Proof: 没序号的

McEliece's book[**?**]:

引理 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 硬件加速的实现方法：下面给出 $A = a_0Y + a_1Y^{16} \in \mathbb{F}_{2^8}$ 的取逆操作，其中 $a_0, a_1 \in \mathbb{F}_{2^4}$:

1. 设 (W, W^2) 是 $\mathbb{F}_{2^2}$ 的基，(Z^2, Z^8) 是 $\mathbb{F}_{2^4}$ 的基，(Y, Y^{16}) 是 $\mathbb{F}_{2^8}$ 的基。

2. 计算 A 的逆元素的方法是：$A^{-1} = (AA^{16})^{-1}A^{16} = ((a_0+a_1)^2WZ + a_0a_1)^{-1}(a_1Y + a_0Y^{16})$

算法思想：这里需要计算的有 $T_1 = (a_0+a_1); T_2 = (WZ)(T_1)^2; T_3 = a_0a_1; T_4 = T_2+T_3; T_5 = (T_4)^{-1}; T_6 = T_5a_1; T_7 = T_5a_0$. 所有的操作都是在 $\mathbb{F}_{2^4}$ 上，所以等同于对长度为 4 的向量进行操作。

1. T_1 和 T_4 是向量加法；

2. T_2 是标量乘法，使用变换矩阵 $P = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ 即可；

3. T_3, T_6 和 T_7 是向量乘法，需要定义向量乘法 $z = x \star y$，具体操作如下页所示；

4. T_5 是有限域取逆操作的硬件实现，具体操作如下页所示。

向量乘法 $z = (z_0, z_1, z_2, z_3) = x \star y = (x_0, x_1, x_2, x_3) \star (y_0, y_1, y_2, y_3)$ 结果如下：

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

可以暂时优化一下, 得到 10 次乘法的结果

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

取逆操作 $y=(y_0,y_1,y_2,y_3)=x^{-1}=(x_0,x_1,x_2,x_3)^{-1}$ 结果如下 (直观上看着是 8 次乘法):

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

注意可以使用复用来减少乘法的次数 (5 次乘法)

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

现在寻求能不能继续减少乘法的数量：先尝试把所有的 T_i 表示出来吧.

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

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

$T_3 =$

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

$T_4 = T_2 + T_3 =$

$$\left(\begin{matrix} (x_1 + x_2)(y_1 + y_2) + (x_0 + x_2)(y_0 + y_2) + (x_2 + x_3)(y_2 + y_3) + (x_0 + x_3)(y_0 + y_3) + x_0 y_0 + x_1 + y_1 + \\ (x_1 + x_3)(y_1 + y_3) + (x_0 + x_2 + 1)(y_0 + y_2 + 1) + (x_0 + x_1)(y_0 + y_1) + x_1 y_1 + 1 \\ (x_0 + x_3)(y_0 + y_3) + (x_0 + x_2)(y_0 + y_2) + (x_0 + x_1 + 1)(y_0 + y_1 + 1) + (x_1 + x_2)(y_1 + y_2) + x_2 y_2 \\ (x_1 + x_3)(y_1 + y_3) + (x_0 + x_2)(y_0 + y_2) + (x_2 + x_3)(y_2 + y_3) + x_3 y_3 + x_1 + y_1 \end{matrix} \right.$$

感觉看着就不大行, 不大能继续化简的样子

Lylia APN function[**?**]

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

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

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

where $1 \leq i \neq j \leq n-1$ 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}[**?**]
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]).

定理 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.

定理 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 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 $\big(x, y\big) \mapsto \big(x(y^2 + xy + \beta x^2)^d, (x + y)(y^2 + xy + \beta x^2)^d\big)$ 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

---

[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)

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 $\beta\neq1$ 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 $\alpha+\alpha^{2^k}\neq1$ and $\frac{\alpha^{2^k+1}}{(\alpha+\alpha^{2^k})^2}\neq1$; 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 $\mu+\mu^{2^k}=1$, $\mu+\mu^2\neq1$ ($\mu+\mu^2\neq1$ 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:

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 [?]

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 [**?**].

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 [**?**].

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 [**?**]

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

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

is APN in Theorem 2.1 of [**?**]

6.