Vectorial functions for symmetric cryptography: immersion and insights

Sihem Mesnager

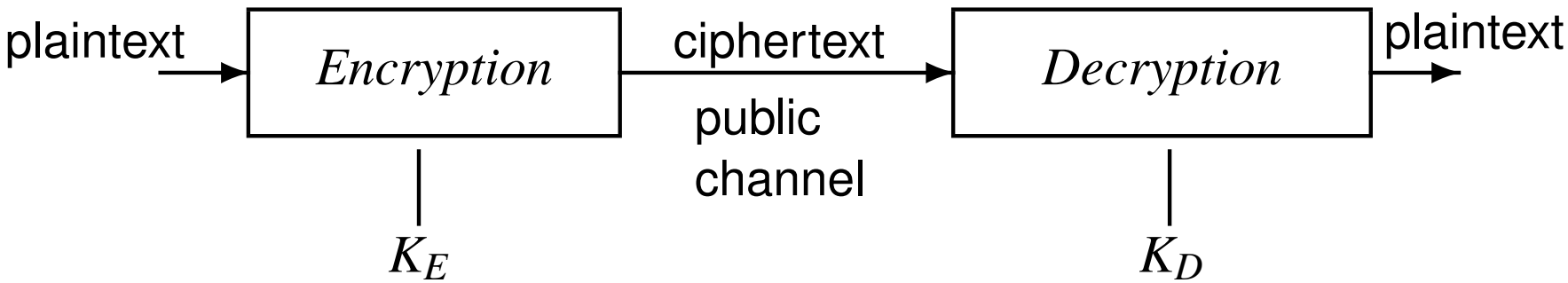
Department of Mathematics, University of Paris VIII
and University Sorbonne Paris Cité, LAGA, CNRS,
and Telecom Paris, Polytechnic Institute of Paris, France

Young Researchers Algebra Conference 2023
July 27, 2023, L'Aquila, Italy

Outline

- Preliminaries on vectorial functions
- Main mathematical problems in symmetric cryptography in block cipher
- the main problem in solving equations over finite fields
  - On the famous equation $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$
    - Ingredients for the resolution
    - The two related problems for solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n, k) = 1$
    - Solving the two problems
  - Impacts (results obtained in 2021, 2022 and 2023)
    - On the APN-ness property of Kasami functions
    - On the bijectivity property of an "exceptional" family of quadrinomials
    - On the resolution of a new equation $F(x + 1) + F(x) = b$ where F is a power "cryptographic" function

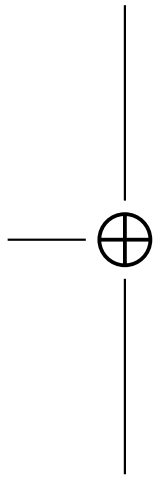
Cryptography



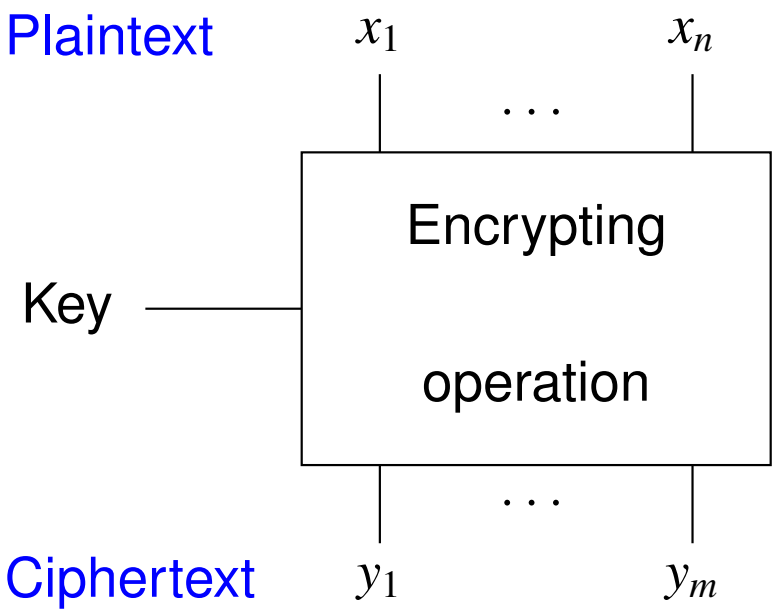
Boolean functions : cryptographic framework

Stream ciphers

Pseudo-random generator with a Boolean function



Block ciphers (AES, DES, etc)



outputs of Boolean functions (depending on the key) over $x_1, \cdots, x_n$

Notation :

- $\mathbb{F}_{2^n}$ the finite field of order 2^n.
- The *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ equals $Tr_{2^n/2}(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Symmetric cryptography

Let

$$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$$

- The (Boolean) functions : $x \mapsto b \cdot F(x) := Tr_{2^m/2}(bF(x))$, $b \in \mathbb{F}_{2^m}$ where $b \neq 0$ are called the *components* of F
  where $Tr_{2^n/2}(x) := \sum_{i=0}^{n-1} x^{2^i}$ (trace function).
- The discrete Hadamard Walsh (Fourier) transform of F :
  $W_F(a,b) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_{2^m/2}(bF(x)) - Tr_{2^n/2}(ax)}$
  where $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \setminus \{0\}$
- three main important cryptographic parameters for F
  1. Nonlinearity and higher-order nonlinearity
  2. Differential uniformity
  3. Boomerang uniformity

  ☞ To make the cryptanalysis very difficult to implement, we must pay attention when choosing the vectorial function F, which has to follow. several recommendations : **cryptographic criteria** !

☞ Linear Cryptanalysis [Matsui (1993)] $\Rightarrow$ nonlinearity $\mathrm{Nl}(F)$ de $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$,

$$\mathrm{Nl}(F) = \min_{b \in \mathbb{F}_{2^m}, b \neq 0} \{\mathrm{nl}(Tr_{2^m/2}(bF))\} = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, b \neq 0} |W_F(a,b)|.$$

★ The higher the value of $\mathrm{Nl}(F)$, the better resistance to linear cryptanalysis.

★ When $n = m$ odd, $\mathrm{Nl}(F)$ is bounded by $2^{n-1} - 2^{\frac{n-1}{2}}$. The functions reaching this upper bound are the AB functions.

★ When $m = 1$, $\mathrm{Nl}(F)$ is bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$. The functions reaching this upper bound are the bent functions (n even).

↪ A very difficult parameter to study mathematically ! !

☞ Differential cryptanalysis [Biham, Shamir (1991)] $\Rightarrow$

- Difference Distribution Table

$$\mathrm{DDT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n},\ F(x+a) + F(x) = b\}, \qquad (1)$$

- Differential uniformity [Nyberg (1992-1993)]

$$\delta_F = \max_{a,b \in \mathbb{F}_{2^n}, a \neq 0} \mathrm{DDT}_F(a,b). \qquad (2)$$

★ The smaller the δ_F value, the better the resistance to differential cryptanalysis.

★ For any function F with $m \leq n$, $\delta_F \geq p^{n-m}$ and $\delta_F \geq 2$ if $p = 2$.

★ If $\delta_F = 1$, the function F (p odd) is non-perfect linear (PN).

★ If $\delta_F = 2$, the function F ($p = 2$) is almost perfectly nonlinear (APN).

A variation of differential cryptanalysis : boomerang cryptanalysis

☞ Boomerang cryptanalysis [Wagner (1999)] $\Rightarrow$

- Boomerang Connectivity Table [Cid. al. (2018)]

$$\mathrm{BCT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n},\ F^{-1}(F(x)+b)+F^{-1}(F(x+a)+b) = a\}. \tag{3}$$

- Boomerang uniformity ([Bourra, Canteaut (2018)])

$$\beta_F = \max_{a,b\in\mathbb{F}_{2^n},a\neq 0} \mathrm{BCT}_F(a,b), \tag{4}$$

★ The smaller the value of β_F, the better the boomerang cryptanalysis resistance (here $n = m$ and F bijective).

★ To secure a block cipher against cryptanalysis boomerang, it must use a function with a value of β_F small.

↪ You have to know how to solve equations over finite fields or at least count the number of solutions : mathematically difficult !

An important example : solving the equation $P_a(x) := x^{2^k+1} + x + a = 0$ over $\mathbb{F}_{2^n}$

- ☞ the polynomial $P_a(x)$ ($a \in \mathbb{F}_{2^n}^\star$) appears in this cryptographic context (APN functions [Budaghyan, Carlet 2006], [Bracken, Tan, Tan 2014], [Canteaut, Perrin, Tian 2019])

but not only since there is an interest in other contexts :

- the general theory of finite fields
- the inverse Galois problem [Abhyankar, Cohen, Zieve, 2000] ;
- the construction of difference sets with Singer parameters [Dillon 2002] ;
- finding cross-correlation between m-sequences [Helleseth, Kholosha, Ness, 2007] ;
- constructing error correcting codes [Bracken, Helleseth 2009] ;
- constructions designs [Tang 2019] ;
- etc.

Solving $x^{2^k+1} + x + a = 0$ over $\mathbb{F}_{2^n}$

What do we know ? (before 2020)

- Solution for $k = 1$ [Berlekamp-Rumsey-Solomon 1967-Williams, 1975]
- Partial results
  Let N_a be the number of solutions of the equation $P_a(x) := x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$.
  - In 2004 : [Bluher, 2004] the number of solutions N_a are only 0, 1 and 3 when $\gcd(k, n) = 1$.
  - In 2008 : [Helleseth-Kholosha 2008] got criteria for $N_a = 1$ and an explicit expression of the unique solution when $\gcd(k, n) = 1$.
  - In 2014 : [Bracken-Tan-Tan 2014] presented a criterion for $N_a = 0$ when n is even and $\gcd(k, n) = 1$.

After 2020 : [Kim and SM, FFA 2020] solving completely $P_a(x) = 0$ (but further in 2021 for any n, k and characteristic p) [papers published in the FFA journal with Kim and some members of his research team]

Main ingredients for the resolution of $P_a(x) := x^{2^k+1} + x + a = 0$ over $\mathbb{F}_{2^n}$

Ingredient 1 : Dickson polynomials

- **Definition** The Dickson polynomial of the first kind of degree k in indeterminate x and with parameter $a \in \mathbb{F}_{2^n}^*$ is

$$D_k(x,a) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i} \binom{k-i}{i} a^k x^{k-2i},$$

  where $\lfloor k/2 \rfloor$ denotes the largest integer less than or equal to $k/2$. In this talk, we consider only Dickson polynomials $D_k(x,1)$, that we shall denote $D_k(x)$.

- **A lot of properties** For all $x \in \mathbb{F}_{2^n}$, for any integer $h, k > 0$.
  - $\deg D_k = k$;
  - $D_k\left(x + \frac{1}{x}\right) = x^k + \frac{1}{x^k}$;
  - D_k permutation over $\mathbb{F}_{2^n}$ if and only if $\gcd(k, 2^{2n}-1) = 1$;
  - $D_{hk}(x) = D_h(D_k(x))$;
  - etc.

Main ingredients for the resolution of $P_a(x) := x^{2^k+1} + x + a = 0$ over $\mathbb{F}_{2^n}$

Let k and n be two positive integers.
Ingredient 2 : Müller-Cohen-Matthews polynomials $f_{k,d}$ are defined over $\mathbb{F}_{2^n}$ as follows :

$$f_{k,d}(X) := \frac{T_k(X^c)^d}{X^{2^k}}$$

where

$$T_k(X) := \sum_{i=0}^{k-1} X^{2^i} \quad \text{and} \quad cd = 2^k + 1.$$

A basic property for such polynomials $f_{k,2^k+1}$ (when $\gcd(k,n) = 1$) :

1. If k is odd, then $f_{k,2^k+1}$ is a permutation on $\mathbb{F}_{2^n}$ ([Müller, Cohen, Matthews 1994]).
2. If k is even, then $f_{k,2^k+1}$ is 2-to-1 on $\mathbb{F}_{2^n}$ ([Dillon, Dobbertin 2004]).

The two related problems for solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$, $\gcd(n,k) = 1$

If k is odd, since $\gcd(q-1, 2^n - 1) = 1$, the zeros of $P_a(x)$ are the images of the zeros of $P_a(x^{q-1})$ by the map $x \mapsto x^{q-1}$.

Now $f_{k,q+1}$ is a permutation polynomial of $\mathbb{F}_{2^n}$ by **Ingredient 2**. Therefore, for any $a \in \mathbb{F}_{2^n}^*$, there exists a unique Y in $\mathbb{F}_{2^n}^*$ such that $a = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}}$. Hence, we have

$$P_a\left(x^{q-1}\right) = x^{q^2-1} + x^{q-1} + \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}} \tag{5}$$

Substituting tx to X in the above identity with $t^{q^2-q} = Y^q T_k\left(\frac{1}{Y}\right)^2$, we get :

$$P_a\left(x^{q-1}\right) = \frac{1}{Y^{q-1}\left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{\frac{2}{q}}}\left(X^{q^2-1} + \left(\sum_{i=1}^{k} Y^{q-2^i}\right) X^{q-1} + Y^{q-1}\right)$$

The two related problems for solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$, $\gcd(n, k) = 1$

we use a key polynomial identity involving Dickson polynomials : a key result due to [Bluher, 2016] :
In the polynomial ring $\mathbb{F}_q[X, Y]$ (where $q := 2^k$) we have the identity

$$X^{q^2-1} + \left(\sum_{i=1}^{k} Y^{q-2^i} \right) X^{q-1} + Y^{q-1} = \prod_{w \in \mathbb{F}_q^*} \left(D_{q+1}(wX) - Y \right).$$

thus

$$P_a\left(x^{q-1}\right) = \frac{1}{Y^{q-1}\left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{\frac{2}{q}}} \left(\prod_{w \in \mathbb{F}_q^*} \left(D_{q+1}(wX) - Y \right) \right).$$

☞ when k is odd, finding the zeros of $P_a(x^{q-1})$ amounts to determine preimages of Y under the Dickson polynomial D_{q+1}.

The two related problems for solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$, $\gcd(n,k) = 1$

When k is even, $f_{k,q+1}$ is 2-to-1, fortunately, we can go back to the odd case by rewriting the equation. Indeed, for $x \in \mathbb{F}_{2^n}$,

$$P_a(x) = x^{2^k+1} + x + a = \left(x^{2^{n-k}+1} + x^{2^{n-k}} + a^{2^{n-k}}\right)^{2^k}$$
$$= \left((x+1)^{2^{n-k}+1} + (x+1) + a^{2^{n-k}}\right)^{2^k}$$

and so

$$\{x \in \mathbb{F}_{2^n} \mid P_a(x) = 0\} = \left\{x+1 \mid x^{2^{n-k}+1} + x + a^{2^{n-k}} = 0,\ x \in \mathbb{F}_{2^n}\right\}. \quad (6)$$

☞ If k is even, then $n-k$ is odd, and we can reduce it to the odd case.

The two related problems for solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$, $\gcd(n,k) = 1$

To summarize all the above discussions :
Let k and n be two positive integers such that $\gcd(k,n) = 1$.

1. Let k be odd and $q = 2^k$. Let $Y \in \mathbb{F}_{2^n}^*$ be (uniquely) defined by $a = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)^{\frac{2}{q}}}$. Then,

$$\{x \in \mathbb{F}_{2^n} \mid P_a(x) = 0\} = \left\{ \frac{z^{q-1}}{YT_k\left(\frac{1}{Y}\right)^{\frac{2}{q}}} \mid D_{q+1}(z) = Y,\ z \in \mathbb{F}_{2^n} \right\}.$$

2. Let k be even and $q' = 2^{n-k}$. Let $Y' \in \mathbb{F}_{2^n}^*$ be (uniquely) defined by $a^{q'} = \frac{1}{f_{n-k,q'+1}\left(\frac{1}{Y'}\right)^{\frac{2}{q'}}}$. Then,

$$\{x \in \mathbb{F}_{2^n} \mid P_a(x) = 0\} = \left\{ 1 + \frac{z^{q'-1}}{Y'T_{n-k}\left(\frac{1}{Y'}\right)^{\frac{2}{q'}}} \mid D_{q'+1}(z) = Y',\ z \in \mathbb{F}_{2^n} \right\}.$$

The two related problems for solving $P_a(x) := x^{q+1} + x + a = 0$; $q = 2^k$, $\gcd(n,k) = 1$

☞ we can split the problem of finding the zeros in $\mathbb{F}_{2^n}$ of P_a into two independent problems : with odd k.

A For $a \in \mathbb{F}_{2^n}^*$, find the unique element Y in $\mathbb{F}_{2^n}^*$ such that

$$a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}. \tag{7}$$

B For $Y \in \mathbb{F}_{2^n}^*$, find the preimages in $\mathbb{F}_{2^n}$ of Y under the Dickson polynomial D_{q+1}, that is, find the elements of the set

$$D_{q+1}^{-1}(Y) = \{z \in \mathbb{F}_{2^n}^\star \mid D_{q+1}(z) = Y\}. \tag{8}$$

On Problem A : find Y such that $a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}$

Solve Problem A

- We used
  1. Müller-Cohen-Matthews polynomials
  2. machinery for computing the computational inverse of a family of polynomials
- Problem A amounts to finding the solutions to a linear equation of the form $x^q + x = b$.

An approach to compute the computational inverse of an element of a family of polynomials

For any $x \in \mathbb{F}_{2^n}$, define

$$Q'_{k,k'}(x) = \frac{x^{q+1}}{\sum_{i=1}^{k'} x^{q^i}} \tag{9}$$

where $q := 2^k$, $k' < n$ is the inverse of k modulo n.
We have

- if $\gcd(n,k) = 1$ and k' is odd, then $Q'_{k,k'}$ is a permutation on $\mathbb{F}_{2^n}$ ([Dillon, Dobbertin, 1999]) ;
- a relation ([Dillon, 1999]) :

$$\Delta_k(X) = Q'_{k,k'}\left(X + X^{2^k}\right) = f_{k,q+1}(X + X^2). \tag{10}$$

where $\Delta_k(X) = (X+1)^{2^{2k}-2^k+1} + X^{2^{2k}-2^k+1} + 1$;

An approach to compute the computational inverse of an element of a family of polynomials [continued]

- the polynomial representation of the inverse $R_{k,k'}$ of $Q'_{k,k'}$ on $\mathbb{F}_{2^n}$ has been studied in [Dillon, Dobbertin, 2004] by introducing the following sequences of polynomials :

$$A_1(x) = x,\ A_2(x) = x^{q+1},\ A_{i+2}(x) = x^{q^{i+1}} A_{i+1}(x) + x^{q^{i+1}-q^i} A_i(x), \quad i \geq 1,$$

$$B_1(x) = 0,\ B_2(x) = x^{q-1},\ B_{i+2}(x) = x^{q^{i+1}} B_{i+1}(x) + x^{q^{i+1}-q^i} B_i(x), \quad i \geq 1.$$

The polynomial expression of $R_{k,k'}$ is then
$R_{k,k'}(x) = \sum_{i=1}^{k'} A_i(x) + B_{k'}(x)$.

On Problem A : find Y such that $a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}$

Solve Problem A :

- we use the fact : $\Delta_k(X) = Q'_{k,k'}\left(X + X^{2^k}\right) = f_{k,q+1}(X + X^2)$;
- we use a well-known key decomposition : every element z of $\mathbb{F}_{2^n}^\star$ can be written (twice) $z = c + \frac{1}{c}$ where $c \in \mathbb{F}_{2^n}^\star \cup M$ with $c \neq 1$ and where $M = \{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\}$
- One has $Y = T + \frac{1}{T}$ where $T \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ or $T \in M \setminus \{1\}$ where $M = \left\{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\right\}$ (observe that $M \setminus \{1\} \subset \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$). Consequently :

$$\frac{1}{Y} = \left(\frac{1}{T+1}\right)^2 + \frac{1}{T+1}.$$

On Problem A : find Y such that $a^{\frac{q}{2}} = \frac{1}{f_{k,q+1}\left(\frac{1}{Y}\right)}$

Solve Problem A : We get

$$\begin{aligned} a^{\frac{q}{2}} = \left(f_{k,q+1}\left(\frac{1}{Y}\right)\right)^{-1} &\iff a^{-\frac{q}{2}} = \Delta_k\left(\frac{1}{T+1}\right) \\ &\iff a^{-\frac{q}{2}} = Q'_{k,k'}\left(\left(\frac{1}{T+1}\right)^q + \left(\frac{1}{T+1}\right)\right) \end{aligned} \tag{11}$$

Next, Problem A amounts to finding the solutions to a linear equation of the form $x^q + x = b$, that we solved.

On Problem B : find $D_{q+1}^{-1}(Y) = \{z \in \mathbb{F}_{2^n}^\star \mid D_{q+1}(z) = Y\}$

Solve Problem B :

1. Write $z = c + \frac{1}{c}$ where $c \in \mathbb{F}_{2^n}^\star$ or $c \in M \setminus \{1\}$, where $M = \{\zeta \in \mathbb{F}_{2^{2n}} \mid \zeta^{2^n+1} = 1\}$;
   One gets (using **properties of Dickson polynomials**)
   $Y = D_{q+1}(z) = c^{q+1} + \frac{1}{c^{q+1}} = T + \frac{1}{T}$ with $T = c^{q+1}$.
   The equation $T + \frac{1}{T} = Y$ has two solutions in $\mathbb{F}_{2^n}^\star \cup M$ for any $Y \in \mathbb{F}_{2^n}^\star$ because it is equivalent to the quadratic equation $\left(\frac{T}{Y}\right)^2 + \frac{T}{Y} = \frac{1}{Y^2}$ and that $Tr_{2^{2n}/2}\left(\frac{1}{Y}\right) = 0$.
2. We handle the two situations separately of those two cases that occur depending on the value of $Tr_{2^n/2}\left(\frac{1}{Y}\right)$:
   - If $Tr_{2^n/2}\left(\frac{1}{Y}\right) = 0$, $T + \frac{1}{T} = Y$ has two solutions in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$;
   - If $Tr_{2^n/2}\left(\frac{1}{Y}\right) = 1$, $T + \frac{1}{T} = Y$ has two solutions in $M \setminus \{1\}$.

Impacts of the resolution of our main equation

- (1) A short-proof APN-ness property of Kasami functions (in 2021)
- (2) A proof of the bijectivity property of an "exceptional" cryptographic family of quadrinomials discovered in 2019 from [Perrin, Udovenko, Biryukov, Crypto'2016] (in 2022)
- (3) Solving the equation $X^{2^{3n}+2^{2n}+2^n-1} + (X+1)^{2^{3n}+2^{2n}+2^n-1} = b$ in $\mathbb{F}_{2^{4n}}$ and an alternative proof of a conjecture on the differential spectrum of the related monomial functions (in 2023)

(1) A direct proof of the APN-ness property of Kasami functions

Kasami (APN) function : $F(X) = X^{q^2-q+1}$, $q = 2^k$, $\gcd(k, n) = 1$

Recall that F is said to be *almost perfect nonlinear* (APN) if for every $a \in \mathbb{F}_{2^n}{}^*$ and every $b \in \mathbb{F}_{2^n}$, the equation $F(x) + F(x + a) = b$ has 0 or 2 solutions.

A power function $F(X) = X^d$ is APN if and only if, for every $b \in \mathbb{F}_{2^n}$ the system

$$\begin{cases} X + Y & = 1 \\ X^d + Y^d & = b \end{cases} \tag{12}$$

has at most one pair $\{X, Y\}$ of solutions in $\mathbb{F}_{2^n}$

(1) A direct proof of the APN-ness property of Kasami functions

Let n odd, $F = G_2 \circ G_1^{-1}$ where $G_1(X) = X^{q+1}$ and $G_2(x) = X^{q^3+1}$.

Equation (12) is equivalent to

$$\begin{cases} x^{q+1} + y^{q+1} & = 1 \\ x^{q^3+1} + y^{q^3+1} & = b \end{cases} \tag{13}$$

Theorem : System (13) has at most one pair $\{x, y\}$ of solutions proving that F is APN ([Carlet, Kim, SM, DCC 2021])

Sketch of the proof : Letting $y = x + z$, $v = z^{q^2-1}$ and $c = b + 1$,

- Proving Equation (13) has at most one pair $\{x, y\}$ of solutions is equivalent to proving that $(\star\star)$ has at most one solution v when $(\star)$ has solutions :

$$\begin{cases} \left(\frac{x}{z}\right)^q + \left(\frac{x}{z}\right) & = \frac{1}{v^{\frac{1}{q-1}}} + 1 \quad (\star) \\ (v+1)^{q+1} + cv & = 0 \quad (\star\star) \end{cases}$$

  for every $c \in \mathbb{F}_{2^n}$.

- For every $c \in \mathbb{F}_{2^n}$, the cubic equation $(v+1)^{q+1} + cv = 0$ has at most one solution v in $\mathbb{F}_{2^n}$ such that $Tr_1^n\left(\frac{1}{v^{\frac{1}{q-1}}} + 1\right) = 0$.

(2) A proof of the bijectivity property of an "exceptional" cryptographic family of quadrinomials

In Crypto'2016, [Perrin, Udovenko, Biryukov, 2016] discovered the butterfly structure (that contains the Dillon APN permutation of six variables), later generalized [Canteaut, Perrin, Tian, 2019], which turns out to be a powerful approach that generates infinite families of cryptographic functions with best-known nonlinearity and differential properties.

Let m odd, k odd, $\gcd(m,k)=1$, $Q=2^m$, $q=2^k$

$$f_{\underline{\epsilon}}(X) := \epsilon_1 \overline{X}^{q+1} + \epsilon_2 \overline{X}^q X + \epsilon_3 \overline{X} X^q + \epsilon_4 X^{q+1}, \quad \overline{X} = X^Q \tag{14}$$

where

$$\underline{\epsilon} = (\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4) = \begin{cases} (\varepsilon_3,\varepsilon_4,\varepsilon_1,\varepsilon_2), & \text{if } k \text{ is odd} \\ (\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4), & \text{if } k \text{ is even,} \end{cases} \in \mathbb{F}_Q^4 \tag{15}$$

and ($\alpha,\beta \in \mathbb{F}_Q$.)

$$\begin{cases} \varepsilon_1 = \alpha^q + \alpha + 1 \\ \varepsilon_2 = \alpha^{q+1} + \alpha + \beta + 1 \\ \varepsilon_3 = \alpha^{q+1} + \alpha^q + \beta + 1 \\ \varepsilon_4 = \alpha^{q+1} + \alpha^q + \alpha + \beta \end{cases} \tag{16}$$

(2) A proof of the bijectivity property of an "exceptional" cryptographic family of quadrinomials

[Li, Li, Helleseth, Qu, 2021]

$\varphi_1 = \epsilon_1\epsilon_3 + \epsilon_2\epsilon_4$, $\varphi_2 = \epsilon_1\epsilon_2 + \epsilon_3\epsilon_4$, $\varphi_3 = \epsilon_1^2 + \epsilon_4^2$,
$\varphi_4 = \epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2 + \epsilon_4^2$

$$\Gamma_0 = \left\{ \underline{\epsilon} \text{ is given by (15) and (16)} \mid \varphi_4 \neq 0, \left(\frac{\varphi_2}{\varphi_4}\right)^q = \frac{\varphi_1}{\varphi_4} \right\}. \quad (17)$$

Theorem (Sufficiency condition) : $f_{\underline{\epsilon}}(X)$ is a permutation on $\mathbb{F}_{Q^2}$ with boomerang uniformity 4 if $\underline{\epsilon} \in \Gamma_0$

Conjecture (Necessity condition) : $f_{\underline{\epsilon}}(X)$ a permutation on $\mathbb{F}_{Q^2}$ with boomerang uniformity 4 only if $\underline{\epsilon} \in \Gamma_0$

(2) A proof of the bijectivity property of an "exceptional" cryptographic family of quadrinomials

[Kim, SM, Choe, Lee, Lee, Jo, DCC 2022]

Problem : Identify $\Gamma = \{\underline{\epsilon} \in \mathbb{F}_Q^4 \mid f_{\underline{\epsilon}}(X) \text{ a permutation on } \mathbb{F}_{Q^2}\}$.

Question : $\Gamma = \Gamma_0$?

$\mu_{Q+1} = \{x \in \mathbb{F}_{Q^2} \mid x^{Q+1} = 1\}$

Proposition : $f_{\underline{\epsilon}}(X)$ is a permutation of $\mathbb{F}_{Q^2}$ if and only if $g_{\underline{\epsilon}}(X) = X^{q+1} h_{\underline{\epsilon}}(X)^{Q-1}$ is a permutation of $\mu_{Q+1} \setminus \{1\}$ where $h_{\underline{\epsilon}}(X) = \epsilon_1 X^{q+1} + \epsilon_2 X^q + \epsilon_3 X + \epsilon_4$.

Idea of the proof :

- $f_{\underline{\epsilon}}(X) = X^{q+1} h_{\underline{\epsilon}}(X^{Q-1})$
- Since $\gcd(q+1, Q-1) = 1$, $X^{q+1} h_{\underline{\epsilon}}(X^{Q-1})$ is a permutation of $\mathbb{F}_{Q^2}$ if and only if $g_{\underline{\epsilon}}(X) = X^{q+1} h_{\underline{\epsilon}}(X)^{Q-1}$ is a permutation of $\mu_{Q+1} = \{x \in \mathbb{F}_{Q^2} \mid x^{Q+1} = 1\}$ [Zieve, 2009].
- $g_{\underline{\epsilon}}(1) = 1$.

(2) A proof of the bijectivity property of an "exceptional" cryptographic family of quadrinomials

[Kim et *al.*, DCC 2022] :

- $\mu_{Q+1} \setminus \{1\} = \{\frac{y+1+\gamma}{y+\gamma} \mid y \in \mathbb{F}_Q\}$, $\gamma \in \mathbb{F}_{Q^2} \setminus \mathbb{F}_Q$, $\gamma^2 = \gamma + 1$.
- Γ is the subset of $\mathbb{F}_Q^4$ of all $\underline{\epsilon}$ such that equation

$$g_{\underline{\epsilon}}\left(\frac{y+1+\gamma}{y+\gamma}\right) = \frac{a+1+\gamma}{a+\gamma} \tag{18}$$

has a unique solution y in $\mathbb{F}_Q$ for every $a \in \mathbb{F}_Q$

(2) A proof of the bijectivity property of an "exceptional" cryptographic family of quadrinomials

Linking to "cubic" equations : Introducing polynomials $R_{\underline{\epsilon}}$, $S_{\underline{\epsilon}}$ and $T_{\underline{\epsilon}}$ in $\mathbb{F}_Q[X]$ whose coefficients depends on $\underline{\epsilon}$, we prove

- When $((R_{\underline{\epsilon}}(a))^q + S_{\underline{\epsilon}}(a) = 0$, Equation (18) has two solutions in $\mathbb{F}_Q$.
- When $((R_{\underline{\epsilon}}(a))^q + S_{\underline{\epsilon}}(a) \neq 0$, Equation (18) has one solution in $\mathbb{F}_Q$ if and only if

$$Y^{q+1} + Y + U_{\underline{\epsilon}}(a) = 0 \tag{19}$$

has one solution in $\mathbb{F}_Q$ where
$Y = ((R_{\underline{\epsilon}}(a))^q + S_{\underline{\epsilon}}(a))^{-1}(y^q + R_{\underline{\epsilon}}(a))$ and $U_{\underline{\epsilon}}(a) = \frac{(R_{\underline{\epsilon}}(a)S_{\underline{\epsilon}}(a)+T_{\underline{\epsilon}}(a))^q}{(R_{\underline{\epsilon}}(a)^q+S_{\underline{\epsilon}}(a))^{q+1}}$.

(2) A proof of the bijectivity property of an "exceptional" cryptographic family of quadrinomials

Proposition :
$\Gamma = \left\{ \epsilon \in \mathbb{F}_Q^4 \mid \varphi_4 \neq 0, \left(\frac{\varphi_2}{\varphi_4}\right)^q = \frac{\varphi_1}{\varphi_4}, \mathrm{Tr}_1^m\left(\frac{\varphi_3}{\varphi_4}\right) = 1 + k \right\} \supsetneq \Gamma_0$

Theorem [Kim et *al.* 2022] :
$f_{\underline{\epsilon}}(X)$ a permutation on $\mathbb{F}_{Q^2}$ if and only if $\underline{\epsilon} \in \Gamma$.

Corollary [Kim, SM, Kim, Jo (2022)] : $f_{\underline{\epsilon}}(X)$ a permutation on $\mathbb{F}_{Q^2}$ with Boomerang uniformity 4 if and only if $\underline{\epsilon} \in \Gamma_0$.

Proposition [Kim, SM, Kim, Jo (2022)] :
$\Gamma \setminus \Gamma_0 = \left\{ \underline{\epsilon} \in \Gamma \mid \mathrm{Tr}_1^m\left(\frac{\varphi_2 \varphi_2{}^Q}{\varphi_4^2}\right) = 1 \right\}$.

Conclusion

Still much to do concerning the resolution of equations over finite fields !

Some open problems (amount many others) :

- Solve the equations in the form $F(x) + F(x+1) = b$, where F is a power functions of finite fields in characteristic 2.
- Study the boomerang uniformity of known functions F whose $\delta(F) = 4$.