Zero-sum distinguishers for the Keccak-f permutation

Christina Boura Anne Canteaut

SECRET Project-Team, INRIA, France
Gemalto, France

June 15, 2010

Zero-Sum Distinguishers

Firstly studied by J.-P. Aumasson and W. Meier in 2009.

Definition (Zero-sum)

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$.
A zero-sum for F of size K is a subset $\{x_1, \ldots, x_K\} \subset \mathbb{F}_2^n$ such that

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

Definition (Zero-sum partition)

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 $X_i = \{x_{i,1}, \ldots, x_{i,2^k}\} \subset \mathbb{F}_2^n$.

Existence and Previous Results

Existence

Their existence is usually due to:

- A possibly low algebraic degree (nonlinear part weakness)
- Low diffusion (linear part weakness)

Known results

- The first direction has been investigated by J.-P. Aumasson and W. Meier for three SHA-3 candidates (Keccak, Luffa and Hamsi);
- Distinguisher for 16 rounds of the Keccak-f permutation.

Our Results

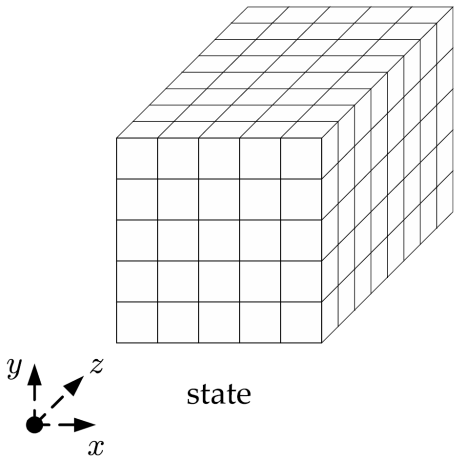
- We show how to impove the bound on the degree of an iterated permutation;
- We combine properties of the linear and nonlinear part of an iterated permutation in the search of zero-sums;

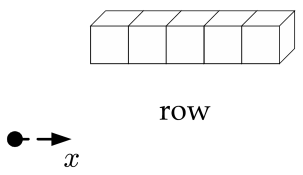
With these, we have the following results for Keccak-f

Distinguishers
for $17, 18, 19$ and 20 rounds
of the Keccak-f permutation.

The Keccak-f permutation

- 1600-bit state, seen as a 3-dimensional $5 \times 5 \times 64$ matrix
- 24 rounds $R = \iota \circ \chi \circ L$
- L linear transformation providing diffusion in all directions
- χ nonlinear transformation, $\deg(\chi) = 2 \quad \deg(\chi^{-1}) = 3$
- χ operates on the 5-bit rows of the state by 320 parallel applications of χ_0





Higher-order derivatives

Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$.

Definition (k-th order derivative of F)

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

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

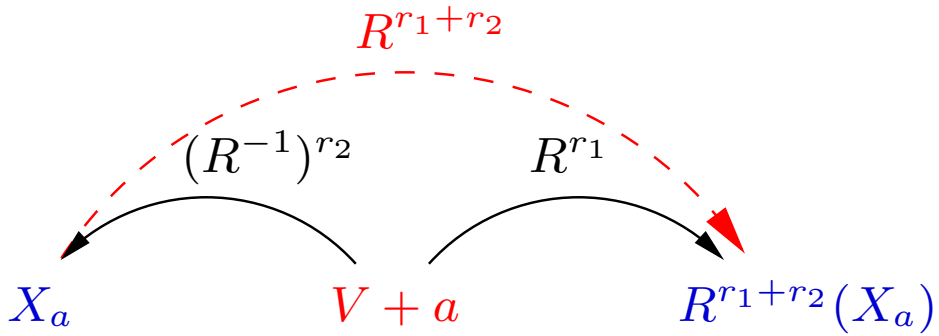
Remark

For every subspace V of dimension $(\deg F + 1)$,

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

General method (Aumasson and Meier '09)

- $\deg(R^{r_1}) \leq 2^{r_1}$ and $\deg((R^{-1})^{r_2}) \leq 3^{r_2}$
- V subspace of $\mathbb{F}_2^{1600}$ with $\dim V = \max(2^{r_1}, 3^{r_2}) + 1$

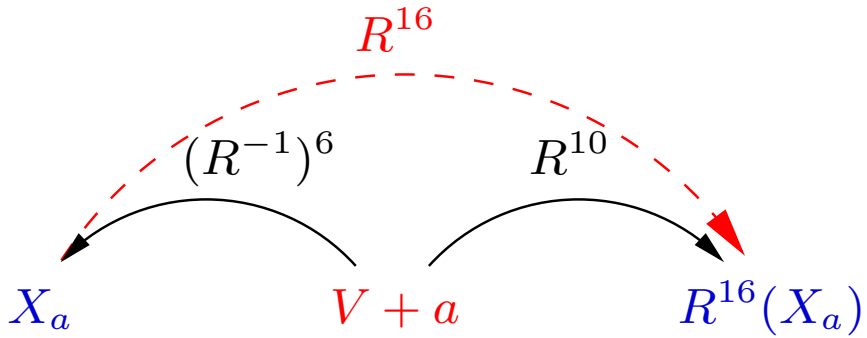


$$X_a = \{(R^{-1})^{r_2}(a + z),\ z \in V\},\quad a \in W$$

is a zero-sum partition of size $2^{\dim V}$ for $r_1 + r_2$ rounds.

General method (Aumasson and Meier '09)

- $\deg(R^{10}) \leq 2^{10}$ and $\deg((R^{-1})^6) \leq 3^6$
- V subspace of $\mathbb{F}_2^{1600}$ with $\dim V = 1025$



Zero-sum partitions of size 2^{1025} for 16 rounds.

Problem

Limitation by the bound on the degree of an iterated permutation

$\deg(R^{-1})^7 \leq \min(1599, 3^7 = 2187)$

Bound on the degree of a composed permutation

Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Problem

Bound the degree of $G \circ F$.

Trivial bound

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

Canteaut-Videau '02

This trivial bound can be improved when the Walsh spectrum of F is divisible by a high power of 2.

Walsh spectrum

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

Definition

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

Definition (Walsh spectrum of f)

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

where $\varphi_a(x) = a \cdot x$.

Definition (Walsh spectrum of a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$)

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

An improved bound on the degree of a composition

Theorem (Canteaut-Videau '02)

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 function G from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$, we have

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

An improved bound on the degree of a composition

Theorem (Canteaut-Videau '02)

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 function G from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$, we have

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

Focus on the following special case:

- The nonlinear part, χ, consists of n/n_0 parallel applications of a small permutation χ_0 over $\mathbb{F}_2^{n_0}$.

Distinguishers for 17 rounds

We have computed that:

- The Walsh spectra of χ_0 and χ_0^{-1} are divisible by 2^3.

As there are 320 parallel applications of χ_0 in a round we have that:

- The Walsh spectra of R and of R^{-1} are divisible by $2^{3\times 320} = 2^{960}$.

So we deduce that:

Bound for the degree of R^{-7}

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

Distinguishers for 17 rounds

We have computed that:

- The Walsh spectra of χ_0 and χ_0^{-1} are divisible by 2^3.

As there are 320 parallel applications of χ_0 in a round we have that:

- The Walsh spectra of R and of R^{-1} are divisible by $2^{3\times 320} = 2^{960}$.

So we deduce that:

Bound for the degree of R^{-7}

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

17 rounds

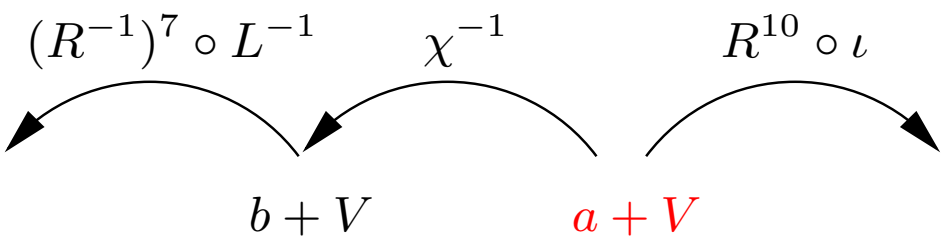
With any V with $\dim V = 1370$
zero-sum partitions of size 2^{1370} for 17 rounds of Keccak-f

Adding one round (18 rounds for Keccak-f)

$$R_8 = \iota \circ \chi \circ L \text{ with } L = \pi \circ \rho \circ \theta$$

We use that χ applies on the rows separately.
Let $B_i = \{x \in \mathbb{F}_2^{1600},\ \mathrm{supp}(x) \subset \text{Row } i\}$
Let V be such that

$$V = \sum_{i \in I} B_i \text{ with } |I| \geq 274$$



A zero-sum partition for 18 rounds of Keccak-f

Adding more rounds

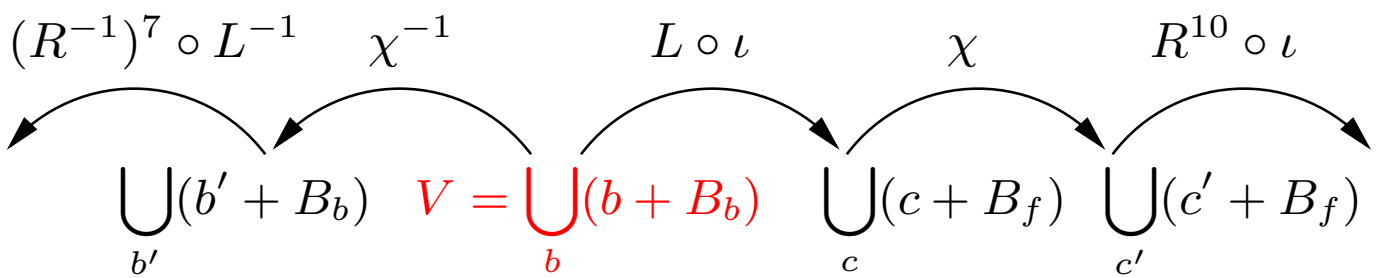
For any V such that

$$B_b = \sum_{i \in I} B_i \subset V \text{ and } B_f = \sum_{j \in J} B_j \subset L(V), |I| \geq 274 \text{ and } |J| \geq 205$$

For any W such that

$$W \subset \sum_{i \in \overline{I}} B_i \text{ and } L(W) \subset \sum_{j \in \overline{J}} B_j \text{ with } |\overline{I}| \leq 46 \text{ and } |\overline{J}| \leq 115$$

we have a zero-sum distinguisher for 19 rounds



Results for 19 rounds and 20 rounds

19 rounds

Let W generated by 4 consecutive slices. Then:

$$L(W) \subset \sum_{i \in I} B_i \text{ with } |I| = 114$$

By adding another 39 linearly independent elements to W, we have

$$\dim W = 139 \text{ and } L(W) \subset \sum_{i \in I'} B_i \text{ with } |I'| = 115$$

64 new zero-sum partitions of size 2^{1461} for 19 rounds of Keccak-f

Results for 19 rounds and 20 rounds

19 rounds

Let W generated by 4 consecutive slices. Then:

$$L(W) \subset \sum_{i \in I} B_i \text{ with } |I| = 114$$

By adding another 39 linearly independent elements to W, we have

$$\dim W = 139 \text{ and } L(W) \subset \sum_{i \in I'} B_i \text{ with } |I'| = 115$$

64 new zero-sum partitions of size 2^{1461} for 19 rounds of Keccak-f

20 rounds

By choosing some W, with $\dim W = 14$ we have found

64 new zero-sum partitions of size 2^{1586} for 20 rounds of Keccak-f

Conclusion

- First structural distinguishers applicable on more than 16 rounds of the Keccak-f permutation;
- Combination of properties of the nonlinear layer and diffusion layer;
- This property does not seem to affect the security of Keccak.

Ongoing work

- Relation with coding theory;
- Application to other hash functions of the SHA-3 contest.