Also, Additionally, Furthermore, Moreover, In addition to, as well as, Particularly, Especially, For instance, To this end, Regarding, As for, With regards to, similarly, Equally, In the same way, Specifically, namely, That is, In other words, To put it another way, Conversely, Whereas, Indeed, Significantly,

Proof: no

Finite Field

Hilbert 90 We have $\mathrm{tr}_1^k(x) = 0$ for $x \in \mathbb{F}_{2^k}$ iff there exist some $y \in \mathbb{F}_{2^k}$ with $x = y^2 + y$.

Theorem[3] The cubic equation $x^3 + x + a = 0$, $a \in \mathbb{F}_{2^k}^*$ has a unique solution iff $\mathrm{tr}_1^k(a^{-1}) \neq \mathrm{tr}_1^k(1)$.

Theorem[3] A necessary and suffcient condition that all three roots of the cubic equation $x^3 + x + a = 0$ lie in $\mathbb{F}_{2^k}$ is that $P_k(a) = 0$ where the polynomials $P_k(x)$ may be defined recursively by the equations

$$P_1(x) = P_2(x) = x$$
$$P_k(x) = P_{k-1}(x) + x^{2^{k-3}} P_{k-2}(x).$$

Number Theory[41]

Lemma 1 *For* $1 \leq e \leq m$,

$$\gcd(2^e + 1, 2^m - 1) = \begin{cases} 1, & \text{if } \gcd(2e, m) = \gcd(e, m) \\ 2^{\gcd(e,m)} + 1, & \text{if } \gcd(2e, m) = 2\gcd(e, m) \end{cases}$$

AES Acceleration

Now we give the process of inversion of $A = a_0 Y + a_1 Y^{16} \in \mathbb{F}_{2^8}$, where $a_0, a_1 \in \mathbb{F}_{2^4}$:

1. Assume (W, W^2) to be the basis of $\mathbb{F}_{2^2}$, (Z^2, Z^8) to be the basis of $\mathbb{F}_{2^4}$, and (Y, Y^{16}) the basis of $\mathbb{F}_{2^8}$.

2. The method to calculate the inversion of A is $A^{-1} = (AA^{16})^{-1}A^{16} = ((a_0 + a_1)^2 WZ + a_0 a_1)^{-1}(a_1 Y + a_0 Y^{16})$.

The idea in the method: We need to obtain the results of $T_1 = (a_0 + a_1); T_2 = (WZ)(T_1)^2; T_3 = a_0 a_1; T_4 = T_2 + T_3; T_5 = (T_4)^{-1}; T_6 = T_5 a_1; T_7 = T_5 a_0$. Note that all the calculation is based on $\mathbb{F}_{2^4}$, which implies we acts on the vectors of length 4.

1. T_1 and T_4 are vectorial addition.

2. T_2 is the scalar multiplication, using the matrix $P = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$.

3. T_3, T_6 and T_7 are vectorial multiplication, and we need to define vectorial multiplication $z = x \star y$ in the following.

4. T_5 is the inversion over finite field in hardware, and the inversion is showed in below.

Vectorial multiplication: $z = (z_0, z_1, z_2, z_3) = x \star y = (x_0, x_1, x_2, x_3) \star (y_0, y_1, y_2, y_3)$:

$$\begin{aligned} z_0 &= x_1y_1 + (x_0 + x_2)(y_0 + y_2) + x_3y_2 + x_2y_3 + x_0y_3 + x_3y_0 + x_1y_2 + x_2y_1 \\ z_1 &= x_0y_0 + (x_0 + x_2)(y_0 + y_2) + x_0y_1 + x_1y_0 + (x_1 + x_3)(y_1 + y_3) \\ z_2 &= x_3y_3 + (x_0 + x_2)(y_0 + y_2) + x_0y_1 + x_1y_0 + x_0y_3 + x_3y_0 + x_1y_2 + x_2y_1 \\ z_3 &= x_2y_2 + (x_0 + x_2)(y_0 + y_2) + x_3y_2 + x_2y_3 + (x_1 + x_3)(y_1 + y_3), \end{aligned}$$

after some calculation, we have another form of 10 multiplication,

$$\begin{aligned} z_0 &= (x_1 + x_2)(y_1 + y_2) + (x_0 + x_2)(y_0 + y_2) + (x_2 + x_3)(y_2 + y_3) + (x_0 + x_3)(y_0 + y_3) + x_0y_0 \\ z_1 &= (x_1 + x_3)(y_1 + y_3) + (x_0 + x_2)(y_0 + y_2) + (x_0 + x_1)(y_0 + y_1) + x_1y_1 \\ z_2 &= (x_0 + x_3)(y_0 + y_3) + (x_0 + x_2)(y_0 + y_2) + (x_0 + x_1)(y_0 + y_1) + (x_1 + x_2)(y_1 + y_2) + x_2y_2 \\ z_3 &= (x_1 + x_3)(y_1 + y_3) + (x_0 + x_2)(y_0 + y_2) + (x_2 + x_3)(y_2 + y_3) + x_3y_3. \end{aligned}$$

Inversion: $y = (y_0, y_1, y_2, y_3) = x^{-1} = (x_0, x_1, x_2, x_3)^{-1}$ has 8 multiplication:

$$\begin{cases} -y_0 = x_1x_2x_3 + x_0x_2 + x_1x_2 + x_2 + x_3 \\ -y_1 = x_0x_2x_3 + x_0x_2 + x_1x_2 + x_1x_3 + x_3 \\ -y_2 = x_1x_0x_3 + x_0x_2 + x_0x_3 + x_0 + x_1 \\ -y_3 = x_1x_2x_0 + x_0x_2 + x_0x_3 + x_1x_3 + x_1 \end{cases}$$

The reuseness of some intermediate variables can decrease the times of multiplication (5 multiplication):

$$\begin{cases} -y_1 = (x_0x_2 + x_1)(x_2 + x_3) + x_3 \\ -y_3 = (x_0x_2 + x_3)(x_0 + x_1) + x_1 \\ -y_0 = (x_0x_2 + y_1)x_3 + y_1 + x_2 + x_3 \\ -y_2 = (x_0x_2 + y_3)x_3 + y_3 + x_0 + x_1. \end{cases}$$

List all T_i:

$$a_0 = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}, a_1 = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix}, T_1 = x + y = \begin{pmatrix} x_0 + y_0 \\ x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix}.$$

$$T_2 = \begin{pmatrix} x_1+y_1+x_3+y_3 \\ x_0+y_0+x_2+y_2 \\ x_0+y_0+x_1+y_1 \\ x_1+y_1 \end{pmatrix}.$$

$T_3 =$

$$\begin{pmatrix} (x_1+x_2)(y_1+y_2)+(x_0+x_2)(y_0+y_2)+(x_2+x_3)(y_2+y_3)+(x_0+x_3)(y_0+y_3)+x_0y_0 \\ (x_1+x_3)(y_1+y_3)+(x_0+x_2)(y_0+y_2)+(x_0+x_1)(y_0+y_1)+x_1y_1 \\ (x_0+x_3)(y_0+y_3)+(x_0+x_2)(y_0+y_2)+(x_0+x_1)(y_0+y_1)+(x_1+x_2)(y_1+y_2)+x_2y_2 \\ (x_1+x_3)(y_1+y_3)+(x_0+x_2)(y_0+y_2)+(x_2+x_3)(y_2+y_3)+x_3y_3 \end{pmatrix}$$

$T_4 = T_2 + T_3 =$

$$\begin{pmatrix} (x_1+x_2)(y_1+y_2)+(x_0+x_2)(y_0+y_2)+(x_2+x_3)(y_2+y_3)+(x_0+x_3)(y_0+y_3)+x_0y_0+x_1+y_1+x_3+y_3 \\ (x_1+x_3)(y_1+y_3)+(x_0+x_2+1)(y_0+y_2+1)+(x_0+x_1)(y_0+y_1)+x_1y_1+1 \\ (x_0+x_3)(y_0+y_3)+(x_0+x_2)(y_0+y_2)+(x_0+x_1+1)(y_0+y_1+1)+(x_1+x_2)(y_1+y_2)+x_2y_2+1 \\ (x_1+x_3)(y_1+y_3)+(x_0+x_2)(y_0+y_2)+(x_2+x_3)(y_2+y_3)+x_3y_3+x_1+y_1 \end{pmatrix}$$

Difficult

Lylia APN function[7]

$$\left(x+Tr_1^n\left(x^{2^i+1}\right)\right)^{2^i+1}$$

has covered all APN function(when $n=8$)

$$\left(x+Tr_1^n\left(x^{2^i+1}\right)\right)^{2^j+1}$$

where $1 \le i \ne j \le n-1$ and n is even. So we guess all functions like this form have been covered.

$$\left(x+Tr_1^n\left(x^{2^i+1}\right)\right)^{2^{2j}-2^j+1}$$

also are CCZ-equivalent to Kasami APN function.

1. EA-equivalent functions are CCZ-equivalent
2. if a function F is a permutation then F is CCZ-equivalent to F^{-1}[18]
3. CCZ-equivalence coincides with
   (a) EA-equivalence for planar functions [36, 38];
   (b) linear equivalence for DO planar functions [36, 38];
   (c) EA-equivalence for all functions whose derivatives are surjective [36];
   (d) EA-equivalence for all Boolean functions [24];
   (e) EA-equivalence for all vectorial bent Boolean functions [25];

(f) EA-equivalence for two quadratic APN functions (conjectured by Edel, proven by Yoshiara [145]).

Theorem 1 (Carlet, Charpin, Zinoviev 1998) *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $F(0) = 0$ and u be a primitive element of $\mathbb{F}_{2^n}$. Then F is APN iff the binary linear code C_F defined by the parity check matrix*

$$H_F = \begin{bmatrix} u & u^2 & \cdots & u^{2^n-1} \\ F(u) & F(u^2) & \cdots & F(u^{2^n-1}) \end{bmatrix}$$

has minimum distance 5.

Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are CCZ equivalent iff G_F and G_G are affine-equivalent,

i.e. if the extended codes with parity check matrices $\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & u & \cdots & u^{2^n-1} \\ F(0) & F(u) & \cdots & F(u^{2^n-1}) \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & u & \cdots & u^{2^n-1} \\ G(0) & G(u) & \cdots & G(u^{2^n-1}) \end{bmatrix}$ are equivalent.

Theorem 2 *Let $k \in \mathbb{Z}^+$, $\epsilon > 0$. Let $P : \mathbb{F}_2^n \to \mathbb{F}_2$ be a polynomial of degree at most k, and $f : \mathbb{F}_2^n \to \mathbb{R}$. Suppose $|\mathbb{E}_x \left[f(x)(-1)^{P(x)} \right]| \geq \epsilon$, then $\|f\|_{U_{k+1}} \geq \epsilon$.*

The converse of Theorem 2 is also true for $k = 1, 2$.

In 2003, algebraic attacks to LFSRs based on stream ciphers, by finding a way of solving the over defined system of multivariate equations whose unknowns are the secret key bits, were proposed by Courtois and Meier[1]. In 2004, the algebraic immunity of a Boolean function, representing its ability to resist this type of attacks, was introduced by Meier[2].

Let $n = 2k$ and $\mathbb{F}_{2^n} = \mathbb{F}_{2^k}^2$. For any $\beta \in \mathbb{F}_{2^k}$ with $\mathrm{Tr}_1^k(\beta) = 1$, then any element X of $\mathbb{F}_{2^n}$ can be written as $X = x + \mu y$ where $x, y \in \mathbb{F}_{2^k}$ and μ is a root of the equation $\mu^2 + \mu + \beta = 0$ over $\mathbb{F}_{2^n}$. Thus, the inverse function X^{2^n-2} can be decomposed (using $(x + \mu y)(x' + \mu y') = 1$ and $0 + 0y = 0 \in \mathbb{F}_{2^n}$ or computing $(x + \mu y)^{2^n-2}$, see for examples [**?**] and [**?**, Theorem 5]) as $\big(x, y\big) \mapsto \big(x(y^2 + xy + \beta x^2)^d, (x + y)(y^2 + xy + \beta x^2)^d\big)$ ((x, y) should be (y, x)), where $d = 2^k - 2$ (clearly such mapping is bijective and is CCZ-equivalent to the inverse function over $\mathbb{F}_{2^n}$). Experiments show that when d has the form 2^i this mapping is a differentially 4-uniform bijection for some integers n and

[1] Courtois N., Meier W.: Algebraic Attacks on Stream Ciphers with Linear Feedback EUROCRYPT 2003, LNCS, vol. 2656, pp. 345-359. Springer, Heidelberg (2003).

[2] Meier W., Pasalic E., Carlet C.: Algebraic attacks and decomposition of Boolean functions. In: Advances in Cryptology-EUROCRYPT 2004, LNCS, vol. 3027, pp. 474-491. Springer, Heidelberg (2004)

i. We now express this mapping with the univariate representation. Assume that μ is a root of the $\mu^2+\mu+\beta=0$ over $\mathbb{F}_{2^n}$. Then the mapping $(x,y)\mapsto (x(y^2+xy+\beta x^2)^d, (x+y)(y^2+xy+\beta x^2)^d)$ can be written as $x+\mu y \mapsto x(y^2+xy+\beta x^2)^d+\mu(x+y)(y^2+xy+\beta x^2)^d$. We have $\mu^2=\mu+\beta, \mu^4=\mu+\beta+\beta^2, \mu^8=\mu+\beta+\beta^2+\beta^4, \cdots, \mu^{2^k}=\mu+\mathrm{Tr}_1^k(\beta)$. Let $X=x+\mu y$. We have $X^{2^k}=x^{2^k}+\mu^{2^k}y^{2^k}=x+(\mu+1)y=X+y$ and so $y=X+X^{2^k}$. We have $x=X+\mu y=X+\mu(X+X^{2^k})=(\mu+1)X+\mu X^{2^k}$. By taking $d=2^i$, we could obtain the function F defined over $\mathbb{F}_{2^n}$ with the univariate representation, which is given in (1).

Let $n=2k$. For any $\beta\in\mathbb{F}_{2^k}$ with $\mathrm{Tr}_1^k(\beta)=1$ (so $\mathrm{Tr}_1^n(\beta)=0$), μ is a root of the equation $\mu^2+\mu+\beta=0$ over $\mathbb{F}_{2^n}$.

$$y^2+xy+\beta x^2=(\beta+1)(\beta+\mu)x^2+(\beta+\mu+1)(\beta+1)x^{2^{k+1}}+x^{2^k+1}.$$

$$x+\mu(x+y)=(\beta+1)x+(\beta+\mu)x^{2^k}$$

Then we define a polynomial over $\mathbb{F}_{2^n}$ as follows:

$$\begin{aligned} F(x) &= (1+\beta)^2x^{2^{k+i+1}+1}+(1+\beta)^2x^{2^{i+1}+1}+(1+\beta)x^{2^{k+i}+2^i+1} \\ &\quad +(\beta+\mu)(\beta+1)x^{2^{k+i+1}+2^k}+(\beta+\mu)(\beta+1)x^{2^{i+1}+2^k}+(\beta+\mu)x^{2^{k+i}+2^i+2^k}. \end{aligned} \tag{1}$$

We now consider the equation $\mu^2+\mu+\beta=0$. Note that $\mathrm{Tr}_1^k(\beta)=\mathrm{Tr}_1^k(\mu^2+\mu)=\mu+\mu^{2^k}$. If we want to get $\mathrm{Tr}_1^k(\beta)=1$ with $\beta\in\mathbb{F}_{2^k}$ then we only need to find an element $\mu\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^k}$ such that $\mu+\mu^{2^k}=1$. Assume that $\mu=x+\alpha y$ (α is a primitive element of $\mathbb{F}_{2^n}$ and clearly we have $\alpha\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^k}$; indeed, primitive element α can replaced by any element in $\alpha\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^k}$), we have $\mu+\mu^{2^k}=y(\alpha+\alpha^{2^k})=1$ and thus $y=(\alpha+\alpha^{2^k})^{2^n-2}\in\mathbb{F}_{2^k}$ since $(\alpha+\alpha^{2^k})^{2^k}=(\alpha+\alpha^{2^k})$. Thus μ can take $\alpha(\alpha+\alpha^{2^k})^{2^n-2}=\frac{\alpha}{\alpha+\alpha^{2^k}}$. Thus we have $\beta=\frac{\alpha}{\alpha+\alpha^{2^k}}+\frac{\alpha^2}{(\alpha+\alpha^{2^k})^2}=\frac{\alpha^{2^k+1}}{(\alpha+\alpha^{2^k})^2}\in\mathbb{F}_{2^k}$ (we also need to assume that $\beta\neq 1$ since (1), for doing this we only need to check that β is a generator of $\mathbb{F}_{2^k}^*$). So the conditions become: 1) any $\alpha\in\mathbb{F}_{2^n}$ such that $\alpha+\alpha^{2^k}\neq 1$ and $\frac{\alpha^{2^k+1}}{(\alpha+\alpha^{2^k})^2}\neq 1$; 2) $\mu=\alpha(\alpha+\alpha^{2^k})^{2^n-2}=\frac{\alpha}{\alpha+\alpha^{2^k}}$ in (1); 3) $\beta=\frac{\alpha^{2^k+1}}{(\alpha+\alpha^{2^k})^2}$. How to choose i to ensure F is a differentially 4-uniform bijection?

Another way to rewrite (1) is as follows: For $n=2k$, $\mu\in\mathbb{F}_{2^n}$ is such that $\mu+\mu^{2^k}=1$, $\mu+\mu^2\neq 1$ ($\mu+\mu^2\neq 1$ is equivalent to $\mu\notin\mathbb{F}_4$; we have $\mu+\mu^{2^k}=1$ implies that $\mu\notin\mathbb{F}_{2^k}$), and $\mu+\mu^2\in\mathbb{F}_{2^k}$. Let $\beta=\mu+\mu^2$ (this implies that $\mathrm{Tr}_1^k(\beta)=\mu+\mu^{2^k}=1$). Then we define a polynomial over $\mathbb{F}_{2^n}$ as follows:

$$\begin{aligned} F(x) &= (1+\beta)^2x^{2^{k+i+1}+1}+(1+\beta)^2x^{2^{i+1}+1}+(1+\beta)x^{2^{k+i}+2^i+1} \\ &\quad +(\beta+\mu)(\beta+1)x^{2^{k+i+1}+2^k}+(\beta+\mu)(\beta+1)x^{2^{i+1}+2^k}+(\beta+\mu)x^{2^{k+i}+2^i+2^k}. \end{aligned} \tag{2}$$

How to choose i?

Simulations for (1):

- For $n = 6$, we take $\beta = 1$ and $i = 2$ have $F(x)$ is CCZ-equivalent to x^{11} and x^{23}.
- For $n = 10$, we take β such that $\mathrm{Tr}_1^5(\beta) = 1$ and $i = 0$ (then F is quadratic) have $F(x)$ is differentially 4-uniform bijection. $F(x)$ is CCZ-inequivalent to x^3. We must consider if this function is CCZ-equivalent to x^{2^k+2} since all terms include z^3 ($z \in \mathbb{F}_{2^k}$) when decomposing this function in to $\mathbb{F}_{2^k}^2$ ($2^k + 2 = 3 \pmod{2^k - 1}$).
- For $n = 12$, by taking β such that $\mathrm{Tr}_1^6(\beta) = 1$ and $d = 2^i = 8$, then $F(x)$ is a differentially 4-uniform bijection.

The quadratic case with four terms (i.e. $i = 0$):

For $n = 2k$ (k odd), $\mu \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ is such that $\mu + \mu^{2^k} = 1$. Let $i = 0$, we have

$$\begin{aligned} F(x) &= (1+\beta+\beta^2+\mu)x^{2^{k+1}+1} + (1+\beta^2)x^3 + (1+\beta^2+\mu\beta+\mu)x^{2^k+2} \\ &\quad +(\beta^2+\beta+\mu\beta+\mu)x^{3\cdot 2^k} \\ &= (1+\mu^4)x^{2^{k+1}+1} + (1+\mu+\mu^3+\mu^4)x^{2^k+2} + (\mu^2+\mu^3+\mu^4)x^{3\cdot 2^k} + (1+\mu^2+\mu^4)x^3 \end{aligned}$$

F is a quadratic bijection over $\mathbb{F}_{2^n}$, we checked by $n = 6, 10, 14, 18, 22$ and this function may be CCZ-equivalent to x^3.

Remark 1 *Indeed, the function $(x + ax + bx^{2^k})^3$ includes similar polynomials and the bijections in [?, ?]. and the functions in [?]. The bijections in [?, Theorem 1-(2)] are included in class Γ_1 in [?] which have boomerang uniformity four. It seems that these bijections can be given by the function $(x+ax+bx^{2^k})^3$. Some recent results in [?, ?]-[?].*

APN Functions

Until now, only a single instance of an APN permutation in even dimension is known, namely for $n = 6$[6]:

$$K : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}, \quad x \mapsto x^3 + x^{10} + gx^{24},$$

where g is an element in $\mathbb{F}_{2^6}^*$ with minimal polynomial $X^6 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[X]$.

We know that two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent[60].

In [2], compared to the 8192 previously-known APN instances, authors found 12733 new CCZ-inequivalent quadratic APN functions in dimension $n = 8$. They also presented 35 and 5 new APN instances in dimension $n = 9$ and

Table 1: All Known APN monomials over $\mathbb{F}_{2^n}$

Family	Function	Conditions	Ref.
Gold	z^{2^i+1}	$\gcd(i,n)=1$	[31]
Kasami	$z^{2^{2i}-2^i+1}$	$\gcd(i,n)=1$	[36]
Welch	z^{2^t+3}	$n=2t+1$	[21]
Niho-1	$z^{2^t+2^{t/2}-1}$	$n=2t+1, t$ even	[20]
Niho-2	$z^{2^t+2^{(3t+1)/2}-1}$	$n=2t+1, t$ odd	[20]
Inverse	$z^{2^{2t}-1}$	$n=2t+1$	[44]
Dobbertin	$z^{2^{4i}+2^{3i}+2^{2i}+2^i-1}$	$n=5i$	[22]

$n=10$, respectively. Remarkably, two new 9-bit APN permutations are given in univariate representation over $\mathbb{F}_{2^9}$ by

$$x \mapsto x^3 + ux^{10} + u^2x^{17} + u^4x^{80} + u^5x^{192},$$
$$x \mapsto x^3 + u^2x^{10} + ux^{24} + u^4x^{80} + u^5x^{136},$$

where $u \in \mathbb{F}_{2^9}^*$ is an element with minimal Ploynoimal $X^3 + X + 1 \in \mathbb{F}_2[X]$.

Remark 2 *Fortunately, Kangquan Li and Nikolay Kaleyski in [37] have generalized above two new 9-bit APN permutations into two infinite families:*

Assume $\gcd(i,m)=1$ *and* $q=2^i$*, for* $(x,y,z) \in \mathbb{F}_{2^m}^3$*, we have*

$$F(x,y,z) = (x^{q+1} + x^qz + yz^q, x^qz + y^{q+1}, xy^q + y^qz + z^{q+1}),$$
$$F(x,y,z) = (x^{q+1} + xy^q + yz^q, xy^q + z^{q+1}, x^qz + y^{q+1} + y^qz)$$

are two APN over $\mathbb{F}_{2^m}^3$ *with some complex restriction. They are semi-bent functions.*

Yuyin Yu and Léo Perrin in [61] present another 5412 new quadratic APN functions. Thus, the number of CCZ-inequivalent quadratic APN functions in dimension 8 increases to 26525 (up to April 30, 2021).

1. $x^3 + \omega x^{36}$, $\omega \in \{u\mathbb{F}_{2^5}^*\} \cup \{u^2\mathbb{F}_{2^5}^*\}$ where $u \in \mathbb{F}_{2^5}^*$ of order 3 in theorem 2 of [24]

2. Let s and k be positive integers with $\gcd(s,3k)=1$ and let $t \in \{1,2\}$, $i=3-t$. Let further $a=2s+1$ and $b=2^{ik}+2^{tk+s}$ and let $\omega=\alpha^{2k}-1$ for a primitive element $\alpha \in \mathbb{F}_{2^{3k}}^*$. If $\gcd(2^{3k}-1,(b-a)/(2^k-1)) \neq \gcd(2^k-1,(b-a)/(2^k-1))$, the function $F:\mathbb{F}_{2^{3k}} \to \mathbb{F}_{2^{3k}}, x \mapsto x^a + \omega x^b$ is APN in theorem 1 of [10].

3. Let s and k be positive integers such that $s \leq 4k-1$, $\gcd(k,2) = \gcd(s,2k) = 1$, and $i = sk \bmod 4, t = 4-i$. Let further $a = 2^s+1$ and $b = 2^{ik}+2^{tk+s}$ and let $\omega = \alpha^{2^k-1}$ for a primitive element $\alpha \in \mathbb{F}_{2^{4k}}^*$. Then, the function $F:\mathbb{F}_{2^{4k}} \to \mathbb{F}_{2^{4k}}, x \mapsto x^a + \omega x^b$ is APN in theorem 2 of [10].

Table 2: All Known APN infinite families with univariate forms (non-monomials) over $\mathbb{F}_{2^n}$

No.	Function	Conditions	Ref.
F1- F2	$z^{2^s+1}+u^{2^k-1}z^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1$, $p\in\{3,4\}, i=sk \pmod p, m=p-i$, $n\geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[10]
F3	$sz^{q+1}+z^{2^i+1}+z^{q(2^i+1)}$ $+cz^{2^iq+1}+c^qz^{2^i+q}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q, z^{2^i+1}+cz^{2^i}+$ c^qz+1 has no solution z with $z^{q+1}=1$	[9]
F4	$z^3+a^{-1}\operatorname{Tr}_1^n(a^3z^9)$	$a\neq 0$	[11]
F5	$z^3+a^{-1}\operatorname{Tr}_1^n(a^3z^9+a^6z^{18})$	$3\mid n, a\neq 0$	[12]
F6	$z^3+a^{-1}\operatorname{Tr}_1^n(a^6z^{18}+a^{12}z^{36})$	$3\mid n, a\neq 0$	[12]
F7-F9	$uz^{2^s+1}+u^{2^m}z^{2^{-m}+2^{m+s}}+$ $vz^{2^{-m}+1}+wu^{2^m+1}z^{2^s+2^{m+s}}$	$n=3m, \gcd(m,3)=\gcd(s,3m)=1, v,w\in\mathbb{F}_{2^m}$ $vw\neq 1, 3\mid m+s, u$ primitive in $\mathbb{F}_{2^n}^*$	[5]
F10	$a^2z^{2^{2m+1}+1}+b^2z^{2^{m+1}+1}+$ $az^{2^{2m}+2}+bz^{2^m+2}+(c^2+c)z^3$	$n=3m, m$ odd, $L(z)=az^{2^{2m}}+bz^{2^m}+cz$ satisfies the conditions of Theorem 2	[8]
F11	$z^3+wz^{2^{i+1}}+w^2z^{3\cdot 2^m}$ $+z^{2^{i+m}+2^m}$	$n=2m, m$ odd, $3\nmid m$, w primitive in $\mathbb{F}_{2^2}, s=m-2, (m-2)^{-1} \pmod n$	[13]
F12	$a\operatorname{Tr}_1^n(bz^3)+a^q\operatorname{Tr}_1^n(b^3z^9)$	$n=2m, m$ odd, $q=2^m$, $a\notin\mathbb{F}_q$, b not a cube	[62]
F13	$L(z)^{2^m+1}+vz^{2^m+1}$	$\gcd(s,m)=1, v\in\mathbb{F}_{2^m}^*, \mu\in\mathbb{F}_{2^{3m}}^*$ $L(z)=z^{2^{m+s}}+z^{2^s}+z$ permutes $\mathbb{F}_{2^{3m}}$	[38]
F14	$u\left[(u^qx+x^qu)^{2^i+1}+(u^qx+x^qu)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}\right]$ $+(u^qx+x^qu)^{2^{2i}+1}+(u^qx+x^qu)^{2^{2i}}(x^q+x)+(x^q+x)^{2^{2i}+1}$	$q=2^m, n=2m, \gcd(3i,m)=1, u$ primitive in $\mathbb{F}_{2^*}^*$	
15	$u\left[(u^qx+x^qu)^{2^i+1}+(u^qx+x^qu)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}\right]$ $+(u^qx+x^qu)^{2^{3i}}(x^q+x)+(u^qx+x^qu)(x^q+x)^{2^{3i}}$	m odd, $q=2^m, n=2m, \gcd(3i,m)=1, u$ primitive in $\mathbb{F}_{2^n}^*$	

Table 3: Your caption.

No.	Function	Conditions	Ref.
F14	$(xy, x^{2^k+1} + \alpha x^{(2^k+1)2^i})$	$\gcd(k,m) = 1$, m even, α non-cubic	[63]
F15	$(xy, x^{2^{3k}+2^{2k}} + ax^{2^{2k}}y^{2^k} + by^{2^k+1})$	$\gcd(k,m) = 1$, P_1 no root in $\mathbb{F}_{2^m}$	[57]
F16	$(xy, x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$	m even, $\gcd(i,m) = 1$, P_2 no root in $\mathbb{F}_{2^m}$	[14]
F17	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}}y + y^{2^{2i}+1})$	$\gcd(3i,m) = 1$	[33]
F18	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + xy^{2^{3i}})$	$\gcd(3i,m) = 1$, m odd	[33]
F19	$(x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2)$	$\gcd(3,m) = 1$	[38]
F20	$(x^{q+1} + By^{q+1}, x^ry + \frac{a}{B}xy^r)$	$0 < k < m, q = 2^k, r = 2^{k+m/2}$, $m \equiv 2 \pmod 4, \gcd(k,m) = 1, a \in \mathbb{F}^*_{2^{m/2}}$, $B \in \mathbb{F}_{2^m}, B$ note a cube, $B^{q+r} \neq a^{q+1}$	[32]
F21	$(x^{q+1} + xy^q + \alpha y^{q+1}$, $x^{q^2+1} + \alpha x^{q^2}y + (1+\alpha)^q xy^{q^2} + \alpha y^{q^2+1})$	$k, m > 0, \gcd(k, m = 1), q = 2^k$, $\alpha \in \mathbb{F}_{2^m}, x^{q+1} + x + \alpha$ has no roots in $\mathbb{F}_{2^m}$	[15]
F22	$(x^3 + xy + xy^2 + \alpha y^3$, $x^5 + xy + \alpha x^2y^2 + \alpha x^4y + (1+\alpha)^2xy^4 + \alpha y^5)$	$\alpha \in \mathbb{F}_{2^m}, x^3 + x + \alpha$ has no roots in $\mathbb{F}_{2^m}$	[15]

4. Let k and s be odd integers with $\gcd(k,s)=1$. Let $b \in \mathbb{F}_{2^{2k}}$ which is not a cube, $c \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$ and $r_i \in \mathbb{F}_{2^k}$ for all $i \in \{1,...,k-1\}$, then the function $F : \mathbb{F}_{2^{2k}} \to \mathbb{F}_{2^{2k}}, x \mapsto bx^{2^s+1} + b^{2^k} x^{2^{k+s}+x^k+cx^{2^k+1}+\sum_{i=1}^{k-1} r_i x^{2^{i+k}+2^i}}$ is APN in Theorem 1 of [4]

5. Let k and s be positive integers such that $k+s = 0 \bmod 3$ and $\gcd(s,3k) = \gcd(3,k) = 1$. Let further $u \in \mathbb{F}^*_{2^{3k}}$ be primitive and let $v, w \in \mathbb{F}_{2^k}$ with $vw \neq 1$. Then, the function

$$F : \mathbb{F}_{2^{3k}} \to \mathbb{F}_{2^{3k}}$$
$$x \mapsto ux^{2^s+1} + u^{2^k} x^{2^{2k}+2^{k+s}} + vx^{2^{2k}+1} + wu^{2^k+1} x^{2^{k+s}+2^s}$$

is APN in Theorem 2.1 of [5]

6.

4.1 YU yuying QAM APN

Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, let $M_\alpha \in \mathbb{F}_{2^n}^{n\times n}$ be a matrix with $M_\alpha(i,u) = \alpha_u^{2^{i-1}}$, i.e.,

$$M_\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^{2^1} & \alpha_2^{2^1} & \cdots & \alpha_n^{2^1} \\ \alpha_1^{2^2} & \alpha_2^{2^2} & \cdots & \alpha_n^{2^2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2^{n-1}} & \alpha_2^{2^{n-1}} & \cdots & \alpha_n^{2^{n-1}} \end{pmatrix}.$$

Definition 1 *Let H be an $n \times n$ matrix over $\mathbb{F}_{2^n}$. H is called a quadratic APN matrix (QAM) if*

(1) H is symmetric and the elements in its main diagonal are zero.

(2) Every nonzero linear combination of the n rows (or "columns" because of H being symmetric) of H has rank $\mathrm{Rank}_{\mathbb{F}_2} = n-1$.

Theorem 3 *Let $F(x) = \sum_{1\le j<i\le n} c_{i,j} x^{2^{i-1}+2^{j-1}} \in \mathbb{F}_{2^n}[x]$ be a quadratic homogeneous functions and $H = M_\alpha^T C_F M_\alpha$, where*

$$C_F(i,j) = \begin{cases} c_{i,j}, & i > j \\ 0, & i = j \end{cases}$$

is a symmetric matrix and M_α is defined above. Then $F(x)$ is APN iff H is a QAM.

Remark 3 *(1) Let $P \in \mathbb{F}_2^{n\times n}$ be an invertible matrix and $H' = P^T H P$. Then H is a QAM iff H' is a QAM.*

(2) Let L be a linear permutation over $\mathbb{F}_{2^n}$ and $H' = (h'_{i,j}) \in \mathbb{F}_{2^n}^{n\times n}$ such that $h'_{i,j} = L(h(i,j))$. Then H is a QAM iff H' is a QAM.

Decomposition of $\mathbb{F}_{2^{2m}}$

The field extension $\mathbb{F}_{2^{2m}}$ over $\mathbb{F}_{2^m}$ has similarities with the extension $\mathbb{C}$ over $\mathbb{R}$. The unit circle of $\mathbb{F}_{2^{2m}}$ is the set

$$U = \left\{ u \in \mathbb{F}_{2^{2m}} : u^{2^m+1} = 1 \right\}$$

of all elements with norm 1. Note that $U \cap \mathbb{F}_{2^m} = \{1\}$.

Remark 4 *The range set of $c = u + u^{2^m}$ for $u \in U \setminus \{1\}$ can be characterized. Define*

$$\mathcal{H}_1 = \left\{ x \in \mathbb{F}_{2^m} : \mathrm{tr}_1^k(\frac{1}{x}) = 1 \right\}.$$

Then we have

$$\mathcal{H}_1 = \left\{ u + u^{2^m} : u \in U \setminus \{1\} \right\}.$$

More precisely, the mapping $u \to \mathrm{tr}_1^k(u)$ from $U \setminus \{1\}$ to $\mathcal{H}_1$ is onto, and $\mathrm{tr}_1^k(u) = \mathrm{tr}_1^k(v)$ iff $u = v$ or $u = v^{2^m}$ for $u, v \in U \setminus \{1\}$.

Denote $\mathcal{T}_1 = \left\{ x \in \mathbb{F}_{2^{2m}} \mid \mathrm{tr}_m^{2m}(x) = x^{2^m} + x = 1 \right\}$. We have, for $g \in \mathcal{T}_1$, $g + g^2 \in \mathbb{F}_{2^m}$ and $\mathrm{tr}_1^m(g + g^2) = 1$, since $(g + g^2)^{2^m} = g^{2^m}(g + 1)^{2^m} = (g + 1)g = g + g^2$ and $\mathrm{tr}_1^m(g + g^2) = g + g^{2^m} = 1$.

We can decompose the finite field $\mathbb{F}_{2^{2m}}$ as follows:

(1) $\mathbb{F}_{2^{2m}} = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, the simplest form.

(2) Polar-Coordinate Decomposition: $\mathbb{F}_{2^{2m}} = \mathbb{F}_{2^m} \times U$, where $U = \left\{ x^{2^m-1} \mid x \in \mathbb{F}_{2^{2m}} \right\}$ or $U = \left\{ x \in \mathbb{F}_{2^{2m}} \mid x^{2^m+1} = 1 \right\}$: since $2^{2m} - 1 = (2^m - 1)(2^m + 1)$ and $\gcd(2^m - 1, 2^m + 1) = 1$, we decompose $x \in \mathbb{F}_{2^{2m}}$ into the multiplication of two elements $\lambda \in \mathbb{F}_{2^m}, \varepsilon \in U$ with $\mathrm{ord}(\lambda) \mid 2^m - 1$ and $\mathrm{ord}(\varepsilon) \mid 2^m + 1$, respectively. This decomposition is frequently used in the proof of properties of Niho type exponents, since Niho type exponents $\mathrm{tr}_1^{2m}(x^d)$ are defined to be linear in $\mathbb{F}_{2^m}$, which means $d \equiv (2^m - 1)s + 2^i \pmod{2^{2m} - 1}$, and we always assume $i = 0$.

(3) Trace-0/Trace-1 Decomposition: $\mathbb{F}_{2^{2m}} = \mathbb{F}_{2^m} \times \mathcal{T}$, where Trace-0 is $\mathbb{F}_{2^m}$ due to $\mathrm{tr}_m^{2m}(x) = 0$ for all $x \in \mathbb{F}_{2^m}$ and Trace-1 means $\mathcal{T} = \mathcal{T}_1 \cup \{1\}$ in [34]. If $X \in \mathbb{F}_{2^{2m}}^*$ has two decomposition xg, yh, where $x, y \in \mathbb{F}_{2^m}^*$ and $g, h \in \mathcal{T}$, then $\mathrm{tr}_m^{2m}(xg) = \mathrm{tr}_m^{2m}(yh)$. And $\mathrm{tr}_m^{2m}(xg) = 0$ means $g = h = 1$, implying $x = y$, while $\mathrm{tr}_m^{2m}(xg) \neq 0$ means $x = y$, implying $h = g$.

Also in [34], with the help of Trace-0/Trace-1 Decomposition, we can derive a decomposition for Trace-0 hyperplane $\mathcal{H}_0$ of $\mathbb{F}_{2^{2m}}$: $\mathcal{H}_0 = \left\{ xg : x \in \mathcal{H}_0^{\mathbb{F}_{2^m}}, g \in \mathcal{T} \right\} \cup \mathbb{F}_{2^m}$, where $\mathcal{H}_0^{\mathbb{F}_{2^m}}$ is the Trace-0 hyperplane of $\mathbb{F}_{2^m}$. The idea is natural, that is, the Trace-0 hyperplane of $\mathbb{F}_{2^{2m}}$ must contain $\mathbb{F}_{2^m}$, besides, others must satisfy $\mathrm{tr}_1^m(x) = 0$ with $x = \mathrm{tr}_m^{2m}(y) = y + y^{2^m} \in \mathbb{F}_{2^m}^*$. Note that $y \in \mathbb{F}_{2^{2m}}$ can be decomposed by Trace-0/Trace-1 Decomposition, then $y = xg$, where $g \in \mathcal{T}$, can hold this property.

Nonlinearity Profile

Only Iwata and Kurosawa gave a class of Boolean functions with higher order nonlinearities in [35] before 2008. In 2008, Carlet[16] gives two lower bounds for the nonlinearity profile of a Boolean function by the nonlinearity profiles of its derivatives, along with nonlinearity profile of Maiorana-McFarland, Welch, Kasami and Inverse functions. In 2009, Sun and Wu deduce the lower bounds of the second-order nonlinearity of three classes of Boolean functions, all of three have high nonlinearity[51]. Meanwhile, Sarkar and Gangopadhyay determine a lower bound of the second-order nonlinearity of a new class of cubic Maiorana-McFarland bent functions[46]. Next year, Gangopadhyay et al. deduce the lower bounds of the second order nonlinearity of two types of Boolean functions[25]. In the same year, Gode and Gangopadhyay obtain a lower bound of the third-order nonlinearities of Kasami functions $\mathrm{tr}_1^n(\mu x^{57})$[29], the lower bound is sharper than those obtained by Carlet in [16]. Then in 2012, Garg and Khalyavin give tighten bounds on the nonlinearity profile of Kasami functions[27]. Then in [52], Sun and Wu give a lower bound of the second-order nonlinearity of a class of Boolean functions. And in 2011, Singh presents lower bounds of two classes of Boolean functions with high nonlinearities[48]. At the same time, Carlet[17] deduces the nonlinearity profile of the simplest Dillon's Partial Spread bent functions. Tang, Carlet and Tang[54] improve the lower bounds in [17] and obtain nonlinearity profile of a class of Maiorana-McFarland bent functions in 2013. And Li, Hu and Gao obtain a lower bounds on the second order nonlinearity of cubic monomial Boolean functions[39], which are better than the existing ones[28]. In the next year, Singh deduce the lower bounds on the third-order nonlinearities of two classes of biquadratic monomial Boolean functions over finite fields[47]. Note that Sun and Wu firstly give the higher-order nonlinearities of Niho type Boolean functions[53] in 2015. In 2016, Wang and Tan deduce a lower bounds on the nonlinearities of a special class of Boolean functions[58]. In 2017, Singh and Paul deduce the lower bounds on the second-order nonlinearities of a class of Boolean functions, and obtain lower bounds on 4th order nonlinearity of 10-variable monomial Partial Spreads $\phi(x) = \mathrm{tr}_1^{10}(\lambda x^{2^5-1})$ where $\lambda \in \mathbb{F}_{2^{10}}^*$[49]. At the same year, Gao and Tang propose a systematic approach for the lower bounds on the second-order nonlinearity of Maiorana-McFarland bent functions[26]. In 2019, Tang et al.[56] completely determine the distributions of the nonlinearities of the derivatives of a class of bent functions, and present a new lower bound on the second-order nonlinearity of this class of bent functions, which is better than the previous one. In 2020, Tang, Mandal and Maitra[55] derive cryptographic properties of the multiplicative inverse functions, and give the bounds related to their nonlinearity profile. At the same year, Yan and Tang improve the lower bounds on the second-order nonlinearity of three classes of Boolean functions[59]. And Liu[40] provide the tight lower bounds on the second-order nonlinearity of three classes of Boolean functions with high nonlinearities. Meanwhile, Sihem, Kwang and Myong[42] investigate an upper bound on the number of the rational zeros of any linearized polynomial over arbitary finite field, and get tighter estimations

of the lower bounds on the second-order nonlinearities of general cubic Boolean functions. In 2022, Singh et al. provide the lower bounds on 4th order nonlinearity of two classes of Boolean functions of degree 5[50]. Meanwhile, Saini and Garg[45] present a lower bound on the $\frac{m}{2}$th-order nonlinearity of a class of bent Boolean function constructed by Dobbertin et al.[23], and the lower bounds are better than the results in [28, 29, 47]. While, Gode, Faruqi and Mishra[30] obtain improved lower bounds on the second-order nonlinearities of few classes of degree 3 monomial Boolean functions for $7 \leq n \leq 13$, compared with the lower bounds in [28, 39, 42].

Theorem 4 *Let f be any n-variable function and r a positive integer smaller than n. We have:*

$$nl_r(f) \geq \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}} nl_{r-1}(D_a f).$$

Obviously, above inequality can be repeatedly applied:

$$nl_r(f) \geq \frac{1}{2^i} \max_{a_1,\ldots,a_i \in \mathbb{F}_{2^n}} nl_{r-i}(D_{a_1} \cdots D_{a_i} f).$$

Another potentially stronger lower bound, given a lower bound on the $(r-1)$-th order nonlinearity is known for all the derivatives (in nonzero directions) of the function:

Theorem 5 *Let f be any n-variable function and r a positive integer smaller than n. We have:*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2 \sum_{a \in \mathbb{F}_{2^n}} nl_{r-1}(D_a f)}.$$

Remark 5 *Theorem 5 is not always better than Theorem 4: In [43], Sihem et al. construct a class of Boolean functions where the bound on the second order nonlinearity in Theorem 4 is tight but the bound in Theorem 5 is strictly worse than the former.*

In [19], Dobbertin et al. studied the cross-correlation function between two m-sequences for Niho type decimation $d = (2^k - 1)s + 1$. They derived the distribution of six-valued cross-correlation function for $s = 3$ and odd k.

APN decomposition

The decomposition [1] we introduced here is based on the TU-decomposition, but before investigating this pattern, we first need the notion of Walsh zeros.

Definition 2 *Let $\mathcal{V}$ and $\mathcal{W}$ be finite-dimensional $\mathbb{F}_2$-vector spaces, with $\dim_{\mathcal{V}} = n, \dim_{\mathcal{V}} = m$, respectively. The Walsh zeroes of a function $F : \mathcal{V} \to \mathcal{W}$, denoted by $\mathcal{Z}_F$, is the set of the coordinates of the zeroes in its Walsh spectrum together with $(0, 0)$, i.e.,*

$$\mathcal{Z}_F = \{(a, b) \in \mathcal{V} \times \mathcal{W} \mid W_F(a, b) = 0\} \cup \{(0, 0)\}.$$

Note that Walsh zeros of a vBF must contain $\{(0,x) : x \in \mathcal{V}\}$, so discussing Walsh zeros is valid for all vBF.

For two functions F and G mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, if $\Gamma_G = \mathcal{A}(\Gamma_F)$ for some affine permutation $\mathcal{A}$ of $\mathbb{F}_2^{n+m}$, then $\mathcal{Z}_G = (\mathcal{L}^T)^{-1}(\mathcal{Z}_F)$, where $\mathcal{L}$ is the linear part of $\mathcal{A}$. Thus, there exists a linear subspace V of $\mathcal{Z}_G$ with dimension n, such that $\mathcal{L}^T(V) = \{(0,x) : x \in \mathcal{V}\}$. Therefore, we have

An APN instance with the worst linearity 2^7

$$\begin{aligned} x \mapsto & x^3 + g^{60}x^5 + g^{191}x^6 + g^{198}x^9 + g^{232}x^{10} + g^{120}x^{12} + \\ & g^{54}x^{17} + g^{64}x^{18} + g^{159}x^{20} + g^{144}x^{24} + g^{248}x^{33} + \\ & g^{203}x^{34} + g^{32}x^{36} + g^{18}x^{40} + g^{216}x^{48} + g^{78}x^{65} + \\ & g^{46}x^{66} + g^{91}x^{68} + g^{27}x^{72} + g^{70}x^{80} + g^{52}x^{96} + \\ & g^{224}x^{129} + g^{18}x^{130} + g^{197}x^{136} + g^{253}x^{144} + x^{160}, \end{aligned}$$

where $g \in \mathbb{F}_{2^8}^*$ is an element with minimal polynomial $X^8 + X^4 + X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.

Algebraic Geometry

The main goal of algebraic geometry is to study solution sets of polynomial equations in several variables. So, in its easiest form, if $f_1, \ldots, f_k \in K[x_1, ..., x_n]$ are polynomials in n variables over a given ground field K we want to consider the set

$$X = \{x \in K^n : f_1(x) = \cdots = f_k(x) = 0\},$$

which is called an (affine) variety.

Genera is the plural form of genus.

Let q be a prime power. For the finite field $\mathbb{F}_q$, let F be an algebraic function field with the full constant field $\mathbb{F}_q$.

An algebraic function field of n variables over a field K is finitely generated field extension K/k which has transcendence degree n over k. As an example, in the polynomial ring $k[X,Y]$, consider the idea l generated by the irreducible polynomial $Y^2 - X^3$ and form the field of fractions of the quotient ring $k[X,Y]/\left(Y^2 - X^3\right)$.

$(0:0:0)$ is not a point at infinity.

the APN functions x^{81} over $\mathbb{F}_{2^9}$ and x^5 over $\mathbb{F}_{2^7}$ have been respectively used in MISTY and KASUMI block ciphers

Regular Expression

We can use the regular expression to find some gibberishes,

References

[1] Christof Beierle, Claude Carlet, Gregor Leander, and Léo Perrin. A further study of quadratic apn permutations in dimension nine. *Finite Fields and Their Applications*, 81:102049, 2022.

[2] Christof Beierle and Gregor Leander. New instances of quadratic APN functions. *IEEE Transactions on Information Theory*, 68(1):670–678, 2022.

[3] E.R. Berlekamp, H. Rumsey, and G. Solomon. On the solution of algebraic equations over finite fields. *Information and Control*, 10(6):553–564, 1967.

[4] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications*, 14(3):703–714, 2008.

[5] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.

[6] KA Browning, JF Dillon, MT McQuistan, and AJ Wolfe. An apn permutation in dimension six. *Finite Fields: theory and applications*, 518:33–42, 2010.

[7] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[8] Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, and Irene Villa. Constructing APN functions through isotopic shifts. *IEEE Transactions on Information Theory*, 66(8):5299–5309, 2020.

[9] Lilya Budaghyan and Claude Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

[10] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic apn binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[11] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[12] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a construction of quadratic apn functions. In *2009 IEEE Information Theory Workshop*, pages 374–378, 2009.

[13] Lilya Budaghyan, Tor Helleseth, and Nikolay S. Kaleyski. A new family of APN quadrinomials. *IEEE Transactions on Information Theory*, 66(11):7081–7087, 2020.

[14] Marco Calderini, Lilya Budaghyan, and Claude Carlet. On known constructions of APN and AB functions and their relation to each other. *IACR Cryptol. ePrint Arch.*, page 1444, 2020.

[15] Marco Calderini, Kangquan Li, and Irene Villa. Two new families of bivariate apn functions. *arXiv preprint arXiv:2204.07462*, 2022.

[16] Claude Carlet. Recursive lower bounds on the nonlinearity profile of boolean functions and their applications. *IEEE Transactions on Information Theory*, 54(3):1262–1272, 2008.

[17] Claude Carlet. More vectorial boolean functions with unbounded nonlinearity profile. *Int. J. Found. Comput. Sci.*, 22(6):1259–1269, 2011.

[18] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[19] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl. Niho type cross-correlation functions via dickson polynomials and kloosterman sums. *IEEE Transactions on Information Theory*, 52(2):613–627, 2006.

[20] Hans Dobbertin. Almost perfect nonlinear power functions on gf(2n): The niho case. *Inf. Comput.*, 151(1-2):57–72, 1999.

[21] Hans Dobbertin. Almost perfect nonlinear power functions on gf(2^{n}): The welch case. *IEEE Trans. Inf. Theory*, 45(4):1271–1275, 1999.

[22] Hans Dobbertin. Almost perfect nonlinear power functions on gf(2n): A new case for n divisible by 5. In Dieter Jungnickel and Harald Niederreiter, editors, *Finite Fields and Their Applications*, pages 113–121, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[23] Hans Dobbertin, Gregor Leander, Anne Canteaut, Claude Carlet, Patrick Felke, and Philippe Gaborit. Construction of bent functions via niho power functions. *Journal of Combinatorial Theory, Series A*, 113(5):779–798, 2006.

[24] Y. Edel, G. Kyureghyan, and A. Pott. A new apn function which is not equivalent to a power mapping. *IEEE Transactions on Information Theory*, 52(2):744–747, 2006.

[25] Sugata Gangopadhyay, Sumanta Sarkar, and Ruchi Telang. On the lower bounds of the second order nonlinearities of some boolean functions. *Information Sciences*, 180(2):266–273, 2010.

[26] Qi Gao and Deng Tang. A lower bound on the second-order nonlinearity of the class of maiorana-mcfarland bent functions. In *Eighth International Workshop on Signal Design and Its Applications in Communications, IWSDA 2017, Sapporo, Japan, September 24-28, 2017*, pages 191–195. IEEE, 2017.

[27] Manish Garg and Andrey Khalyavin. Higher-order nonlinearity of kasami functions. *Int. J. Comput. Math.*, 89(10):1311–1318, 2012.

[28] Ruchi Gode and Sugata Gangopadhyay. On second order nonlinearities of cubic monomial boolean functions. *Cryptology ePrint Archive*, 2009.

[29] Ruchi Gode and Sugata Gangopadhyay. Third-order nonlinearities of a subclass of kasami functions. *Cryptography and Communications*, 2(1):69–83, 2010.

[30] Ruchi Telang Gode, Shahab Faruqi, and Ashutosh Mishra. Improved lower bounds on second order non-linearities of cubic boolean functions. In Manoj Sahni, José M. Merigó, Ritu Sahni, and Rajkumar Verma, editors, *Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy*, pages 31–43, Singapore, 2022. Springer Singapore.

[31] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Trans. Inf. Theory*, 14(1):154–156, 1968.

[32] Faruk Göloğlu and Lukas Kölsch. Equivalences of biprojective almost perfect nonlinear functions. *arXiv preprint arXiv:2111.04197*, 2021.

[33] Faruk Göloğlu. Biprojective almost perfect nonlinear functions. *IEEE Transactions on Information Theory*, 68(7):4750–4760, 2022.

[34] Faruk Göloğlu and Dáša Krasnayová. Proofs of several conjectures on linear codes from boolean functions. *Discrete Mathematics*, 342(2):572–583, 2019.

[35] Tetsu Iwata and Kaoru Kurosawa. Probabilistic higher order differential attack and higher order bent functions. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *Advances in Cryptology - ASIACRYPT'99*, pages 62–74, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[36] Tadao Kasami. The weight enumerators for several clauses of subcodes of the 2nd order binary reed-muller codes. *Inf. Control.*, 18(4):369–394, 1971.

[37] Kangquan Li and Nikolay S. Kaleyski. Two new infinite families of APN functions in triviariate form. *IACR Cryptol. ePrint Arch.*, page 1522, 2022.

[38] Kangquan Li, Yue Zhou, Chunlei Li, and Longjiang Qu. Two new families of quadratic apn functions. *IEEE Transactions on Information Theory*, 68(7):4761–4769, 2022.

[39] Xuelian Li, Yupu Hu, and Juntao Gao. Lower bounds on the second order nonlinearity of boolean functions. *Int. J. Found. Comput. Sci.*, 22(6):1331–1349, 2011.

[40] Qian Liu. The lower bounds on the second-order nonlinearity of three classes of boolean functions, 2023.

[41] Robert J McEliece. *Finite fields for computer scientists and engineers*, volume 23. Springer Science & Business Media, 2012.

[42] Sihem Mesnager, Kwang Ho Kim, and Myong Song Jo. On the number of the rational zeros of linearized polynomials and the second-order nonlinearity of cubic boolean functions. *Cryptography and Communications*, 12(4):659–674, 2020.

[43] Sihem Mesnager, Gavin McGrew, James Davis, Dayton Steele, and Katherine Marsten. A comparison of carlet's second-order nonlinearity bounds. *International Journal of Computer Mathematics*, 94(3):427–436, 2017.

[44] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer, 1993.

[45] Kezia Saini and Manish Garg. On the higher-order nonlinearity of a boolean bent function class (constructed via niho power functions). *Cryptography and Communications*, 14(5):1055–1066, 2022.

[46] Sumanta Sarkar and S Gangopadhyay. On the second order nonlinearity of a cubic maiorana-mcfarland bent function. *Finite Fields and Their Applications*, 2009, 2009.

[47] Brajesh Kumar Singh. On third-order nonlinearity of biquadratic monomial boolean functions. *Int. J. Eng. Math.*, 2014:1–7, 2014.

[48] Deep Singh. Second-order nonlinearities of some classes of cubic boolean functions based on secondary constructions. *Int'l J. Comput. Sci. Inform. Technol*, 2(2):786–791, 2011.

[49] Deep Singh and Amit Paul. Higher order nonlinearity of some cryptographic functions. *International Journal of Computational and Applied Mathematics*, 12(2):195–205, 2017.

[50] Deep Singh, Amit Paul, Neerendra Kumar, Veronika Stoffová, and Chaman Verma. Resiliency and nonlinearity profiles of some cryptographic functions. *Mathematics*, 10(23):4473, 2022.

[51] Guanghong Sun and Chuankun Wu. The lower bounds on the second order nonlinearity of three classes of boolean functions with high nonlinearity. *Information Sciences*, 179(3):267–278, 2009.

[52] Guanghong Sun and Chuankun Wu. The lower bound on the second-order nonlinearity of a class of boolean functions with high nonlinearity. *Appl. Algebra Eng. Commun. Comput.*, 22(1):37–45, 2011.

[53] Guanghong Sun and Chuankun Wu. Higher order nonlinearity of niho functions. *Fundam. Informaticae*, 137(3):403–412, 2015.

[54] Deng Tang, Claude Carlet, and Xiaohu Tang. On the second-order nonlinearities of some bent functions. *Information Sciences*, 223:322–330, 2013.

[55] Deng Tang, Bimal Mandal, and Subhamoy Maitra. Further cryptographic properties of the multiplicative inverse function. *Discrete Applied Mathematics*, 307:191–211, 2022.

[56] Deng Tang, Haode Yan, Zhengchun Zhou, and Xiaosong Zhang. A new lower bound on the second-order nonlinearity of a class of monomial bent functions. *Cryptography and Communications*, 12(1):77–83, 2020.

[57] Hiroaki Taniguchi. On some quadratic apn functions. *Des. Codes Cryptography*, 87(9):1973–1983, sep 2019.

[58] Qichun Wang and Chik How Tan. On the second-order nonlinearity of the hidden weighted bit function. *Discret. Appl. Math.*, 215:197–202, 2016.

[59] Haode Yan and Deng Tang. Improving lower bounds on the second-order nonlinearity of three classes of boolean functions. *Discrete Mathematics*, 343(5):111698, 2020.

[60] Satoshi Yoshiara. Equivalences of quadratic apn functions. *Journal of Algebraic Combinatorics*, 35:461–475, 2012.

[61] Yuyin Yu and Léo Perrin. Constructing more quadratic APN functions with the QAM method. *Cryptography and Communications*, 14(6):1359–1369, 2022.

[62] Lijing Zheng, Haibin Kan, Yanjun Li, Jie Peng, and Deng Tang. Constructing new apn functions through relative trace functions. *IEEE Transactions on Information Theory*, 68(11):7528–7537, 2022.

[63] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.