A zero-sum property for the KECCAK-f permutation with 18 rounds

Christina Boura, Anne Canteaut

▶ **To cite this version:**

Christina Boura, Anne Canteaut. A zero-sum property for the KECCAK-f permutation with 18 rounds. IEEE International Symposium on Information Theory, ISIT 2010, Jun 2010, Austin, Texas, United States. pp.2488-2492. hal-00738232

HAL Id: hal-00738232
https://hal.science/hal-00738232v1

Submitted on 3 Oct 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Zero-Sum property for the KECCAK-f Permutation with 18 Rounds

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@inria.fr, Anne.Canteaut@inria.fr

Abstract. A new type of distinguishing property, named the zero-sum property has been recently presented by Aumasson and Meier [1]. It has been applied to the inner permutation of the hash function KECCAK and it has led to a distinguishing property for the KECCAK-f permutation up to 16 rounds, out of 24 in total. Here, we additionally exploit some spectral properties of the KECCAK-f permutation and we improve the previously known upper bounds on the degree of the inverse permutation after a certain number of rounds. This result enables us to extend the zero-sum property to 18 rounds of the KECCAK-f permutation, which was the number of rounds in the previous version of KECCAK submitted to the SHA-3 competition.

1 Introduction

KECCAK [2] is a hash function family which has been moved forward to the second round of the SHA-3 competition launched by the NIST. It is based on the sponge construction and uses as a building block an iterated permutation. The KECCAK-f permutation operates on a 1600-bit state; it consists of 24 rounds of a simpler round transformation which has algebraic degree 2 with respect to $\mathbb{F}_2$.

The most interesting analysis of this inner permutation until now is a distinguishing property exhibited by Aumasson and Meier [1]. This type of distinguishing property, named a *zero-sum property*, can be seen as a generalization of an integral property (a.k.a. saturation property) [6, 9]. For a given function F, it corresponds to the existence of some sets of input vectors which sum to zero, and which are such that their respective images by F also sum to zero.

Such sets of inputs, named zero-sums, can be exhibited if the respective degrees of the permutation F and of its inverse F^{-1} after a certain number of rounds is sufficiently low. But, finding a precise estimate for the degree of the function after several rounds is a difficult problem. This question has been partly addressed by Canteaut and Videau in [4]: they have shown that in the special case that all values occurring in the Walsh spectrum of F are divisible by a high power of 2, the degree of the function $F \circ F$ grows much slower than $\deg(F)^2$. This result can be used to find upper bounds on the degree of an iterated function. In particular, it can be applied to improve the trivial bound on the degree of several rounds of the inverse round transformation used in KECCAK-f permutation. Combined with another technique, this enables us to exhibit zero-sums for the KECCAK-f permutation with 18-rounds, which is the permutation which was initially proposed for the SHA-3 candidate [2]. Our result then contradicts the so-called hermetic sponge strategy used by the designers, which aims at using an inner permutation without any structural distinguishing property. However, the existence of this distinguishing property for the inner permutation does not seem to threaten the whole hash function. Moreover, the new version of KECCAK [3] has 24 rounds.

The rest of the paper is organised as follows. Section 2 presents the zero-sum property and the principle of the corresponding distinguisher. Section 3 recalls some well-known properties of Boolean functions, with a focus on their spectral representation. The link between the divisibility of the Walsh coefficients of a function and the degree of the product of its Boolean components, which is a result due to Canteaut and Videau [4], is also presented. Section 4 briefly describes the KECCAK hash function and Section 5 presents the new distinguishing property we have found on 18 rounds of the Keccak-f permutation.

2 The zero-sum property

2.1 Definition

The notion of zero-sum distinguisher has been introduced by J.-P. Aumasson and W. Meier in [1]. For a function F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$, a *zero-sum* is a set of inputs $x_1, \ldots, x_k$ in $\mathbb{F}_2^n$ summing to zero such that their respective images by F sum also to zero, *i.e.*,

$$\bigoplus_{i=1}^{k} x_i = \bigoplus_{i=1}^{k} F(x_i) = 0,$$

where the sum is defined by the addition in $\mathbb{F}_2^n$ (and in $\mathbb{F}_2^m$), *i.e.*, the bitwise exclusive-or. Since it is expected that a randomly chosen function does not have many zero-sums, the existence of several such sets of inputs can be seen as a distinguishing property of F.

2.2 Finding zero-sums

For an iterated function, the existence of many zero-sums is usually due either to the particular structure of the round transformation (*e.g.*, a multiset property like in the AES) or to a low degree. The zero-sum properties exhibited in [1] for the inner permutation used in some hash functions are based on the algebraic degrees of the round transformation and of its inverse. Actually, the algebraic degree of 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 1 (Higher-order derivative). *[10] 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*

$$D_a F(x) = F(x \oplus a) \oplus F(x).$$

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

$$D_V F = D_{a_1} D_{a_2} \ldots D_{a_k} F,$$

where $(a_1, \ldots, a_k)$ is any basis of V. Moreover, we have for any $x \in \mathbb{F}_2^n$

$$D_V F(x) = \bigoplus_{v \in V} F(x \oplus v).$$

In the following, 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.

It is well-known that the degree of any first-order derivative of a function is strictly less than the degree of the function and this simple remark leads to the following useful result, which is also exploited in higher-order differential attacks [7].

Proposition 1. *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. Then, for every subspace V of dimension $(\deg F + 1)$ we have*

$$D_V F(x) = 0, \quad \textit{for every} \quad x \in \mathbb{F}_2^n.$$

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 [1] and also by Knudsen and Rijmen in the case of a known-key property of a block cipher [8]. The only information needed for finding such zero-sums on the iterated permutation is an upper bound on the algebraic degrees of both the round transformation and its inverse.

More precisely, we suppose that F is a function which operates on an n-bit state, and that F is composed of n_r smaller transformations:

$$F = R_{n_r} \circ \ldots \circ R_1.$$

Let $d_1 < n$ be the degree of the function composed of the last r_1 transformations, *i.e.*, $F_{r_1} = R_{n_r} \circ \ldots \circ R_{n_r - r_1 + 1}$ and let $d_2 < n$ be the degree of the inverse of the first $r_2 = (n_r - r_1)$ transformations, *i.e.*, $G_{r_2} = R_1^{-1} \circ \ldots \circ R_{r_2}^{-1}$. Then, we can find many zero-sums of size 2^{d+1} where $d = \max(d_1, d_2)$ as follows:

1. Choose a set of $(n - d - 1)$ bits in the intermediate state after r_2 rounds, and fix them to an arbitrary value;
2. For each of the 2^{d+1} possible intermediate states z obtained when the other $(d + 1)$ bits take all possible values, compute r_2 rounds backwards to obtain the 2^{d+1} input states $x = G_{r_2}(z)$.

The sum of these input states is then the value of a derivative of order $(d+1)$ of a function with degree d_2 and thus it vanishes. Now, the images of these input states under F correspond to the images of the intermediate states z under F_{r_1}. Then, by computing r_1 rounds forwards, we obtain 2^{d+1} output states. The sum of these output states is the value of a derivative of order $(d + 1)$ of F_{r_1}, which has degree less than d. Thus, this sum vanishes, implying that the x's form a zero-sum. It is worth noticing that this technique provides several zero-sums having a particular property. Actually, for a given choice of the $(n-d-1)$ fixed bits in the intermediate state, taking all possible values for the corresponding constant leads to 2^{n-d-1} zero-sums of sizes 2^{d+1} which form a partition of the input space into zero-sums.

3 Walsh Spectrum and Degree of a Composed Function

The previously known zero-sum properties exploit the degree of an iterated function after a certain number of rounds. It is obvious that a function whose degree does not grow very much when the number of rounds is increasing is a good candidate for this type of attack. The lower the degree is the more we can extend the attack to a high number of rounds.

It is therefore natural to be interested in the estimation of the degree of a composed function. If F and G are two mappings from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$, the degree of the composition $G \circ F$ is bounded by the trivial bound:

$$\deg(G \circ F) \leq \deg(G)\deg(F).$$

A. Canteaut and M. Videau [4] showed that this trivial bound can be improved in the special case when the values occurring in the Walsh spectrum of F are divisible by a high power of 2. Here, we recall this result in order to highlight the underlying property of the function.

In the following, the usual scalar product of two vectors x and y will be denoted by $x \cdot y$. For any $a \in \mathbb{F}_2^n$, φ_a will be the linear Boolean function of n variables $x \mapsto a \cdot x$.

For every Boolean function f of n variables, we associate the following quantity derived from the Hamming weight of f:

$$\mathcal{F}(f) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} = 2^n - 2\mathrm{wt}(f).$$

We use this quantity to define the *Walsh spectrum* of a Boolean function. The *Walsh spectrum* of a Boolean function f measures the correlation between f and the linear functions $\varphi_a, a \in \mathbb{F}_2^n$. It then corresponds to the multiset:

$$\{\mathcal{F}(f + \varphi_a), a \in \mathbb{F}_2^n\},$$

where $f + \varphi_a : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $x \mapsto f(x) + a \cdot x$.

The Walsh spectrum of a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ consists of the Walsh spectra of all Boolean functions $\varphi_b \circ F$, $b \in \mathbb{F}_2^n$, $b \neq 0$, *i.e.*, of all nonzero linear combinations of its coordinates. Therefore, it corresponds to the multiset

$$\{\mathcal{F}(\varphi_b \circ F + \varphi_a), b \in \mathbb{F}_2^n \setminus \{0\}, a \in \mathbb{F}_2^n\}.$$

Definition 2. *The Walsh spectrum of a function F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ is said to be 2^ℓ-divisible if all of its values are divisible by 2^ℓ.*

The divisibility of the Walsh spectrum of a vectorial function F may provide an upper bound on the degree of $G \circ F$, where G is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. In some cases, this bound improves the trivial bound.

Theorem 1. *[4] Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ such that its Walsh spectrum is 2^ℓ-divisible. Then, for any function G from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$, we have*

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

In order to prove this result, one has to analyze the algebraic normal form of $G \circ F$. Let F_i (resp. G_i) be the i-th Boolean coordinate of F (resp. of G). The i-th Boolean coordinate of the composition is then equal to $G_i(F_1, \ldots, F_n)$ and therefore the algebraic normal form of any coordinate of $G \circ F$ can be written as a sum of terms of the form $\sum_J \prod_{j \in J} F_j$.

The study of the Walsh spectrum of the product of Boolean functions becomes thus necessary. The following lemma, which establishes a relationship between the Walsh spectrum of a product of Boolean functions and the Walsh spectrum of its sum, is proved in [5].

Lemma 1. *Let $f_1, \ldots, f_k$ be k Boolean functions of n variables, with $k > 0$. We have*

$$\mathcal{F}(\sum_{i=1}^{k} f_i) = 2^{n-1}\left[(-1)^k + 1\right] + \sum_{I \subset \{1,\ldots,k\}} (-2)^{|I|-1} \mathcal{F}(\prod_{i \in I} f_i).$$

Moreover, for any nonzero $a \in \mathbb{F}_2^n$, we have

$$\mathcal{F}(\sum_{i=1}^{k} f_i + \varphi_\alpha) = \sum_{I \subset \{1,\ldots,k\}} (-2)^{|I|-1} \mathcal{F}(\prod_{i \in I} f_i + \varphi_\alpha).$$

Using this lemma, Canteaut and Videau proved in [4] the following theorem that provides a bound on the degree of the product of Boolean functions, if it is known that the Walsh spectrum of their sum is 2^ℓ-divisible.

Theorem 2. *[4] Let $f_1, \ldots, f_k$ be k Boolean functions of n variables, with $k > 0$. Suppose that for any subset I of $\{1, \ldots, k\}$ we have*

$$\forall \alpha \in \mathbb{F}_2^n, \ \mathcal{F}(\sum_{i \in I} f_i + \varphi_\alpha) \equiv 0 \mod 2^\ell.$$

Then, for any subset $I \subset \{1, \ldots, k\}$ of size at most ℓ we have

$$\forall \alpha \in \mathbb{F}_2^n, \ \mathcal{F}(\prod_{i \in I} f_i + \varphi_\alpha) \equiv 0 \mod 2^{\ell+1-|I|}.$$

Therefore,

$$\deg\left(\prod_{i \in I} f_i\right) \leq n - \ell + |I|.$$

By remarking that the degree of $G \circ F$ cannot exceed the degree of a product of $\deg(G)$ Boolean components of F, the proof of Theorem 1 comes directly from this last result. Here, it is worth noticing that some information on the Walsh spectra of the coordinates of $G \circ F$ may be deduced from Theorem 2, but in most cases, it is not possible to derive the whole Walsh spectrum of $G \circ F$, because it requires the knowledge of the Walsh spectra of all linear combinations of the coordinates of $G \circ F$. For this reason, in the general case, Theorem 2 cannot be iterated several times in order to get a direct bound on the degree of F^r for $r > 2$.

4 The KECCAK-f Permutation

KECCAK [2] is a family of hash functions submitted to the SHA-3 competition launched by NIST for finding a new hash function standard. It is one of the fourteen functions selected by NIST for the second round of the competition. The mode of operation of the KECCAK hash functions is the sponge construction. KECCAK's building block is then a permutation, composed of several iterations of very similar round transformations.

Within the KECCAK-family, the function which has been submitted to the SHA-3 competition operates on a 1600-bit state, which is represented by a 3-dimensional binary matrix of size $5 \times 5 \times 64$.

The authors have given some names to the different parts of the state, in order to facilitate the description of every individual mapping that operates on the state. In particular, we can see the state as 64 parallel slices, each one containing 5 rows and 5 columns. KECCAK's permutation is denoted by KECCAK-$f[b]$, where b is the size of the state. So, for the SHA-3 candidate, $b = 1600$.

Keccak-$f[1600]$ is an iterated permutation, consisting of a sequence of n_r rounds R. The number of rounds, n_r, was 18 in the original submission [2], and it has been updated to 24 for the second round of the competition [3].

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. χ is a nonlinear permutation operating on a 5-bit word, and it is applied to each row of the KECCAK's 1600-bit state.

$$\chi : \mathbb{F}_2^5 \to \mathbb{F}_2^5,$$

with

$$\chi(x_0, x_1, x_2, x_3, x_4) = \begin{pmatrix} x_0 + x_2 + x_1 x_2 \\ x_1 + x_3 + x_2 x_3 \\ x_2 + x_4 + x_3 x_4 \\ x_3 + x_0 + x_4 x_0 \\ x_4 + x_1 + x_0 x_1 \end{pmatrix}$$

In other words, 320 parallel applications of χ are implemented in order to provide confusion. Then, χ is a permutation of degree 2. The inverse permutation, denoted by χ^{-1}, is a permutation of degree 3. We will be interested in the sequel in estimating the degree of several iterations of this round transformation and of its inverse.

5 Zero-sum Distinguisher for the Keccak-f[1600] Permutation

5.1 Previous Results

Aumasson and Meier [1] have used the method described in Section 2 and have found many zero-sums for 16 rounds of the permutation. They use the trivial bound on the degree of a composed function. It is worth noticing that this bound only depends on the degree of χ, since the other four permutations all have degree 1. Then, Aumasson and Meier deduced from the trivial bound that the degree of the permutation after 10 rounds is at most $2^{10} = 1024$ and that the degree of the inverse permutation after 6 rounds is at most $3^6 = 729$. Thus, they fix $1600 - 1025 = 575$ bits in an intermediate state after 6 rounds to some arbitrary value and compute 6 rounds backwards. This method leads to many zero-sums of size 2^{1025}.

5.2 The Walsh Spectrum of the KECCAK-f Permutation

Now, we extend the result by Aumasson and Meier by noticing that the degree of the inverse of KECCAK-f permutation after 7 rounds is much lower than the trivial bound $\min(3^7 = 2187, 1599)$[3].

[3] This minimum comes from the fact that the degree of a permutation over $\mathbb{F}_2^n$ cannot exceed $n - 1$.

For this, we need to compute the divisibility of the Walsh spectrum of the round transformation. We have computed the Walsh spectrum of the nonlinear permutation χ and we have found that its Walsh spectrum is 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^{-1} is 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^{-1} is divisible by 2^3 holds for any other choice of the quadratic permutation χ over $\mathbb{F}_2^5$. Now, a lower bound on the divisibility of the Walsh spectrum of the function χ applied on the entire state can be easily deduced thanks to the following well-known lemma.

Lemma 2. *Let F, G be two functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ and let H be the function from $\mathbb{F}_2^n \times \mathbb{F}_2^n$ into $\mathbb{F}_2^n \times \mathbb{F}_2^n$ defined by*

$$(x_1, \ldots, x_n, y_1, \ldots, y_n) \mapsto (F(x_1, \ldots, x_n), G(y_1, \ldots, y_n)).$$

Let $a = (a_1, a_2), b = (b_1, b_2)$ in $\mathbb{F}_2^n \times \mathbb{F}_2^n$. Then, we have that

$$\mathcal{F}(\varphi_b \circ H + \varphi_a) = \mathcal{F}(\varphi_{b_1} \circ F + \varphi_{a_1})\mathcal{F}(\varphi_{b_2} \circ G + \varphi_{a_2}).$$

In KECCAK-f round transformation, there are 320 parallel applications of the permutation χ. Similarly, for the inverse permutation, χ^{-1} is applied 320 times. As the Walsh spectra of χ and χ^{-1} are both divisible by 2^3, we deduce from the above lemma that the Walsh spectra of χ and χ^{-1} applied on the whole 1600-bit state are divisible by $2^{3 \cdot 320} = 2^{960}$.

As χ is the only nonlinear transformation in the KECCAK-f permutation we have that the Walsh spectrum of the round transformation is 2^{960}-divisible since the Walsh spectrum remains invariant by composition with a linear permutation.

5.3 The Degree of the Inverse KECCAK-f Permutation after 7 rounds

We now use the high divisibility of the round transformation of the KECCAK-f permutation to compute the degree of the inverse KECCAK-f permutation after 7 rounds.

We denote by R^{-1} the inverse of the round transformation. We exploit the trivial bound which shows that 6 rounds of the inverse permutation have degree at most $3^6 = 729$. Then, we use Theorem 1 and prove the following:

$$\begin{aligned} \deg(R^{-7}) &= \deg(R^{-6} \circ R^{-1}) \leq 1600 - 960 + \deg(R^{-6}) \\ &\leq 1600 - 960 + 729 \\ &= 1369. \end{aligned}$$

Therefore we see that, after 7 rounds, the degree of the permutation is at most 1369. This new bound then leads to many zero-sums of size 2^{1370} for the KECCAK-f permutation with 17 rounds.

5.4 Extending the Zero-sum property to One More Round

Now, we show that some of the previously found zero-sums can be extended to 18 rounds. Actually, the previous zero-sums are obtained from a set of intermediate states after 7 rounds, which is the

set Z of all states having $1600-1370 = 230$ bits fixed to an arbitrary value (the other 1370 bits take all possible values). Then, Z corresponds to a coset of a 1370-dimensional subspace V, $Z = a + V$ for some constant a. Such a zero-sum is obtained for any choice of the constant, and for any choice of the 230 positions. However, we now suppose that those positions correspond to a collection of any 46 rows. Then, since χ applies to the rows separately, variables from different rows are not mixed after the application of χ. This means that $\chi(a + V) = b + V$, for some b where χ is considered on the whole 1600-bit state. Then, we can find zero-sums for the KECCAK-f permutation after 18 rounds as follows.

Finding zero-sums for KECCAK-f with 18 rounds

1. Choose any 46 rows in the internal state and fix the corresponding 230 bits to an arbitrary value.
2. For the 2^{1370} possible values for the remaining bits, compute $\pi^{-1} \circ \rho^{-1} \circ \theta^{-1}$ followed by 7 rounds backwards of the round transformation to obtain 2^{1370} initial states.

Then, we have that

- these 2^{1370} initial states sum to zero as the corresponding sum is the value of a derivative of order 1370 of a function of degree at most 1369.
- Their images by 18 rounds of the KECCAK-f transformation sum also to zero, since this sum is the value of a derivative of order 1370 of the function $\iota \circ R_9 \circ R_{10} \circ \ldots \circ R_{18}$ which has degree at most 1024.

Moreover, exactly as in [1], this algorithm leads to several partitions of the input space $\mathbb{F}_2^{1600}$ into zero-sums of size 2^{1370}, which is clearly a structural distinguishing property. Therefore, this result contradicts, for the original version of KECCAK, the "hermetic sponge" design principle.

6 Conclusions

We have extended to 18 rounds the zero-sum property found by Aumasson and Meier. We have explored the spectral properties of the round transformation of KECCAK-f and we have shown that the use of a quadratic round transformation which applies of the 5-bit rows of the internal state separately leads to a high divisibility of its Walsh spectrum. This property implies that the degree of several iterations of the inverse round transformation does not grow as fast as the trivial bound $\deg(R^{-1})^r$. Taking benefit of this situation, we are able to exhibit many zero-sums for the KECCAK-f permutation with 18 rounds, while the existence of such zero-sums was only known up to 16 rounds. It is worth noticing that 18 rounds was the initial parameter proposed for the SHA-3 candidate KECCAK, but this value has been increased to 24 rounds by the designers. However, even if it points out that KECCAK-f with 18 rounds does not have an ideal behaviour, this property does not seem to affect the security of KECCAK.

References

1. 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.

2. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Keccak sponge function family main document. Submission to NIST (Round 1), 2009.
3. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Keccak sponge function family main document. Submission to NIST (Round 2), 2009.
4. 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.
5. A. Canteaut and M. Videau. Weakness of block ciphers using highly nonlinear confusion functions. Research report RR-4367, INRIA, February 2002.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.