Bounds on the algebraic degree of iterated constructions

Christina Boura

DTU Compute

June 10, 2013

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

Example (**ANF** of a permutation F of $\mathbf{F}_2^4$)

$$(y_0, y_1, y_2, y_3) = F(x_0, x_1, x_2, x_3)$$

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

The algebraic degree of F is 3.

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:

- Algebraic attacks
- Higher-order differential attacks and distinguishers
- Cube attacks

Higher-order derivatives

Let $F : \mathbf{F}_2^n \to \mathbf{F}_2^m$.
Derivative of F at $a \in \mathbf{F}_2^n$: $D_a(x) = F(x) \oplus F(x+a)$.

Definition. For any k-dimensional subspace V of $\mathbf{F}_2^n$, the k-th order derivative of F with respect to V is the function defined by

$$D_V F(x) = D_{a_1} \dots D_{a_k}(x) = \bigoplus_{v \in V} F(x+v), \quad \text{for every} \quad x \in \mathbf{F}_2^n.$$

where $(a_1, \dots, a_k)$ is a basis of V.

Example: ($k = 2$, $V = \langle a, b \rangle$)

$$\begin{aligned} D_V(x) &= D_a D_b(x) = D_a(F(x) \oplus F(x+b)) \\ &= F(x) \oplus F(x+a) \oplus F(x+b) \oplus F(x+a+b) \end{aligned}$$

Higher-order differential cryptanalysis

Introduced by Knudsen in 1994. Based on the following properties:

Let $F : \mathbf{F}_2^n \to \mathbf{F}_2^m$ of degree d.

Proposition. For every $a \in \mathbf{F}_2^n$ we have

$$D_a F \leq d - 1.$$

Proposition. [Lai 94] For every $V \subset \mathbf{F}_2^n$, with $\dim V > d$

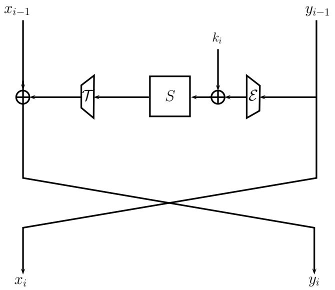
$$D_V(x) = 0, \text{ for every } x \in \mathbf{F}_2^n.$$

The $\mathcal{KN}$ cipher [Knudsen – Nyberg 95]

6-round Feistel cipher

- $\mathcal{E} : \mathbf{F}_2^{32} \to \mathbf{F}_2^{33}$ linear
- $\mathcal{T} : \mathbf{F}_2^{33} \to \mathbf{F}_2^{32}$ linear
- k_i: 33-bit subkey
- $S : x \mapsto x^3$ over $\mathbf{F}_2^{33}$

Algebraic degree of S: 2



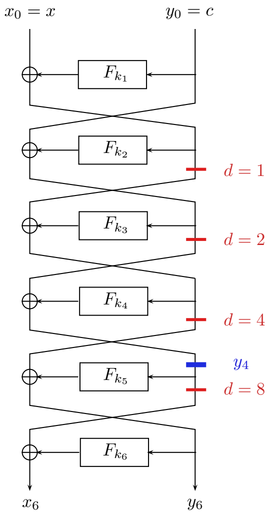
Higher-order differential attack on $\mathcal{KN}$

[Jakobsen – Knudsen 97]

$$
\begin{aligned}
y_0(x) &= c \\
y_1(x) &= x + F_{k_1}(c) := x + c' \\
y_2(x) &= F_{k_2}(x + c') + c \\
y_3(x) &= F_{k_3}(F_{k_2}(x + c') + c) + x + c' \\
y_4(x) &= F_{k_4}(F_{k_3}(F_{k_2}(x + c') + c) + x + c') \\
&+ F_{k_2}(x + c') + c
\end{aligned}
$$

$$G = F_{k_4} \circ F_{k_3} \circ F_{k_2}.$$

$$\boxed{\deg(G) \leq 2^3}$$



If $V \subset \mathbf{F}_2^{32}$ with $\dim(V) = 9$, then:

$$D_V y_4(x) = 0, \text{ for all } x \in \mathbf{F}_2^{32}.$$

By definition:

$$\bigoplus_{v \in V} y_4(v + w) = 0, \text{ for all } w \in \mathbf{F}_2^{32}. \tag{1}$$

We can see that:

$$x_6(x) = F_{k_6}(y_6(x)) + y_4(x),$$

and by inverting the terms:

$$y_4(x) = x_6(x) + F_{k_6}(y_6(x)). \tag{2}$$

Key recovery

By combining equations (1) and (2), we obtain the attack equation:

$$\bigoplus_{v \in V} F_{k_6}(y_6(v+w)) + \bigoplus_{v \in V} x_6(v+w) = 0.$$

The right subkey k_6 is the one for which the equation is verified.

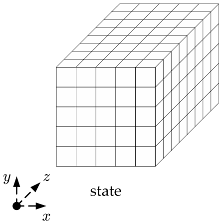
Complexity of the attack:

- Data Complexity: 2^9 plaintexts.
- Time Complexity: 2^{33+8}.

Distinguisher for 4 and 5 rounds with data complexity 2^5 and 2^9 respectively.

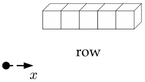
SHA-3 [Bertoni – Daemen – Peeters – VanAssche 08]

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
- $\deg \chi = 2$, $\deg \chi^{-1} = 3$



Outline

Outline

A trivial bound

Proposition: Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ and G a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. Then

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

Example: Round function R of AES is of degree 7. Then

$$\deg(R^2) = \deg(R \circ R) \leq 7^2 = 49.$$

A bound based on the Walsh spectrum

[Canteaut – Videau '02]

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

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

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

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

Application to SHA-3

It can be computed that:

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

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

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

Bound for the degree of R^{-7}

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

Application to SHA-3

It can be computed that:

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

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

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

Bound for the degree of R^{-7}

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

$$\deg(R^7) \leq \min(1599, 2187)$$

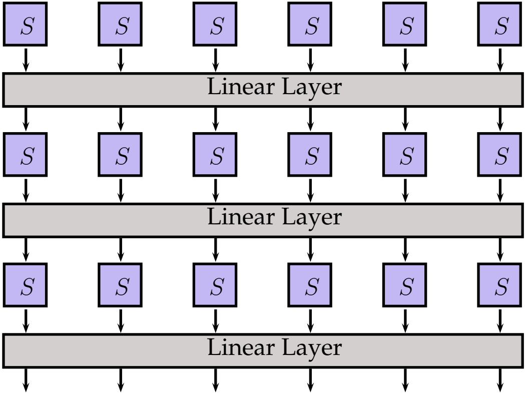
Outline

Some first bounds on the degree

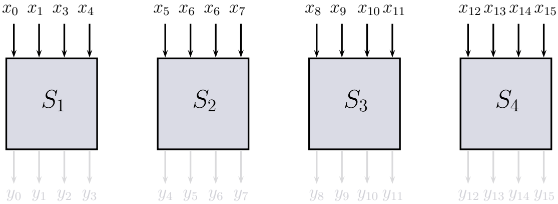
A bound on the degree of SPN constructions

Influence of the inverse permutation

Substitution Permutation Networks

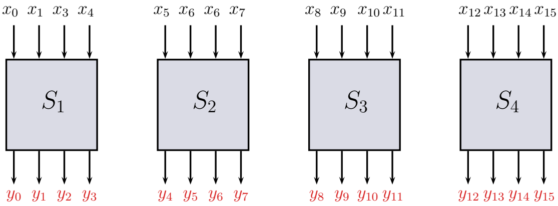


How to estimate the evolution of the degree of such constructions?



After several rounds, all coordinates can be expressed as a sum of monomials.

Each monomial is a **product** of variables in $X = \{x_0, \ldots, x_{15}\}$.



After several rounds, all coordinates can be expressed as a sum of monomials.

Each monomial is a **product** of variables in $Y = \{y_0, \ldots, y_{15}\}$.

The coordinates $y_0 - y_3$ are outputs of the same Sbox (equally for the others).

What is the consequence on the degree of the product ?

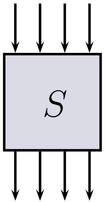
The notion of δ_k

Definition : For a permutation S define $\delta_k(\mathsf{S})$ as the maximum degree of the product of k coordinates of S.

$\rightarrow \delta_1(S) :=$ algebraic degree of S

Example:

$\deg S = 3$



k	δ_k
1	3

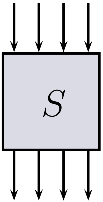
The notion of δ_k

Definition : For a permutation S define δ_k(S) as the maximum degree of the product of k coordinates of S.

$\rightarrow \delta_1(S) :=$ algebraic degree of S

Example:

$\deg S = 3$



k	δ_k
1	3
2	3
3	3

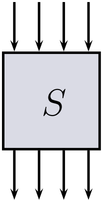
The notion of δ_k

Definition : For a permutation S define $\delta_k(S)$ as the maximum degree of the product of k coordinates of S.

$\rightarrow \delta_1(S) :=$ algebraic degree of S

Example:

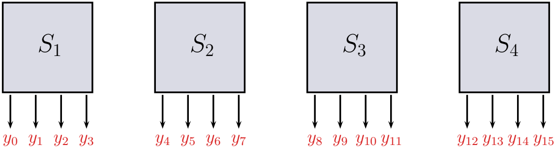
$\deg S = 3$



k	δ_k
1	3
2	3
3	3
4	4

S permutation of $\mathbf{F}_2^n$:
$\delta_k(S) = n$ iff $k = n$.

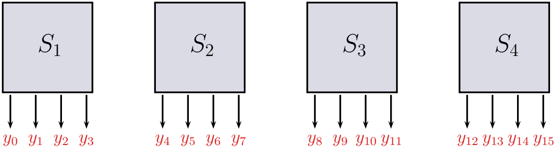
Example: Product of 6 coordinates.



$\pi = y_0 y_1 y_3 y_8 y_9 y_{10}$.

$$\deg(\pi) \leq \delta_3(S_1) + \delta_3(S_3) = 6.$$

Example: Product of 6 coordinates.

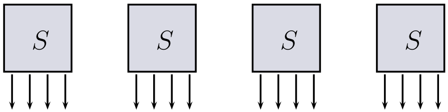


$\pi = y_0 y_5 y_8 y_{10} y_{13} y_{15}$.

$$\deg(\pi) \leq \delta_1(S_1) + \delta_1(S_2) + \delta_2(S_3) + \delta_2(S_4) = 12.$$

The degree of the product is relatively low if many coordinates coming from the same Sbox are involved!!!

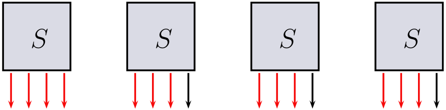
Towards the bound



Find the maximal degree of the product π of d outputs.

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

Towards the bound



Find the maximal degree of the product π of d outputs.

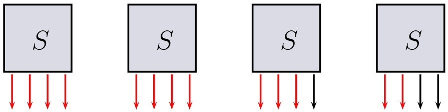
$x_i = \#$ Sboxes for which exactly i coordinates are involved in π.

Example ($d = 13$)

- $x_4 = 1$, $x_3 = 3$:

$$\deg(\pi) \leq \delta_3 x_3 + \delta_4 x_4 = 3 \cdot 3 + 4 \cdot 1 = 13.$$

Towards the bound



Find the maximal degree of the product π of d outputs.

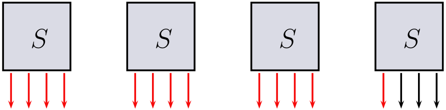
$x_i = \#$ Sboxes for which exactly i coordinates are involved in π.

Example ($d = 13$)

- $x_4 = 2$, $x_3 = 1$, $x_2 = 1$:

$$\deg(\pi) \leq \delta_2 x_2 + \delta_3 x_3 + \delta_4 x_4 = 3 \cdot 1 + 3 \cdot 1 + 4 \cdot 2 = 14.$$

Towards the bound



Find the maximal degree of the product π of d outputs.

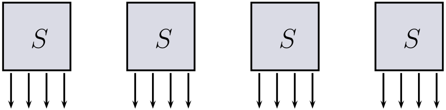
$x_i = \#$ Sboxes for which exactly i coordinates are involved in π.

Example ($d = 13$)

- $x_4 = 3$, $x_1 = 1$:

$$\deg(\pi) \leq \delta_1 x_1 + \delta_4 x_4 = 3 \cdot 1 + 4 \cdot 3 = 15.$$

Towards the bound



Find the maximal degree of the product π of d outputs.

$x_i = \#$ 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	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
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

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

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
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

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

A bound on the degree of SPN constructions

[Boura – Canteaut – De Cannière - FSE 2011]

Theorem. Let F be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$ corresponding to the parallel application of an Sbox, S, defined over $\mathbf{F}_2^{n_0}$.
Then, for any G from $\mathbf{F}_2^n$ into $\mathbf{F}_2^\ell$, we have

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

where

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

Application to SHA-3

Non-linear layer: Parallel application of a 5×5 Sbox χ, with $\deg(\chi) = 2$.

$$\gamma(\chi) = \max_{1 \le k \le 4} \frac{5-k}{5-\delta_k(\chi)}$$

k	1	2	3	4	5
δ_k	2	4	4	4	5

$$\gamma(\chi) = \max\left(\frac{4}{3}, \frac{3}{1}, \frac{2}{1}, \frac{1}{1}\right) = 3$$

We deduce

$$\boxed{\deg(G \circ F) \le 1600 - \frac{1600 - \deg(G)}{3}}$$

R: Round function of Keccak-f

For $r = 11, \ldots, 16$:

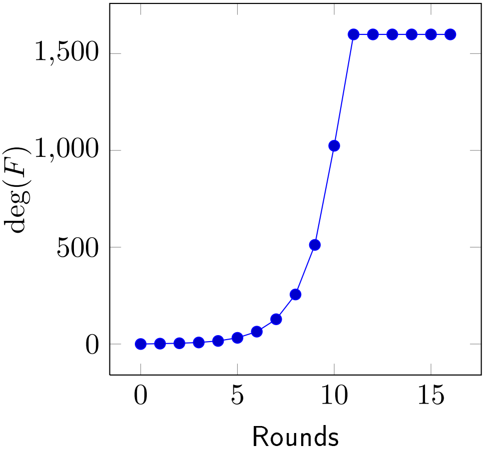
$$\deg(R^r) \leq 1600 - \frac{1600 - \deg(R^{r-1})}{3}$$

Example : $r = 11$

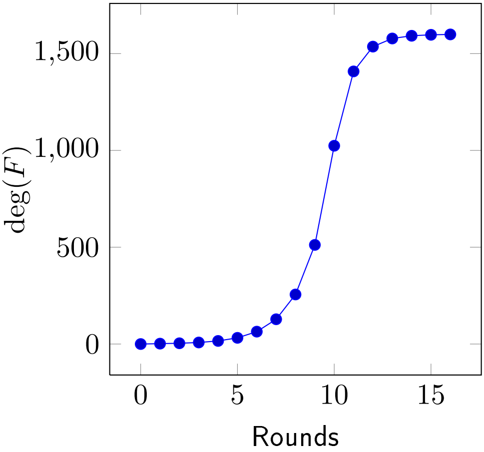
$$\begin{aligned} \deg(R^{11}) &\leq 1600 - \frac{1600 - \deg(R^{10})}{3} \\ &= 1600 - \frac{1600 - 1024}{3} \\ &= 1408. \end{aligned}$$

r	$\deg(R^r)$
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256
9	512
10	1024
11	**1408**
12	**1536**
13	**1578**
14	**1592**
15	**1597**
16	**1599**

SPN Bound vs. Trivial Bound



SPN Bound vs. Trivial Bound

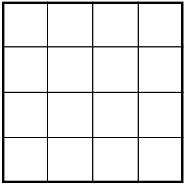


Application to AES

One round:

$$\mathtt{MC} \circ \mathtt{SR} \circ \mathtt{SB} \circ \mathtt{AK}.$$

- AK: AddRoundKey
- SB: SubBytes (Sboxes of degree 7)
- SR: ShiftRows
- MC: MixColumns



The Super Sbox technique

Two rounds:

$$R^2 = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AK} \circ \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AK}.$$

Equivalently:

$$R^2 = \texttt{MC} \circ \texttt{SR} \circ \texttt{SB} \circ \texttt{AK} \circ \texttt{MC} \circ \texttt{SB} \circ \texttt{SR} \circ \texttt{AK}.$$

Denote:

$$\texttt{SuperSbox} = \texttt{SB} \circ \texttt{AK} \circ \texttt{MC} \circ \texttt{SB}.$$

Then:

$$R^2 = \texttt{MC} \circ \texttt{SR} \circ \texttt{SuperSbox} \circ \texttt{SR} \circ \texttt{AK}.$$

Bound on up to 4 rounds

SuperSbox: $\mathbf{F}_2^{32} \to \mathbf{F}_2^{32}$: Two non-linear layers composed of Sboxes of degree 7, separated by a linear layer.

$$\deg(\texttt{SuperSbox}) \leq 32 - \frac{32-7}{7} \leq 28.$$

(Trivial Bound: $\deg(R^2) \leq 7^2 = 49$!!!)

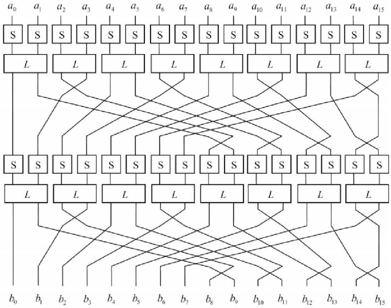
Bound for r rounds:

$$\deg(R^r) = \deg(R^{r-1} \circ R) \leq 128 - \frac{128 - \deg(R^{r-1})}{7}.$$

- $r = 3$: $\deg(R^3) \leq 113$
- $r = 4$: $\deg(R^4) \leq 125$

Exercice (JH hash function [Wu 08])

42 rounds of a 1024-bit permutation R
S: Permutation over $\mathbf{F}_2^4$ of degree 3.



What is the degree after 2 rounds?

Outline

Some first bounds on the degree

A bound on the degree of SPN constructions

Influence of the inverse permutation

An observation on SHA-3

$$\begin{aligned}\chi^{-1}(x_0,\ldots,x_4) = & (x_0+x_2+x_4+x_1x_2+x_1x_4+x_3x_4+x_1x_3x_4,\\ & x_0+x_1+x_3+x_0x_2+x_0x_4+x_2x_3+x_0x_2x_4,\\ & x_1+x_2+x_4+x_0x_1+x_1x_3+x_3x_4+x_0x_1x_3,\\ & x_0+x_2+x_3+x_0x_4+x_1x_2+x_2x_4+x_1x_2x_4,\\ & x_1+x_3+x_4+x_0x_1+x_0x_3+x_2x_3+x_0x_2x_3).\end{aligned}$$

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

An interesting property

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

An interesting property

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

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

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

Proof: We show that if

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

Let $\pi(x) = \prod_{i \in K} F_i(x)$, with $|K| = k$. The coefficient a of $\prod_{j \notin L} x_j$ in the ANF of π for $|L| = \ell$,

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

since, $\deg \prod_{j \in L} (1 + F_j^{-1}(y)) < n - k$.

Application to SHA-3

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

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

Case of SHA-3: For $F = \chi^{-1}$ and $\ell = 2$,

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

A new bound on the degree

[Boura – Canteaut IEEE-IT 13]

Corollary: 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

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

Consequence on the bound on SPN constructions

Recall the bound:

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

where

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

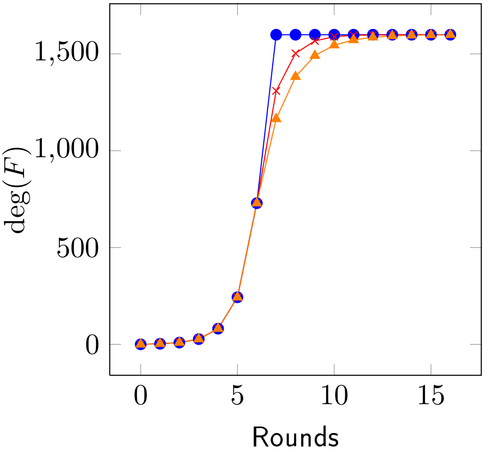
We can show that

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

For the inverse of Keccak-f:

$$\gamma(\chi^{-1}) \leq 2$$

Bound on the degree of the inverse of Keccak-f



Application to $\mathcal{KN}$

Higher-order differential attack due to the low degree of the round permutation.

How to "repair" the cipher?

[Nyberg 93]:

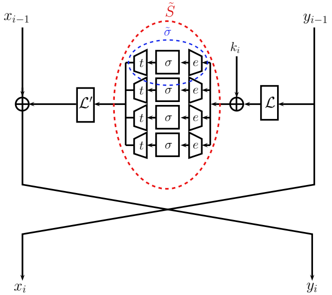
Replace S by the **inverse** of a quadratic permutation.

- The quadratic permutation and its inverse **will have the same properties** regarding differential and linear attacks.
- The quadratic permutation **is not involved** neither in the encryption, nor in the decryption.

The $\mathcal{KN}'$ cipher

$$\begin{array}{rccc} \widetilde{\sigma}: & \mathbf{F}_2^8 & \to & \mathbf{F}_2^8 \\ & x & \mapsto & t \circ \sigma\left(e(x)\right)) \end{array}$$

$e : \mathbf{F}_2^8 \to \mathbf{F}_2^9$ affine expansion
$t : \mathbf{F}_2^9 \to \mathbf{F}_2^8$ truncation
$x : \sigma(x) = x^{171}$ (the **inverse** of x^3 over $\mathbf{F}_{2^9}$)
$\mathbf{deg}(\widetilde{S}) = \mathbf{5}$



$$\begin{array}{ccc} \mathbf{F}_2^{32} \times \mathbf{F}_2^{32} & \to & \mathbf{F}_2^{32} \times \mathbf{F}_2^{32} \\ (x, y) & \mapsto & (y, x + \mathcal{L}' \circ \widetilde{S}\left(\mathcal{L}(x) + k_i\right)) \end{array}$$

Attacking $\mathcal{KN}'$

Jakobsen-Knudsen attack:

$$\deg(y_4) \leq 5 \times 5 \times 5$$

Attacking $\mathcal{KN}'$

Jakobsen-Knudsen attack:

$$\boxed{\deg(y_4) \leq 5 \times 5 \times 5}$$

unfeasible

Attacking $\mathcal{KN}'$

Jakobsen-Knudsen attack:

$$\boxed{\deg(y_4) \leq 5 \times 5 \times 5}$$

unfeasible

Set,

$$F_k(x) = \mathcal{L}' \circ \widetilde{S}\left(\mathcal{L}(x) + k\right) \ .$$

Then,

$$\begin{aligned}
y_0 &= c \\
y_1 &= \boldsymbol{x} + F_{k_1}(y_0) := \boldsymbol{x} + c' \\
y_2 &= F_{k_2}\left(\boldsymbol{x} + c'\right) + c \\
y_3 &= F_{k_3}\left(F_{k_2}\left(\boldsymbol{x} + c'\right) + c'\right) + \boldsymbol{x} + c'
\end{aligned}$$

$$\boxed{y_4 = y_2 + F_{k_4}(y_3)}$$

Application of the new bound

$$y_4 + y_2 = G \circ S(x)$$

Using the bound with the inverse :

$$\deg(G \circ S) < 36 - \left\lfloor \frac{35 - \deg(G)}{2} \right\rfloor ,$$

From a previous Corollary: $(\deg(G) \leq 22)$, thus

$$\deg(y_4) \leq \deg(G \circ S) \leq 29$$

Application of the new bound

$$y_4 + y_2 = G \circ S(x)$$

Using the bound with the inverse :

$$\deg(G \circ S) < 36 - \left\lfloor \frac{35 - \deg(G)}{2} \right\rfloor ,$$

From a previous Corollary: $(\deg(G) \leq 22)$, thus

$$\deg(y_4) \leq \deg(G \circ S) \leq 29$$

Distinguisher on 5 rounds of $\mathcal{KN}'$ with data complexity 2^{30} that improves the generic distinguisher.

Generalization to balanced functions (not permutations)

DES: Eight different 6×4 Sboxes.

Can the bound be generalized to balanced functions from $\mathbf{F}_2^n$ to $\mathbf{F}_2^m$, with $m < n$?

Generalization to balanced functions (not permutations)

DES: Eight different 6×4 Sboxes.

Can the bound be generalized to balanced functions from $\mathbf{F}_2^n$ to $\mathbf{F}_2^m$, with $m < n$?

Corollary: Let F be a balanced function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$ and G be a function from $\mathbf{F}_2^m$ into $\mathbf{F}_2^k$. For any permutation F^* *expanding* F, we have

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