Zero-sum distinguishers for iterated permutations and application to Keccak-f and Hamsi-256

Christina Boura **Anne Canteaut**

SECRET Project-Team, INRIA, France
Gemalto, France

August 12, 2010

Outline

Zero-sums and zero-sum partitions

Zero-sums

- For **block ciphers** (known-key attack) [Knudsen - Rijmen 07]
- For **hash functions** [Aumasson - Meier 09]

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

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

Zero-sums and low-weight words in a linear code

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$.
$\mathcal{C}_F$: linear code of length 2^n and dimension $2n$ defined by

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

Proposition

$\{x_{i_1}, \dots, x_{i_K}\} \subset \mathbb{F}_2^n$ is a zero-sum for F if and only if the codeword with support $\{i_1, \dots, i_K\}$ belongs to $\mathcal{C}_F^{\perp}$.
Most notably,

- *there exists at least a 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 APN function,* i.e.

$$\max_{a,b \neq 0} \#\{x \in \mathbb{F}_2^n,\ F(x+a) + F(x) = b\} = 2.$$

Zero-sum partitions

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.

Exploiting a low degree for finding zero-sum partitions

Higher-order derivatives

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

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

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

Proposition

For every subspace V with $\dim V > \deg F$,

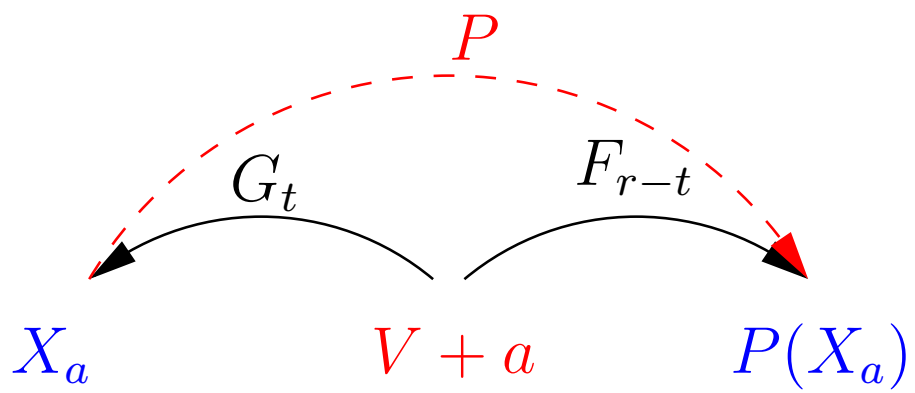
$$D_V F(x) = \sum_{v \in V} F(x+v) = 0, \quad \textit{for every} \quad x \in \mathbb{F}_2^n.$$

Exploiting a low degree (Aumasson-Meier 09)

$$\boldsymbol{P = R_r \circ \cdots \circ R_1}$$

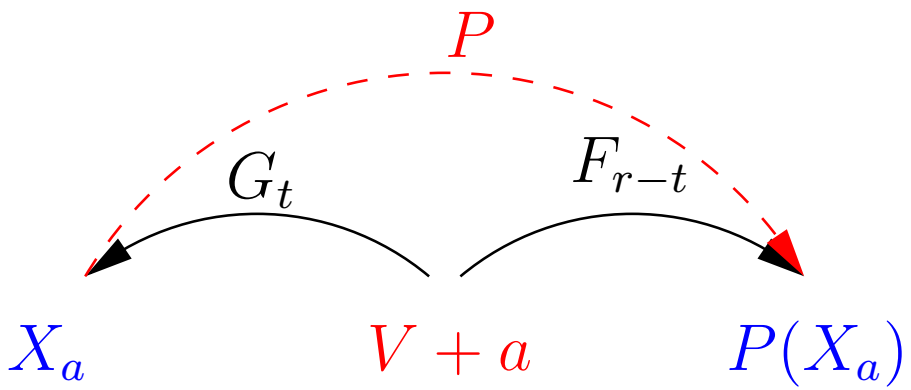
- Let $F_{r-t} = R_r \circ \cdots \circ R_{t+1}$ and $G_t = R_1^{-1} \circ \cdots \circ R_t^{-1}$.
- Let $V \subset \mathbb{F}_2^n$ with $\dim V > \max(\deg F_{r-t}, \deg G_t)$.
- Let $V \oplus W = \mathbb{F}_2^n$.

.



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

is a zero-sum partition of $\mathbb{F}_2^n$ of size $2^{\dim V}$ for P.



$$\sum_{x \in X_a} x = \sum_{z \in V} G_t(z + a) = D_V G_t(a) = 0$$

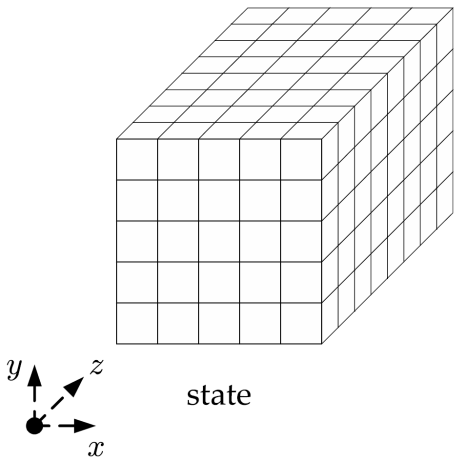
$$\sum_{x \in X_a} P(x) = \sum_{z \in V} F_{r-t}(z + a) = D_V F_{r-t}(a) = 0$$

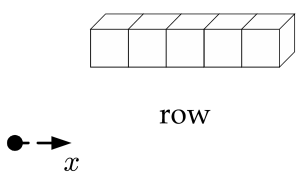
Keccak [Bertoni-Daemen-Peeters-Van Assche 08]

Sponge construction

Keccak-f permutation

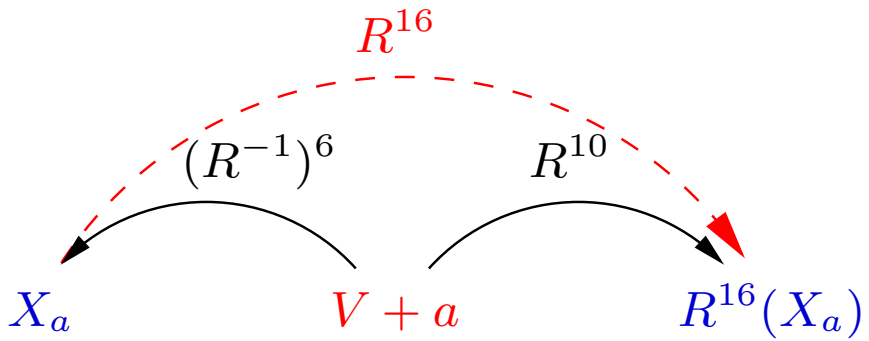
- 1600-bit state, seen as a 3-dimensional $5 \times 5 \times 64$ matrix
- 24 rounds $R = \iota \circ \chi \circ L$
- L linear transformation providing diffusion in all directions
- χ nonlinear transformation, $\deg(\chi) = 2 \quad \deg(\chi^{-1}) = 3$. 320 parallel applications of χ_0 over $\mathbb{F}_2^5$





Zero-sum partitions for 16-round Keccak-f [Aumasson-Meier 09]

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

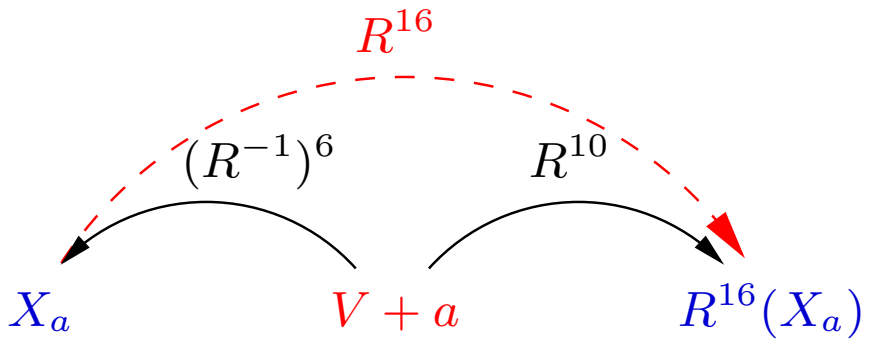


$$X_a = \{(R^{-1})^6(a + z), z \in V\},\ a \in W$$

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

Zero-sum partitions for 16-round Keccak-f [Aumasson-Meier 09]

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



$$X_a = \{(R^{-1})^6(a + z), z \in V\},\ a \in W$$

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

Problem

Improve the trivial bound

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

Definition (Imbalance of a Boolean function)

For any Boolean function f of n variables

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

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

$$\{\mathcal{F}(f + \varphi_a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a \cdot x}, a \in \mathbb{F}_2^n\},$$

Bound on the degree of a composed permutation (2)

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

$$\{\mathcal{F}(\varphi_b \circ F + \varphi_a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x}, \ \ a, b \in \mathbb{F}_2^n, b \neq 0\}.$$

Theorem (Canteaut-Videau 02)

If all values in the Walsh spectrum of F are divisible by 2^ℓ, then for every $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$

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

Zero-sum partitions for 17-round Keccak-f

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}

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

Zero-sum partitions for 17-round Keccak-f

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 $2^{3\times 320} = 2^{960}$.

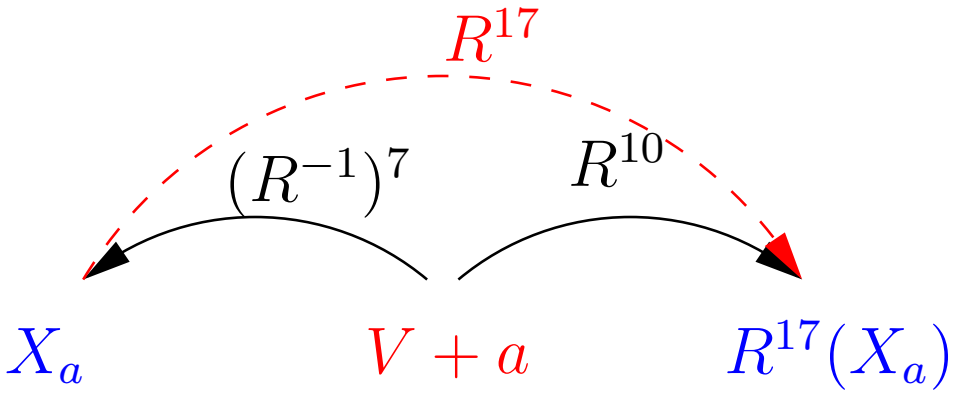
So we deduce that:

Bound for the degree of R^{-7}

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

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

Zero-sum partitions for 17-round Keccak-f (2)



$$X_a = \{(R^{-1})^7(a + z),\ z \in V\},\quad a \in W$$

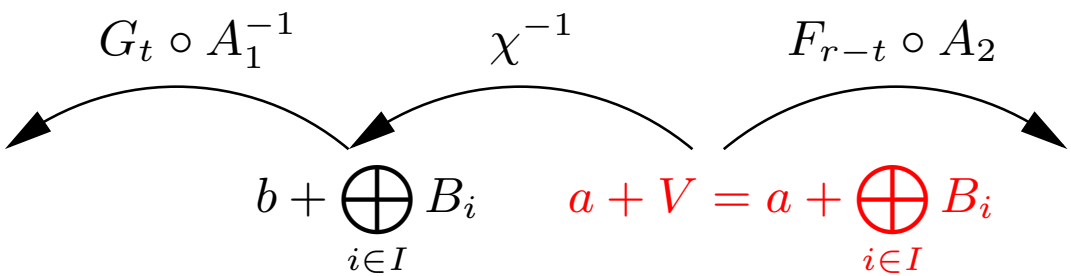
is a zero-sum partition of size 2^{1370} for 17 rounds of Keccak-f.

Adding one round

- χ: parallel applications of χ_0 over $\mathbb{F}_2^{n_0}$.
- $B_i = \{x \in \mathbb{F}_2^n, \text{ supp}(x) \subset \text{Row } i\}$
- Choose

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

  where $\dim V > \max(\deg F_{r-t}, \deg G_t)$.
- Decompose $R_{t+1} = A_2 \circ \chi \circ A_1$.



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

form a zero-sum partition for the $(r+1)$-round permutation P.

Exploiting the linear part for finding zero-sum partitions

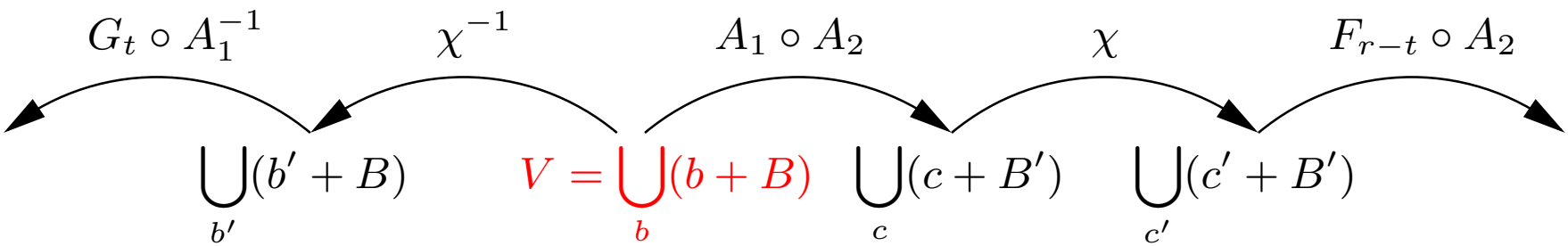
Exploiting the structure of the diffusion part

- $R_{t+1} = A_2 \circ \chi \circ A_1$
- L: linear part of $A_1 \circ A_2$
- Let V such that

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

with $\dim B > \deg G_t$ and $\dim B' > \deg F_{r-t}$.

- Let $V \oplus W = \mathbb{F}_2^n$.



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

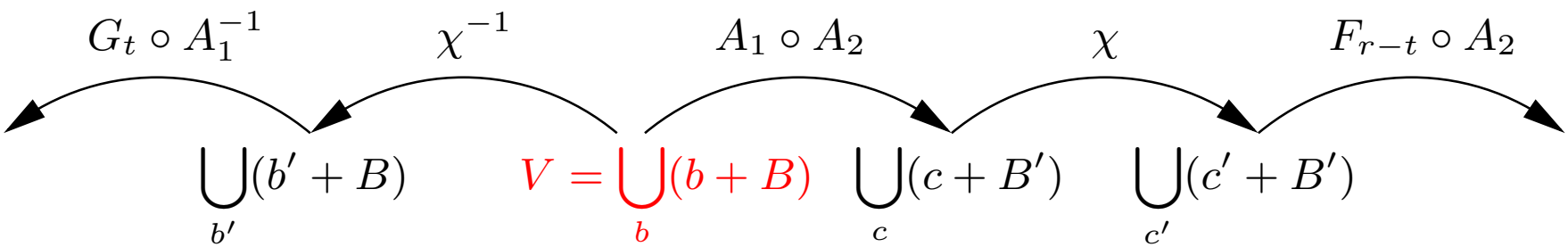
form a zero-sum partition for the $(r+2)$-round permutation P.

Exploiting the structure of the diffusion part (2)

- $R_{t+1} = A_2 \circ \chi \circ A_1$
- L: linear part of $A_1 \circ A_2$
- Let W such that

$$W \subset \bigoplus_{i \in \overline{\mathcal{I}}} B_i = \overline{B} \text{ and } L(W) \subset \bigoplus_{j \in \overline{\mathcal{J}}} B_j = \overline{B'}$$

  with $\dim \overline{B} < n - \deg G_t$ and $\dim \overline{B'} < n - \deg F_{r-t}$.
- Let $V \oplus W = \mathbb{F}_2^n$.



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

form a zero-sum partition for the $(r+2)$-round permutation P.

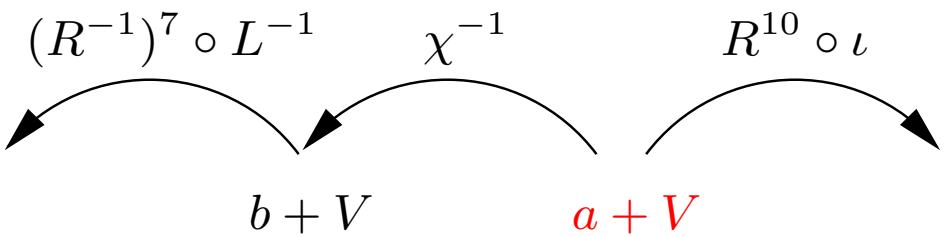
Application to Keccak-f

Zero-sum partitions for 18 rounds of 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 $B_i = \{x \in \mathbb{F}_2^{1600},\ \mathrm{supp}(x) \subset \mathrm{Row}\ i\}$
Let V be such that

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



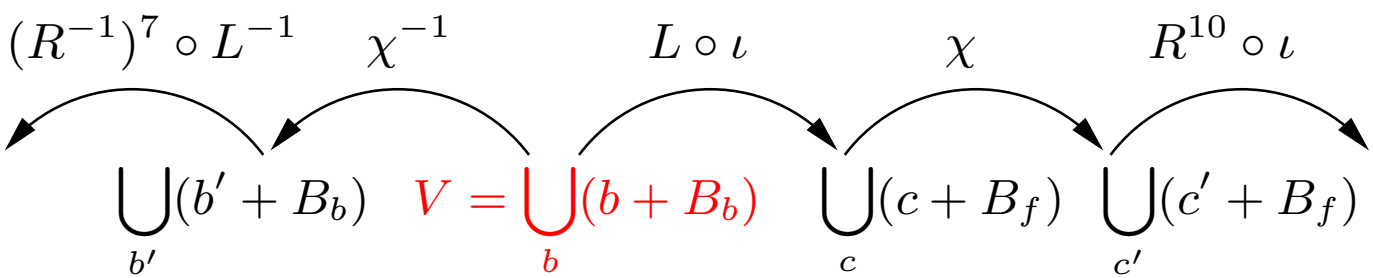
A zero-sum partition for 18 rounds of Keccak-f

Zero-sum partitions for 19 rounds of Keccak-f

We search for W such that

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

with $|\overline{\mathcal{I}}| \leq 46$ and $|\overline{\mathcal{J}}| \leq 115$



Zero-sum partitions for 19 rounds of Keccak-f (2)

- W with $\dim W = 100$ and spanned by 4 consecutive slices:

$$W = \bigoplus_{i=0}^{19} B_i \Rightarrow L(W) \subset \bigoplus_{j \in \mathcal{J}} B_j \text{ with } |\mathcal{J}| = 114.$$

64 zero-sum partitions of size 2^{1500} for 19 rounds.

- W with $\dim W = 139$.

  Add 39 linearly independent vectors x with

$$L(x) \in \bigoplus_{j \in \mathcal{J}} B_j \cup B_a$$

64 zero-sum partitions of size 2^{1461} for 19 rounds.

Zero-sum partitions for 20 rounds of Keccak-f

We search for W such that

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

with $|\overline{\mathcal{I}}| \leq 46$ and $|\overline{\mathcal{J}_2}| \leq 115$.

W with $\dim W = 14$.

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

$L(W)$ belongs to the union of the first 4 slices.

64 zero-sum partitions of size 2^{1586} for 20 rounds.

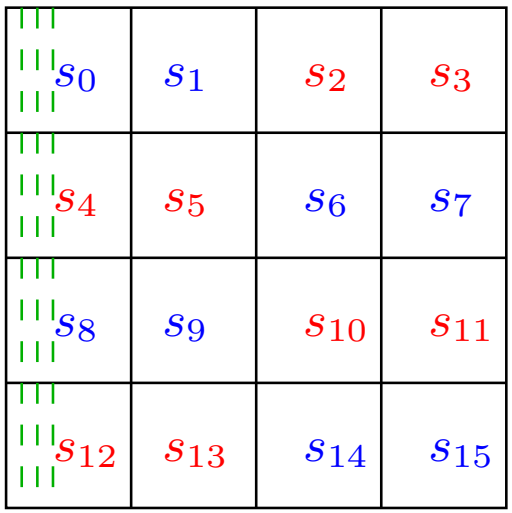
Application to Hamsi-256

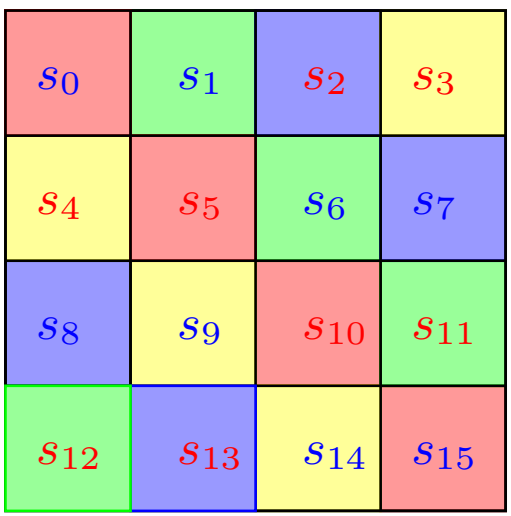
Hamsi-256 [O. Küçük 08]

Davies-Meyer construction

Finalization permutation P_f

- 512-bit state
- 6 rounds $R = L \circ S$
- L linear transformation
- S nonlinear transformation, consisting of 128 parallel applications of a 4×4 Sbox of degree 3





Zero-sum partitions for the permutation P_f of Hamsi-256

- We choose

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

$$X_a = \{((R^{-1})^2 \circ S^{-1})(a+z),\ z \in V\},\quad a \in W$$

form a zero-sum partition of size 2^{19} for P_f.

- Take for V any subspace generated by 10 elements in a 32-bit word.

Zero-sum partitions of size 2^{10} for P_f.

Conclusion

- New family of distinguishers for cryptographic building-blocks;
- These results do not seem to threaten the security of the hash functions but invalidate the proofs;
- The bound on the degree of iterated permutations can be further improved;
- The impact of these distinguishers must be studied.