Higher-order Differential Properties for Keccak and Luffa

Christina Boura[1,2] **Anne Canteaut**[1] **Christophe De Cannière**[3]

[1]SECRET Project-Team, INRIA, France
[2]Gemalto, France
[3]Katholieke Universiteit Leuven,Belgium

February 15, 2011

Outline

Outline

Objective of this paper

- Study the algebraic degree of some hash function proposals and of their inner primitives.
- Use these results to construct higher-order differential distinguishers and zero-sum structures.

Previous work (related with the SHA-3 competition)

- Zero-sum Distinguishers for Keccak, Luffa and Hamsi. [Aumasson-Meier 09, Aumasson et al. 09, Boura-Canteaut 10]
- Higher-order differential attack on Luffa v1. [Watanabe et al. 10]

Bound on the degree of iterated permutations

Question

How to estimate the algebraic degree of an iterated permutation after r rounds?

Bound on the degree of iterated permutations

Question

How to estimate the algebraic degree of an iterated permutation after r rounds?

Trivial Bound

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

Bound on the degree of iterated permutations

Question

How to estimate the algebraic degree of an iterated permutation after r rounds?

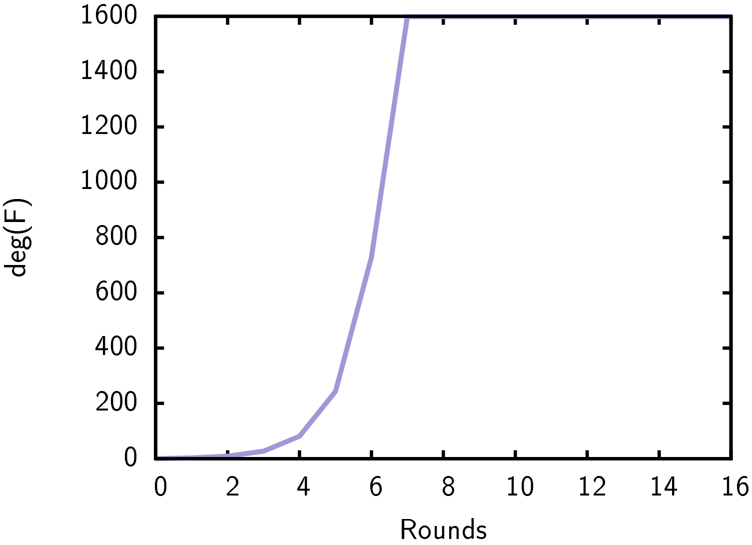
Trivial Bound

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

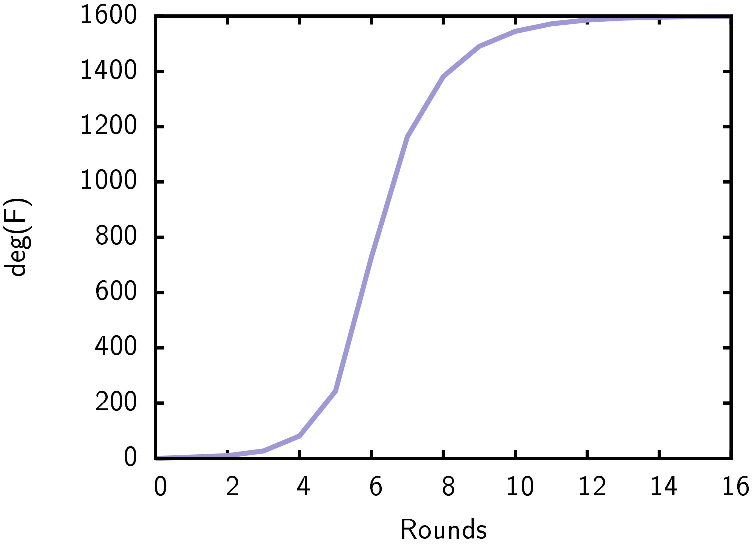
[Canteaut-Videau 02]: **Improvement** when the Walsh spectrum of F is divisible by a high power of 2.

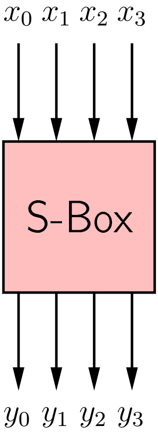
Outline

Towards a new bound on the degree $(\deg F = 3)$



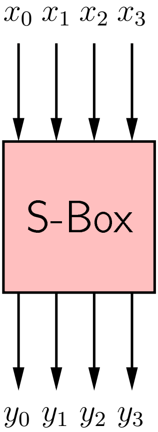
Towards a new bound on the degree $(\deg F = 3)$





Question

If S is **balanced**, what is the degree of the product of $\boldsymbol{k}$ coordinates of S?

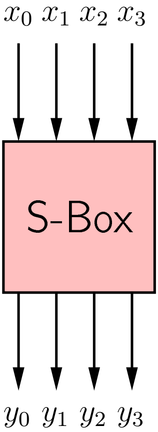


Question

If S is **balanced**, what is the degree of the product of $\boldsymbol{k}$ coordinates of S?

Definition

$\boldsymbol{\delta_k}$: maximum degree of the product of $\boldsymbol{k}$ coordinates of S



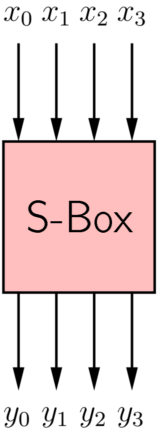
Question

If S is **balanced**, what is the degree of the product of $\boldsymbol{k}$ coordinates of S?

Definition

$\boldsymbol{\delta_k}$: maximum degree of the product of $\boldsymbol{k}$ coordinates of S

$\boldsymbol{k}$	$\boldsymbol{\delta_k}$
1	3



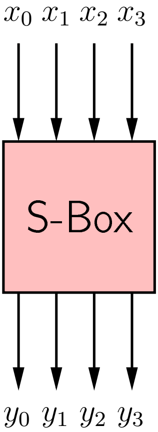
Question

If S is **balanced**, what is the degree of the product of $\boldsymbol{k}$ coordinates of S?

Definition

$\boldsymbol{\delta_k}$: maximum degree of the product of $\boldsymbol{k}$ coordinates of S

$\boldsymbol{k}$	$\boldsymbol{\delta_k}$
1	3
2	3
3	3



Question

If S is **balanced**, what is the degree of the product of $\boldsymbol{k}$ coordinates of S?

Definition

$\boldsymbol{\delta_k}$: maximum degree of the product of $\boldsymbol{k}$ coordinates of S

$\boldsymbol{k}$	$\boldsymbol{\delta_k}$
1	3
2	3
3	3
4	4

F **permutation** of $\mathbb{F}_2^n$:
$\boldsymbol{\delta_k} = n$ iff $k = n$.

The new bound

Theorem. Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ corresponding to the concatenation of m smaller Sboxes, $S_1, \ldots, S_m$, defined over $\mathbb{F}_2^{n_0}$. Then, for any function G from $\mathbb{F}_2^n$ into $\mathbb{F}_2^\ell$, we have

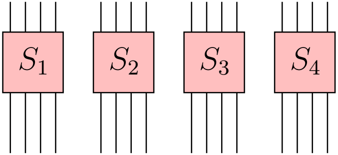
$$\mathbf{deg}(G \circ F) \leq n - \frac{n - \mathbf{deg}(G)}{\gamma},$$

where

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

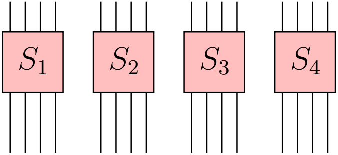
Most notably, if all Sboxes are balanced, we have

$$\mathbf{deg}(G \circ F) \leq n - \frac{n - \mathbf{deg}(G)}{n_0 - 1}.$$



Problem

Multiply d output bits from S_1, S_2, S_3, S_4 in such a way that the degree of their product π, $\deg(\pi)$ is maximized.

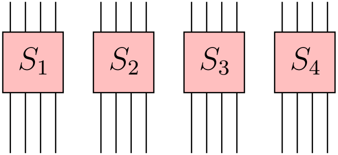


Problem

Multiply d output bits from S_1, S_2, S_3, S_4 in such a way that the degree of their product π, $\deg(\pi)$ is maximized.

Definition

$x_i = \#$ Sboxes for which exactly i coordinates are involved in π.



Problem

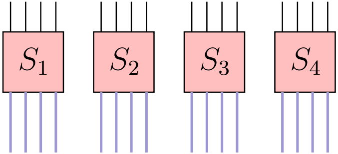
Multiply d output bits from S_1, S_2, S_3, S_4 in such a way that the degree of their product π, $\deg(\pi)$ is maximized.

Definition

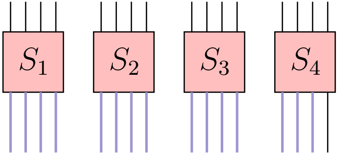
$x_i = \#$ Sboxes for which exactly i coordinates are involved in π.

$$\deg(\pi) \leq \max_{(x_1,x_2,x_3,x_4)} (\delta_1 x_1 + \delta_2 x_2 + \delta_3 x_3 + \delta_4 x_4)$$

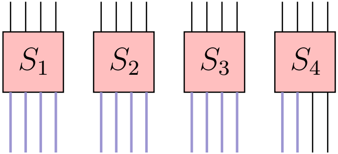
with $x_1 + 2x_2 + 3x_3 + 4x_4 = d$.



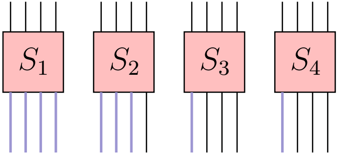
d	x_4	x_3	x_2	x_1	$\deg(\pi)$
16	4	-	-	-	16
15					
14					
13					
12					
11					
10					
9					
⋮	⋮	⋮	⋮	⋮	⋮



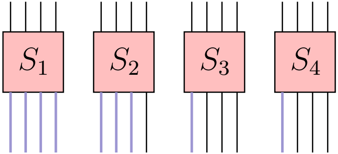
d	x_4	x_3	x_2	x_1	$\deg(\pi)$
16	4	-	-	-	16
15	3	1	-	-	15
14					
13					
12					
11					
10					
9					
⋮	⋮	⋮	⋮	⋮	⋮



d	x_4	x_3	x_2	x_1	$\deg(\pi)$
16	4	-	-	-	16
15	3	1	-	-	15
14	3	-	1	-	15
13					
12					
11					
10					
9					
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

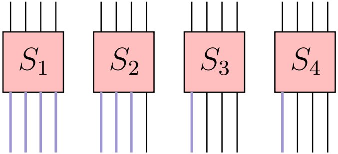


d	x_4	x_3	x_2	x_1	$\deg(\pi)$
16	4	-	-	-	16
15	3	1	-	-	15
14	3	-	1	-	15
13	3	-	-	1	15
12	2	1	-	1	14
11	2	-	1	1	14
10	2	-	-	2	14
9	1	1	-	2	13
⋮	⋮	⋮	⋮	⋮	⋮



d	x_4	x_3	x_2	x_1	$\deg(\pi)$
16	4	-	-	-	16
15	3	1	-	-	15
14	3	-	1	-	15
13	3	-	-	1	15
12	2	1	-	1	14
11	2	-	1	1	14
10	2	-	-	2	14
9	1	1	-	2	13
⋮	⋮	⋮	⋮	⋮	⋮

$$16 - \deg(\pi) \geq \frac{16 - d}{3}$$



d	x_4	x_3	x_2	x_1	$\deg(\pi)$
16	4	-	-	-	16
15	3	1	-	-	15
14	3	-	1	-	15
13	3	-	-	1	15
12	2	1	-	1	14
11	2	-	1	1	14
10	2	-	-	2	14
9	1	1	-	2	13
⋮	⋮	⋮	⋮	⋮	⋮

$$\deg(\pi) \leq 16 - \frac{16 - d}{3}$$

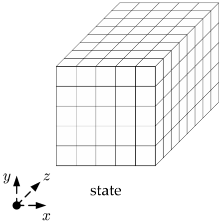
Outline

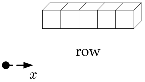
Keccak [Bertoni-Daemen-Peeters-Van Assche 08]

3rd round SHA-3 candidate
Sponge construction

Keccak-f Permutation

- 1600-bit state, seen as a 3-dimensional $5 \times 5 \times 64$ matrix
- 24 rounds R
- Nonlinear layer: 320 parallel applications of a 5×5 S-box χ
- $\deg \chi = 2$, $\deg \chi^{-1} = 3$





Zero-Sums and Zero-sum Partitions

- For **block ciphers** (known-key attack) [Knudsen - Rijmen 07]
- For **hash functions** [Aumasson - Meier 09, Boura - Canteaut 10]

Definition[Zero-Sum]
Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$.
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 Zero-sum Partitions

- For **block ciphers** (known-key attack) [Knudsen - Rijmen 07]
- For **hash functions** [Aumasson - Meier 09, Boura - Canteaut 10]

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.

The new bound applied on Keccak-f

Let $\boldsymbol{R}$ be the round function of Keccak-f and $\boldsymbol{R}^{-1}$ its inverse.
For any $\boldsymbol{F}$,

$$\mathbf{deg}(\boldsymbol{F} \circ \boldsymbol{R}) \leq \mathbf{1600} - \frac{\mathbf{1600} - \mathbf{deg}(\boldsymbol{F})}{\mathbf{3}}$$

$$\mathbf{deg}(\boldsymbol{F} \circ \boldsymbol{R}^{-1}) \leq \mathbf{1600} - \frac{\mathbf{1600} - \mathbf{deg}(\boldsymbol{F})}{\mathbf{3}}$$

Observation [Duan-Lai 11] For χ^{-1} : $\boldsymbol{\delta_2} = \mathbf{3}$
Then,

$$\mathbf{deg}(\boldsymbol{F} \circ \boldsymbol{R}^{-1}) \leq \mathbf{1600} - \frac{\mathbf{1600} - \mathbf{deg}(\boldsymbol{F})}{\mathbf{2}}$$

r	$\deg(R^r)$	$\deg(R^{-r})$
1	2	3
2	4	9
3	8	27
4	16	81
5	32	243
6	64	729
7	128	1164
8	256	1382
9	512	1491
10	1024	1545
11	1408	1572
12	1536	1586
13	1578	1593
14	1592	1596
15	1597	1598
16	1599	1599

Zero-Sum Partitions for the full Keccak-f (24 rounds)

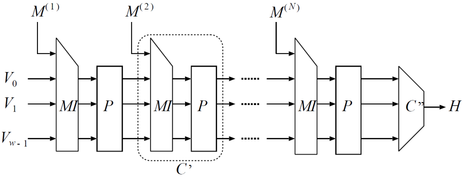
Starting with any collection of 315 rows after the linear layer in the 12-th round, we get

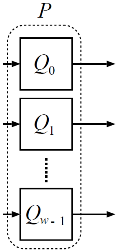
zero-sum partitions of size 2^{1575}

for the full Keccak-f permutation.

Luffa [De Cannière, Sato and Watanabe 08]

- "Sponge-like" construction;
- Linear message injection function *MI*;
- Permutation P, splitted into w parallel 256-bit permutations $Q_0, \ldots, Q_{w-1}$;
- Q_j : 8-round permutation. Every round called Step;





The Step function:

- SubCrumb: 64 parallel 4×4 Sboxes of degree 3;
- MixWord: Linear layer mixing the 32-bit words two by two.

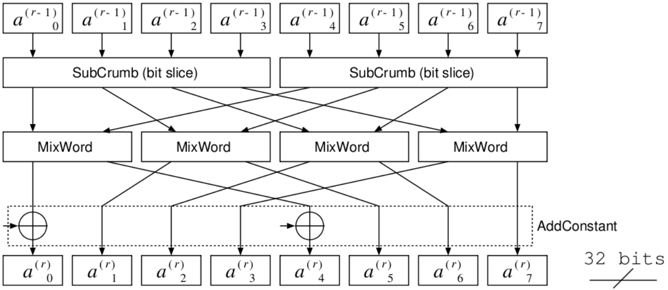


Figure: The Step function

The Step function:

- SubCrumb: 64 parallel 4×4 Sboxes of degree 3;
- MixWord: Linear layer mixing the 32-bit words two by two.

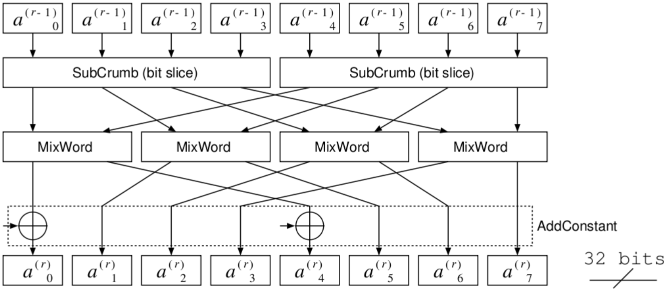


Figure: The Step function

Different Sbox for Luffa v1 and Luffa v2!

Bound on the degree of Q_j for Luffa v1

For $r \leq 5$, bound by Watanabe et al.

r	$\deg x^r$
1	3
2	8
3	20
4	51
5	130

Bound on the degree of Q_j for Luffa v1

For $r \leq 5$, bound by Watanabe et al.

r	$\deg x^r$
1	3
2	8
3	20
4	51
5	130
6	214
7	242
8	251

For $r \geq 6$, we apply,

$$\deg(\mathtt{Step}^{r+1}) \leq \frac{512 + \deg(\mathtt{Step}^r)}{3}$$

Higher-order differentials for the Luffa v1 hash function

- Degree of Luffa v1 hash function, applied to 256-bit messages is at most 251.
- Distinguisher for **full** Luffa v1 with 2^{240} 1-block messages.

Improvement of the previous attack applied to Luffa v1 reduced to 7 steps out of 8. [Watanabe et al. 10]

An observation on the Sbox of Luffa v2

$$
\begin{aligned}
y_0 &= 1 + x_0 + x_1 + x_1x_2 + x_0x_3 + x_1x_3 + \boldsymbol{x_0x_1x_3} + \boldsymbol{x_0x_2x_3} \\
y_1 &= x_0 + x_3 + x_0x_1 + x_1x_2 + x_0x_3 + x_1x_3 + \boldsymbol{x_0x_1x_3} + \boldsymbol{x_0x_2x_3} \\
y_2 &= 1 + x_1 + x_3 + x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3 + \boldsymbol{x_0x_1x_2} + \boldsymbol{x_0x_1x_3} \\
y_3 &= 1 + x_1 + x_2 + x_0x_3 + x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3 + \boldsymbol{x_0x_1x_2} \\
&+ \boldsymbol{x_0x_1x_3}
\end{aligned}
$$

An observation on the Sbox of Luffa v2

$$
\begin{aligned}
y_0 &= 1 + x_0 + x_1 + x_1x_2 + x_0x_3 + x_1x_3 + \boldsymbol{x_0x_1x_3} + \boldsymbol{x_0x_2x_3} \\
y_1 &= x_0 + x_3 + x_0x_1 + x_1x_2 + x_0x_3 + x_1x_3 + \boldsymbol{x_0x_1x_3} + \boldsymbol{x_0x_2x_3} \\
y_2 &= 1 + x_1 + x_3 + x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3 + \boldsymbol{x_0x_1x_2} + \boldsymbol{x_0x_1x_3} \\
y_3 &= 1 + x_1 + x_2 + x_0x_3 + x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3 + \boldsymbol{x_0x_1x_2} \\
&+ \boldsymbol{x_0x_1x_3}
\end{aligned}
$$

$$
d = y_0+y_1+y_2+y_3 = 1+x_1+x_2+x_0x_1+x_0x_3
$$

An observation on the Sbox of Luffa v2

$$
\begin{aligned}
y_0 &= 1 + x_0 + x_1 + x_1x_2 + x_0x_3 + x_1x_3 + \boldsymbol{x_0x_1x_3} + \boldsymbol{x_0x_2x_3} \\
y_1 &= x_0 + x_3 + x_0x_1 + x_1x_2 + x_0x_3 + x_1x_3 + \boldsymbol{x_0x_1x_3} + \boldsymbol{x_0x_2x_3} \\
y_2 &= 1 + x_1 + x_3 + x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3 + \boldsymbol{x_0x_1x_2} + \boldsymbol{x_0x_1x_3} \\
y_3 &= 1 + x_1 + x_2 + x_0x_3 + x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3 + \boldsymbol{x_0x_1x_2} \\
&+ \boldsymbol{x_0x_1x_3}
\end{aligned}
$$

$$
d = y_0+y_1+y_2+y_3 = 1+x_1+x_2+x_0x_1+x_0x_3
$$

The sum of the four coordinates is of degree 2!

Algebraic degree of the Q_j permutation

Sum of 2 distinct monomials of degree 3 in 4 variables, x_i, x_j, x_k, x_ℓ, where $d = x_i + x_j + x_k + x_l$:

$$x_i x_j x_k + x_i x_j x_\ell \quad = \quad x_i x_j x_k + x_i x_j (x_i + x_j + x_k + d)$$

Algebraic degree of the Q_j permutation

Sum of 2 distinct monomials of degree 3 in 4 variables, x_i, x_j, x_k, x_ℓ, where $d = x_i + x_j + x_k + x_l$:

$$\begin{aligned} x_i x_j x_k + x_i x_j x_\ell &= x_i x_j x_k + x_i x_j (x_i + x_j + x_k + d) \\ &= x_i x_j x_k + x_i x_j + x_i x_j + x_i x_j x_k + x_i x_j d \end{aligned}$$

Algebraic degree of the Q_j permutation

Sum of 2 distinct monomials of degree 3 in 4 variables, x_i, x_j, x_k, x_ℓ, where $d = x_i + x_j + x_k + x_l$:

$$
\begin{aligned}
x_i x_j x_k + x_i x_j x_\ell &= x_i x_j x_k + x_i x_j (x_i + x_j + x_k + d) \\
&= x_i x_j x_k + x_i x_j + x_i x_j + x_i x_j x_k + x_i x_j d
\end{aligned}
$$

Algebraic degree of the Q_j permutation

Sum of 2 distinct monomials of degree 3 in 4 variables, x_i, x_j, x_k, x_ℓ, where $d = x_i + x_j + x_k + x_l$:

$$\begin{aligned} x_i x_j x_k + x_i x_j x_\ell &= x_i x_j x_k + x_i x_j (x_i + x_j + x_k + d) \\ &= x_i x_j d \end{aligned}$$

Algebraic degree of the Q_j permutation

Sum of 2 distinct monomials of degree 3 in 4 variables, x_i, x_j, x_k, x_ℓ, where $d = x_i + x_j + x_k + x_l$:

$$\begin{aligned} x_i x_j x_k + x_i x_j x_\ell &= x_i x_j x_k + x_i x_j (x_i + x_j + x_k + d) \\ &= x_i x_j d \end{aligned}$$

- $x_0^r, x_1^r, x_2^r, x_3^r$ output words of r rounds of `Step`.
- $d^r = x_0^r + x_1^r + x_2^r + x_3^r$.

Algebraic degree of the Q_j permutation

Sum of 2 distinct monomials of degree 3 in 4 variables, x_i, x_j, x_k, x_ℓ, where $d = x_i + x_j + x_k + x_l$:

$$\begin{aligned} x_i x_j x_k + x_i x_j x_\ell &= x_i x_j x_k + x_i x_j (x_i + x_j + x_k + d) \\ &= x_i x_j d \end{aligned}$$

- $x_0^r, x_1^r, x_2^r, x_3^r$ output words of r rounds of `Step`.
- $d^r = x_0^r + x_1^r + x_2^r + x_3^r$.

Then,

$$\deg x_i^{r+1} \leq 2 \max_j \deg x_j^r + \deg d^r$$

Algebraic degree of the Q_j permutation

Sum of 2 distinct monomials of degree 3 in 4 variables, x_i, x_j, x_k, x_ℓ, where $d = x_i + x_j + x_k + x_l$:

$$\begin{aligned} x_i x_j x_k + x_i x_j x_\ell &= x_i x_j x_k + x_i x_j (x_i + x_j + x_k + d) \\ &= x_i x_j d \end{aligned}$$

- $x_0^r, x_1^r, x_2^r, x_3^r$ output words of r rounds of Step.
- $d^r = x_0^r + x_1^r + x_2^r + x_3^r$.

Then,

$$\deg x_i^{r+1} \leq 2 \max_j \deg x_j^r + \deg d^r$$

$$\deg d^{r+1} \leq 2 \max_j \deg x_j^r$$

Upper bounds on the algebraic degree of Q_j in Luffa v2

r	$\deg x^r$	$\deg d^r$
1	3	2
2	8	6
3	22	16
4	60	44
5	164	120

Upper bounds on the algebraic degree of Q_j in Luffa v2

r	$\deg x^r$	$\deg d^r$
1	3	2
2	8	6
3	22	16
4	60	44
5	164	120
6	225	210
7	245	240
8	252	250

For $r \geq 6$, we apply,

$$\deg(\texttt{Step}^{r+1}) \leq \frac{512 + \deg(\texttt{Step}^r)}{3}$$

Higher-order differential distinguishers for Luffa v2

Results

- Degree of the compression function at most 252.
- All-zero higher-order differentials for the full compression function.

Not extendable to the hash function, because of the addition of a blank round for all the messages.

Outline

Application to Grøstl-256

Permutation P

- 512-bit state, seen as an 8×8 matrix.
- 10 rounds of AES-like transformations.
- AES Sbox of degree 7.

Application to Grøstl-256

Permutation P

- 512-bit state, seen as an 8×8 matrix.
- 10 rounds of AES-like transformations.
- AES Sbox of degree 7.

Round	$\deg(R^r)$
1	7
2	49
3	343
4	**487**
5	**508**
6	**511**

Application to Grøstl-256

Permutation P

- 512-bit state, seen as an 8×8 matrix.
- 10 rounds of AES-like transformations.
- AES Sbox of degree 7.

Round	$\deg(R^r)$
1	7
2	49
3	343
4	**487**
5	**508**
6	**511**

Zero-sum partitions of size 2^{509}.

Conclusions

- New bound on the degree of iterated permutations.
- Zero-sum distinguishers for the full Keccak-f permutation.
  (Contradiction of the so-called hermetic sponge strategy)
- All-zero higher-order differentials for the Luffa hash family.
- Application to AES-based candidates.

Conclusions

- New bound on the degree of iterated permutations.
- Zero-sum distinguishers for the full Keccak-f permutation.
  (Contradiction of the so-called hermetic sponge strategy)
- All-zero higher-order differentials for the Luffa hash family.
- Application to AES-based candidates.

Thank you for your attention!