New bounds on the algebraic degree of iterated permutations

Christina Boura
(joint work with Anne Canteaut and Christophe De Cannière)

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

January 27, 2012
1. Motivation

2. A first bound on the degree

3. Connecting the degree with the inverse permutation

4. Application on the $\mathcal{KN}$ block cipher
Outline

1. Motivation
2. A first bound on the degree
3. Connecting the degree with the inverse permutation
4. Application on the $\mathcal{KN}$ block cipher
The SHA-3 competition for hash functions

- In 2004, Wang et al. provided collision attacks for most of the standardized hash functions (MD4, MD5, SHA-0, SHA-1 etc.).
The SHA-3 competition for hash functions

- In 2004, Wang et al. provided collision attacks for most of the standardized hash functions (MD4, MD5, SHA-0, SHA-1 etc.)

- Little confidence on the security of SHA-2.
The SHA-3 competition for hash functions

- In 2004, Wang et al. provided collision attacks for most of the standardized hash functions (MD4, MD5, SHA-0, SHA-1 etc..)

- Little confidence on the security of SHA-2.

- In 2007 NIST launched the SHA-3 public competition for defining a new hash function standard.
SHA-3 timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2008</td>
<td>64 candidates received</td>
</tr>
<tr>
<td>December 2008</td>
<td>51 candidates accepted for the 1st round</td>
</tr>
<tr>
<td>July 2009</td>
<td>14 candidates accepted for the 2nd round</td>
</tr>
<tr>
<td>December 2010</td>
<td>5 finalists selected</td>
</tr>
<tr>
<td>2012</td>
<td>Winner must be announced</td>
</tr>
</tbody>
</table>

Important to evaluate the security of the left candidates under:

- Attacks (preimages, second-preimages, collisions)
- Distinguishers
SHA-3 timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2008</td>
<td>64 candidates received</td>
</tr>
<tr>
<td>December 2008</td>
<td>51 candidates accepted for the 1st round</td>
</tr>
<tr>
<td>July 2009</td>
<td>14 candidates accepted for the 2nd round</td>
</tr>
<tr>
<td>December 2010</td>
<td>5 finalists selected</td>
</tr>
<tr>
<td>2012</td>
<td>Winner must be announced</td>
</tr>
</tbody>
</table>

Important to evaluate the security of the left candidates under:

- **Attacks** (preimages, second-preimages, collisions)
- **Distinguishers**

Distinguishers can invalidate security proofs and can be the starting point for attacks.
Algebraic degree of a vectorial function \( F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m \)

**Example:**

\[
F(x_0, x_1, x_2, x_3, x_4) = (x_0 + x_2 + x_4 + x_1x_2 + x_1x_4 + x_3x_4 + x_1x_3x_4,
\]
\[
x_0 + x_1 + x_3 + x_0x_2 + x_0x_4 + x_2x_3 + x_0x_2x_4,
\]
\[
x_1 + x_2 + x_4 + x_0x_1 + x_1x_3 + x_3x_4 + x_0x_1x_3,
\]
\[
x_0 + x_2 + x_3 + x_0x_4 + x_1x_2 + x_2x_4 + x_1x_2x_4,
\]
\[
x_1 + x_3 + x_4 + x_0x_1 + x_0x_3 + x_2x_3 + x_0x_2x_3).
\]
Algebraic degree of a vectorial function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$

Example:

$$F(x_0, x_1, x_2, x_3, x_4) = (x_0 + x_2 + x_4 + x_1x_2 + x_1x_4 + x_3x_4 + x_1x_3x_4, x_0 + x_1 + x_3 + x_0x_2 + x_0x_4 + x_2x_3 + x_0x_2x_4, x_1 + x_2 + x_4 + x_0x_1 + x_1x_3 + x_3x_4 + x_0x_1x_3, x_0 + x_2 + x_3 + x_0x_4 + x_1x_2 + x_2x_4 + x_1x_2x_4, x_1 + x_3 + x_4 + x_0x_1 + x_0x_3 + x_2x_3 + x_0x_2x_3).$$

The algebraic degree of $F$ is 3.
Higher order differential cryptanalysis [Knudsen 94]

Generalization of “classical” differential cryptanalysis.
Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$.

**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

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

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

$$D_V F(x) = \bigoplus_{v \in V} F(x + v) = 0, \quad \text{for every} \quad x \in \mathbb{F}_2^n.$$
Higher order differential cryptanalysis [Knudsen 94]

Some alternatives:
- Cube attacks [Dinur-Shamir08]
- Algebraic attacks [Courtois-Meier 02][Courtois-Meier 03]
- Zero-sum distinguishers [Aumasson-Meier09][Boura-Canteaut10]

Vulnerable to these attacks: Functions possessing a low algebraic degree.
Higher order differential cryptanalysis [Knudsen 94]

Some alternatives:

- Cube attacks [Dinur-Shamir08]
- Algebraic attacks [Courtois-Meier 02][Courtois-Meier 03]
- Zero-sum distinguishers [Aumasson-Meier09][Boura-Canteaut10]

Vulnerable to these attacks: Functions possessing a low algebraic degree.

Our work: Evaluating the security of some SHA-3 candidates under these types of attacks.
Iterative structure of symmetric constructions

Most **symmetric constructions** (*i.e.* block ciphers, hash functions) are based on an inner function, called the **round function**, that is iterated many times.

Most of these inner functions, are **permutations**.

**Examples:**
- **AES-128**: (10 rounds of \( F : \mathbb{F}_2^{128} \rightarrow \mathbb{F}_2^{128} \))
- **DES**: (16 rounds of \( F : \mathbb{F}_2^{64} \rightarrow \mathbb{F}_2^{64} \))
- **Keccak** hash function: (24 rounds of \( F : \mathbb{F}_2^{1600} \rightarrow \mathbb{F}_2^{1600} \))

What is the **algebraic degree** of such iterated constructions **after a certain number of rounds**?
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

\[
\deg(G \circ F) \leq \deg G \deg F
\]

Theorem [Canteaut-Videau 02] Let \( F \) be a function from \( \mathbb{F}_2^n \) into \( \mathbb{F}_2^n \) such that all values \( \text{wt}(\varphi_b \circ F + \varphi_a), a, b \in \mathbb{F}_2^n, \quad b = 0 \) are divisible by \( 2^\ell \), for some integer \( \ell \). Then, for any \( G : \mathbb{F}_2^n \to \mathbb{F}_2^n \), we have

\[
\deg(G \circ F) \leq n - 1 - \ell + \deg(G).
\]
Outline

1. Motivation

2. A first bound on the degree

3. Connecting the degree with the inverse permutation

4. Application on the $\mathcal{KN}$ block cipher
Case of SP Networks

- **Non-linear layer**: Parallel application of small-sized Sboxes
- **Linear layer**: Linear permutation
Case of SP Networks

- **Non-linear layer**: Parallel application of small-sized Sboxes
- **Linear layer**: Linear permutation

How can we **bound the degree** of such constructions?
Question

If $S$ is a permutation, what is the degree of the product of $k$ coordinates of $S$?

$\text{deg } S = 3$

$x_0 \ x_1 \ x_2 \ x_3$

$y_0 \ y_1 \ y_2 \ y_3$
\[ \text{deg } S = 3 \]

**Question**

If \( S \) is a permutation, what is the degree of the product of \( k \) coordinates of \( S \)?

**Definition**

\( \delta_k \) : maximum degree of the product of \( k \) coordinates of \( S \)
A first bound on the degree

**Question**

If $S$ is a permutation, what is the degree of the product of $k$ coordinates of $S$?

**Definition**

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

\[
\begin{array}{c|c}
 k & \delta_k \\
 1 & 3 \\
\end{array}
\]

deg $S = 3$

$x_0 \ x_1 \ x_2 \ x_3$

$\downarrow \ \downarrow \ \downarrow \ \downarrow$

S-Box

$y_0 \ y_1 \ y_2 \ y_3$
\[ \text{deg } S = 3 \]

**Question**

If \( S \) is a permutation, what is the degree of the product of \( k \) coordinates of \( S \)?

**Definition**

\[ \delta_k : \text{maximum degree of the product of } k \text{ coordinates of } S \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>( \delta_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
**A first bound on the degree**

**Question**

If $S$ is a permutation, what is the degree of the product of $k$ coordinates of $S$?

**Definition**

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

$$
\begin{array}{c|c}
  k & \delta_k \\
  \hline
  1 & 3 \\
  2 & 3 \\
  3 & 3 \\
  4 & 4 \\
\end{array}
$$

$F$ permutation of $\mathbb{F}_2^n$:

$\delta_k = n$ iff $k = n$. 

$\deg S = 3$

$x_0 \ x_1 \ x_2 \ x_3$

$S$-Box

$y_0 \ y_1 \ y_2 \ y_3$
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

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

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

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

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

Problem

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

Definition

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

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

Definition

\[ x_i = \# \text{ Sboxes for which exactly } i \text{ coordinates are involved in } \pi. \]

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

with \( x_1 + 2x_2 + 3x_3 + 4x_4 = d. \)
A first bound on the degree

deg(\pi) = \delta_4 \cdot x_4 = 4 \cdot 4 = 16

<table>
<thead>
<tr>
<th>$d$</th>
<th>$x_4$</th>
<th>$x_3$</th>
<th>$x_2$</th>
<th>$x_1$</th>
<th>deg(\pi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
deg(\pi) = \delta_3 \cdot x_3 + \delta_4 \cdot x_4 = 3 \cdot 1 + 4 \cdot 3 = 15
A first bound on the degree

\[
\begin{array}{|c|c|c|c|c|c|}
\hline
 d & x_4 & x_3 & x_2 & x_1 & \text{deg}(\pi) \\
\hline
16 & 4 & - & - & - & 16 \\
15 & 3 & 1 & - & - & 15 \\
14 & 3 & - & 1 & - & 15 \\
13 & & & & & \\
12 & & & & & \\
11 & & & & & \\
10 & & & & & \\
9 & & & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\hline
\end{array}
\]

\[
\text{deg}(\pi) = \delta_2 \cdot x_2 + \delta_4 \cdot x_4 = 3 \cdot 1 + 4 \cdot 3 = 15
\]
A first bound on the degree

<table>
<thead>
<tr>
<th>$d$</th>
<th>$x_4$</th>
<th>$x_3$</th>
<th>$x_2$</th>
<th>$x_1$</th>
<th>deg($\pi$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>14</td>
<td>3</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$S_1$ $S_2$ $S_3$ $S_4$
A first bound on the degree

\[ 16 - \deg(\pi) \geq \frac{16 - d}{3} \]
A first bound on the degree

\[ \text{deg}(\pi) \leq 16 - \frac{16 - d}{3} \]

<table>
<thead>
<tr>
<th>(d)</th>
<th>(x_4)</th>
<th>(x_3)</th>
<th>(x_2)</th>
<th>(x_1)</th>
<th>(\text{deg}(\pi))</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>14</td>
<td>3</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>
Trivial bound vs. New bound
A first bound on the degree

Trivial bound vs. New bound
An application: The Keccak case

Keccak [Bertoni-Daemen-Peeters-VanAssche 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 \( 5 \times 5 \) S-box \( \chi \)
- \( \deg \chi = 2, \deg \chi^{-1} = 3 \)
The new bound applied on Keccak-\(f\)

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

\[
\deg(F \circ R) \leq 1600 - \frac{1600 - \deg(F)}{3}
\]

\[
\deg(F \circ R^{-1}) \leq 1600 - \frac{1600 - \deg(F)}{3}
\]
The new bound applied on Keccak-\textit{f}

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

\[
\begin{align*}
\deg(F \circ R) &\leq 1600 - \frac{1600 - \deg(F)}{3} \\
\deg(F \circ R^{-1}) &\leq 1600 - \frac{1600 - \deg(F)}{3}
\end{align*}
\]

\textbf{Example:}

\[
\deg(R^{11}) = \deg(R^{10} \circ R) \leq 1600 - \frac{1600 - \deg(R^{10})}{3} \leq 1408
\]
<table>
<thead>
<tr>
<th>$r$</th>
<th>$\text{deg}(R^r)$</th>
<th>$\text{deg}(R^{-r})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>81</td>
</tr>
<tr>
<td>5</td>
<td>32</td>
<td>243</td>
</tr>
<tr>
<td>6</td>
<td>64</td>
<td>729</td>
</tr>
<tr>
<td>7</td>
<td>128</td>
<td>1164</td>
</tr>
<tr>
<td>8</td>
<td>256</td>
<td>1382</td>
</tr>
<tr>
<td>9</td>
<td>512</td>
<td>1491</td>
</tr>
<tr>
<td>10</td>
<td>1024</td>
<td>1545</td>
</tr>
<tr>
<td>11</td>
<td>1408</td>
<td>1572</td>
</tr>
<tr>
<td>12</td>
<td>1536</td>
<td>1586</td>
</tr>
<tr>
<td>13</td>
<td>1578</td>
<td>1593</td>
</tr>
<tr>
<td>14</td>
<td>1592</td>
<td>1596</td>
</tr>
<tr>
<td>15</td>
<td>1597</td>
<td>1598</td>
</tr>
<tr>
<td>16</td>
<td>1599</td>
<td>1599</td>
</tr>
</tbody>
</table>
Zero-Sums

- 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

\[
\bigoplus_{i=1}^{K} x_i = \bigoplus_{i=1}^{K} F(x_i) = 0.
\]
Zero-sums for full Keccak-$f$

\[ X_a = \left\{ (R^{-1})^{11}(a + z), \ z \in V \right\}, \ a \in W \]

is a zero-sum of size $2^{1575}$ for 24 rounds of Keccak-$f$. 
Zero-sums for full Keccak-$f$

\[ X_a = \{(R^{-1})^{11}(a + z), \ z \in V\}, \ a \in W \]

is a zero-sum of size $2^{1575}$ for 24 rounds of Keccak-$f$.

Invalidates the hermetic sponge strategy.
Zero-sums permit to gain Belgian beers!

Congratulations to the winners of the third KECCAK cryptanalysis prize

16 February 2010

We are happy to announce that Christina Boura and Anne Canteaut are the winners of the third KECCAK cryptanalysis prize for their paper entitled *A zero-sum property for the KECCAK-f permutation with 18 rounds*. We are currently arranging practical details with the winners to give them the awarded Lambic-based beers and book. Congratulations to them!
Connecting the degree with the inverse permutation

Outline

1. Motivation
2. A first bound on the degree
3. Connecting the degree with the inverse permutation
4. Application on the $\mathcal{KN}$ block cipher
An observation on Keccak

\( \chi(x_0, x_1, x_2, x_3, x_4) = (x_0 + x_2 + x_1 x_2, \\
x_1 + x_3 + x_2 x_3, \\
x_2 + x_4 + x_3 x_4, \\
x_3 + x_0 + x_4 x_0, \\
x_4 + x_1 + x_0 x_1). \)

\( \chi^{-1}(x_0, x_1, x_2, x_3, x_4) = (x_0 + x_2 + x_4 + x_1 x_2 + x_1 x_4 + x_3 x_4 + x_1 x_3 x_4, \\
x_0 + x_1 + x_3 + x_0 x_2 + x_0 x_4 + x_2 x_3 + x_0 x_2 x_4, \\
x_1 + x_2 + x_4 + x_0 x_1 + x_1 x_3 + x_3 x_4 + x_0 x_1 x_3, \\
x_0 + x_2 + x_3 + x_0 x_4 + x_1 x_2 + x_2 x_4 + x_1 x_2 x_4, \\
x_1 + x_3 + x_4 + x_0 x_1 + x_0 x_3 + x_2 x_3 + x_0 x_2 x_3). \)
An observation on Keccak

\[ \chi(x_0, x_1, x_2, x_3, x_4) = (x_0 + x_2 + x_1x_2, \]
\[ x_1 + x_3 + x_2x_3, \]
\[ x_2 + x_4 + x_3x_4, \]
\[ x_3 + x_0 + x_4x_0, \]
\[ x_4 + x_1 + x_0x_1). \]

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

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

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

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

Theorem: Let $F$ be a permutation on $\mathbb{F}_2^m$. Then, for any integers $k$ and $\ell$,

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

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

Let \( \pi(x) = \prod_{i \in K} F_i(x) \), with \( |K| = k \). The coefficient \( a \) of \( \prod_{j \not\in L} x_j \) in the ANF of \( \pi \) for \( |L| = \ell \),

\[
a = \sum_{x \in \mathbb{F}_2^n} \pi(x) \mod 2
\]

\[
= \# \{ x \in \mathbb{F}_2^n : x_j = 0, j \in L \text{ and } F_i(x) = 1, i \in K \} \mod 2
\]

\[
= \# \{ y \in \mathbb{F}_2^n : y_i = 1, i \in K \text{ and } F_j^{-1}(y) = 0, j \in L \} \mod 2
\]

\[
= \# \{ y \in \mathbb{F}_2^n : y_i = 1, i \in K \text{ and } \prod_{j \in L} (1 + F_j^{-1}(y)) = 1, j \in L \} \mod 2
\]

\[
= 0
\]

since, \( \deg \prod_{j \in L} (1 + F_j^{-1}(y)) < n - k \).
Corollary: Let $F$ be a permutation on $\mathbb{F}_2^n$. Then, for any integer $\ell$,

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

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

$$\delta_2(\chi^{-1}) < 5 - 1 \text{ iff } \deg(\chi) < 5 - 2$$
Corollary: Let $F$ be a permutation of $\mathbb{F}_2^n$ and let $G$ be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. Then, we have

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

1. Motivation
2. A first bound on the degree
3. Connecting the degree with the inverse permutation
4. Application on the $\mathcal{KN}$ block cipher
The $\mathcal{KN}$ cipher [Knudsen-Nyberg 95]

6-round Feistel cipher

$L : \mathbb{F}_2^{32} \rightarrow \mathbb{F}_2^{33}$ linear
$L' : \mathbb{F}_2^{33} \rightarrow \mathbb{F}_2^{32}$ linear

$k_i : 33$-bit subkey

$\sigma : x \mapsto x^3$ over $\mathbb{F}_2^{29}$

$S : \mathbb{F}_2^{233} \rightarrow \mathbb{F}_2^{233}$

with $x \mapsto x^3$

\[ \mathbb{F}_2^{32} \times \mathbb{F}_2^{32} \rightarrow \mathbb{F}_2^{32} \times \mathbb{F}_2^{32} \]

\[ (x, y) \mapsto (y, x + L' \circ S (L(x) + k_i)) \]
Higher-order differential attack on $\mathcal{KN}$ cipher

[Jakobsen-Knudsen 97]

If $y_0$ is constant, then

$$\deg x_r \leq (\deg S)^{r-2}$$

**Distinguishing property for $r$ rounds.**

For any $y_0 \in \mathbb{F}_2^{32}$, for any affine subspace $V \subset \mathbb{F}_2^{32}$ of dimension $2^{r-2} + 1$,

$$\bigoplus_{x \in V} [E_k^{(r)}(x, y_0)] = 0.$$ 

For 6-round $\mathcal{KN}$

- **Distinguisher** on 4 rounds with data complexity $2^5$, using that $\deg x_4 < 5$.
- **Distinguisher** on 5 rounds with data complexity $2^9$, using that $\deg x_5 < 9$.
- **Attack** on 6-round $\mathcal{KN}$ with data complexity $2^5$ and time complexity $2^{70}$. 

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

$$
\tilde{\sigma} : \mathbb{F}_2^8 \rightarrow \mathbb{F}_2^8 \\
x \mapsto t \circ \sigma (e(x))
$$

$$
e : \mathbb{F}_2^8 \rightarrow \mathbb{F}_2^9 \text{ affine expansion} \\
t : \mathbb{F}_2^9 \rightarrow \mathbb{F}_2^8 \text{ truncation} \\
x : \sigma(x) = x^{171} \text{ (the inverse of } x^3 \text{ over } \mathbb{F}_{2^9} \text{)} \\
\text{deg}(\tilde{S}) = 5
$$

$$
\mathbb{F}_2^{32} \times \mathbb{F}_2^{32} \rightarrow \mathbb{F}_2^{32} \times \mathbb{F}_2^{32} \\
(x, y) \mapsto (y, x + \mathcal{L}' \circ \tilde{S} (\mathcal{L}(x) + k_i))
$$
Attacking $\mathcal{KN}'$

**Jakobsen-Knudsen attack:**

\[ \deg(x_5) \leq 5 \times 5 \times 5 \]
Attacking $\mathcal{KN}'$

Jakobsen-Knudsen attack:

$$\deg(x_5) \leq 5 \times 5 \times 5$$

infeasible
Attacking $\mathcal{KN}'$

Jakobsen-Knudsen attack:

$$\deg(x_5) \leq 5 \times 5 \times 5$$

infeasible

Set,

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

Then,

$$x_2 = x_0 + F_{k_1}(y_0)$$
$$x_3 = y_0 + F_{k_2}(x_0 + F_{k_1}(y_0))$$
$$x_4 = x_0 + F_{k_1}(y_0) + F_{k_3}(y_0 + F_{k_2}(x_0 + F_{k_1}(y_0)))$$

$$x_5 = x_3 + F_{k_4}(x_4)$$
Application of the new bound

\[ x_5 + x_3 = G \circ S(x) \]

Using the new bound:

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

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

\[ \deg(x_5) \leq \deg(G \circ S) \leq 29 \]
Application of the new bound

\[ x_5 + x_3 = G \circ S(x) \]

Using the new bound:

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

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

\[ \deg(x_5) \leq \deg(G \circ S) \leq 29 \]

**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 $6 \times 4$ Sboxes.

Can the new bound be generalized to balanced functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ with $m < n$?
Generalization to balanced functions (not permutations)

**DES:** Eight different $6 \times 4$ Sboxes.

Can the new bound be **generalized** to balanced functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ with $m < n$?

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

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

- **New bound** on the degree of iterated permutations, having as a non-linear layer small balanced Sboxes.
- The degree of $F^{-1}$ affects the degree of $G \circ F$.
- **Generalization** of this result to balanced functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ with $m < n$.
- Application of these results to various hash functions (Keccak, JH, Grøstl, ECHO, Photon, Hamsi, Luffa) and block ciphers (AES, $\mathcal{KN}$).
Conclusion

- **New bound** on the degree of iterated permutations, having as a non-linear layer small balanced Sboxes.
- The degree of $F^{-1}$ affects the degree of $G \circ F$.
- **Generalization** of this result to balanced functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ with $m < n$.
- Application of these results to various hash functions (Keccak, JH, Grøstl, ECHO, Photon, Hamsi, Luffa) and block ciphers (AES, $\mathcal{KN}$).

Merci pour votre attention!