



SHANGHAI JIAO TONG  
UNIVERSITY

SCHOOL OF ELECTRONIC INFORMATION AND ELECTRICAL ENGINEERING

## APN functions

Zhaole Li

Workshop of APN function, 2022



Section 1  
Introduction



Given two positive integers  $n$  and  $m$ , a vectorial Boolean  $(n, m)$ -function, or simply  $(n, m)$ -function, is any function  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ . 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<sup>1</sup>, is a chosen plaintext attack for block ciphers in general.

An  $(n, m)$ -function  $F$  is called differentially  $\delta$ -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  $\delta$  solutions. We denote the minimum of these integers  $\delta$  by  $\delta_F$  and call it the differential uniformity of  $F$ . For every  $(n, m)$ -function  $F$ , we have  $\delta_F \geq \max(2, 2^{n-m})$ .

---

<sup>1</sup>E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology* 4 (1), pp. 3–72, 1991.

We can have  $\delta_F = 2$  only when  $m \geq n$ , 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  $X = (x^{2^0}, x^{2^1}, \dots, x^{2^{n-1}})^T$  and  $x = x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n$  where  $x_i \in \mathbb{F}_2$  for  $1 \leq i \leq n$ . We have

$$F(x) = \bar{x}^T M^T E M \bar{x}, \quad (1)$$

where  $\bar{x} = (x_1, x_2, \dots, x_n)^T$  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  $\bar{a} = (a_1, \dots, a_n)^T$ , we have

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

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

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

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

has 2 solutions for  $\bar{a} \in \mathbb{F}_2^n \setminus \{0\}$  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  $\mathbb{F}_2$ -linear combination of the  $n$  rows of  $H$  has rank  $n-1$ .

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

- ① So if  $H_\alpha, H_\beta$  are corresponding matrices for  $F(x)$  relative to the  $\alpha, \beta$  respectively. Then we confirm  $H_\beta = P^T H_\alpha P$  where the invertible  $n \times n$  matrix  $P$  satisfying that

$$(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n)P.$$

- ② So if  $F(x), F'(x)$  is the quadratic function defined by  $H_\alpha, H_\beta$  related to  $\alpha$ , 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  $H' = P^T H P$  relative to  $\alpha$  be  $F(x) = \sum_{1 \leq t < i \leq n} c_{i,t} x^{2^{i-1} + 2^{t-1}}$ , define  $E, E'$  as before, hence we have

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

where  $\bar{x} = (x_1, \dots, x_n)^T \in \mathbb{F}_2^n$ . We set  $W = M^T E M, W' = M^T E' M$ , then  $W + W^T = H$  and  $W' + W'^T = H' = P^T H P = P^T W P + P^T W^T P$ . □

## Lemma

*Suppose  $H = (h_{u,v})_{n \times n}$  is a symmetric matrix over  $\mathbb{F}_{2^n}$  with diagonal 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.  $W_2 = W_1 + A$ . □

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



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

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

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

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

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



## 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 quadratic functions defined by  $H$  and  $H'$  relative to  $\alpha$  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  $\alpha = \{\alpha_1, \dots, \alpha_n\}$ , we have the dual basis  $\theta = \{\theta_1, \dots, \theta_n\}$  such that

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

Thus we have  $(M^T)^{-1} = M_\theta$  and the element in  $i$ -th row and  $j$ -th column 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  $Q(x) = \sum_{1 \leq v < u \leq n} \text{Tr}(\theta_u x) \text{Tr}(\theta_v x) h_{u,v}$  over  $\mathbb{F}_{2^n}$  which is EA-equivalent to

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  $Q'(x)$ :

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

$L(\text{Tr}(x)) = \text{Tr}(x)$  since  $L$  is a linear permutation. Therefore it deduces 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  $H \in \mathbb{F}_{2^n}^{n \times n}$  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  $1 \leq r < c \leq n$  and  $a_{i,j} = a_{j,i}, a_{i,i} = 0$  for  $1 \leq i, j \leq r$ . Let  $A[:, k], A[k]$  be the  $k$ -th column and  $k$ -th row of  $A$ , respectively. Set  $b = \sum_{k=1}^c \lambda_k A[:, k]$ , where  $0 \neq (\lambda_1, \dots, \lambda_c) \in \mathbb{F}_2^c$ . Assume  $t = \text{Rank}_{\mathbb{F}_2} \{b[1], b[2], \dots, b[r]\}$ . 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  $(\lambda_{r+1}, \dots, \lambda_c) = 0$ , then  $t = r - 1$ ;
- ② if  $(\lambda_{r+1}, \dots, \lambda_c) \neq 0$ , then  $t = r$ ;

- ① Assume  $(\lambda_{r+1}, \dots, \lambda_c) = 0$ , 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  $b = \text{Rank}_{\mathbb{F}_2}(\sum_{k=1}^r \lambda_k B[k])$ , so if  $t < r - 1$ , then we have  $\text{Rank}_{\mathbb{F}_2}(\sum_{k=1}^r \lambda_k A[k]) < r - 1 + (c - r) = c - 1$ , contradiction.
- ② Assume  $(\lambda_{r+1}, \dots, \lambda_c) \neq 0$ , w.l.o.g. let  $\lambda_c = 1$ , then substitute  $A[:, c]$  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  $(\lambda'_1, \dots, \lambda'_r) \in \mathbb{F}_2^r \setminus \{0\}$ . W.l.o.g. suppose  $\lambda'_1 \neq 0$ , then substitute  $A'[1]$  with  $\sum_{i=1}^r \lambda'_i A'[i]$  and get a new matrix  $A''$ , then substitute  $A''[:, 1]$  with  $\sum_{i=1}^r \lambda'_i A''[:, i]$  and 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.



## 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  $c$  columns 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  $1 \leq r < c \leq n$  of a QAM  $H$  must have 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 doesn'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  $n-1$  columns 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  $c = (x_1, \dots, x_{n-1})^T$ . Then we choose suitable  $c$  to make  $H$  a QAM.

## Example

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

$$\begin{pmatrix} 0 & h_{1,2} & h_{1,3} & c_1 \\ h_{2,1} & 0 & h_{2,3} & c_2 \\ h_{3,1} & h_{3,2} & 0 & c_3 \\ c_1 & c_2 & c_3 & 0 \end{pmatrix} \quad (2)$$

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



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

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

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  $V_1 = \text{Span}(A[1])$ . After fixing the value for  $c_1$ , we need to modify  $c_2$ , but the range of  $c_2$  is more complex:  $c_2 \notin \text{Span}(A[2])$  and  $c_2 \notin \text{Span}(A[1] + A[2])$ . And  $c_3$  has the same condition:  $c_3 \notin \text{Span}(A[3])$ ,  $c_3 \notin \text{Span}(A[3] + A[1])$ ,  $c_3 \notin \text{Span}(A[3] + A[2])$  and  $c_3 \notin \text{Span}(A[3] + A[2] + A[1])$ .



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

---

**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

```
1 for each  $c_i \in S_{e_i}$  do
2   if  $i = n - 1$  then
3      $h_{n-1,n} = h_{n,n-1} = c_{n-1}$ ;
4     return  $H$ 
5   end
6    $h_{i,n} = h_{n,i} = c_i$ ;
7    $S_{e_{i+1}} \leftarrow S_{e_{i+1}} \cap S_{e_{i+1}+e_i}$ ;
8    $i \leftarrow i + 1$ ;
9 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,

## 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  $8 \times 8$  matrix such that  $c_{1,2} = c_{2,1} = 1$  and  $c_{i,j} = 0$  for all the others. Suppose  $M$  is an  $8 \times 8$  matrix such that  $m_{i,j} = (g^{11})^{2^{i-1}+2^{j-1}}$  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  $V = \text{Span}(g^{34}, g^{81}, g^{83}, g^{170}, g^{106})$ , 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  $\text{Rank}_{\mathbb{F}_2}(0, g^{34}, g^{81}, g^{83}, g^{170}, g^{106}, c_{13}) = 6$ , 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  $A = \{a_i | 1 \leq i \leq 7\}$ ;

## Example

3 Thus we have

$$H'_8 = P^T H_8 P = \begin{pmatrix} 0 & g^{34} & g^{81} & g^{83} & g^{170} & g^{106} & a & \mathbf{c}_7 \\ g^{34} & 0 & g^{68} & g^{162} & g^{166} & g^{85} & x_{12} & \mathbf{c}_6 \\ g^{81} & g^{68} & 0 & g^{136} & g^{69} & g^{77} & x_{11} & \mathbf{c}_5 \\ g^{83} & g^{162} & g^{136} & 0 & g^{17} & g^{138} & x_{10} & \mathbf{c}_4 \\ g^{170} & g^{166} & g^{69} & g^{17} & 0 & g^{34} & x_9 & \mathbf{c}_3 \\ g^{106} & g^{85} & g^{77} & g^{138} & g^{34} & 0 & x_8 & \mathbf{c}_2 \\ a & x_{12} & x_{11} & x_{10} & x_9 & x_8 & 0 & \mathbf{c}_1 \\ \mathbf{c}_7 & \mathbf{c}_6 & \mathbf{c}_5 & \mathbf{c}_4 & \mathbf{c}_3 & \mathbf{c}_2 & \mathbf{c}_1 & 0 \end{pmatrix}.$$

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  $c_{13} \in A$ .

## Example

- 5 Similarly,  $U = \text{Span}(g^{34}, g^{68}, g^{162}, g^{166}, g^{85})$ , 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  $E = \text{Span}(g^{34}, g^{81}, g^{83}, g^{170}, g^{106}, c_{13})$ , then  $E$  can partition  $\mathbb{F}_{2^8}$  into 4 parts.
- 7  $F = \text{Span}(g^{34}, g^{68}, g^{162}, g^{166}, g^{85}, c_{12})$  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