Shanghai Jiao Tong University
School of Electronic Information and Electrical Engineering

APN functions

Zhaole Li

Workshop of APN function, 2022

Section 1

Introduction

Vectorial Boolean functions

Given two positive integers n and m, a vectorial Boolean (n, m)-function, or simply (n, m)-function, is any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. When $m = 1$, we often call it n-variable Boolean function.

One can identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$.

The differential attack, introduced by Biham and Shamir[1], is a chosen plaintext attack for block ciphers in general.

An (n, m)-function F is called differentially δ-uniform, if for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$, the equation $F(x) + F(x + a) = b$ has at most δ solutions. We denote the minimum of these integers δ by δ_F and call it the differential uniformity of F. For every (n, m)-function F, we have $\delta_F \geq \max(2, 2^{n-m})$.

[1] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4 (1), pp. 3–72, 1991.

Shanghai Jiao Tong University

We can have $\delta_F = 2$ only when $n \geq m$, and this case is specially defined for $n = m$:

Definition (APN functions)

An (n, n)-function F is called almost perfect nonlinear (APN) if it is differentially 2-uniform, i.e. if for every $a \in \mathbb{F}_2^n \setminus \{0_n\}$ and every $b \in \mathbb{F}_2^n$, the equation $F(x) + F(x + a) = b$ has 0 or 2 solutions (i.e. the derivative $D_a F(x) = F(x) + F(x + a)$ is 2-to-1). Equivalently, $|D_a F(x), x \in \mathbb{F}_2^n| = 2^{n-1}$. In other words, for distinct elements $x, y, z, t \in \mathbb{F}_2^n$, the equality $x + y + z + t = 0_n$ implies $F(x) + F(y) + F(z) + F(t) \neq 0_n$.

Definition

Let F and F' be two functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.

1. F and F' are Extended affine equivalent (EA-equivalent) if

$$F'(x) = L_1(F(L_2(x))) + L(x),$$

   where L_1 and L_2 are affine permutations on $\mathbb{F}_2^n$, and L is an affine function on $\mathbb{F}_2^n$.

2. F and F' are Carlet–Charpin–Zinoviev equivalent (CCZ-equivalent) if there exists an affine permutation which maps G_F onto $G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$ is the graph of F, and $G_{F'}$ is the graph of F'.

Remark:

1. CCZ-equivalence is a generalization of EA-equivalence.
2. If a function is APN, then its CCZ-equivalent functions are all APN.
3. Two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent.

Section 2

A matrix approach for constructing quadratic APN functions

Let $F(x) = \sum_{1 \leq t < i \leq n} c_{i,t} x^{2i-1+2^{t-1}} \in \mathbb{F}_{2^n}[x]$ be a quadratic function. We define an $n \times n$ matrix $E = (e_{i,t})_{n \times n}$ by setting $e_{i,t} = c_{i,t}$ for $i > t$, otherwise $e_{i,t} = 0$. Let $X = (x^{2^0}, x^{2^1}, ..., x^{2^{n-1}})^T$ and $x = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$ where $x_i \in \mathbb{F}_2$ for $1 \leq i \leq n$. We have

$$F(x) = \overline{x}^T M^T E M T \overline{x}, \tag{1}$$

where $\overline{x} = (x_1, x_2, ..., x_n)^T$ and $M = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2^{n-1}} & \alpha_2^{2^{n-1}} & \dots & \alpha_n^{2^{n-1}} \end{pmatrix}$.

When $a = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$ and $\overline{a} = (a_1, ..., a_n)^T$, we have

$$\begin{aligned} D_aF(x) =& F(x+a) + F(x) + F(a) \\ =& (\overline{x}+\overline{a})^T M^T EM(\overline{x}+\overline{a}) + \overline{x}^T M^T EM\overline{x} + \overline{a}^T M^T EM\overline{a} \\ =& \overline{x}^T M^T (E+E^T) M\overline{a}. \end{aligned}$$

So we define a symmetric matrix $C_F = E + E^T$ with diagnoal elements are all zero, so is $H = M^T C_F M$. When F is quadratic, $D_aF(x)$ is a linear function, so F is APN iff $\max\{\dim_{\mathbb{F}_2}(Ker(D_a)) | a \in \mathbb{F}_{2^n}\} = 1$.

Matrices when F is APN

$D_aF(x) = \overline{x}^T H \overline{a}$ has 2 solutions iff $\mathrm{Rank}_{\mathbb{F}_2}(H\overline{a})^T = n-1$, and $H\overline{a}$ is the linear combination of n colomums of H. Thus

$$D_a(x) = \overline{x}^T H \overline{a} = 0,$$

has 2 solutions for $\overline{a} \in \mathbb{F}_2^n \setminus \{0\}$ iff F is APN.

Definition

Let $H = (h_{u,v})_{n\times n}$ 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 of H has rank $n-1$.

Properties of QAMs

Shanghai Jiao Tong University

F is an APN function with the correspondence matrix is QAM related to basis $\{\alpha_1, ..., \alpha_n\}$.

1. So if H_α, H_β are corresponding matrices for $F(x)$ relative to the α, β respectively. Then we confirm $H_\beta = P^T H_\alpha P$ where the invertible $n \times n$ matrix P satisfying that
$$(\beta_1, ..., \beta_n) = (\alpha_1, ..., \alpha_n)P.$$
2. So if $F(x), F'(x)$ is the quadratic function defined by H_α, H_β related to α, are two functions EA-equivalent?

The relation between $F(x)$ and $F'(x)$

The answer is yes: $F'(x)$ is EA-equivalent to $F(x)$.

Proof.

Set the functions defined by H and $H' = P^T HP$ relative to α be $F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}}$, define E, E' as before, hence we have

$$F(x) = \overline{x}^T M^T EM\overline{x}, F'(x) = \overline{x}^T M^T E' M\overline{x},$$

where $\overline{x} = (x_1, ..., x_n)^T \in \mathbb{F}_2^n$. We set $W = M^T EM, W' = M^T E' M$, then $W + W^T = H$ and $W' + W'^T = H' = P^T HP = P^T WP + P^T W^T P$. $\square$

The Lemma for the symmetric matrix with zero diagnoal

Shanghai Jiao Tong University

Lemma

Suppose $H = (h_{u,v})_{n\times n}$ *is a symmetric matrix over* $\mathbb{F}_{2^n}$ *with diagnoal elements are all zeros, define a set* $S = \{W|W + W^T = H\}$*, if* $W_1 + W_1^T = W_2 + W_2^T = H$*, then there exists a symmetric matrix* A *such that* $W_2 = W_1 + A$*.*

Proof.

Obviously for any symmetric matrix A, we have

$$(W_1 + A) + (W_1 + A)^T = W_1 + W_1^T + A + A^T = W_1 + W_1^T = H$$

which implies that $W_1 + A \in S$ for any symmetric matrix A.
By fixing W_1, we define another set $S' = \{W_1 + A|A \text{ is symmetric}\}$, then $\#S'$ is the number of symmetric matrices over $\mathbb{F}_{2^n}$, i.e. $\#S' = (2^n)^{n+\frac{n(n-1)}{2}}$. Note that $\#S = \#S'$, and all elements of S' belong to S, so $S' = S$, i.e. $W_2 = W_1 + A$. □

SHANGHAI JIAO TONG UNIVERSITY

Proof.

Since $W' + W'^T = H' = P^T H P = P^T W P + P^T W^T P$, according to lemma above, there exists a symmetric matrix A such that $W' = P^T W P + A$. Thus

$$
\begin{aligned}
F'(x) =& \overline{x}^T M^T E' M \overline{x} = \overline{x}^T W' \overline{x} \\
=& \overline{x}^T (P^T W P + A) \overline{x} = \overline{x}^T P^T M^T E M P \overline{x} + \overline{x}^T A \overline{x} \\
=& G(x) + \overline{x}^T A \overline{x},
\end{aligned}
$$

where $G(x) = \overline{x}^T P^T M^T E M P \overline{x}$, is affine equivalent to $F(x)$.

$$
\overline{x}^T A \overline{x} = \sum_{i=1}^{n} a_{i,i} x_i.
$$

is a linear function since A is symmetric, so $F'(x)$ is EA-equivalent to $G(x)$. Thus $F'(x)$ is EA-equivalent to $F(x)$.

The relation between H and $L(H)$

Theorem

Let $H = (h_{u,v}) \in \mathbb{F}_{2^n}^{n\times n}$ be a symmetric matrix with main diagonal elements all zeros, and L be a linear permutation on $\mathbb{F}_{2^n}$. Let $H' = (h'_{u,v}) \in \mathbb{F}_{2^n}^{n\times n}$ such that $h'_{u,v} = L(h_{u,v})$ for all $1 \leq u, v \leq n$. Then the the quadratic functions defined by H and H' relative to α are EA-equivalent. And H is a QAM iff H' is a QAM.

Proof.

Just as before, we have $H = M^T(E + E^T)M = M^T C_F M$, then $C_F = (M^T)^{-1} H M^{-1}$. For the basis $\alpha = \{\alpha_1, ..., \alpha_n\}$, we have the dual basis $\theta = \{\theta_1, ...\theta_n\}$ such that

$$Tr(\alpha_i\theta_j) = \begin{cases} 0, \text{ for } & i \neq j; \\ 1, \text{ for } & i = j. \end{cases}$$

Thus we have $(M^T)^{-1} = M_\theta$ and the element in i-th row and j-th colomum is $\theta_j^{2^{i-1}}$. Hence we have $C_F = M_\theta H M_\theta^T$, so

$$c_{i,t} = \sum_{1 \leq u,v \leq n} \theta_u^{2^{i-1}} \theta_u^{2^{t-1}} h_{u,v}.$$

Choose $\eta_{u,v} \in \mathbb{F}_{2^n}$ such that $\eta_{u,v} + \eta_{v,u} = h_{u,v}$ and $h_{u,v} = 0$, then we have a quadratic function $Q(x) = \sum_{1 \leq v < u \leq n} Tr(\theta_u x) Tr(\theta_v x) h_{u,v}$ over $\mathbb{F}_{2^n}$ which is EA-equivalent to

Proof

Proof.

$F(x)$, using the same technique we get $Q'(x)$ which is also EA-equivalent to $F'(x)$. Thus we only need to confirm the relation between $Q(x)$ and $Q'(x)$:

$$
\begin{aligned}
Q'(x) &= \sum_{1\leq v<u\leq n} Tr(\theta_u x)Tr(\theta_v x)h'_{u,v} = \sum_{1\leq v<u\leq n} Tr(\theta_u x)Tr(\theta_v x)L(h_{u,v}) \\
&= L(\sum_{1\leq v<u\leq n} Tr(\theta_u x)Tr(\theta_v x)h_{u,v}) = L(Q(x)).
\end{aligned}
$$

$L(Tr(x)) = Tr(x)$ since L is a linear permutation. Therefore it duduces that $F(x)$ and $F'(x)$ are EA-equivalent. □

Before introducing the algorithms for constructing quadratic APN functions, we give some results on matrices over $\mathbb{F}_{2^n}$ which are useful.

Lemma

Let $H \in \mathbb{F}_{n\times n}^{2^n}$ be a symmetric matrix with main diagonal elements all zero. Then every nonzero linear combination over $\mathbb{F}_2$ of the n rows of H has rank at most $n-1$.

Theorem

Let $A = (a_{i,j}) \in \mathbb{F}_{2^n}^{r\times c}$ with $1 \le r < c \le n$ and $a_{i,j} = a_{j,i}, a_{i,i} = 0$ for $1 \le i, j \le r$. Let $A[:, k], A[k]$ be the k-th colomum and k-th row of A, respectively. Set $b = \sum_{k=1}^{c} \lambda_k A[:, k]$, where $0 \ne (\lambda_1, ..., \lambda_c) \in \mathbb{F}_2^c$. Assume $t = \mathrm{Rank}_{\mathbb{F}_2}\{b[1], b[2], ..., b[r]\}$. Then if every nonzero linear combination over $\mathbb{F}_2$ of the r rows of A has rank at least $c-1$, we have

1. *if $(\lambda_{r+1}, ..., \lambda_c) = 0$, then $t = r - 1$;*
2. *if $(\lambda_{r+1}, ..., \lambda_c) \ne 0$, then $t = r$;*

Proof

1. Assume $(\lambda_{r+1}, ..., \lambda_c) = 0$, then $b = \sum_{k=1}^{r} \lambda_k A[:, k]$, so $t \leq r - 1$; Let B is the matrix of first $r \times r$ submatrix of A, then $b = \mathrm{Rank}_{\mathbb{F}_2}(\sum_{k=1}^{r} \lambda_k B[k])$, so if $t < r - 1$, then we have $\mathrm{Rank}_{\mathbb{F}_2}(\sum_{k=1}^{r} \lambda_k A[k]) < r - 1 + (c - r) = c - 1$, contradiction.
2. Assume $(\lambda_{r+1}, ..., \lambda_c) \neq 0$, w.l.o.g. let $\lambda_c = 1$, then substitude $A[:, c]$ with b, we get a new $r \times c$ matrix A'. If $t < r$, we have $\sum_{k=1}^{r} \lambda'_k A'[k, c] = 0$ for $(\lambda'_1, ..., \lambda'_r) \in \mathbb{F}_2^r \setminus \{0\}$. W.l.o.g. suppose $\lambda'_1 \neq 0$, then substitude $A'[1]$ with $\sum_{i=1}^{r} \lambda'_i A'[i]$ and get a new matrix A'', then substitude $A''[:, 1]$ with $\sum_{i=1}^{r} \lambda'_i A''[:, i]$ and get get a new matrix A''', note that $A' = AP$, where P is a invertible matrix; $A'' = P'A'$, $A''' = A''P''$, where P', P'' are also invertible matrices, so every nonzero linear combination over $\mathbb{F}_2$ of the r rows of A''' has rank at least $c{-}1$. However, we have $A'''[1, c] = A'''[1, 1] = 0$, contradiction.

Exclude some improper matrices

Corollary

$H = (h_{u,v})_{n\times n}$ is a symmetric matrix over $\mathbb{F}_{2^n}$ and A is the $r \times c$ submatrix consisting of the first r rows and the first c colomums of H. Suppose $B = A^T$, then if A has the property that every nonzero linear combination over $\mathbb{F}_2$ of the r rows of A has rank at least $c-1$, so does B.

Note that every submatrix $A = (a_{i,j}) \in \mathbb{F}_{2^n}^{r\times c}$ with $1 \le r < c \le n$ of a QAM H must has the property that every nonzero linear combination over $\mathbb{F}_2$ of the r rows of the submatrix has rank at least $c-1$. Thus, if a matrix has a submatrix which don't have that property, it cannot be a QAM. Using the corollary, checking the property of submatrix A is enough.

Given an $n \times n$ QAM matrix H over $\mathbb{F}_{2^n}$, we wish to get some new QAMs by assigning some different values of H. Since H is a QAM, the $n-1 \times n-1$ submatrix A consists of the first $n-1$ rows and the first $n-1$ colomums of H, and any nonzero linear combination of the $n-1$ rows of A has rank $n-2$. Thus $H = \begin{pmatrix} A & c \\ c^T & 0 \end{pmatrix}$, where $c = (x_1, ..., x_{n-1})^T$. Then we choose suitable c to make H a QAM.

How to choose suitable c

Example

Let $n = 4$ and we give the H over $\mathbb{F}_{2^4}$:

$$\begin{pmatrix} \boxed{\begin{matrix} 0 & h_{1,2} & h_{1,3} \\ h_{2,1} & 0 & h_{2,3} \\ h_{3,1} & h_{3,2} & 0 \end{matrix}} & \begin{matrix} c_1 \\ c_2 \\ c_3 \end{matrix} \\ \begin{matrix} c_1 & c_2 & c_3 \end{matrix} & 0 \end{pmatrix} \tag{2}$$

The matrix framed is the submatrix A, clearly any nonzero linear combination of the $4-1$ rows of A has rank $4-2$. Then we need to test whether $[A, c]$ has the similar property:

1. if $c_1 \in \mathrm{Span}(A[1])$, then the first row of $[A, c]$ has rank $4-2$, so H is not a QAM;
2. if $c_1 + c_2 \in \mathrm{Span}(A[1] + A[2])$, then the sum of the first two rows of $[A, c]$ has rank $4-2$, so H is not a QAM;
3. $\cdots$;

How to choose suitable c

From the example above, we need only to choose $c = (c_1, ..., c_{n-1})^T \in \mathbb{F}_{2^n}^{n-1}$ to satisfy

$$\lambda_1 c_1 + \cdots + \lambda_{n-1} c_{n-1} \in \mathbb{F}_{2^n} \setminus \mathrm{Span}(\lambda_1 A[1] + \cdots + \lambda_{n-1} A[n-1]),$$

where $\lambda_i \in \mathbb{F}_2$ for all $1 \leq i \leq n-1$.
First we only modify c_1, we can simplify the set as below: Let $S_1 = \mathbb{F}_{2^n} \setminus V_1$, where $V_1 = \mathrm{Span}(A[1])$. After fixing the value for c_1, we need to modify c_2, but the range of c_2 is more complex: $c_2 \notin \mathrm{Span}(A[2])$ and $c_2 \notin \mathrm{Span}(A[1] + A[2])$. And c_3 has the same condition: $c_3 \notin \mathrm{Span}(A[3])$, $c_3 \notin \mathrm{Span}(A[3] + A[1])$, $c_3 \notin \mathrm{Span}(A[3] + A[2])$ and $c_3 \notin \mathrm{Span}(A[3] + A[2] + A[1])$.

An algorithm for choosing suitable c

Let A be the submatrix of H consisting of the first $n-1$ rows and colomums, $S = \{S_\lambda : \lambda = (\lambda_1, \ldots, \lambda_{n-1}) \in \mathbb{F}_2^{n-1} \setminus \{0\}\}$ where $S_\lambda = \mathbb{F}_{2^n} \setminus \mathrm{Span}(\sum_{j=1}^{n-1} \lambda_j A[j])$.

Algorithm 1: The algorithm for choosing suitable c

Input : A QAM H over $\mathbb{F}_{2^n}$; A set S as defined above; An index $i = 1$.

Output: Some QAMs

for *each* $c_i \in S_{e_i}$ **do**
    if $i = n-1$ **then**
        $h_{n-1,n} = h_{n,n-1} = c_{n-1}$;
        return H
    end
    $h_{i,n} = h_{n,i} = c_i$;
    $S_{e_{i+1}} \leftarrow S_{e_{i+1}} \cap S_{e_{i+1}+e_i}$;
    $i \leftarrow i + 1$;
end

Thus, given a QAM H, we can assign the values of the last colomum of H to get some new QAMs by using algorithm. Furthermore, assigning the values of the more colomums of H can get more QAMs, but it needs to apply the algorithm several times. If we want to find new APN functions on $\mathbb{F}_{2^n}$ for $n \geq 8$, we must change values of a QAM for at least two colomums by experimental results,

SHANGHAI JIAO TONG UNIVERSITY

Example

x^3 is a well-known quadratic APN function on $\mathbb{F}_{2^n}$. Let $n = 8$, g be the primitive element of $\mathbb{F}_{2^8}$ with $g^8 + g^4 + g^3 + g^2 + 1 = 0$, C be an 8×8 matrix such that $c_{1,2} = c_{2,1} = 1$ and $c_{i,j} = 0$ for all the others. Suppose M is an 8×8 matrix such that $m_{i,j} = (g^1 1)^{2^{i-1}+2^{j-1}}$ for $1 \leq i, j \leq 8$. Then the corresponding QAM of x^3 is

$$H_8 = \begin{pmatrix} 0 & g^{34} & g^{81} & g^{83} & g^{170} & g^{106} & \mathbf{c}_{13} & \mathbf{c}_7 \\ g^{34} & 0 & g^{68} & g^{162} & g^{166} & g^{85} & \mathbf{c}_{12} & \mathbf{c}_6 \\ g^{81} & g^{68} & 0 & g^{136} & g^{69} & g^{77} & \mathbf{c}_{11} & \mathbf{c}_5 \\ g^{83} & g^{162} & g^{136} & 0 & g^{17} & g^{138} & \mathbf{c}_{10} & \mathbf{c}_4 \\ g^{170} & g^{166} & g^{69} & g^{17} & 0 & g^{34} & \mathbf{c}_9 & \mathbf{c}_3 \\ g^{106} & g^{85} & g^{77} & g^{138} & g^{34} & 0 & \mathbf{c}_8 & \mathbf{c}_2 \\ \mathbf{c}_{13} & \mathbf{c}_{12} & \mathbf{c}_{11} & \mathbf{c}_{10} & \mathbf{c}_9 & \mathbf{c}_8 & 0 & \mathbf{c}_1 \\ \mathbf{c}_7 & \mathbf{c}_6 & \mathbf{c}_5 & \mathbf{c}_4 & \mathbf{c}_3 & \mathbf{c}_2 & \mathbf{c}_1 & 0 \end{pmatrix}.$$

Example

We assign values for c_i for $1 \leq i \leq 13$ to get new QAMs. Let H_8 be a QAM, then:

1. $V = \mathrm{Span}(g^{34}, g^{81}, g^{83}, g^{170}, g^{106})$, and V can partition $\mathbb{F}_{2^8}$ into 8 sets: $\mathbb{F}_{2^8} = V \cup (V + a_1) \cup (V + a_2) \cup (V + a_3) \cup (V + a_4) \cup (V + a_5) \cup (V + a_6) \cup (V + a_7)$;
2. $\mathrm{Rank}_{\mathbb{F}_2}(0, g^{34}, g^{81}, g^{83}, g^{170}, g^{106}, c_{13}) = 6$, i.e. $c_{13} \in \mathbb{F}_{2^8} \setminus V$. Suppose c_{13} is the linear combination of $g^{34}, g^{81}, g^{83}, g^{170}, g^{106}$ with a set $A = \{a_i | 1 \leq i \leq 7\}$;

SHANGHAI JIAO TONG UNIVERSITY

Example

3 Thus we have

$$H_8' = P^T H_8 P = \begin{pmatrix} 0 & g^{34} & g^{81} & g^{83} & g^{170} & g^{106} & a & \mathbf{c_7} \\ g^{34} & 0 & g^{68} & g^{162} & g^{166} & g^{85} & x_{\mathbf{12}} & \mathbf{c_6} \\ g^{81} & g^{68} & 0 & g^{136} & g^{69} & g^{77} & x_{\mathbf{11}} & \mathbf{c_5} \\ g^{83} & g^{162} & g^{136} & 0 & g^{17} & g^{138} & x_{\mathbf{10}} & \mathbf{c_4} \\ g^{170} & g^{166} & g^{69} & g^{17} & 0 & g^{34} & x_{\mathbf{9}} & \mathbf{c_3} \\ g^{106} & g^{85} & g^{77} & g^{138} & g^{34} & 0 & x_{\mathbf{8}} & \mathbf{c_2} \\ a & x_{\mathbf{12}} & x_{\mathbf{11}} & x_{\mathbf{10}} & x_{\mathbf{9}} & x_{\mathbf{8}} & 0 & \mathbf{c_1} \\ \mathbf{c_7} & \mathbf{c_6} & \mathbf{c_5} & \mathbf{c_4} & \mathbf{c_3} & \mathbf{c_2} & \mathbf{c_1} & 0 \end{pmatrix}.$$

4 If H_8 is a QAM then H_8' is also a QAM, and they are EA-equivalent. So we only need to consider $c_{13} \in A$.

Avoiding EA-equivalent APN functions

Example

5 Similarly, $U = \mathrm{Span}(g^{34}, g^{68}, g^{162}, g^{166}, g^{85})$, and $B \cup (B + g^{34})$ be a partition of $\mathbb{F}_{2^8} \setminus U$.

6 When c_{13} and c_{12} have been chosen, let $E = \mathrm{Span}(g^{34}, g^{81}, g^{83}, g^{170}, g^{106}, c_{13})$, then E can partition $\mathbb{F}_{2^8}$ into 4 parts.

7 $F = \mathrm{Span}(g^{34}, g^{68}, g^{162}, g^{166}, g^{85}, c_{12})$ and $G \cup (G + g^{34})$ be a partition of $\mathbb{F}_{2^8} \setminus F$.

Shanghai Jiao Tong University

Thank You

Zhaole Li · APN functions