Cryptographic Boolean Functions with Maximum Algebraic Immunity

Konstantinos Limniotis[1,2] and Nicholas Kolokotronis[3]

[1]Dept. of Informatics & Telecommunications, National and Kapodistrian University of Athens, 15784 Athens, Greece
Email: klimn@di.uoa.gr

[2]Hellenic Data Protection Authority, Kifissias 1-3, 11523 Athens, Greece
Email: klimniotis@dpa.gr

[3]Dept. of Informatics & Telecommunications, University of Peloponnese, End of Karaiskaki St., 22100 Tripolis, Greece
E-mail: nkolok@uop.gr

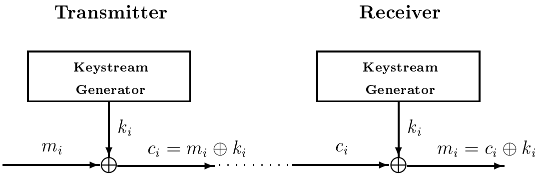
3rd CryCybIW Conference, Hellenic Military Academy,
May 27th, 2016

Talk Outline

1. Introduction
   - Problem Statement
   - Definitions
   - Previous work
2. New constructions of functions with maximum AI
   - Annihilators as codewords of punctured RM codes
   - Secondary constructions
     - Application to the Carlet–Feng construction
     - Behavior w.r.t other cryptographic criteria
3. Conclusions

Stream ciphers

Simplest Case: Binary additive stream cipher



- Suitable in environments characterized by a limited computing power or memory, and the need to encrypt at high speed
- The seed of the keystream generators constitutes the secret key
- Security depends on
  - Pseudorandomness of the keystram k_i
  - Properties of the underlying functions (mainly Boolean functions) that form the keystream generator

Problem Statement

Cryptographic criteria

- Several criteria to assess the resistance against attacks
  - balancedness
  - algebraic degree
  - correlation immunity
  - nonlinearity
- Much research effort has been put during last decades on achieving these properties

Cryptanalytic Advances

- Many cryptographic functions failed to thwart more recent attacks
  - (fast) algebraic attacks (Courtois-Meier, 2003)
- Design of functions being tolerant against these attacks, achieving all main cryptographic criteria, is still an active research area

Boolean Functions

A Boolean function f on n variables is a mapping from $\mathbb{F}_2^n$ onto $\mathbb{F}_2$

- The vector $f = \big(f(0,0,\ldots,0), f(1,0,\ldots,0), \ldots, f(1,1,\ldots,1)\big)$ of length 2^n is the truth table of f
- The Hamming weight of f is denoted by $\mathrm{wt}(f)$
  - f is balanced if and only if $\mathrm{wt}(f) = 2^{n-1}$
- The support $\mathrm{supp}(f)$ of f is the set $\{\boldsymbol{b} \in \mathbb{F}_2^n : f(\boldsymbol{b}) = 1\}$

Example: Truth table of balanced f with $n = 3$

x_1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1
$f(x_1, x_2, x_3)$	0	1	0	0	0	1	1	1

Algebraic Normal Form and degree of functions

- Algebraic Normal Form (ANF) of f:

$$f(x) = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} a_{\boldsymbol{v}} x^{\boldsymbol{v}}, \quad \text{where } x^{\boldsymbol{v}} = \prod_{i=1}^{n} x_i^{v_i}$$

.

  - The sum is performed over $\mathbb{F}_2$ (XOR addition)
- The degree $\deg(f)$ of f is the highest number of variables that appear in a product term in its ANF.
- In the previous example: $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_1$.
  - $\deg(f) = 2$
- If $\deg(f) \leq r$, then $\boldsymbol{f}$ is a codeword of the rth order binary Reed–Muller code$\mathrm{RM}(r, n)$
- The punctured Reed–Muller code $\mathrm{RM}^{\star}(r, n)$ is known to be cyclic having as zeros the elements α^t, for all nonzero $t \in \mathbb{Z}_N$ satisfying $\mathrm{wt}(t) < n - r$

Univariate representation of Boolean functions

- $\mathbb{F}_2^n$ is isomorphic to the finite field $\mathbb{F}_{2^n}$,
- $\Rightarrow$ Any function $f \in \mathbb{B}_n$ can also be represented by a univariate polynomial, mapping $\mathbb{F}_{2^n}$ onto $\mathbb{F}_2$, as follows

$$f(x) = \sum_{i=0}^{2^n-1} \beta_i x^i$$

  where $\beta_0, \beta_{2^n-1} \in \mathbb{F}_2$ and $\beta_{2i} = \beta_i^2 \in \mathbb{F}_{2^n}$ for $1 \le i \le 2^n - 2$
- The coefficients of the polynomial are associated with the Discrete Fourier Transform (DFT) of f
- The degree of f can be directly deduced by the univariate representation - i.e. by the DFT of f
- The univariate representation is more convenient in several cases

Algebraic attacks

Milestones

- Algebraic attacks (Courtois-Meier, 2003)
- Fast algebraic attacks (Courtois, 2003)
- The basic idea is to reduce the degree of the mathematical equations employing the secret key
- Known cryptographic Boolean functions failed to thwart these attacks
- The notion of algebraic immunity has been introduced (Meier-Pasalic-Carlet, 2004), to assess the strength of a function against such attacks

Annihilators and algebraic immunity

Definition

Given $f \in \mathbb{B}_n$, we say that $g \in \mathbb{B}_n$ is an annihilator of f if and only if g lies in the set

$$\mathcal{AN}(f) = \{g \in \mathbb{B}_n : f * g = 0\}$$

Definition

The algebraic immunity $\mathsf{AI}(f)$ of $f \in \mathbb{B}_n$ is defined by

$$\mathsf{AI}(f) = \min_{g \neq 0}\{\deg(g) : \ g \in \mathcal{AN}(f) \cup \mathcal{AN}(f+1)\}$$

- A high algebraic immunity is prerequisite for preventing algebraic attacks (Meier-Pasalic-Carlet, 2004)
- Well-known upper bound: $\mathsf{AI}(f) \leq \lceil \frac{n}{2} \rceil$

Fast algebraic attacks

- Extensions of the conventional algebraic attacks
- Aiming at identifying $g, h \in \mathbb{B}_n$, for a given function $f \in \mathbb{B}_n$, such that $fg = h$ with $\deg(g) = e < \mathsf{AI}(f)$, $\deg(h) = d$ and $e + d < n$
  - A pair (e, d) with $e + d \geq n$ always exists
- We say that f admits a (e, d) pair if there exist functions g, h with the aforementioned properties.
- Functions that have no (e, d) pair such that $e + d < n$ are called perfect algebraic immune
- Maximum AI does not imply resistance to fast algebraic attacks
  - A perfect algebraic immune function though has always maximum AI (Pasalic, 2008)

Constructions of functions with maximum AI

- Dalai-Maitra-Sarkar, 2006: Majority function
- Carlet-Dalai-Gupta-Maitra-Sarkar, 2006: Iterative construction
- Li-Qi, 2006, Su-Tang-Zeng, 2014: Modification of the majority function
- Sarkar-Maitra, 2007: Rotation Symmetric Boolean functions (RSBF) of odd n
  - Su-Tang, 2014: RSBF for arbitrary n
- Carlet, 2008: Based on properties of affine subspaces
  - Further investigation in Carlet-Zeng-Li-Hu, 2009
  - Generalization (for odd n) in Limniotis-Kolokotronis-Kalouptsidis, 2011
- Balanceness and/or high nonlinearity are not always attainable, whereas they do not behave well w.r.t. fast algebraic attacks

The Carlet-Feng (CF) construction

- Carlet-Feng, 2008: $\mathrm{supp}(f) = \{1, \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}-1}\}$, where α a primitive element of the finite field $\mathbb{F}_{2^n}$.
  - Degree $n-1$ (i.e. the maximum possible)
  - High nonlinearity is ensured
    - Best currently known lower bound (Tang et. al., 2013)

$$\mathsf{nl}(f) \geq 2^{n-1} - (\frac{n\ln(2)}{\pi} + 0.74)2^{n/2} - 1$$

    - Experiments show that the actual values of nonlinearities are much higher
  - Optimal against fast algebraic attacks, as subsequently shown (Liu-Zhang-Lin, 2012)
- Other important constructions have been also recently proved (e.g. Tang-Carlet-Tang, 2013, Li-Carlet-Zeng-Li-Hu-Shan, 2014)

Generalizations of Carlet-Feng construction

- Rizomiliotis, 2010: A new construction based on the univariate representation
  - Associate the AI with the rank of a well-determined matrix
  - For n odd, equivalent to the CF construction
- Zeng-Carlet-Shan-Hu, 2011: Modifications of the Rizomiliotis construction
- Further generalizations in Limniotis-Kolokotronis-Kalouptsidis, 2013:
  - Finding swaps between $\mathrm{supp}(f)$ and $\mathrm{supp}(f+1)$ that preserve maximum AI
  - $\Rightarrow$ Algorithm singleswap(*for* n *odd*)
  - Why restricted to odd n?
    - If n is odd, then $f \in \mathbb{B}_n$ has maximum algebraic immunity $\frac{n+1}{2}$ if and only if f is balanced and has no nonzero annihilators of degree at most $\frac{n-1}{2}$.

Alg. singleswap

- Basic tool: The $(2^{n-1}) \times (2^n - 1)$ binary matrix $R_{(n+1)/2,n-1}$ (Rizomiliotis, 2010)

$$R_{(n+1)/2,n-1} = \begin{pmatrix} e_0 & e_1 & \dots & e_E & 0 & \dots & 0 \\ 0 & e_0 & \dots & e_{E-1} & e_E & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \vdots & \vdots & \dots & 0 \\ 0 & 0 & \dots & \vdots & \vdots & \dots & e_E \end{pmatrix}$$

- $E = 2^{n-1} - 1$
- $e_0 + e_1 x + \ldots + e_E x^E$: the generator polynomial of $\mathrm{RM}^\star(\frac{n-1}{2}, n)$
- For any $0 \leq r < 2^n - 1$ each column vector $\boldsymbol{v}^r$ of $R_{(n+1)/2,n-1}$ is

$$\boldsymbol{v}^r = \begin{cases} (e_r \ \cdots \ e_1 \ e_0 \ \ \mathbf{0}_{E-r})^T, & \text{if } r \leq E \\ (\mathbf{0}_{r-E} \ e_E \ \cdots \ e_{r-E})^T, & \text{otherwise} \end{cases}$$

Alg. singleswap (*Cont.*)

- Goal: For α^m, $m > 2^{n-1}-1$, find α^j, $j \leq 2^{n-1}-1$, such that replacing (swapping) α^j with α^m in the support of the CF function retains the maximum AI
- Limniotis-Kolokotronis-Kalouptsidis, 2013: Consider the left-hand square upper-diagonal sub-matrix R'

$$\left(\begin{array}{cccc|ccc} e_0 & e_1 & \dots & e_E & 0 & \dots & 0 \\ 0 & e_0 & \dots & e_{E-1} & e_E & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & e_1 & \vdots & \dots & 0 \\ 0 & 0 & \dots & e_0 & \vdots & \dots & e_E \end{array}\right)$$

- Solve the system $R'\boldsymbol{z} = \boldsymbol{v}^m$
  - Via backward substitution
- Each $0 \leq j \leq 2^{n-1}-1$ such that $z_j = 1$ is an answer

Alg. singleswap (*Cont.*)

Algorithm 1 singleswap(n, f, α^m, k)

Input: odd integer n, function $f \in \mathbb{B}_n$ with $\mathrm{supp}(f) = \{\alpha^0, \ldots, \alpha^E\}$
element $\alpha^m \notin \mathrm{supp}(f)$, and integer k

$S \leftarrow \varnothing$
$\boldsymbol{z} \leftarrow \mathbf{0}$ ▷ all–zero vector of length $E+1$
$i \leftarrow E$
while $(i \geq E - k + 1)$ **do**
  $z_i \leftarrow v_i^m$
  if $i \neq E$ **then**
    for $r = i+1, \ldots, E$ **do**
      $z_i \leftarrow z_i + v_i^r * z_r$
    end
  end
  if $z_i = 1$ **then**
    $S \leftarrow S \cup i$
  end
  $i \leftarrow i - 1$
end

Output: $S = \{j_1, \ldots, j_r\} \subset \{E-k+1, \ldots, E\}$: for all $1 \leq \ell \leq r$ the function $g \in \mathbb{B}_n$ with $\mathrm{supp}(g) = \mathrm{supp}(f) \cup \{\alpha^m\} \setminus \{\alpha^{j_\ell}\}$ has maximum AI

- We may simply find k entries of $\boldsymbol{z}$, for any $k \ll 2^{n-1}$
  - The algorithm computes the last k entries $z_E, \ldots, z_{E-k+1}$ in decreasing order
- The overall computational complexity is described by $\mathcal{O}(k^2)$

New approach

Limniotis-Kolokotronis, 2015

- Generalization of the above, so as to find arbitrary number of swaps retaining the maximum AI (for odd n)
- Properties of punctured Reed–Muller codes $\mathrm{RM}^\star(\frac{n-1}{2}, n)$ are employed
  - Due to Alg. singleswap, efficient application to the CF function

Useful terminology

- For two codewords (polynomials) of a binary code

$$h(x) = \sum_{i=0}^{N-1} h_i\, x^i \quad \text{and} \quad c(x) = \sum_{i=0}^{N-1} c_i\, x^i$$

  we have $h \preceq c \Leftrightarrow h_i \leq c_i$ for all i.
- A minimal codeword is any codeword $v(x)$ such that there is no nonzero codeword $v'(x)$ of the code with $v' \prec v$.

Annihilators as codewords

In the sequel: n odd, α a primitive element of $\mathbb{F}_{2^n}$

Theorem

Let $f \in \mathbb{B}_n$ be balanced with $\mathrm{supp}(f) = \{\alpha^{r_0}, \alpha^{r_1}, \ldots, \alpha^{r_E}\}$ and $r_0 = 0$. Then, AI$(f) = \frac{n+1}{2}$ if and only if there is no nonzero even weight codeword $v(x)$ of the code $\mathrm{RM}^\star(\frac{n-1}{2}, n)$ such that $v(x) \preceq c(x) = 1 + x^{r_1} + \cdots + x^{r_E}$.

Proof (Sketch)

- We consider the DFT representation of any annihilator g of $f+1$
- If $\deg(g) \leq \frac{n-1}{2}$, then specific DFT coefficients should be zero
  - Such a requirement leads to the proof of the claim

Annihilators as minimal codewords

Proposition

Let $f \in \mathbb{B}_n$ have $\mathsf{AI}(f) = \frac{n+1}{2}$, where $\mathrm{supp}(f) = \{\alpha^{r_0}, \ldots, \alpha^{r_E}\}$ and $r_0 = 0$. For all $\alpha^j \notin \mathrm{supp}(f)$, there exists a unique nonzero even weight minimal codeword $v(x)$ of $\mathrm{RM}^\star(\frac{n-1}{2}, n)$ such that $x^j \prec v(x)$ and $v(x) \preceq c(x) = 1 + x^{r_1} + \cdots + x^{r_E} + x^j$.

If f is the CF function:

- For any $j > E$, there exists a unique nonzero even-weight minimal codeword $u_j(x)$ of $\mathrm{RM}^\star(\frac{n-1}{2}, n)$, with $x^j \prec u_j(x)$ and $u_j(x) \preceq c^{(j)}(x) = \sum_{i=0}^{E} x^i + x^j$.
  - Direct corollary from the previous Proposition
- The codewords u_j have a main role in developing new construction of functions with maximum AI, as shown next

Key result

Proposition

Let $c(x) = c_1(x) + c_2(x)$, where $c_1(x) \preceq \sum_{i=0}^{E} x^i$, $c_2(x) \preceq \sum_{i=E+1}^{N-1} x^i$. If $\exists$ nonzero even weight codeword $v(x)$ of $\mathrm{RM}^\star(\frac{n-1}{2}, n)$ with $v(x) \preceq c(x)$, then $v(x)$ necessarily has the form

$$v(x) = \sum_{j \in J} \delta_j \, u_j(x)\,, \quad \delta_j \in \mathbb{F}_2, \quad J \subseteq \{E < i < N : x^i \preceq c_2(x)\}$$

Proof (Sketch)

- Suppose there exists exists minimal codeword $v'(x) \preceq c(x)$ not having the above form
- It holds $v'(x) = v'_1(x) + v'_2(x)$, where $v'_1(x) \preceq c_1(x)$, $v'_2(x) \preceq c_2(x)$.
- Let $J' = \{E < i < N : x^i \preceq v'_2(x)\}$. Then $u' + v'$ is also an even weight codeword of $\mathrm{RM}^\star(\frac{n-1}{2}, n)$, where $u' = \sum_{j \in J'} u_j(x)$
- But $u' + v' \preceq \sum_{i=0}^{E} x^i \Rightarrow \deg(u' + v') \leq E$ - a contradiction.

A property that ensures maximum AI

Theorem

Let $g \in \mathbb{B}_n$, where

- $\mathrm{supp}(g) = \{\alpha^0, \alpha^1, \ldots, \alpha^E\} \cup A \setminus B$,
- $A = \{\alpha^{j_1}, \ldots, \alpha^{j_r}\} \subset \mathrm{supp}(f+1)$ and $B = \{\alpha^{i_1}, \ldots, \alpha^{i_r}\} \subset \mathrm{supp}(f)$, where
    a. $i_s \neq 0$, for all $1 \leq s \leq r$,
    b. $x^{i_s} \prec u_{j_s}(x)$ for all $1 \leq s \leq r$,
    c. $x^{i_s} \not\prec u_{j_t}(x)$ for all $1 \leq t \leq r$ with $t \neq s$.

Then $\mathrm{AI}(g) = \frac{n+1}{2}$.

Proof (Sketch)

- Let $\mathrm{supp}(g) = \{\alpha^0, \alpha^{r_1}, \ldots, \alpha^{r_E}\}$
- The choice of sets A, B ensures that there is no $A' \subseteq \{j_1, \ldots, j_r\}$ such that $\sum_{j \in A'} u_j(x) \prec 1 + x^{r_1} + \ldots + x^{r_E}$

Towards developing a new construction

- Having knowledge of u_j, we may proceed by a new construction due to the previous Theorem
- Basic idea: Start from the CF function f and swap elements between $\mathrm{supp}(f)$ and $\mathrm{supp}(f+1)$ such as:
  - If $A \subset \mathrm{supp}(f+1)$ that is "swapped" to $\mathrm{supp}(f)$, then for any j such that $\alpha^j \in A$, there exists a position at the codeword polynomial $u_j(x)$ where the corresponding coefficient is nonzero, whereas the corresponding coefficients of all other $u_{j'}(x)$, $j' \in A$, are zero.
- Crucial point: Efficient identification of $u_j(x)$ for all desired j is needed
- The answer: Alg. singleswap!
  - It is easily proved that Alg. singleswap returns exactly the coefficients of $u_j(x)$

The new algorithm

- Putting all together...

Algorithm 2 modifyCF (n, f, M, k)

Input: odd integer n, function $f \in \mathbb{B}_n$ with $\mathrm{supp}(f) = \{\alpha^0, \ldots, \alpha^E\}$
set $M = \{\alpha^{m_1}, \ldots, \alpha^{m_r}\} \subset \mathrm{supp}(f+1)$, and integer k

1: **for** $i = 1, \ldots, r$ **do**
2: $\quad S^{(i)} \leftarrow$ singleswap (n, f, α^{m_i}, k)
3: **end**
4: $S = \varnothing$
5: **for** $i = 1, \ldots, r$ **do**
6: $\quad$ Choose $j_i \in S^{(i)} \setminus \bigcup_{p \neq i} S^{(p)}$ so that $\forall p \neq i,\ \exists j_i' \in S^{(p)}$ with $j_i' < j_i$
7: $\quad S \leftarrow S \cup \{j_i\}$
8: **end**

Output: $S = \{j_1, \ldots, j_r\} \subset \{0, 1, \ldots, E\}$: the function $g \in \mathbb{B}_n$ with
$\mathrm{supp}(g) = \mathrm{supp}(f) \cup M \setminus \{\alpha^{j_1}, \ldots, \alpha^{j_r}\}$ has maximum AI

- In general, many choices for selecting j_i from $S^{(i)}$
- Its worst–case computational complexity is $\mathcal{O}(rkL)$, for $L = \max\{k, r \log_2 k\}$.
  - Line 2: $\mathcal{O}(k^2)$
  - Line 6: For each candidate element of $S^{(i)}$, we apply binary search on at most $r-1$ ordered arrays with length at most k

Other cryptographic criteria

Proposition

There always exists a Boolean function g constructed via Alg. modifyCF such that $\deg(g) = n - 1$.

Proposition

It holds $\mathsf{nl}(g) > 2^{n-1} - \left(\frac{\ln 2}{\pi} n + 0.74\right) 2^{n/2} - 2r - 1$, where r is the number of swapped pairs.

Discussion

- Maximum possible algebraic degree is attainable
- High nonlinearity can be achieved
    - Due to the fact that the CF function has high nonlinearity

An example

- $n = 7$, $f \in \mathbb{B}_7$ a CF function,
  $M = \{\alpha^{80}, \alpha^{81}, \alpha^{90}, \alpha^{91}\} \subset \mathrm{supp}(f+1)$ (random choice)

Application of Alg. singleswap to f, for each element of M

m_i	Set $S^{(i)}$ of all possible j_i
80	0 3 6–9 11–15 17 18 21–24 28 29 33 36 38–41 43 45–47 53 54 56 58 61 63
81	0–2 4–7 11 13 14 18 19 21 22 25 26 29 31–33 38–45 49 51 53–55 57 58–61 63
90	0 2 3 7 10 15–17 19 22 24 27 29 32 33 38–40 45 46 48 50 51 53–56 58 60 61 63
91	0–6 9 10 12 15 17 18 20 21 24–26 28 31 32 37–41 43 45 48 52–60 63

- All possible single swaps have been computed (Alg. singleswap has been executed for $k = 2^{n-1} = 64$)
  - For each $m_i \in \{80, 81, 90, 91\}$, all possible j_i such that $g \in \mathbb{B}_7$ with $\mathrm{supp}(g) = \mathrm{supp}(f) \setminus \{\alpha^{j_i}\} \cup \{\alpha^{m_i}\}$ has maximum AI, are given
- Proceed with the next step of Alg. modifyCF

An example (*Cont.*)

Find entries that appear in exactly one row

m_i	Set $S^{(i)}$ of all possible j_i
80	0 3 6–9 11–15 17 18 21–24 28 29 33 36 38–41 43 45–47 53 54 56 58 61 63
81	0–2 4–7 11 13 14 18 19 21 22 25 26 29 31–33 38–45 49 51 53–55 57 58–61 63
90	0 2 3 7 10 15–17 19 22 24 27 29 32 33 38–40 45 46 48 50 51 53–56 58 60 61 63
91	0–6 9 10 12 15 17 18 20 21 24–26 28 31 32 37–41 43 45 48 52–60 63

New function $g \in \mathbb{B}_7$ with maximum AI

- $\mathrm{supp}(g) = \mathrm{supp}(f) \setminus \{\alpha^{47}, \alpha^{49}, \alpha^{50}, \alpha^{52}\} \cup \ M$
  - Even if we had executed singleswap for $k = 17$ (instead of 64), we would get the same result
- For the specific example, 108 different functions can be generated
  - Possible choices:
    - $\{47, 36, 23, 8\}$ (from $S^{(1)}$),
    - $\{49, 44, 42\}$ (from $S^{(2)}$),
    - $\{50, 27, 16\}$ (from $S^{(3)}$),
    - $\{52, 37, 20\}$ (from $S^{(4)}$).

An example (*Cont.*)

Behavior w.r.t. other cryptographic criteria

- $\deg(g) = 6$ - i.e. the maximum possible
- $\mathsf{nl}(g) = 52$
  - Slightly lower than $\mathsf{nl}(f) = 54$, (f is the CF function)
  - Most of all possible 108 functions have also nonlinearity 52
    - Nonlinearity equal to 54 is attainable (although higher values were not observed, for the specific example)
- The same behavior w.r.t. fast algebraic attacks, as the CF function
  - g does not admit any pair (e, d) with $e = 1$ and $e + d \leq n - 1$, whilst for $e > 1$ there is no any pair (e, d) satisfying $e + d < n - 1$.

Conclusions - Future research

Summary

- New construction of functions with maximum AI (n odd)
  - Having the CF function f as a starting point, it seems that other cryptographic criteria are also satisfied
  - Arbitrary number of swaps between $\mathrm{supp}(f)$ and $\mathrm{supp}(f+1)$ that preserve maximum AI

Open problems

- Identify other possible swaps that satisfy the desired property
- Nonlinearity and fast algebraic attacks should be further elaborated
- Possible extension to the even case
  - Main difference: Adding an element of the $\mathrm{supp}(f+1)$ into $\mathrm{supp}(f)$ does not necessarily reduce AI
  - However, research in progress shows that such elements can be identified for the CF function

References

N. Courtois, and W. Meier.
Algebraic attacks on stream ciphers with linear feedback,
Eurocrypt 2003, (LNCS, Springer) 2656, 2003.

N. Courtois.
Fast algebraic attacks on stream ciphers with linear feedback,
Crypto 2003 (LNCS, Springer) 2729, 2003.

W. Meier, E, Pasalic, and C. Carlet.
Algebraic attacks and decomposition of Boolean functions,
Eurocrypt 2004 (LNCS, Springer) 3027, 2004.

C. Carlet, and K. Feng.
An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity,
Asiacrypt 2008 (LNCS, Springer) 5350, 2008.

References *(Cont.)*

P. Rizomiliotis.
On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation,
IEEE Trans. Inform. Theory 56, 4014–4024, 2010.

M. Liu, Y. Zhang, and D. Lin.
Perfect algebraic immune functions,
Asiacrypt 2012 (LNCS, Springer) 7658, 172–189, 2012.

K. Limniotis, N. Kolokotronis, and N. Kalouptsidis.
Secondary constructions of Boolean functions with maximum algebraic immunity,
Cryptogr. Comm. 5, 179–199, Springer, 2013.

References *(Cont.)*

D. Tang, C. Carlet, and X. Tang.
Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks,
IEEE Trans. Inform. Theory 59, 653–664, 2013.

J. Li, C. Carlet, X. Zeng, C. Li, L. Hu, and J. Shan.
Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks,
Des. Codes Cryptogr. 76, Springer, 2015.

K. Limniotis, and N. Kolokotronis.
Boolean functions with maximum algebraic immunity based on properties of punctured Reed–Muller codes,
BalkanCryptSec 2015 (LNCS, Springer) 9540, 2016.

Questions & Answers

Thank you for your attention!