On the algebraic degree of some SHA-3 candidates

Christina Boura and **Anne Canteaut**

SECRET Project-Team, INRIA Paris-Rocquencourt
Gemalto, France

March 22, 2012

Outline

Outline

Iterated permutations

Most of the symmetric constructions (hash functions, block ciphers ...) are based on a **permutation iterated a high number of times**.

Important to estimate the algebraic degree of such iterated permutations.

Functions with a low degree are vulnerable to:

- Higher-order differential attacks and distinguishers (e.g. zero-sum distinguishers ...)
- Cube attacks
- Algebraic attacks

Algebraic degree of a vectorial function $F : \mathbf{F}_2^n \to \mathbf{F}_2^m$

Example (Inverse of Keccak's Sbox):

$$\begin{aligned} F(x_0, x_1, x_2, x_3, x_4) \quad = \quad & (x_0 + x_2 + x_4 + x_1x_2 + x_1x_4 + x_3x_4 + x_1x_3x_4, \\ & x_0 + x_1 + x_3 + x_0x_2 + x_0x_4 + x_2x_3 + x_0x_2x_4, \\ & x_1 + x_2 + x_4 + x_0x_1 + x_1x_3 + x_3x_4 + x_0x_1x_3, \\ & x_0 + x_2 + x_3 + x_0x_4 + x_1x_2 + x_2x_4 + x_1x_2x_4, \\ & x_1 + x_3 + x_4 + x_0x_1 + x_0x_3 + x_2x_3 + x_0x_2x_3). \end{aligned}$$

Algebraic degree of a vectorial function $F : \mathbf{F}_2^n \to \mathbf{F}_2^m$

Example (Inverse of Keccak's Sbox):

$$\begin{aligned} F(x_0, x_1, x_2, x_3, x_4) \quad = \quad & (x_0 + x_2 + x_4 + x_1x_2 + x_1x_4 + x_3x_4 + x_1x_3x_4, \\ & x_0 + x_1 + x_3 + x_0x_2 + x_0x_4 + x_2x_3 + x_0x_2x_4, \\ & x_1 + x_2 + x_4 + x_0x_1 + x_1x_3 + x_3x_4 + x_0x_1x_3, \\ & x_0 + x_2 + x_3 + x_0x_4 + x_1x_2 + x_2x_4 + x_1x_2x_4, \\ & x_1 + x_3 + x_4 + x_0x_1 + x_0x_3 + x_2x_3 + x_0x_2x_3). \end{aligned}$$

The algebraic degree of F is 3.

Degree of an iterated function

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

Find a good estimate of $\deg(G \circ F)$.

Degree of an iterated function

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

Find a good estimate of $\deg(G \circ F)$.

Trivial bound

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

Degree of an iterated function

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

Find a good estimate of $\deg(G \circ F)$.

Trivial bound

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

When the Walsh coefficients of F are divisible by 2^ℓ.
[Canteaut-Videau '02]

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

When F is the concatenation of smaller balanced functions over $\mathbf{F}_{2^{n_0}}$ [Boura Canteaut DeCannière '11]

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

The case of Keccak

Keccak [Bertoni *et al.* 08]

Nonlinearity : 5×5 nonlinear permutation χ.
$\deg(\chi) = 2$, $\deg(\chi^{-1}) = 3$.

The resistance of Keccak against **zero-sum distinguishers** has been widely studied.

- **Trivial bound**: 16-round distinguisher.
- **[Canteaut Videau 02]**: 18-round distinguisher.
- **[Boura Canteaut DeCannière '11]**: 24-round distinguisher.

The case of Keccak

Keccak [Bertoni *et al.* 08]

Nonlinearity : 5×5 nonlinear permutation χ.
$\deg(\chi) = 2$, $\deg(\chi^{-1}) = 3$.

The resistance of Keccak against **zero-sum distinguishers** has been widely studied.

- **Trivial bound**: 16-round distinguisher.
- **[Canteaut Videau 02]**: 18-round distinguisher.
- **[Boura Canteaut DeCannière '11]**: 24-round distinguisher.

Observation of [Duan-Lai 11]:

The product of any **two** coordinates of χ^{-1} is of degree 3.

Outline

A new result

$\boldsymbol{\delta_k(F)}$: **maximal degree** of the **product** of k coordinates of F

[Duan-Lai 11]: $\boldsymbol{\delta_2(\chi^{-1}) = 3}$.

Question: Is $\delta_2(\chi^{-1})$ related to $\deg(\chi)$?

A new result

$\boldsymbol{\delta_k(F)}$: **maximal degree** of the **product** of k coordinates of F

[Duan-Lai 11]: $\boldsymbol{\delta_2(\chi^{-1}) = 3}$.

Question: Is $\delta_2(\chi^{-1})$ related to $\deg(\chi)$?

Theorem: Let F be a permutation of $\mathbf{F}_2^n$. Then, for any integers k and ℓ,

$$\delta_\ell(F) < n - k \text{ if and only if } \delta_k(F^{-1}) < n - \ell.$$

Application to Keccak

Corollary: Let F be a permutation of $\mathbf{F}_2^n$. Then, for any integer ℓ

$$\delta_\ell(F) < n-1 \text{ if and only if } \deg(F^{-1}) < n-\ell.$$

Case of Keccak: For $F = \chi^{-1}$ and $\ell = 2$,

$$\delta_2(\chi^{-1}) < 5-1 \text{ iff } \deg(\chi) < 5-2$$

A new bound

Theorem: When F is a permutation,

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

Consequence when F is the concatenation of smaller permutations

Proposition [Boura Canteaut DeCannière '11]

Let $F = (S, \ldots, S)$, where S is a permutation of $\mathbf{F}_{2^{n_0}}$. Then,

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

where

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

In particular,

$$\gamma(S) \leq \max\left(\frac{n_0 - 1}{n_0 - \deg S}, n_0 - 2\right).$$

Consequence when F is the concatenation of smaller permutations

Proposition

Let $F = (S, \ldots, S)$, where S is a permutation of $\mathbf{F}_{2^{n_0}}$. Then,

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

where

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

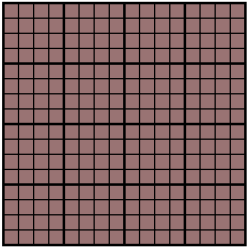
In particular,

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

Outline

ECHO

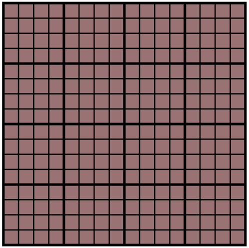
ECHO [Benadjila *et al.* 08]



- 2048-bit state (16 **AES** states)
- `BIG.SubWords` $= 2$ rounds of **AES**
- 16 parallel applications of `BIG.SubWords`.

ECHO

ECHO [Benadjila *et al.* 08]

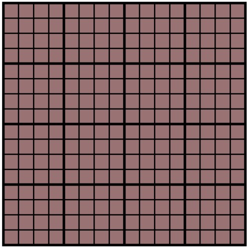


- 2048-bit state (16 **AES** states)
- `BIG.SubWords` $= 2$ rounds of **AES**
- 16 parallel applications of `BIG.SubWords`.

What is the degree of `BIG.SubWords`?

ECHO

ECHO [Benadjila *et al.* 08]



- 2048-bit state (16 **AES** states)
- BIG.SubWords $=2$ rounds of **AES**
- 16 parallel applications of BIG.SubWords.

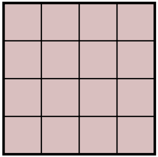
What is the degree of BIG.SubWords?

Trivial approach:

$$\deg(\texttt{BIG.SubWords}) \leq 7^2 = 49.$$

The degree of BIG.SubWords

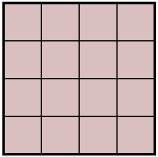
$\texttt{BIG.SubWords} = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AC} \circ \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AC}$



$\texttt{MC} := \texttt{MixColumns}$ $\texttt{SR} := \texttt{ShiftRows}$ $\texttt{SB} := \texttt{SubBytes}$ $\texttt{AC} := \texttt{AddConstant}$

The degree of BIG.SubWords

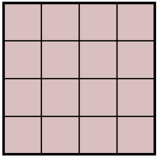
$\mathtt{BIG.SubWords} = \mathtt{MC} \circ \mathtt{SR} \circ \mathtt{SB} \circ \mathtt{AC} \circ \mathtt{MC} \circ \mathtt{SR} \circ \mathtt{SB} \circ \mathtt{AC}$



MC := MixColumns SR := ShiftRows SB := SubBytes AC := AddConstant

The degree of BIG.SubWords

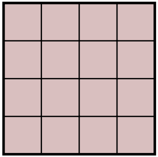
$\texttt{BIG.SubWords} = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AC} \circ \texttt{MC} \circ \texttt{SB} \circ \texttt{SR} \circ \texttt{AC}$



$\texttt{MC} := \texttt{MixColumns}$ $\texttt{SR} := \texttt{ShiftRows}$ $\texttt{SB} := \texttt{SubBytes}$ $\texttt{AC} := \texttt{AddConstant}$

The degree of BIG.SubWords

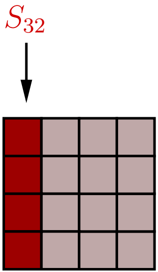
$$\texttt{BIG.SubWords} = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AC} \circ \texttt{MC} \circ \texttt{SB} \circ \texttt{SR} \circ \texttt{AC}$$



MC := MixColumns   SR := ShiftRows   SB := SubBytes   AC := AddConstant

The degree of BIG.SubWords

$\texttt{BIG.SubWords} = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AC} \circ \texttt{MC} \circ \texttt{SB} \circ \texttt{SR} \circ \texttt{AC}$

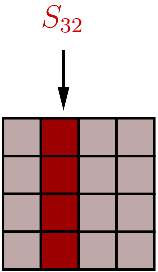


4 parallel applications of S_{32}.

$\texttt{MC} := \texttt{MixColumns}$ $\texttt{SR} := \texttt{ShiftRows}$ $\texttt{SB} := \texttt{SubBytes}$ $\texttt{AC} := \texttt{AddConstant}$

The degree of BIG.SubWords

$$\texttt{BIG.SubWords} = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AC} \circ \texttt{MC} \circ \texttt{SB} \circ \texttt{SR} \circ \texttt{AC}$$

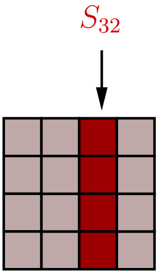


4 parallel applications of S_{32}.

$\texttt{MC} := \texttt{MixColumns}$ $\texttt{SR} := \texttt{ShiftRows}$ $\texttt{SB} := \texttt{SubBytes}$ $\texttt{AC} := \texttt{AddConstant}$

The degree of BIG.SubWords

$\texttt{BIG.SubWords} = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AC} \circ \texttt{MC} \circ \texttt{SB} \circ \texttt{SR} \circ \texttt{AC}$

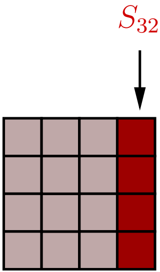


4 parallel applications of S_{32}.

$\texttt{MC} := \texttt{MixColumns}$ $\texttt{SR} := \texttt{ShiftRows}$ $\texttt{SB} := \texttt{SubBytes}$ $\texttt{AC} := \texttt{AddConstant}$

The degree of BIG.SubWords

$\texttt{BIG.SubWords} = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AC} \circ \texttt{MC} \circ \texttt{SB} \circ \texttt{SR} \circ \texttt{AC}$

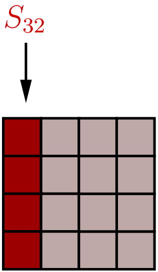


4 parallel applications of S_{32}.

$\texttt{MC}$:= MixColumns $\texttt{SR}$:= ShiftRows $\texttt{SB}$:= SubBytes $\texttt{AC}$:= AddConstant

The degree of BIG.SubWords

BIG.SubWords $=$ MC $\circ$ SR $\circ$ SB $\circ$ AC $\circ$ MC $\circ$ SB $\circ$ SR $\circ$ AC



4 parallel applications of S_{32}.

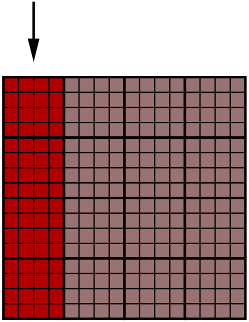
$$\deg(S_{32}) \leq 32 - \frac{32-7}{7} \leq \mathbf{28}.$$

MC := MixColumns SR := ShiftRows SB := SubBytes AC := AddConstant

The degree of ECHO

4 parallel applications of

S_{512}



After the $\mathbf{1}^{\text{st}}$ Sbox layer of the $\mathbf{2}^{\text{nd}}$ round:

$$\deg \leq 7 \cdot 28 = \mathbf{196}$$

After $\mathbf{2}$ rounds:

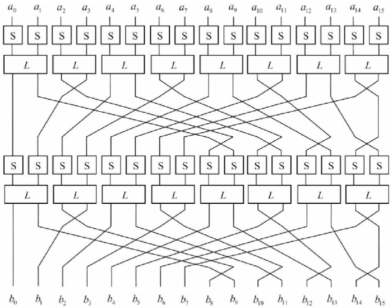
$$\deg(S_{512}) \leq 512 - \frac{512 - 196}{7} \leq \mathbf{466}$$

After $\mathbf{4}$ rounds:

$$\deg(R^4) \leq 2048 - \frac{2048 - 466}{466} \leq \mathbf{2045}$$

The degree of JH

JH [Wu 08]
42 rounds of a 1024-bit permutation R

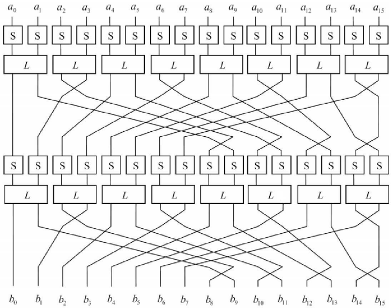


S: Permutation over $\mathbf{F}_2^4$ of degree $\mathbf{3}$.

The degree of JH

JH [Wu 08]

42 rounds of a 1024-bit permutation R



S: Permutation over $\mathbf{F}_2^4$ of degree $\mathbf{3}$. Then,

$$\deg(R^6) \leq 3^6 = \mathbf{729}.$$

The degree of JH

For $r \leq 8$, $\boldsymbol{R^r}$ can be seen as the concatenation of 2^{9-r} permutations $\boldsymbol{S^r}$ over $\mathbf{F}_2^{2^{r+1}}$.

$\boldsymbol{r}$	$\mathbf{deg}(\boldsymbol{S^r})$
1	**3**
2	**6**
3	**12**
4	**25**
5	**51**
6	**102**
7	**204**
8	**409**

Then, $\gamma(S^8) \leq \mathbf{409}$, implying

$$\deg(\boldsymbol{R^{16}}) \leq 1024 - \frac{1024 - \deg(S^8)}{\gamma(S^8)} \leq \mathbf{1022}.$$

Conclusion

- The degree of F^{-1} affects the degree of $G \circ F$.
- **New bounds** on the degree of several iterated cryptographic primitives (ECHO, JH, Rijndael...)

Conclusion

- The degree of F^{-1} affects the degree of $G \circ F$.
- **New bounds** on the degree of several iterated cryptographic primitives (ECHO, JH, Rijndael...)

Thank you for your attention