F_{r-t-1} \circ A_2)(b) = 0 \end{aligned}$$

since $\deg(F_{r-t-1} \circ A_2) = \deg(F_{r-t-1}) \leq d$. □

4.2 Multiset property on several rounds

Now, we consider some multiset properties on several rounds which arise both from the particular structure of the round transformation and from the linear part, and we show how they can be exploited to further extend the already known zero-sum partitions to more rounds. For the sake of clarity, we first describe a 2-round multiset property for Rounds $(t+1)$ and $(t+2)$. We decompose those two rounds into

$$R_{t+2} \circ R_{t+1} = A_2 \circ \chi \circ A \circ \chi \circ A_1$$

where A_1, A_2 and A have degree 1.

Theorem 2. *Let d_1 and d_2 be such that $\deg(F_{r-t-2}) \leq d_1$ and $\deg(G_t) \leq d_2$. Let L denote the linear part of the affine permutation A. Let W be a k-dimensional subspace of $\mathbb{F}_2^n$ satisfying both following conditions*

(i) *there exists a set $\mathcal{I} \subset \{0, \ldots, n_r - 1\}$ such that*

$$W \subset \bigoplus_{i \in \mathcal{I}} B_i \text{ and } |\mathcal{I}| \leq n_r - \left\lceil \frac{d_2+1}{n_0} \right\rceil .$$

(ii) *there exists a set* $\mathcal{J} \subset \{0, \ldots, n_r - 1\}$ *such that*

$$L(W) \subset \bigoplus_{j \in \mathcal{J}} B_j \text{ and } |\mathcal{J}| \leq n_r - \left\lceil \frac{d_1 + 1}{n_0} \right\rceil .$$

Let V *denote the complement of* W*. Then, the sets*

$$X_a = \{(G_t \circ A_1^{-1} \circ \chi^{-1})(a + z),\ z \in V\},\ \ a \in W$$

form a zero-sum partition of $\mathbb{F}_2^n$ *of size* 2^{n-k} *for the* r*-round permutation* P*.*

Proof. The definition of the sets X_a means that we choose the intermediate states z after the nonlinear layer in R_{t+1} in a coset of V. The required properties on W imply that there exist two subspaces B_b and B_f such that

$$B_b = \bigoplus_{i \in \overline{\mathcal{I}}} B_i \subset V \text{ and } B_f = \bigoplus_{j \in \overline{\mathcal{J}}} B_j \subset L(V)$$

with $\overline{\mathcal{I}} = \{0, \ldots, n_r - 1\} \setminus \mathcal{I}$ and $\overline{\mathcal{J}} = \{0, \ldots, n_r - 1\} \setminus \mathcal{J}$, where the last relation comes from the fact that $L(V)$ and $L(W)$ are complementary. From the second property, we deduce that $A(V)$ can be seen as a union of cosets of B_f:

$$A(V) = \bigcup_{b \in \mathcal{E}} (b + B_f) ,$$

where $\mathcal{E}$ is a subset of $\mathbb{F}_2^n$. Moreover, the same property holds for the image by A of any coset of V. Then, since χ applies to the rows separately, variables from different rows are not mixed after the application of χ. This implies that

$$\chi(A(V)) = \bigcup_{b \in \mathcal{E}'} (b + B_f) ,$$

where $\mathcal{E}'$ is another subset of $\mathbb{F}_2^n$. By definition, the images by P of all elements in X_a correspond to the images of $a + z$, $z \in V$, by $F_{r-t-2} \circ A_2 \circ \chi \circ A$. It follows that their sum is given by

$$\begin{aligned} \sum_{z \in V} F_{r-t-2} \circ A_2 \circ \chi \circ A(a + z) &= \sum_{b \in \mathcal{E}'} \sum_{x \in B_f} (F_{r-t-2} \circ A_2)(b + x) \\ &= \sum_{b \in \mathcal{E}'} D_{B_f}(F_{r-t-2} \circ A_2)(b) = 0 . \end{aligned}$$

Actually, this derivative vanishes since

$$\dim B_f \geq n - n_0 |\mathcal{J}| > d_1 .$$

Now, we compute backwards the images of $a + V$ by $G_t \circ A_1^{-1} \circ \chi^{-1}$. Since V satisfies $B_b \subset V$, it can be written as a union of cosets of B_b. As χ^{-1} does not mix the rows, we deduce that

$$\chi^{-1}(a + V) = \bigcup_{b \in \mathcal{E}''} (b + B_b) ,$$

for some set $\mathcal{E}'' \subset \mathbb{F}_2^n$. Then, the sum of the corresponding input states $x \in X_a$ is given by

$$\begin{aligned} \sum_{x \in X_a} x = \sum_{z \in V} (G_t \circ A_1^{-1} \circ \chi^{-1})(a + z) &= \sum_{b \in \mathcal{E}''} \sum_{x \in B_b} (G_t \circ A_1^{-1})(b + x) \\ &= \sum_{b \in \mathcal{E}''} D_{B_b}(G_t \circ A_1^{-1})(b) = 0 . \end{aligned}$$

Actually, this derivative vanishes since

$$\dim B_b \geq n - n_0 |\mathcal{I}| > d_2 .$$

□

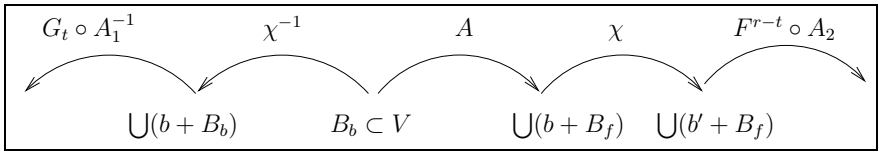

Fig. 1. General method with a 2-round multiset property

Figure 1 summarizes the steps of our method.

Remark 1. There is a simple necessary condition on the existence of some W as in the previous theorem. We define the weight of any $x \in \mathbb{F}_2^n$ with respect to the decomposition into rows, $H_w(x)$, as the number of rows on which x does not vanish. Then, a subspace W defined as in the previous theorem satisfies

$$\forall x \in W,\ H_w(x) \leq n_r - \left\lceil \frac{d_2+1}{n_0} \right\rceil \text{ and } H_w(L(x)) \leq n_r - \left\lceil \frac{d_1+1}{n_0} \right\rceil . \tag{2}$$

Obviously, this condition is also sufficient when $\dim W = 1$. In particular, the search for zero-sum partitions by the method described in Theorem 2 can be avoided by choosing for the linear part of the round transformation a function L such that

$$\min_{x \neq 0} \left(H_w(x) + H_w(L(x))\right) > 2n_r - \left\lceil \frac{d_1+1}{n_0} \right\rceil - \left\lceil \frac{d_2+1}{n_0} \right\rceil .$$

Now, we can obviously use a similar property of the diffusion not only for 2 rounds of the round transformation, but for a higher number of rounds.

Theorem 3. *Let d_1 and d_2 be such that $\deg(F_{r-t-2}) \leq d_1$ and $\deg(G_t) \leq d_2$. Let L denote the linear part of the affine permutation A. Let W be a k-dimensional subspace of $\mathbb{F}_2^n$ satisfying all following conditions for two nonzero integers s_b and s_f:*

(i) *there exists a set $\mathcal{I}_1 \subset \{0, \ldots, n_r - 1\}$ such that*

$$W \subset \bigoplus_{i \in \mathcal{I}_1} B_i \text{ and } |\mathcal{I}_1| \leq n_r - \left\lceil \frac{d_2+1}{n_0} \right\rceil .$$

(ii) *there exists a set $\mathcal{J}_1 \subset \{0, \ldots, n_r - 1\}$ such that*

$$L(W) \subset \bigoplus_{j \in \mathcal{J}_1} B_j \text{ and } |\mathcal{J}_1| \leq n_r - \left\lceil \frac{d_1+1}{n_0} \right\rceil .$$

(iii) *for all s, $1 \leq s < s_f$, there exists a set $\mathcal{J}_{s+1} \subset \{0, \ldots, n_r - 1\}$ such that*

$$L\left(\bigoplus_{j \in \mathcal{J}_s} B_j\right) \subset \bigoplus_{j \in \mathcal{J}_{s+1}} B_j \text{ and } |\mathcal{J}_{s_f}| \leq n_r - \left\lceil \frac{d_1+1}{n_0} \right\rceil .$$

(iv) *for all s, $1 \leq s < s_b$, there exists a set $\mathcal{I}_{s+1} \subset \{0, \ldots, n_r - 1\}$ such that*

$$L^{-1}\left(\bigoplus_{j \in \mathcal{I}_s} B_j\right) \subset \bigoplus_{j \in \mathcal{I}_{s+1}} B_j \text{ and } |\mathcal{I}_{s_b}| \leq n_r - \left\lceil \frac{d_2+1}{n_0} \right\rceil .$$

Let V denote the complement of W. Then, the sets

$$X_a = \{(G_t \circ A_1^{-1} \circ (\chi^{-1} \circ A^{-1})^{s_b - 1} \circ \chi^{-1})(a + z),\ z \in V\},\ \ a \in W$$

form a zero-sum partition of $\mathbb{F}_2^n$ of size 2^{n-k} for the $(r + s_b + s_f - 2)$-round permutation P.

It is worth noticing that there is no requirement on the sizes of the intermediate states $\mathcal{I}_2, \ldots, \mathcal{I}_{s_b-1}$ and $\mathcal{J}_2, \ldots, \mathcal{J}_{f_b-1}$. However, by definition, the conditions on the sizes of $\mathcal{I}_{s_b}$ and $\mathcal{I}_{s_f}$ obviously imply that the same bounds hold for the corresponding intermediate sets.

5 Application to the KECCAK-f permutation

5.1 The KECCAK-f permutation

KECCAK [4] is one of the fourteen hash functions selected for the second round of the SHA-3 competition. Its mode of operation is the sponge construction. The inner primitive in KECCAK is a permutation, composed of several iterations of very similar round transformations. Within the KECCAK-family, the SHA-3 candidate operates on a 1600-bit state, which is represented by a 3-dimensional binary matrix of size $5 \times 5 \times 64$. Then, the state can be seen as 64 parallel slices, each one containing 5 rows and 5 columns. The permutation in KECCAK is denoted by KECCAK-$f[b]$, where b is the size of the state. So, for the SHA-3 candidate, $b = 1600$.

The number of rounds in KECCAK-$f[1600]$ was 18 in the original submission, and it has been updated to 24 for the second round. Every round R consists of a sequence of 5 permutations modifying the state:

$$R = \iota \circ \chi \circ \pi \circ \rho \circ \theta.$$

The functions θ, ρ, π, ι are transformations of degree 1 providing diffusion in all directions of the 3-dimensional state. Then, keeping the same notation as in the previous section, we have $A_1 = \pi \circ \rho \circ \theta$, which is linear and $A_2 = \iota$, which corresponds to the addition of a constant value. Therefore, the linear part of $A = A_1 \circ A_2$ corresponds to $L = \pi \circ \rho \circ \theta$. The nonlinear layer, χ, is a quadratic permutation which is applied to each row of the 1600-bit state. In other words, 320 parallel applications of χ_0 are implemented in order to provide confusion. The inverse permutation, denoted by χ^{-1}, is a permutation of degree 3.

We need to define a numbering for the $n = 1600$ bits of the internal state of KECCAK-f. We associate to the bit of the state positioned at the intersection of the i-th row and the j-th column of the k-th slice, *i.e.*, to the element (i, j, k), $0 \leq i \leq 4$, $0 \leq j \leq 4$, $0 \leq k \leq 63$, the number $25k + 5j + i$. We recall that the elements of the form $(0, 0, z)$ are found in the center of each slice. Then, the 5-dimensional subspace corresponding to the j-th row in the k-th slice, $0 \leq j \leq 4$, $0 \leq k \leq 63$, is defined by

$$B_{5k+j} = \langle e_{25k+5j}, e_{25k+5j+1}, e_{25k+5j+2}, e_{25k+5j+3}, e_{25k+5j+4} \rangle.$$

Aumasson and Meier [2] used the trivial bound on the degree of a composed function in order to find many zero-sum partitions for 16 rounds of the KECCAK-f permutation. Actually, the degree of the permutation after 10 rounds is at most $2^{10} = 1024$ and the degree of the inverse after 6 rounds is at most $3^6 = 729$. Thus, they choose the intermediate states after $t = 6$ rounds in a coset of a subspace V of dimension 1025 and compute 6 rounds backwards. This method leads to many zero-sum partitions of size 2^{1025}.

5.2 Zero-sum partitions for 18 rounds of KECCAK-f

We first show that the degree of 7 rounds of the inverse KECCAK-f permutation cannot exceed 1369 and thus is much lower than the estimation given by the trivial bound $\min(3^7 = 2187, 1599)$. Actually, all elements in the Walsh spectrum of the nonlinear permutation χ_0 are divisible by 2^3. Since the Walsh spectra of a permutation and of its inverse are the same, we deduce that the Walsh spectrum of χ_0^{-1} is also divisible by 2^3. It is worth noticing that $2^{\frac{n+1}{2}}$ is the lowest possible divisibility for the Walsh spectrum of a quadratic permutation of $\mathbb{F}_2^n$, n odd. Then, the fact that the Walsh spectrum of χ_0^{-1} is divisible by 2^3 holds for any other choice for the quadratic permutation χ_0 over $\mathbb{F}_2^5$. There are $n_r = 320$ parallel applications of χ_0. Then, we deduce from (1) that the Walsh spectra of R and R^{-1} applied on the whole 1600-bit state are divisible by $2^{3 \times 320} = 2^{960}$. Using that 6 rounds of the inverse of the round permutation have degree at most $3^6 = 729$, Theorem 1 leads to

$$\deg(R^{-7}) = \deg(R^{-6} \circ R^{-1}) \leq 1600 - 960 + \deg(R^{-6}) \leq 1369\ .$$

This new bound allows us to find zero-sum partitions for 17 rounds of the permutation, by choosing the intermediate states after $t = 7$ rounds in the cosets of a subspace V of dimension 1370 and by computing 7 rounds backwards. Moreover, we can apply Proposition 3 with $t = 7$: by choosing $V = \bigoplus_{i \in \mathcal{I}} B_i$ where $\mathcal{I}$ is any collection of 274 rows, we can find some zero-sum partitions of size 2^{1370} for 18 rounds of KECCAK-f.

5.3 Zero-sum partitions for 19 rounds of KECCAK-f

Now, we apply Theorem 2 with $t = 7$ to 19 rounds of KECCAK-f. As previously explained, $F_{r-t-2} = F_{10}$ has degree at most 1024 and $G_t = G_7$ has degree at most 1369. We then need to find a subspace W such that there exist two sets of rows, $\mathcal{I}, \mathcal{J} \subset \{0, \ldots, n_r - 1\}$ satisfying

$$W \subset \bigoplus_{i \in \mathcal{I}} B_i \text{ with } |\mathcal{I}| \leq 46 \text{ and } L(W) \subset \bigoplus_{j \in \mathcal{J}} B_j \text{ with } |\mathcal{J}| \leq 115 \,.$$

Here, we take for W the subspace spanned by the first 4 slices, *i.e.*, $W = \bigoplus_{i=0}^{19} B_i$. Then, we can check that there exists a subset $\mathcal{J}$ of size 114 such that $L(W) \subset \bigoplus_{j \in \mathcal{J}} B_j$, implying that the second condition is satisfied. The first condition obviously holds by definition of W. Since $\dim W = 5 \times 20 = 100$, we deduce from Theorem 2 that we have found a zero-sum partition of size 2^{1500} for 19 rounds of KECCAK-f. It is worth noticing that the previous situation occurs when W is the subspace spanned by any 4 consecutive slices. Actually, all the step-mappings in the KECCAK-f round permutation except ι are translation invariant in the z axis direction. Therefore, we obtain 64 zero-sum partitions of this type for the 19-round KECCAK-f.

Though, we can further improve the complexity of the 19-round distinguisher by increasing the dimension of W, without at the same time increasing the cardinality of $\mathcal{J}$, where $L(W) \subset \bigoplus_{j \in \mathcal{J}} B_j$. In order to achieve this, we add to W a number of linearly independent vectors whose images by L lie in $\bigoplus_{j \in \mathcal{J}} B_j$ for the set $\mathcal{J}$ as before. The new considered subspace W is generated by the rows $0, \ldots, 19$ and by the following 39 linearly independent vectors.

$$\begin{array}{lllll}
e_{450} \oplus e_{460}, & e_{450} \oplus e_{465}, & e_{451} \oplus e_{461}, & e_{451} \oplus e_{466}, & e_{464} \oplus e_{469}, \\
e_{475} \oplus e_{485}, & e_{475} \oplus e_{490}, & e_{476} \oplus e_{486}, & e_{476} \oplus e_{491}, & e_{478} \oplus e_{498}, \\
e_{489} \oplus e_{494}, & e_{650} \oplus e_{660}, & e_{650} \oplus e_{665}, & e_{651} \oplus e_{666}, & e_{652} \oplus e_{662}, \\
e_{659} \oplus e_{664}, & e_{662} \oplus e_{672}, & e_{667} \oplus e_{672}, & e_{668} \oplus e_{673}, & e_{1100} \oplus e_{1110}, \\
e_{1102} \oplus e_{1112}, & e_{1102} \oplus e_{1117}, & e_{1103} \oplus e_{1113}, & e_{1103} \oplus e_{1118}, & e_{1105} \oplus e_{1110}, \\
e_{1106} \oplus e_{1116}, & e_{1125} \oplus e_{1135}, & e_{1127} \oplus e_{1137}, & e_{1127} \oplus e_{1142}, & e_{1138} \oplus e_{1143}, \\
e_{1150} \oplus e_{1160}, & e_{1152} \oplus e_{1162}, & e_{1162} \oplus e_{1167}, & e_{1163} \oplus e_{1168}, & e_{1175} \oplus e_{1180}, \\
e_{1175} \oplus e_{1185}, & e_{1175} \oplus e_{1190}, & e_{1177} \oplus e_{1187}, & e_{1188} \oplus e_{1193}. &
\end{array}$$

These 39 elements correspond to words whose support belongs to a single column and that have a Hamming weight of 2. Actually, any word X with support belonging to a single column and having even weight satisfies $\theta(X) = X$. Then, if X is a word of this type, the weight of $L(X)$, with respect to our definition in Remark 1, is exactly 2. One can easily check that $W \subset \bigoplus_{i \in \mathcal{I}} B_i$, with $|\mathcal{I}| = 46$ and $L(W) \subset \bigoplus_{j \in \mathcal{J}} B_j$, with $|\mathcal{J}| = 115$. Since $\dim W = 5 \times 20 + 39 = 139$, Theorem 2 leads to 64 new zero-sum partitions of size 2^{1461} for 19 rounds of KECCAK-f.

5.4 Zero-sum partitions for 20 rounds of KECCAK-f

For finding a zero-sum partition for 20 rounds of KECCAK-f, we now apply Theorem 3 with $s_f = 2$, *i.e.*, we compute one additional step forwards. Then, we need to find a subspace W such that there exist some sets of rows, $\mathcal{I}$, $\mathcal{J}_1$ and $\mathcal{J}_2$ with $|\mathcal{I}| \leq 46$ and $|\mathcal{J}_2| \leq 115$ satisfying

$$W \subset \bigoplus_{i \in \mathcal{I}} B_i, \;\; L(W) \subset \bigoplus_{j \in \mathcal{J}_1} B_j \text{ and } L\left(\bigoplus_{j \in \mathcal{J}_1} B_j\right) \subset \bigoplus_{j \in \mathcal{J}_2} B_j \,.$$

As previously mentioned, the image by L of 4 consecutive slices involves 114 rows only. Then, we only have to find a subspace W such that the first condition holds and that $L(W)$ belongs to the union of 4 consecutive slices, namely slices s to $s+3$. For this search, we concentrate as before on the words with Hamming weight 2 whose support belongs to a single column. We want to find all words X of this form such that the two rows that are affected by $L(X)$ are positioned in at most two out of the four consecutive slices s to $s + 3$, for a

fixed s. For this, we need to look at the translation offsets of ρ, which is the function translating the bits in the z-direction. These offsets are given in Table 2(a). Let (x, y, z) and (x, y', z) be the coordinates of the two bits in the support of X. Let c_1 and c_2 be the offsets corresponding to the positions (x, y) and (x, y'). Then the image of X by L will affect two slices at distance $|c_1 - c_2|$.

Suppose that we can find two translation offsets in the same column of Table 2(a) having a difference smaller than or equal to 3, namely $c_1 = \text{Offset}(x_0, y_1)$, and $c_2 = \text{Offset}(x_0, y_2)$ with $0 \leq (c_2 - c_1) \leq 3$. Then, the word in the slice $z_0 = s - c_1 \bmod 64$ with support $\{(x_0, y_1, z_0), (x_0, y_2, z_0)\}$ will have an image belonging to the slices s and $s + (c_2 - c_1)$. The appropriate pairs of translation constants derived from Table 2(a) are given in Table 2(b).

	$x=3$	$x=4$	$x=0$	$x=1$	$x=2$
$y=2$	25	39	3	10	43
$y=1$	55	20	36	44	6
$y=0$	28	27	0	1	62
$y=4$	56	14	18	2	61
$y=3$	21	8	41	45	15

(a) The translation offsets of ρ for the SHA-3 candidates.

	(y_1, y_2)	(c_1, c_2)	$c_2 - c_1$
$x=0$	$(0,2)$	$(0,3)$	3
$x=1$	$(0,4)$	$(1,2)$	1
	$(1,3)$	$(44,45)$	1
$x=2$	$(0,4)$	$(62,61)$	1
$x=3$	$(1,4)$	$(55,56)$	1
	$(0,2)$	$(28,25)$	3

(b) Appropriate pairs of offsets.

By using this technique, we find the following subspace W of dimension 14:

$$W = \langle\, e_1 \oplus e_{21},\quad e_{25} \oplus e_{35},\quad e_{26} \oplus e_{46},\quad e_{51} \oplus e_{71},\quad e_{102} \oplus e_{122},$$
$$e_{127} \oplus e_{147},\quad e_{152} \oplus e_{172},\quad e_{258} \oplus e_{273},\quad e_{283} \oplus e_{298},\quad e_{308} \oplus e_{323},$$
$$e_{531} \oplus e_{541},\quad e_{556} \oplus e_{566},\quad e_{581} \oplus e_{591},\quad e_{1003} \oplus e_{1013} \rangle.$$

Clearly $W \subset \bigoplus_{i \in \mathcal{I}} B_i$ with $|I| < 114$ and we have computed that $L(W)$ belongs to the union of the slices $1, 2, 3$ and 4. Since $\dim W = 14$ we deduce from Theorem 2 that we have found a zero-sum partition of size 2^{1586} for 20 rounds of Keccak-f. As previously explained, there are 64 such zero-sum partitions, obtained by translating the previous W in the z-direction.

6 Application to the Hamsi-256 finalization permutation

Hamsi [16] is another candidate among the fourteen functions selected for the second round of the SHA-3 competition. It is based on a Davies-Meyer construction. It uses a finalization permutation P_f which operates on a 512-bit internal state corresponding to the concatenation of the 256-bit chaining value and of a 256-bit codeword resulting from the expansion of the last 32-bit message block. In Hamsi-256, P_f consists of 6 rounds of a round transformation $R = L \circ S$, where S corresponds to 128 parallel applications of a 4×4 Sbox of degree 3. Using that three iterations of the round transformation have degree at most $3^3 = 27$, Proposition 2 leads to zero-sum partitions of size 2^{28}, as reported in [1]. However, our techniques can be used for exhibiting zero-sum partitions of smaller size.

First, we define a numbering for the bits of the internal state. The j-th bit in the word which lies in the k-th column and i-th row is numbered by $128k + 4j + i$, where $0 \leq j \leq 31$, $0 \leq i \leq 3$ and $0 \leq k \leq 3$. We also define the subspace B_i, $0 \leq i < 128$ spanned by a column of the internal state: $B_i = \langle e_{4i}, e_{4i+1}, e_{4i+2}, e_{4i+3} \rangle$ (the columns of the internal state play the same role as the rows in KECCAK).

Here, we choose the intermediate state after $t = 3$ rounds of P_f into the 19-dimensional subspace

$$V = \bigoplus_{i=14}^{16} B_i \oplus \langle e_{68}, e_{237}, e_{241}, e_{245}, e_{249}, e_{507}, e_{511} \rangle \ .$$

Then, we consider the sets $X_a = \{((R^{-1})^2 \circ S^{-1})(a + z),\ z \in V\}$. Actually, we apply the same technique as in Theorem 2. Both V and $S^{-1}(V)$ can be seen as the union of some cosets of $B_{14} \oplus B_{15} \oplus B_{16}$. Since two iterations of R^{-1} have degree at most 9, all elements in X_a sum to zero because $\dim(\bigoplus_{i=14}^{16} B_i) > 9$. Moreover, $\langle e_0, e_4, e_8, e_{12} \rangle \subset L(V)$ and it has been observed in [1] that 3 rounds of R have degree 3 with respect to the first four lsbs of the first word of the internal state. Therefore, since $L(V)$ can be seen as a union of cosets of $B_f = \langle e_0, e_4, e_8, e_{12} \rangle$, and $D_{B_f} R^3(x) = 0$ for all x, we deduce that the images of all elements in X_a under six rounds of R sum to zero. Many zero-sum partitions of size 2^{19} can be constructed by this method, since we only need that $L(V)$ contains the subspace spanned by the first four consecutive bits of any word in the internal state.

Also, zero-sum partitions of size 2^{10} can be easily found for P_f. Consider any 10 elements in a 32-bit word of the state matrix after 3 rounds of the permutation and fix the other bits of the state to an arbitrary value. Then 3 rounds of the permutation applied to this state have degree at most 9. This is because there is only one variable per active Sbox, so every bit after the first round will be a linear function in the variables considered. But 3 rounds of the inverse permutation applied to the state have also degree at most 9, as after the application of L^{-1} there will be variables only in one word per column, implying again at most one active bit per Sbox.

7 Conclusions

We have found zero-sum distinguishers for the finalization permutation of Hamsi-256 and for 20 rounds of KECCAK-f, pointing out that these permutations do not behave like random permutations. For Hamsi-256, this property does not seem to lead to an attack on the hash function since the finalization permutation only applies to the 2^{288} internal states, which can be obtained from the message expansion. For KECCAK reduced to 20 rounds (out of 24), even if the security of the hash function is not affected, our results contradict the so-called hermetic sponge strategy.

Acknowledgments. We would like to thank Christophe De Cannière for his valuable comments and especially for the indication of a better bound on the degree of iterated permutations. This new bound improves in part the results on the KECCAK hash function, presented in this paper.

References

1. J.-P. Aumasson, E. Käsper, L.R. Knudsen, K. Matusiewicz, R. Ødegaard, T. Peyrin, and M. Schläffer. Distinguishers for the compression function and output transformation of hamsi-256. In *Australasian Conference on Information Security and Privacy - ACISP 2010*, Lecture Notes in Computer Science. Springer, 2010. To appear.
2. J.-P. Aumasson and W. Meier. Zero-sum distinguishers for reduced KECCAK-f and for the core functions of Luffa and Hamsi. Presented at the rump session of Cryptographic Hardware and Embedded Systems - CHES 2009, 2009.
3. M. Bellare and D. Micciancio. A new paradigm for collision-free hashing: Incrementality at reduced cost. In *Advances in Cryptology - EUROCRYPT'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 163–192. Springer, 1997.

4. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. KECCAK sponge function family main document. Submission to NIST (Round 2), 2009.
5. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Note on zero-sum distinguishers of KECCAK-f. Public comment on the NIST Hash competition, available at `http://keccak.noekeon.org/NoteZeroSum.pdf`, 2010.
6. A.E. Brouwer and L.M.G.M. Tolhuizen. A sharpening of the johnsson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters. *Designs, Codes and Cryptography*, 3(2):95–98, 1993.
7. A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to primitive narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, January 1998.
8. A. Canteaut and M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. In *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 518–533. Springer-Verlag, 2002.
9. C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.
10. J. Daemen, L.R. Knudsen, and V. Rijmen. The block cipher Square. In *Fast Software Encryption - FSE'97*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer-Verlag, 1997.
11. S.M. Dodunekov and V. Zinoviev. A note on Preparata codes. In *Proceedings of the 6th Intern. Symp. on Information Theory, Moscow-Tashkent Part 2*, pages 78–80, 1984.
12. M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. In *Advances in Cryptology - ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 88–105. Springer, 2009.
13. L. R. Knudsen. Truncated and higher order differentials. In *Fast Software Encryption - FSE'94*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer-Verlag, 1995.
14. L.R. Knudsen and V. Rijmen. Known-key distinguishers for some block ciphers. In *Advances in cryptology - ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 315–324. Springer, 2007.
15. L.R. Knudsen and D. Wagner. Integral cryptanalysis. In *Fast Software Encryption - FSE 2002*, volume 2365 of *Lecture Notes in Computer Science*, pages 112–127. Springer-Verlag, 2002.
16. O. Küçük. The Hash Function Hamsi. Submission to NIST (Round 2), 2009.
17. X. Lai. Higher order derivatives and differential cryptanalysis. In *Proc. "Symposium on Communication, Coding and Cryptography", in honor of J. L. Massey on the occasion of his 60'th birthday.* Kluwer Academic Publishers, 1994.
18. F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes.* North-Holland, 1977.
19. D. Wagner. A generalized birthday problem. In *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 288–303. Springer-Verlag, 2002.