On the algebraic degree of some SHA-3 candidates

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. We present a study on the algebraic degree of iterated permutations seen as multivariate polynomials. Our main result shows that this degree depends on the algebraic degree of the inverse of the permutation which is iterated. It leads among others to an improvement of the bound on the degree presented in [6]. This result has some consequences in hash function analysis since several attacks or distinguishers exploit a low algebraic degree, like higher-order differential attacks, cube attacks and cube testers, or algebraic attacks. Here, we explain how this result has consequences on the evolution of the degree of the KECCAK-f permutation and we present some applications of this improved bound to the inner permutations of the hash functions ECHO and JH.

1 Introduction

In most modern hash functions, as also in block ciphers, for implementation and other practical reasons, the structure relies on an inner function, that is iterated a high number of times for providing security. This transformation, called the round function, is often a permutation. The algebraic degree of this permutation, *i.e.*, the degree of the corresponding *multivariate* polynomials, is a quantity that plays an important role for the security of symmetric primitives. Actually, a cryptographic primitive of low algebraic degree is vulnerable to many attacks, for instance higher-order differential attacks [17,16,18], algebraic attacks [9,8] or cube attacks [11]. For hash functions in particular, a low algebraic degree of its inner primitive can be exploited for constructing higher-order differentials or zero-sum distinguishers. Such type of distinguishers have already been presented for some candidates of the SHA-3 competition [2,19,5,6].

In [14], Duan and Lai noticed that even if the inverse of the KECCAK nonlinear permutation χ over $\mathbf{F}_2^5$ has degree 3, the product of any two output coordinates of χ^{-1} has also degree 3 in the five variables. This surprising remark is then exploited in order to show that the degree of the inverse KECCAK-f permutation does not grow with the number of rounds as much as it would be expected for a cubic function. This fact can for example be used to improve the complexity of the 24-round zero-sum distinguisher presented in [6].

We demonstrate here that this observed phenomenon is not accidental, but comes from the fact that the χ permutation itself has degree 2 only. More generally, we show that even if the inverse of the round permutation F is never used in practice in a hash function, its degree plays a fundamental role in the degree of the composition $G \circ F$ and in consequence in the overall degree of the primitive. Even if the degree of the round function is high, if the degree of its inverse is low, the degree of the complete function will be lower than believed.

This result helps in general the understanding of the evolution of the algebraic degree of iterated permutations. Several earlier works have established new bounds on the degree of such permutations: most notably, [7] connects the degree of $G \circ F$ with the divisibility of the Walsh spectrum of F by a high power of 2, while the result of [6] applies to the family of functions composed of

several smaller balanced functions. Our new result provides among others a better comprehension of this last bound, by associating it to the degree of the inverse permutation.

Besides KECCAK, our results apply to two other candidate functions of the SHA-3 competition, ECHO and JH. We provide an analysis on the way that the algebraic degrees of these two functions evolve with the number of rounds, and we show that in both cases this evolution is much slower than expected. As an additional illustration, we can use these bounds to construct zero-sum distinguishers for round-reduced versions of these two functions.

The rest of the paper is organized as follows. After some preliminaries on the algebraic degree of a vectorial function, the technique of higher-order differential attacks and zero-sum distinguishers are recalled in Section 2. Section 3 presents the main result on the influence of the inverse of a permutation F on the degree of $G \circ F$ and includes some corollaries. Section 4 shows how these results apply to two SHA-3 candidates, namely ECHO and JH, in order to predict the evolution of the degrees of their building-blocks with the number of rounds.

2 Exploiting a low algebraic degree in cryptanalysis

2.1 Degree of a vectorial function

The whole paper focuses on functions F from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. The *coordinates* of such a function F are the m Boolean functions F_i, $1 \leq i \leq m$, such that $F(x) = (F_1(x), \ldots, F_m(x))$ for all x.

The *algebraic degree* of F is usually defined by the algebraic degrees of its coordinates as follows.

Definition 1. *Let f be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2$. Then, f can be uniquely written as a multivariate polynomial in $\mathbf{F}_2[x_1, \ldots, x_n]/(x_1^2 - x_1), \ldots, (x_n^2 - x_n)$, named its* algebraic normal form*:*

$$f(x_1, \ldots, x_n) = \sum_{u=(u_1,\ldots,u_n) \in \mathbf{F}_2^n} a_u \prod_{i=1}^{n} x_i^{u_i} \ .$$

The (algebraic) degree *of f is then defined as*

$$\deg f = \max\{wt(u) : u \in \mathbf{F}_2^n, a_u \neq 0\} \ ,$$

where wt denotes the Hamming weight of a binary vector.

For a function F from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$, $m \geq 1$, the (algebraic) degree of F is the maximal algebraic degree of its coordinates.

2.2 Higher-order differentials and zero-sum distinguishers

It should be difficult to distinguish a good hash function from a function that has been chosen at random. The presence of structural distinguishers can in some cases bring to light exploitable weaknesses that can lead to an attack against the function. In other cases, a distinguishing property can invalidate the related security proof.

A special class of distinguishers, taking advantage of the possible low algebraic degree of the function, are the *higher-order differential distinguishers*. They are derived from the *higher order differential attack* introduced by Knudsen [16]. If F is a function over $\mathbf{F}_2^n$, such distinguishers correspond to the value of any derivative of F with respect to a subspace of $\mathbf{F}_2^n$ with dimension $\deg(F) + 1$.

Definition 2. *[17] Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. For any $a \in \mathbf{F}_2^n$ 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 $\mathbf{F}_2^n$ and for any basis of V, $\{a_1, \ldots, a_k\}$, the k-th order derivative of F with respect to V is the function defined by*

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

It is well-known that the degree of any first-order derivative of a function is strictly less than the degree of the function. By generalizing this simple remark, we get the following property that is exploited in higher-order differential attacks [16] for every subspace V of dimension $(\deg F + 1)$:

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

In hash function cryptanalysis a recently introduced class of distinguishers, that exploits the above situation, are the zero-sum distinguishers [1,5].

Definition 3. *Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$. A* zero-sum *for F of size K is a subset $\{x_1, x_2, \ldots, x_K\} \subset \mathbf{F}_2^n$ such that*

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

Zero-sums can lead to stronger distinguishing properties, called *zero-sum partitions*, if F is a permutation over $\mathbf{F}_2^n$.

Definition 4. *Let F be a permutation from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$. A* zero-sum partition *for F of size $K = 2^k$ is a collection of 2^{n-k} disjoint zero-sums $X_i = \{x_{i,1}, \ldots, x_{i,2^k}\} \subset \mathbf{F}_2^n$* i.e.*,*

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

This type of analysis takes profit of the absence of a secret key during the computation. Thus, to construct a zero-sum partition of complexity 2^k for an r-round permutation F over $\mathbf{F}_2^n$, one has to choose a subspace $V \subset \mathbf{F}_2^n$ after t rounds of the permutation, of dimension k strictly greater than both the degree of the permutation restricted to $r-t$ rounds and the degree of its inverse restricted to t rounds.

The lower these two degrees are, the lower the complexity of the distinguisher will be. This application is then an example of the importance of correctly estimating the degree of an iterated permutation. In the following section we analyze this general problem.

3 On the degree of $G \circ F$ when F is a permutation

3.1 Previous results and their application to Keccak

A SHA-3 candidate that has received a lot of analysis concerning the existence of zero-sum partitions for its underlying permutation, is the finalist function Keccak [4]. Its inner permutation Keccak-f, uses for providing confusion, a parallel application of a non-linear permutation χ over $\mathbf{F}_2^5$. The algebraic degree of χ is 2 and the degree of χ^{-1} is 3.

We present here the evolution of the bounds on the algebraic degree of permutations, through the example of KECCAK. The first results on KECCAK-f were given by Aumasson and Meier in [1]. They were based on the following estimation on the degree of an iterated permutation, that we will call *trivial bound*.

Proposition 1. *Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ and G be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$, for some m. Then,*

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

The authors used this estimation in order to bound the degree of KECCAK-f restricted to 10 rounds and of its inverse up to 6 rounds. This led to a 16-round distinguisher.

For extending these results to more rounds, a better estimation for the degree should be adopted. A first approach [5] was to use a bound presented by Canteaut and Videau in [7], that proposed a clear improvement to the trivial bound for permutations, whose Walsh spectrum can be divided by a high power of 2.

Proposition 2. *[7] Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ and G be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. Assume that all Walsh coefficients of F,* i.e.*, all*

$$\sum_{x \in \mathbf{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x}, \ a, b \in \mathbf{F}_2^n$$

are divisible by 2^ℓ for some integer $\ell \geq 1$, then

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

By using this bound, the previous results of Aumasson and Meier were extended to 18 rounds by Boura and Canteaut [5].

More recently, another one approach to improve the trivial bound was employed [6]. It was shown that the trivial bound can be improved when F corresponds to the parallel applications of smaller balanced functions, *i.e.*, $F = (S_1, \ldots, S_s)$. This particular situation is actually very common in cryptography for obvious implementation reasons.

Theorem 1. *[6] Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ corresponding to the concatenation of m smaller Sboxes, $S_1, \ldots, S_m$, defined over $\mathbf{F}_2^{n_0}$. Let δ_k be the maximal degree of the product of any k coordinates of anyone of these smaller Sboxes. Then, for any function G from $\mathbf{F}_2^n$ into $\mathbf{F}_2^\ell$, we have*

$$\deg(G \circ F) \leq n - \frac{n - \deg(G)}{\gamma} \ ,$$

where

$$\gamma = \max_{1 \leq i \leq n_0 - 1} \frac{n_0 - i}{n_0 - \delta_i} \ .$$

This last bound has led to the construction of the first 24-round distinguishers on KECCAK-f of complexity 2^{1590} and thus it affects the hermetic sponge strategy. Some months later, Duan and Lai [14] made the following interesting observation. They noticed, that even if χ^{-1} was of algebraic degree 3, the degree of the product of any two coordinates of this permutation is also 3 in the five variables. This observations improved the complexity of the overall distinguisher to 2^{1575}.

We show in the sequel that this *a priori* surprising result can be explained by the fact that χ is of low degree.

3.2 Main result

Our results rely on the following theorem which bounds the maximum degree for the product of any k coordinates of a permutation F, for all $1 \leq k \leq n$. The following notation will then be extensively used.

Definition 5. *Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. For any integer k, $1 \leq k \leq m$, $\delta_k(F)$ denotes the maximal algebraic degree of the product of any k (or fewer) coordinates of F:*

$$\delta_k(F) = \max_{K \subset \{1,\ldots,m\}, |K| \leq k} \deg \left(\prod_{i \in K} F_i \right) .$$

In particular, $\delta_1(F) = \deg F$.

Our main result is the following theorem.

Theorem 2. *Let F be a permutation on $\mathbf{F}_2^n$. Then, for any integers k and ℓ, $\delta_\ell(F^{-1}) < n - k$ if and only if $\delta_k(F) < n - \ell$.*

Proof. We only have to show that if $\delta_\ell(F^{-1}) < n - k$ then $\delta_k(F) < n - \ell$. Indeed, the reciprocal relation is obtained by exchanging the roles of F and F^{-1}.

Let $\pi : x \mapsto \prod_{i \in K} F_i(x)$, with $|K| \leq k$. For $L \subset \{1, \ldots, n\}$, with $|L| \leq \ell$, we denote by a_L the coefficient of the monomial $\prod_{j \notin L} x_j$ of degree $n - |L|$. We will show that $a_L = 0$.

$$\begin{aligned} a_L &= \sum_{\substack{x \in \mathbf{F}_2^n \\ x_j = 0, j \in L}} \pi(x) \mod 2 \\ &= \#\{x \in \mathbf{F}_2^n : \, x_j = 0, j \in L \text{ and } F_i(x) = 1, i \in K\} \mod 2 \\ &= \#\{y \in \mathbf{F}_2^n : y_i = 1, i \in K \text{ and } F_j^{-1}(y) = 0, j \in L\} \mod 2 , \end{aligned}$$

where the last equality comes from the fact that F is a permutation, implying that there is a one-to-one correspondence between x and $y = F(x)$. Additionally, $F_j^{-1}(y) = 0$ for all $j \in L$ if and only if $\prod_{j \in L}(1 + F_j^{-1}(y)) = 1$. Then,

$$a_L = \#\{y \in \mathbf{F}_2^n : y_i = 1, i \in K \text{ and } \prod_{j \in L}(1 + F_j^{-1}(y)) = 1\} \mod 2 . \tag{1}$$

Now, we define the Boolean function

$$\begin{array}{rcl} H_{K,L} : \{x \in \mathbf{F}_2^n : x_i = 1, i \in K\} & \to & \mathbf{F}_2 \\ x & \mapsto & \prod_{i \in L}(1 + F_i^{-1}(x)) . \end{array}$$

We have

$$a_L = wt(H_{K,L}) \mod 2 .$$

$H_{K,L}$ is a function of $n - k$ variables and it has degree at most $\delta_\ell(F^{-1})$. Then, as by hypothesis $\delta_\ell(F^{-1}) < n-k$, $H_{K,L}$ is of even Hamming weight and thus $a_L = 0$, which means that $\delta_k(F) < n-\ell$. □

By taking $F = \chi$ in the above theorem, we are now able to explain the observation made in [14]. Since $\delta_1(\chi) = \deg \chi = 2$, we have $\delta_2(\chi^{-1}) < 4$.

The following (less precise) result can be derived from the trivial bound on $\delta_\ell(F^{-1})$.

Corollary 1. *Let F be a permutation of $\mathbf{F}_2^n$ and let G be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. Then, we have*

$$\deg(G \circ F) < n - \left\lfloor \frac{n-1-\deg G}{\deg(F^{-1})} \right\rfloor .$$

Proof. Obviously, $\deg(G \circ F) \leq \delta_{\deg G}(F)$. But the previous theorem shows that $\delta_{\deg G}(F) < n - \ell$ for some integer ℓ if and only if $\delta_\ell(F^{-1}) < n - \deg G$. However, we have from the trivial bound that $\delta_\ell(F^{-1}) \leq \ell \deg(F^{-1})$. It follows that $\delta_\ell(F^{-1}) < n - \deg G$ for any integer ℓ satisfying

$$\ell \leq \left\lfloor \frac{n-1-\deg G}{\deg(F^{-1})} \right\rfloor .$$

Indeed,

$$\left\lfloor \frac{n-1-\deg G}{\deg(F^{-1})} \right\rfloor = \begin{cases} \left\lfloor \frac{n-\deg G}{\deg(F^{-1})} \right\rfloor & \text{if } n - \deg G \not\equiv 0 \bmod \deg(F^{-1}) \\ \frac{n-\deg G}{\deg(F^{-1})} - 1 & \text{otherwise.} \end{cases}$$

Therefore, in all cases, we have

$$\deg(F^{-1}) \left\lfloor \frac{n-1-\deg G}{\deg(F^{-1})} \right\rfloor < n - \deg G ,$$

implying that

$$\delta_\ell(F^{-1}) \leq \ell \deg(F^{-1}) \leq \deg(F^{-1}) \left\lfloor \frac{n-1-\deg G}{\deg(F^{-1})} \right\rfloor < n - \deg G .$$

We then deduce that

$$\delta_{\deg G}(F) < n - \left\lfloor \frac{n-1-\deg G}{\deg(F^{-1})} \right\rfloor .$$

□

Obviously, the upper bound of the previous theorem gets better when the degree of F^{-1} decreases. Moreover, if G is balanced, this bound is relevant only if it improves the obvious bound $\deg(G \circ F) < n$. Some information is thus provided if $\deg G \leq n - 1 - \deg F^{-1}$.

3.3 Some corollaries

Some simple corollaries of Theorem 2 can be obtained by setting $k = 1$ in the theorem. In this case, we have $\deg(F^{-1}) < n - \ell$ if and only if $\delta_\ell(F) < n - 1$. We then deduce the following result and its well-known consequence.

Corollary 2. *Let F be a permutation of $\mathbf{F}_2^n$. Then,*

$$\deg(F^{-1}) = n - \min\{k \ : \ \delta_k(F) \geq n - 1\} .$$

In particular, $\deg(F^{-1}) = n - 1$ *if and only if* $\deg(F) = n - 1$.

Moreover, for any integer k such that

$$k \leq \left\lceil \frac{n-1}{\deg F} \right\rceil - 1$$

we have

$$\delta_k(F) \leq k \deg F < n - 1 \, .$$

It follows that

$$\min\{k \ : \ \delta_k(F) \geq n-1\} \geq \left\lceil \frac{n-1}{\deg F} \right\rceil \, ,$$

implying that

$$\deg(F^{-1}) \leq n - \left\lceil \frac{n-1}{\deg F} \right\rceil \, .$$

We then recover in a different way the bound on $\deg(F^{-1})$ which can be derived from Katz theorem [15] on the divisibility of the Walsh spectrum of a permutation. Actually, all Walsh coefficients of F are divisible by $\left\lceil \frac{n-1}{\deg F} \right\rceil + 1$ and it is well-known that the degree of a function whose Walsh coefficients are divisible by 2^ℓ is at most $(n+1-\ell)$ (see e.g. [7, Prop. 3]).

Corollary 2 also implies the following.

Corollary 3. *Let F be a permutation of $\mathbf{F}_2^n$. Then, the product of k coordinates of F has degree $(n-1)$ if and only if $n - \deg(F^{-1}) \leq k \leq n-1$.*

In particular, $\delta_{n-1}(F) = n-1$.

Proof. The previous corollary implies that the smallest k such that $\delta_k(F) \geq n-1$, is equal to $n - \deg(F^{-1})$. Moreover, it is known that $\delta_k(F) = n$ if and only if $k = n$. Finally, since $n - \deg(F^{-1}) \leq n-1$, we deduce that $\delta_{n-1}(F) = n-1$ for any permutation of $\mathbf{F}_2^n$. □

The above results can also be used for improving the bound on $\deg(G \circ F)$ of Theorem 1. In particular, a better estimation of the constant γ is provided.

Theorem 3. *Let F be a permutation from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ corresponding to the concatenation of s smaller permutations, $S_1, \ldots, S_s$, defined over $\mathbf{F}_2^{n_0}$. Then, for any function G from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$, we have*

$$\deg(G \circ F) \leq n - \frac{n - \deg(G)}{\gamma} \, ,$$

where

$$\gamma = \max_{1 \leq i \leq n_0 - 1} \frac{n_0 - i}{(n_0 - \max_{1 \leq j \leq s} \delta_i(S_j))} \, .$$

Most notably, we have

$$\gamma \leq \max_{1 \leq j \leq s} \max \left(\frac{n_0 - 1}{n_0 - \deg(S_j)}, \ \frac{n_0}{2} - 1, \ \deg(S_j^{-1}) \right) \, .$$

Proof. We denote by γ_i the quantity

$$\gamma_i = \frac{n_0 - i}{n_0 - \max_{1 \leq j \leq s} \delta_i(S_j)},$$

and we will try to compute the maximal γ_i for $1 \leq i \leq n_0 - 1$, *i.e.* γ.

For $i = 1$,

$$\gamma_1 = \max_{1 \le j \le s} \frac{n_0 - 1}{(n_0 - \deg(S_j))}.$$

For $2 \le i < n_0 - \max_{1 \le j \le s} \deg(S_j^{-1})$, we get from Corollary 3 that $\max_{1 \le j \le s} \delta_i(S_j) \le n_0 - 2$, and thus

$$\gamma_i = \max_{1 \le j \le s} \frac{n_0 - i}{(n_0 - \delta_i(S_j))} \le \frac{n_0 - i}{2} \le \frac{n_0 - 2}{2}.$$

Finally, for the remaining indexes, *i.e.* for $i \ge n_0 - \max_{1 \le j \le s} \deg(S_j^{-1})$, we get that

$$\gamma_i = \max_{1 \le j \le s} \frac{n_0 - i}{(n_0 - \delta_i(S_j))} \le n_0 - i \le \max_{1 \le j \le s} \deg(S_j^{-1}).$$

□

The bound of Corollary 1 can be generalized to balanced functions F from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$ with $m < n$. Even if such functions do not possess an inverse, we can consider permutations that *extend* in some way the function and can be used in the place of F^{-1}. In such a way, we are able to predict in some manner the evolution of the algebraic degree of ciphers that do not use permutations for providing confusion, but balanced functions from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$ with $m < n$, as this is the case for DES.

4 Applications to some hash functions

In this section, we will show how the previous results and in particular Theorem 3 can be used in order to predict the evolution of the algebraic degree of some chosen permutations that are the main building blocks of two SHA-3 candidates, ECHO and JH.

4.1 Application to ECHO

The ECHO [3] hash function has been designed by Benadjila *et al.* for the NIST SHA-3 competition. It uses the HAIFA mode of operation. Its compression function has a 2048-bit input (corresponding to the chaining value and a message block whose respective lengths depend on the size of the message digest), and it outputs a 512-bit or a 1024-bit value. It relies on a 2048-bit AES-based permutation P.

The permutation P updates a 2048-bit state, which can be seen as a 4×4 AES state, composed of 128-bit words. In every round `R`, three operations modify the state. These are the `BIG.SubWords`, `BIG.ShiftRows` and `BIG.MixColumns` transformations. These transformations can be seen as generalizations of the three classical AES transformations. In particular,

- `BIG.SubWords` is a nonlinear transformation applied independently to every 128-bit cell. It consists of two AES rounds.
- The `BIG.ShiftRows` and `BIG.MixColumns` transformations are exact analogues of the AES `ShiftRows` and `MixColumns` transformations respectively, with the only difference that they do not operate on bytes but on 128-bit words.

The number of rounds r is specified to be 8 for the 256-bit candidate. Finally, each bit in the output of the compression function is defined as a linear combination of some output bits of P and some input bits.

We will see how the algebraic degree of the permutation P varies with the number of rounds. We will show that the degree does not increase as predicted and reaches its maximum value much later than expected. The algebraic degree of the permutation P was believed to be high, as in every round `R` the input has to pass twice through the Sbox layer, of degree 7. As $7^4 = 2401$, two rounds seemed to be enough to achieve the highest possible degree.

`BIG.SubWords` is the only source of nonlinearity in the round permutation. It is a 128-bit transformation corresponding to two rounds of AES. We start by determining the algebraic degree of `BIG.SubWords`. By using the SuperSbox view [10], we can see two rounds of AES as the parallel application of eight copies of a function S_{32} operating on 32-bit words, followed by a linear transformation. S_{32} corresponds to a so-called SDS transformation: it consists of two layers of four 8×8 balanced Sboxes of degree 7, separated by a linear layer. Therefore, we can use Theorem 2 of [6] and get that

$$\deg R^2 = \deg S_{32} \leq 32 - \frac{32-7}{7} < 29 \; .$$

The two-round permutation $\mathtt{R}^2$ is a permutation of the set of 2048-bit states, but it can be decomposed as four parallel applications of a permutation S_{512} operating on 512-bit words, followed by a linear layer. We will determine the degree of any of these four applications. After the first round of the permutation P every bit of the state consists of polynomials of degree at most 28. By applying to this state the first layer of Sboxes in every `BIG.SubWords`, the degree gets at most $7 \cdot 28 = 196$. We can apply now the bound of Theorem 2 to get the following bound on the degree of $\mathtt{R}^2$:

$$\deg \mathtt{R}^2 = \deg S_{512} \leq 512 - \frac{512-196}{7} < 467 \; .$$

Let $F = \mathtt{R}^2$. F is then a permutation of degree at most 466. From Theorem 3, the constant γ associated to this permutation is at most 466, as the degrees of $\mathtt{R}^2$ and of its inverse are both upper-bounded by 466, therefore

$$\deg F^2 = \deg \mathtt{R}^4 \leq 2048 - \frac{2048-466}{466} < 2046.$$

The same bounds hold for the inverse round transformation. Due to this observation, we are able to distinguish the inner permutation in ECHO from a random one. This can be done for instance by constructing zero-sum structures. By choosing the intermediate states after 4 rounds of the permutation in the cosets of any subspace V with dimension 2^{2046}, we get zero-sum partitions for the entire P permutation.

4.2 Application to JH

JH [20] is a hash function family, having some members submitted to the NIST hash function competition. It has been chosen in late 2010 to be one of the five finalists of the contest.

The compression function in JH is constructed from a block cipher with constant key. This compression function is based on an inner permutation, named E_d and is composed of 42 steps of a round function R_d, where $d = 8$ for the SHA-3 candidate.

R_d applies to a state of 2^{d+2} bits, divided into 4-bit words. It consists of 3 different layers: an Sbox layer, a linear layer and a permutation layer P_d.

- The **Sbox layer** corresponds to the parallel application of 2^d Sboxes to the state. Two different Sboxes, S_0 and S_1, are used in JH. Both of them, as also their inverses, are of degree 3. The selection of the Sbox to use is made by the round constant bits, which are not xored to the state as done in other constructions.
- The **linear layer** mixes the 2^d words two by two.
- The **permutation** P_d permutes the words of the state.

Two rounds of R_d, for $d = 4$, can be seen in Figure 1.

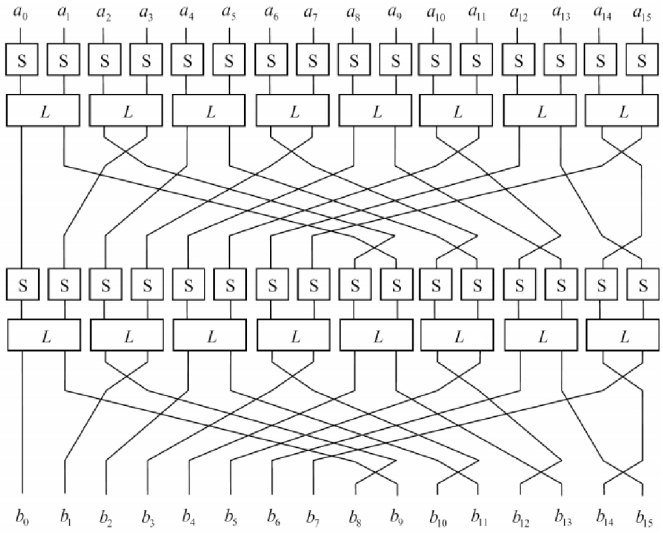

Fig. 1. Two rounds of R_4

A round of the permutation is of algebraic degree 3, as the only source of nonlinearity of the cipher comes from the 4-bit Sboxes. Thus, if we try to estimate the evolution of the degree by using the trivial bound, we can see that the degree of the permutation after 6 rounds is at most $\deg(R_8^6) \leq 3^6 = 729$ and consequently the maximal degree seems to be reached just after 7 rounds of encryption. We will show again by applying the results of Section 3 that the algebraic degree of JH does not increase as expected.

An important observation on the structure of the R_8 permutation is that for $r \leq 8$, r rounds of R^8, denoted by R_8^r, can be seen as the concatenation of 2^{9-r} permutations S_r over $\mathbf{F}_2^{2^{r+1}}$. Thus, for $2 \leq r \leq 8$ a bound on the degree of R_8^r can be obtained with the help of Theorem 2 in [6]:

$$\deg(R_8^r) \leq 2^{r+1} - \frac{2^{r+1} - \deg(R_8^{r-1})}{3}.$$

The bounds on the degree up to 8 rounds of the permutation, given by the above formula, can be seen in Table 1. The same bounds hold for the inverse permutation.

# **Rounds**	**Bound on** $\deg(R_8^r)$
1	3
2	6
3	12
4	25
5	51
6	102
7	204
8	409

Table 1. Upper bounds on the degree of up to 8 rounds of the JH permutation.

Using now Theorem 3, we get that the constant $\gamma(S_8)$ of the permutation S_8 over $\mathbf{F}_2^{512}$ is at most 409. Thus we have that

$$\deg R_8^{16} \leq 1024 - \frac{1024 - \deg(R_8^8)}{\gamma(S_8)} < 1023.$$

Because of this result, the P_8 permutation reduced to 32 rounds can be distinguished from a random permutation by constructing zero-sum partitions by choosing the intermediate states after 16 rounds of the permutation in the cosets of any subspace V with dimension 2^{2023}.

5 Conclusions

Our work points out that, in many situations, the algebraic degree of an iterated function does not grow as fast as expected with the number of rounds. In particular, the degree of the inverse of the iterated permutation has some influence on the degree of the iterated function. This observation can be used for exhibiting non-ideal behaviors in the inner functions of some hash constructions. However, turning such distinguishers into real attacks, like a (second)-preimage attack on a hash function, is a difficult problem. The most promising approach consists in combining some properties of the algebraic normal form of an inner function (e.g., its low degree) and the solving of some algebraic system, as proposed in [18,13]. Another open problem is to determine the impact of our result on some stream ciphers which appear to be vulnerable to several attacks exploiting the existence of some function with a low degree [11,12].

References

1. J.-P. Aumasson, E. Käsper, L.R. Knudsen, K. Matusiewicz, R. Ødegård, T. Peyrin, and M. Schläffer. Distinguishers for the compression function and output transformation of Hamsi-256. In *Information Security and Privacy - ACISP 2010*, volume 6168 of *Lecture Notes in Computer Science*, pages 87–103. Springer, 2010.
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. R. Benadjila, O. Billet, H. Gilbert, G. Macario-Rat, T. Peyrin, M. Robshaw, and Y. Seurin. SHA-3 Proposal: ECHO. Submission to NIST (Round 2), available at `http://crypto.rd.francetelecom.com/echo`, 2009.
4. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. The KECCAK reference. Submission to NIST (Round 3), available at `http://keccak.noekeon.org/Keccak-reference-3.0.pdf`, 2011.
5. C. Boura and A. Canteaut. Zero-sum distinguishers for iterated permutations and application to Keccak-f and Hamsi-256. In *Selected Areas in Cryptography - SAC 2010*, volume 6544 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2010.

6. C. Boura, A. Canteaut, and C. De Cannière. Higher-order differential properties of Keccak and Luffa. In *Fast Software Encryption - FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 252–269. Springer, 2011.
7. 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.
8. N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 345–359. Springer-Verlag, 2003.
9. N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In *Advances in Cryptology - ASIACRYPT'02*, volume 2501 of *Lecture Notes in Computer Science*, pages 267–287. Springer-Verlag, 2002.
10. J. Daemen and V. Rijmen. Understanding Two-Round Differentials in AES. In *Security and Cryptography for Networks - SCN 2006*, volume 4116 of *Lecture Notes in Computer Science*. Springer, 2006. pp. 78-94.
11. I. Dinur and A. Shamir. Cube attacks on tweakable black box polynomials. In *Advances in Cryptology - EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 278–299. Springer, 2009.
12. I. Dinur and A. Shamir. Breaking Grain-128 with dynamic cube attacks. In *Fast Software Encryption - FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 167–187. Springer, 2011.
13. I. Dinur and A. Shamir. An improved algebraic attack on Hamsi-256. In *Fast Software Encryption - FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 88–106. Springer, 2011.
14. M. Duan and X. Lai. Improved zero-sum distinguisher for full round Keccak-f permutation. IACR ePrint Report 2011/023, January 2011. `http://eprint.iacr.org/2011/023`.
15. N. Katz. On a theorem of Ax. *American Journal of Mathematics*, 93:485–499, 1971.
16. 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.
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. S. Moriai, T. Shimoyama, and T. Kaneko. Higher order differential attak of CAST cipher. In *Fast Software Encryption - FSE'98*, volume 1372 of *Lecture Notes in Computer Science*, pages 17–31. Springer, 1998.
19. D. Watanabe, Y. Hatano, T. Yamada, and T. Kaneko. Higher order differential attack on step-reduced variants of *Luffa* v1. In *Fast Software Encryption - FSE 2010*, volume 6147 of *Lecture Notes in Computer Science*, pages 270–285. Springer, 2010.
20. H. Wu. The hash function JH. Submission to NIST (Round 3) available at `http://www3.ntu.edu.sg/home/wuhj/research/jh/`, 2011.