제 9 장 해 설

§ 9.4 Reed-Solomon 부호

§ 9.5 McEliece 암호체계

§9.4 Reed-Solomon 부호

素數 p 와 양의 정수 m에 대하여 $q = p^m$ 이라고 할 때, Galois 체 $\mathbb{F}_q$ 에서

$$\mathbb{F}_q{}^* = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}, \quad \alpha^{q-1} = 1$$

인 원소 $\alpha \in \mathbb{F}_q$ 를 체 $\mathbb{F}_q$ 의 원시원소라 하고 원시원소 α 를 근으로 가지는 체 $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ 위의 최고차 항의 계수가 1인 m 차의 기약다항식 $p(x)$ 를 체 $\mathbb{F}_p$ 위의 원시다항식이라고 한다.

정리 1 체 $\mathbb{F}_2$ 위의 m 차의 원시다항식

$$p(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} + x^m \in \mathbb{F}_2[x]$$

에 대하여 Galois 체 $\mathbb{F}_{2^m}$ 의 원소 α 를 $p(\alpha) = 0$ 인 원시원소라 하고 또 $n = 2^m - 1$ 이라고 하자. 또, $V_n = \mathbb{F}_2[x]/I$, $I = (x^n - 1)$ 이라고 할 때, V_n 에서의 순환 $(n, n-m)$ 부호

$$C' = \{f(x) + I \mid f(x) \in (p(x))\} = (p(x))/I$$

에 대하여

$$C = \{(a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_2{}^n \mid a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + I \in C'\}$$

이라고 하면 다음이 성립한다.

(1) 원소 $f(x) + I \in V_n$ 에 대하여 $f(x) + I \in C' \Leftrightarrow f(\alpha) = 0$ 이다.

(2) C 는 체 $\mathbb{F}_2$ 위의 순환 $(n, n-m)$ 부호이고 다음이 성립한다.

$$(a_0, a_1, \cdots, a_{n-1}) \in C \iff a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} = 0$$

그리고 C 는 이진 Hamming 부호 $\mathrm{Ham}(m, 2)$ 이다.

(3) $\mathrm{Ham}(m, 2)$ 는 체 $\mathbb{F}_2$ 위의 순환 $(n, n-m)$ 부호이다.

증 명 체 $\mathbb{F}_2$ 위에서 원시다항식 $p(x)$ 는 x^n-1 의 약수이므로 V_n 에서의 $C' = (p(x))/I$ 가 정의되고, 또 $\deg p(x) = m$ 이므로 C' 은 V_n 에서의 순환 $(n, n-m)$ 부호이다.

(1) 먼저 $f(x)+I \in C'$ 이면, 적당한 다항식 $c(x) \in \mathbb{F}_2[x]$ 에 대하여 $f(x) = c(x)p(x)$ 이고 이때 $f(\alpha) = c(\alpha)p(\alpha) = 0$ 이다. 또, $f(\alpha) = 0$ 이면, $p(x) \mid f(x)$ 즉 $f(x) \in (p(x))$이므로 $f(x)+I \in C'$ 이다.

(2) C' 은 벡터공간 V_n 에서의 순환 $(n, n-m)$ 부호이고 또 C 는 체 $\mathbb{F}_2$ 위의 순환 $(n, n-m)$ 부호이다. 그리고, (1) 에 의하여 다음이 성립한다.

$$\begin{aligned} & (a_0, a_1, \cdots, a_{n-1}) \in C \\ \Leftrightarrow\ & a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + I \in C' \\ \Leftrightarrow\ & a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0 \end{aligned}$$

그런데 Galois 체 $\mathbb{F}_{2^m}$ 을 체 $\mathbb{F}_2$ 위의 벡터공간으로 생각할 때,

$$\mathscr{B} = \{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$$

는 $\mathbb{F}_{2^m}$ 의 기저이고, 또 $p(\alpha) = 0$ 이므로 다음이 성립한다.

$$\alpha^m = -c_0 - c_1\alpha - \cdots - c_{m-1}\alpha^{m-1} = c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1}$$

따라서 $\mathbb{F}_{2^m}$ 의 원소 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 은 다음과 같이 $1, \alpha, \cdots, \alpha^{m-1}$ 의 일차결합으로 나타내어진다(여기서 $d_0, d_1, \cdots, d_{n-1} \in \mathbb{F}_2$)

$$\begin{aligned} 1 &= 1 \\ \alpha &= \alpha \\ \alpha^2 &= \alpha^2 \\ &\vdots \\ \alpha^{m-1} &= \alpha^{m-1} \\ \alpha^m &= c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{m-1}\alpha^{m-1} \\ &\vdots \\ \alpha^{n-1} &= d_0 + d_1\alpha + d_2\alpha^2 + \cdots + d_{m-1}\alpha^{m-1} \end{aligned}$$

이제 체 $\mathbb{F}_2$ 위의 $m\times n$ 행렬 H 를

$$H=\begin{bmatrix} 1 & 0 & \cdots & 0 & c_0 & \cdots & d_0 \\ 0 & 1 & \cdots & 0 & c_1 & \cdots & d_1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{m-1} & \cdots & d_{m-1} \end{bmatrix}$$

이라고 하면 다음이 성립한다.

$$(a_0, a_1, \cdots, a_{n-1}) \in C \iff a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$$

$$\iff H\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

따라서 부호 C 는 행렬 H 를 홀짝 검사행렬로 가지는 선형부호이다.

그런데 α 는 체 $\mathbb{F}_{2^m}$ 의 원시원소이므로

$$\mathbb{F}_{2^m}{}^* = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}, \quad \alpha^n = 1$$

이므로 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 은 모두 서로 다르므로 행렬 H 의 n 개의 열벡터 전체는 벡터공간 $\mathbb{F}_2{}^m$ 의 영벡터가 아닌 n 개의 벡터 전체와 일치하고 따라서 C 는 이진 Hamming 부호 $\mathrm{Ham}(m, 2)$ 이다.

(3) 위의 (2) 에 의하여 C 는 체 $\mathbb{F}_2$ 위의 순환 $(n, n-m)$ 부호이고, 또 C 는 이진 Hamming 부호 $\mathrm{Ham}(m, 2)$ 이다.

그러므로 $\mathrm{Ham}(m, 2)$ 는 체 $\mathbb{F}_2$ 위의 순환 $(n, n-m)$ 부호이다.

보기 1 체 $\mathbb{F}_2$ 위의 4 차의 다항식 $p(x) = 1+x+x^4$ 은 원시다항식이다 (보기 4.2.5 참조).

이제 Galois 체 $\mathbb{F}_{2^4}$ 의 원소 α 를 $p(\alpha) = 0$ 인 원시원소라고 하면,

$$\mathbb{F}_{2^4}{}^* = \{1, \alpha, \alpha^2, \cdots, \alpha^{14}\}, \quad \alpha^{15} = 1$$

이고 체 $\mathbb{F}_2$ 위에서 $p(x)$ 는 다항식 $x^{15}-1$ 의 약수이다.

따라서 $V_{15} = \mathbb{F}_2[x]/I$, $I = (x^{15}-1)$ 이라고 하면, 체 $\mathbb{F}_2$ 위의 15 차원

벡터공간 V_{15} 에서의 순환 $(15, 11)$ 부호

$$C' = \{f(x) + I \in V_n \mid f(x) \in (p(x))\} = (p(x))/I$$

가 정의된다. 따라서

$$C = \{(a_0, \cdots, a_{14}) \in \mathbb{F}_2{}^{15} \mid a_0 + a_1 x + \cdots + a_{14} x^{15} \in C'\}$$

이라고 하면, C는 체 $\mathbb{F}_2$ 위의 순환 $(15, 11)$ 부호이고,

$$C = \{(a_0, a_1, \cdots, a_{14}) \in \mathbb{F}_2{}^{15} \mid a_0 + a_1\alpha + \cdots + a_{14}\alpha^{14} = 0\}$$

이고, 또 $p(\alpha) = \alpha^4 + \alpha + 1 = 0$ 즉 $\alpha^4 = 1 + \alpha$ 이므로 다음이 성립한다.

$$\begin{aligned}
1 &= 1 \\
\alpha &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha^3 \\
\alpha^4 &= 1 + \alpha \\
\alpha^5 &= \alpha + \alpha^2 \\
\alpha^6 &= \alpha^2 + \alpha^3 \\
\alpha^7 &= 1 + \alpha + \alpha^3 \\
\alpha^8 &= 1 + \alpha^2 \\
\alpha^9 &= \alpha + \alpha^3 \\
\alpha^{10} &= 1 + \alpha + \alpha^2 \\
\alpha^{11} &= \alpha + \alpha^2 + \alpha^3 \\
\alpha^{12} &= 1 + \alpha + \alpha^2 + \alpha^3 \\
\alpha^{13} &= 1 + \alpha^2 + \alpha^3 \\
\alpha^{14} &= 1 + \alpha^3
\end{aligned}$$

따라서 체 $\mathbb{F}_2$ 위의 4×15 행렬 H를

$$H = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}$$

로 정하면,

$$(a_0, a_1, \cdots, a_{14}) \in C \iff a_0 + a_1\alpha + \cdots + a_{14}\alpha^{14} = 0$$

$$\iff H\begin{bmatrix} a_0 \\ a_1 \\ \\ \vdots \\ a_{14} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

이므로 행렬 H는 순환 $(15, 11)$부호 C의 홀짝 검사행렬이고, 따라서 C는 이진 Hamming 부호 Ham $(4, 2)$이다. 예를 들어, 수신된 벡터가

$$w = (0,1,0,1,1,0,0,0,1,0,1,1,1,0,1) \in \mathbb{F}_2{}^{15}$$

일 때, H를 이용하여 w의 신드롬을 구하면 다음 결과를 얻는다.

$$S(w) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ \\ \vdots \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

따라서 $S(w) = S(e_5)$이므로 w의 5번째 성분을 수정하여 w를 다음과 같은 부호어로 복호한다.

$$v = 010110001011101 - 000010000000000$$
$$= 010\mathbf{0}00010111101$$

한편, w에 대응하는 $\mathbb{F}_2[x]/I$의 원소는

$$w(x) = x + x^3 + x^4 + x^8 + x^{10} + x^{11} + x^{12} + x^{14} + I$$

이므로 적당한 다항식 $c(x) \in \mathbb{F}_2[x]$에 대하여

$$w(x) + I = c(x)\,p(x) + 1 + x + I$$

이고 따라서 적당한 다항식 $h(x) \in \mathbb{F}_2[x]$에 대하여

$$w(x) = c(x)\,p(x) + 1 + x + h(x)\,(x^{15} - 1)$$

이므로

$$w(\alpha) = c(\alpha)\,p(\alpha) + 1 + \alpha = 1 + \alpha + 0\,\alpha^2 + 0\,\alpha^3$$

이고 따라서 $w(\alpha)$는 w의 신드롬 $S(w)$에 대응한다.

정리 2 Galois 체 $\mathbb{F}_q$에서 α가 원시원소이고 $n = q-1 \geq 2$일 때, $3 \leq d \leq n$인 양의 정수 d에 대하여 체 $\mathbb{F}_q$ 위의 $d-1$차의 다항식

$$g(x) = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{d-1})$$

를 정하고 $V_n = \mathbb{F}_q[x]/I$, $I = (x^n-1)$이라고 하면, 체 $\mathbb{F}_q$ 위의 벡터공간 V_n에서의 순환 $(n, n-d+1)$ 부호

$$C' = \{f(x) + I \mid f(x) \in (g(x))\} = (g(x))/I$$

가 정의된다. 이 때,

$$C = \{(a_0, \cdots, a_{n-1}) \in \mathbb{F}_q \mid a_0 + \cdots + a_{n-1}x^{n-1} + I \in C'\}$$

이라고 하면 다음이 성립한다.

(1) $f(x) + I \in C' \iff f(\alpha^{c+i}) = 0 \quad (0 \leq i \leq d-2)$

(2) C는 체 $\mathbb{F}_q$ 위의 순환 $(n, n-d+1)$ 부호이다.

그리고, 체 $\mathbb{F}_q$ 위의 $(d-1)\times n$ 행렬

$$H = \begin{bmatrix} 1 & \alpha^c & \alpha^{2c} & \cdots & \alpha^{(n-1)c} \\ 1 & \alpha^{c+1} & \alpha^{2(c+1)} & \cdots & \alpha^{(n-1)(c+1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{c+d-2} & \alpha^{2(c+d-2)} & \cdots & \alpha^{(n-1)(c+d-2)} \end{bmatrix}$$

는 순환부호 C의 홀짝 검사행렬이다.

부호 C, C'을 **길이** n, **意圖거리**(designed distance) d인 **Reed-Solomon 부호** 또는 **RS 부호**라고 한다.

실제로, C의 최소거리는 $d(C) = d$이다(정리 6.11.5 참조).

증 명 체 $\mathbb{F}_q$의 원소 $\alpha, \alpha^2, \cdots, \alpha^{d-1}$는 모두 x^n-1의 근이다.

한편, α는 체 $\mathbb{F}_q$의 원시원소이고 $q-1 = n$이므로

$$\alpha^i = 1 \iff n \mid i$$

이고 또 $d-1 \leq n-1$이므로 $\alpha, \alpha^2, \cdots, \alpha^{d-1}$는 모두 서로 다르다.

그런데, $g(x)=(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{d-1})$ 이므로 $\mathbb{F}_q[x]$ 에서 $g(x)$ 는 x^n-1 의 약수이다. 따라서 C' 이 정의되고, C' 은 벡터공간 V_n 에서의 순환 $(n, n-d+1)$ 부호이다.

그리고,

$$f(x)+I\in C' \iff g(x)\mid f(x)$$

이므로 다음이 성립한다.

$$\begin{aligned} f(x)+I\in C' &\iff g(x)\mid f(x) \\ &\iff f(\alpha)=f(\alpha^2)=\cdots=f(\alpha^{d-1})=0 \end{aligned}$$

그리고, C 는 체 $\mathbb{F}_q$ 위의 순환 $(n, n-d+1)$ 부호이고 다음이 성립한다.

$$\begin{aligned} &(a_0, a_1, \cdots, a_{n-1})\in C \\ \iff\ & a_0+a_1x+\cdots+a_{n-1}x^{n-1}+I\in C' \\ \iff\ & a_0+a_1\alpha^{c+i}+\cdots+a_{n-1}\alpha^{(n-1)(c+i)}=0 \quad (0\le i\le d-2) \\ \iff\ & [1\ \ \alpha^{c+i}\ \ \cdots\ \ \alpha^{(n-1)(c+i)}]\begin{bmatrix} a_0 \\ a_1 \\ \\ \vdots \\ a_{n-1}\end{bmatrix}=0 \quad (0\le i\le d-2) \\ \iff\ & H\begin{bmatrix} a_0 \\ a_1 \\ \\ \vdots \\ a_{n-1}\end{bmatrix}=\begin{bmatrix} 0 \\ 0 \\ \\ \vdots \\ 0\end{bmatrix} \end{aligned}$$

따라서 체 $\mathbb{F}_q$ 위의 $(d-1)\times n$ 행렬 H 는 부호 C 의 홀짝 검사행렬이다.

Reed 와 Solomon 은 1960 년에 공동으로 이러한 $g(x)$ 를 생성다항식으로 가지는 V_n 에서의 순환부호 $C'=(g(x))/(x^n-1)$ 을 고안해내었다.

보기 2 체 $\mathbb{F}_5 = \{0,1,2,3,4\}$ 에서 $\alpha = 2$ 는 체 $\mathbb{F}_5$의 원시원소이다. 실제로, $\alpha = 2$, $\alpha^2 = 4$, $\alpha^3 = 3$, $\alpha^4 = 1$ 이므로 $\mathbb{F}_5{}^* = \langle \alpha \rangle$ 이다.

이제 체 $\mathbb{F}_5$ 위에서

$$g(x) = (x-\alpha)(x-\alpha^2)$$

이라고 하면, $g(x)$ 는 다음과 같다.

$$\begin{aligned} g(x) &= (x-2)(x-4) \\ &= x^2 - (2+4)x + 2 \cdot 4 \\ &= x^2 - 1x + 3 = x^2 + 4x + 3 \\ &= 3 + 4x + x^2 \end{aligned}$$

따라서 정리 6.10.3 에서와 같이 정의한 Reed-Solomon 부호 C는 체 $\mathbb{F}_5$ 위의 순환 $(4,2)$ 부호이고, 체 $\mathbb{F}_5$ 위의 2×4 행렬

$$G = \begin{bmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{bmatrix}$$

는 C의 생성행렬이므로 다음이 성립한다.

$$\begin{aligned} C &= \langle (3,4,1,0), (0,3,4,1) \rangle \\ &= \{ a_1(3,4,1,0) + a_2(0,3,4,1) \mid a_1, a_2 \in \mathbb{F}_5 \} \end{aligned}$$

그리고, 정리 6.10.3 에 의하여 체 $\mathbb{F}_5$ 위의 2×4 행렬

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \end{bmatrix}$$

는 C 의 홀짝 검사행렬이다.

한편, $v = (3,4,1,0) \in C$ 이고 $d(v) = 3$ 이므로 C에는 Hamming 무게 3 인 부호어가 존재하고 따라서 $d(C) \le 3$ 이다.

그런데, H의 임의의 두 열벡터는 일차독립이므로 C 에는 Hamming 무게가 1 또는 2 인 부호어는 존재하지 않는다.

그러므로 $d(C) = 3$ 이다.

보기 3 체 $\mathbb{F}_2$ 위에서 $p(x) = x^2 + x + 1$ 는 원시다항식이다.

이제 $p(\alpha) = 0$ 인 원소 α 를 도입하면, 다음과 같이 α 를 원시원소로 가지는 Galois 체 $\mathbb{F}_{2^2}$ 를 얻는다(보기 4.2.3).

$$\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\},$$
$$\alpha^2 + \alpha = 1, \quad \alpha^2 = 1+\alpha, \quad \alpha^3 = 1$$

이 때,

$$g(x) = (x-\alpha)(x-\alpha^2)$$

이라고 하면, $g(x)$ 는 다음과 같다.

$$g(x) = x^2 - (\alpha+\alpha^2)x + \alpha^3 = x^2 + x + 1$$

따라서 정리 6.10.3 에서와 같이 정의한 Reed-Solomon 부호 C 는 Galois 체 $\mathbb{F}_4$ 위의 순환 $(3, 1)$ 부호이고, 또 체 $\mathbb{F}_2$ 위의 행렬

$$G = [1 \;\; 1 \;\; 1]$$

는 C 의 생성행렬이므로

$$C = \{(0,0,0), (1,1,1), (\alpha,\alpha,\alpha), (\alpha^2,\alpha^2,\alpha^2)\}$$

이고 분명히 $d(C) = 3$ 이다.

한편, 정리 6.10.3 에 의하여 Galois 체 $\mathbb{F}_4$ 위의 2×3 행렬

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{bmatrix}$$

는 C 의 홀짝 검사행렬이고 따라서 Reed-Solomon 부호 C 는

$$\begin{cases} a_0 + a_1\alpha + a_2\alpha^2 = 0 \\ a_0 + a_1\alpha^2 + a_2\alpha = 0 \end{cases}$$

의 해공간이다.

§9.5 McEliece 암호체계

집합 $\{1, 2, \cdots, n\}$ 위의 치환

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

에 대하여, n 차의 항등항렬 I_n 의 제 1 행, 제 2 행, $\cdots$, 제 n 행을 각각

제 i_1 행, 제 i_2 행 , $\cdots$, 제 i_n 행

으로 옮겨놓은 행렬을 π 에 대응하는 n 차의 **치환행렬**(permutation matrix)이라고 한다. 여기서 π 의 역치환은

$$\pi^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

이므로 π 에 대응하는 치환행렬 P 는 정칙행렬이고 P 의 역행렬은 π^{-1} 에 대응하는 치환행렬이며 $P^{-1} = P^T$ 이다.

보기 1 치환 $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ 에 대하여 π 의 역치환은

$$\pi^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

이고, π 와 π^{-1} 에 대응하는 4 차의 치환행렬은 각각 다음과 같다.

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \qquad P^{-1} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

그리고 $P^{-1} = P^T$ 이다.

집합 $\{1, 2, \cdots, n\}$ 위의 치환 전체의 개수는 $n!$ 이므로 n 차의 치환행렬은 $n!$ 개 존재한다. 실제로, 치환행렬은 각 행과 각 열의 성분 중에서 1 인 것이 단 하나 있고 나머지 성분은 모두 0 인 정사각행렬이다.

행렬 P를 치환

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & m \\ i_1 & i_2 & \cdots & i_m \end{pmatrix} \qquad \left[\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \right]$$

에 대응하는 m차의 [n차의 치환행렬이라고 할 때, 체 F 위의 $m \times n$ 행렬 $A = [a_{ij}]_{m \times n}$에 대하여

$$B = PA \qquad [B = AP]$$

라고 하면, B는 행렬 A의

제 1 행, 제 2 행, …, 제 m행을 각각 제 i_1 행, 제 i_2 행, …, 제 i_m 행으로

[제 1 열, 제 2 열, …, 제 n열을 각각 제 i_1 열, 제 i_2 열, …, 제 i_n 열로]

옮겨놓은 행렬이다.

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix} = \begin{bmatrix} a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{11} & a_{12} & a_{13} & a_{14} \end{bmatrix},$$

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} a_{13} & a_{11} & a_{14} & a_{12} \\ a_{23} & a_{21} & a_{24} & a_{22} \\ a_{33} & a_{31} & a_{34} & a_{32} \end{bmatrix}$$

이제 이진 선형부호를 이용한 암호체계에 대하여 논하기로 한다.

McEliece는 이른바 Goppa부호를 사용한 암호체계를 1976 년에 발표하였다. 이 Goppa 부호는 다음과 같은 이진 선형 $(2^m, 2^m - mt, 2t+1)$ 부호이다.

$$n = 2^m, \quad k = 2^m - mt, \quad d = 2t+1 \quad (m = 10, t = 50)$$

체 $\mathbb{F}_2$ 위의 선형 $(n, k, 2t+1)$ 부호 C에서, $t \geq 1$이라 하고 $k \times n$ 행렬 G와 $(n-k) \times n$ 행렬 H가 각각 C의 생성행렬, 홀짝 검사행렬이라 하고 또 임의의 k차의 정칙행렬 S와 n차의 치환 행렬 P에 대하여

$$G' = SGP$$

이라고 하자. 이 때, G'은 체 $\mathbb{F}_2$ 위의 $k \times n$ 행렬이고 $r(G') = r(G) = k$ 이다.

이제 $e=(c_1, c_2, \cdots, c_n)\in \mathbb{F}_2{}^n$를 $wt(e)=t$ 인 벡터라 하고 임의의 벡터 $(a_1, a_2, \cdots, a_k)\in \mathbb{F}_2{}^k$ 에 대하여 다음과 같이 놓자.

$$[b_1\ b_2\cdots b_n]=[a_1\ a_2\cdots a_k]G'+[c_1\ c_2\cdots c_n]$$

$$[y_1\ y_2\cdots y_n]=[b_1\ b_2\cdots b_n]P^{-1}$$

$$[c_1'\ c_2'\cdots c_n']=[c_1\ c_2\cdots c_n]P^{-1}$$

$$[x_1\ x_2,\ \cdots x_n]=[a_1\ a_2\cdots a_k]SG$$

이 때,

$$\begin{aligned}[y_1\ y_2\cdots y_n]&=[a_1\ a_2\cdots a_k]SG+[c_1\ c_2\cdots c_n]P^{-1}\\&=[a_1\ a_2\cdots a_k]SG+[c_1'\ c_2'\cdots c_n']\\&=[x_1\ x_2\cdots x_n]+[c_1'\ c_2'\cdots c_n']\end{aligned}$$

이므로

$$v=(x_1, x_2, \cdots, x_n),\quad w=(y_1, y_2, \cdots, y_n),\quad e'=(c_1', c_2', \cdots, c_n')$$

이라고 하면,

$$v=w-e'$$

이고 또

$$[x_1\ x_2\cdots x_n]=([a_1\ a_2\cdots a_k]S)G,\quad C=(G\text{의 행공간})$$

이므로 $v\in C$이다. 한편, P^{-1}는 치환행렬이고

$$[c_1'\ c_2'\cdots c_n']=[c_1\ c_2\cdots c_n]P^{-1}$$

이므로 $e'=(c_1', c_2', \cdots, c_n')$ 은 벡터 $e=(c_1, c_2, \cdots, c_n)$의 성분의 순서를 바꾸어 놓은 벡터이고 따라서 $wt(e')=wt(e)=t$이다.

이제 $w=(y_1, y_2, \cdots, y_n)$를 알고 있다고 하자.

이 때, w의 신드롬 $S(w)$를 구하고

$$S(w)=S(e'),\qquad wt(e')=t$$

인 벡터 e'을 구하면, $w+C=e'+C$이므로 $w-e'=v\in C$인 부호어 v가 단 하나 존재한다.

한편, $k\times n$ 행렬 G는 선형 (n, k) 부호 C의 생성행렬이므로 G의 k 개의 행벡터는 부호 C의 기저를 이룬다. 따라서 $v=(x_1, x_2, \cdots, x_n)\in C$에 대하여

$$[z_1\ z_2\cdots z_k]G=[x_1\ x_2\cdots x_n]$$

인 체 $\mathbb{F}_2$의 원소 $z_1, z_2, \cdots, z_k$가 단 한 벌 존재한다. 그런데

$$([a_1\ a_2\cdots a_k]S)G=[x_1\ x_2\cdots x_n]$$

이므로

$$[a_1\ a_2\cdots a_k]S=[z_1\ z_2\cdots z_k]$$

이고 따라서

$$[a_1\ a_2\cdots a_k]=[z_1\ z_2\cdots z_k]S^{-1}$$

를 계산하여 벡터 $(a_1, a_2, \cdots, a_k)$를 구할 수 있다.

이진 선형 $(n, k, 2t+1)$ 부호 C

생성행렬 G, 홀짝 검사행렬 H

$G'=SGP$

$\mathbb{F}_2{}^k$	$\mathbb{F}_2{}^n$
	$e=(c_1, c_2, \cdots, c_n)$, $wt(e)=t$
$(a_1, a_2, \cdots, a_k)$	$[b_1\ b_2\cdots b_n]$
	$=[a_1\ a_2\cdots a_k]G'+[c_1\ c_2\cdots c_n]$
	$[y_1\ y_2\cdots y_n]=[b_1\ b_2\cdots b_n]P^{-1}$
$[a_1\ a_2\cdots a_k]$	$w=(y_1, y_2, \cdots, y_n)$,
$=[z_1\ z_2\cdots z_k]S^{-1}$	$v=w-e'=(x_1, x_2, \cdots, x_n)\in C$
	$[z_1\ z_2\cdots z_k]G=[x_1\ x_2\cdots x_n]$

[McEliece 암호체계]

이 암호체계는 앞에서 얻은 결과에 근거를 둔 암호체계이며 여기서 C는 이진 선형 $(1024, 524, 101)$ 부호이고 평문은 524 비트이고 암호문은 1024 비트이다.

(1) 수신자 A는 완전부호인 이진 선형 $(n, k, 2t+1)$ 부호 C를 택하고 또 C의 생성행렬인 체 $\mathbb{F}_2$ 위의 $k \times n$ 행렬 G를 택한다. 그리고, 체 $\mathbb{F}_2$ 위의 k차의 정칙행렬 S와 n차의 치환행렬 P를 택하고,

$$G' = SGP$$

를 계산하여 행렬 G'은 공개하고 S, G, P는 공개하지 않는다.

(2) 송신자 U는 평문을 $(a_1, a_2, \cdots, a_k) \in \mathbb{F}_2{}^k$로 나타낸다.

(3) 송신자 U는 Hamming 무게가 t인 벡터 $e = (c_1, c_2, \cdots, c_n) \in \mathbb{F}_2{}^n$를 택하고

$$[b_1\ b_2 \cdots b_n] = [a_1\ a_2 \cdots a_k]\, G' + [c_1\ c_2 \cdots c_n]$$

를 계산하여 암호문 $(b_1, b_2, \cdots, b_n)$을 A에게 전송한다.

(4) 수신자 A는 수신된 암호문과 자신의 비밀 열쇠 P를 이용하여

$$[y_1\ y_2 \cdots y_n] = [b_1\ b_2 \cdots b_n]\, P^{-1}$$

를 계산하여 $w = (y_1, y_2, \cdots, y_n)$를 구한다. 그리고, A는 부호 C의 홀짝 검사행렬 H를 이용하여 w의 신드롬 $S(w)$를 구하고 $S(w) = S(e')$인 오류벡터 e'을 구하여 w를 부호어 $v = w - e' = (x_1, x_2, \cdots, x_n)$으로 복호한다.

(5) 수신자 A는 자신의 비밀 열쇠 G를 이용하여

$$[z_1\ z_2 \cdots z_k]\, G = [x_1\ x_2 \cdots x_n]$$

인 $(z_1, z_2, \cdots, z_k) \in \mathbb{F}_2{}^k$를 구하고 비밀 열쇠 S를 이용하여

$$[a_1\ a_2 \cdots a_k] = [z_1\ z_2 \cdots z_k]\, S^{-1}$$

를 계산하여 평문 $(a_1, a_2, \cdots, a_k)$를 구한다.

앞의 단계 (1)에서 생성행렬 G가 $G = [I_k \mid D]$의 꼴이면, 등식

$$([a_1\ a_2 \cdots a_k]S)G = [x_1\ x_2 \cdots x_n]$$

즉, $$([a_1\ a_2 \cdots a_k]S)[I_k \mid D] = [x_1\ x_2 \cdots x_n]$$

으로부터

$$([a_1\ a_2 \cdots a_k]S)I_k = [x_1\ x_2 \cdots x_k]$$

즉, $$[a_1\ a_2 \cdots a_k]S = [x_1\ x_2 \cdots x_k]$$

을 얻으므로 다음이 성립한다.

$$[a_1\ a_2 \cdots a_k] = [x_1\ x_2 \cdots x_k]S^{-1}$$

그러므로 앞의 단계 (5)에서 수신자 A는 $(z_1, z_2, \cdots, z_k) \in \mathbb{F}_2{}^k$를 구할 필요없이 벡터 $v = (x_1, x_2, \cdots, x_n)$의 처음 k개의 성분 $x_1, \cdots, x_k$와 비밀열쇠 S를 이용하여

$$[a_1\ a_2 \cdots a_k] = [x_1\ x_2 \cdots x_k]S^{-1}$$

를 계산하고 이로부터 평문 $(a_1, a_2, \cdots, a_k)$를 구한다.

이 암호체계는 몇 가지 약점을 가지고 있지만, 부호이론을 이용한 암호체계라는 점에서 매우 중요하다.

다음 보기는 McEliece의 암호체계에 대한 이해를 돕기 위한 예이다.

보기 2 체 $\mathbb{F}_2$ 위의 4×7 행렬

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

를 생성행렬로 가지는 이진 선형 $(7, 3, 3)$ 부호 C를 생각해 보자.

이 선형부호는 완전부호이고, 또 체 $\mathbb{F}_2$ 위의 3×7 행렬

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

는 C의 홀짝 검사행렬이다.

(1) 수신자 A는 체 $\mathbb{F}_2$ 위의 4차의 정칙행렬 S와 7차의 치환행렬 P를 각각 다음과 같이 택한다.

$$S=\begin{bmatrix}1&1&1&0\\1&0&1&0\\0&1&1&0\\1&0&1&1\end{bmatrix},\qquad P=\begin{bmatrix}0&0&1&0&0&0&0\\1&0&0&0&0&0&0\\0&0&0&0&1&0&0\\0&1&0&0&0&0&0\\0&0&0&0&0&0&1\\0&0&0&0&0&1&0\\0&0&0&1&0&0&0\end{bmatrix}$$

그리고

$$SG=\begin{bmatrix}1&1&1&0&0&1&0\\1&0&1&0&0&0&1\\0&1&1&0&1&0&0\\1&0&1&1&1&0&0\end{bmatrix},\quad G'=SGP=\begin{bmatrix}1&0&1&0&1&1&0\\0&0&1&1&1&0&0\\1&0&0&0&1&0&1\\0&1&1&0&1&0&1\end{bmatrix}$$

를 계산하여 G'은 공개하고 S, G, P는 공개하지 않는다.

(2) 송신자 U는 평문을 $(a_1,a_2,a_3,a_4)=(0,1,0,0)$으로 나타낸다.

(3) 송신자 U는 Hamming 무게가 1인 벡터 $e=(0,0,0,0,1,0,0)$를 택하여,

$$\begin{aligned}[b_1\ b_2\cdots\ b_7]&=[a_1\ a_2\cdots\ a_7]G'+[0\ 0\ 0\ 0\ 1\ 0\ 0]\\&=[0\ 1\ 0\ 0]G'+[0\ 0\ 0\ 0\ 1\ 0\ 0]\\&=[0\ 0\ 1\ 1\ 1\ 0\ 0]+[0\ 0\ 0\ 0\ 1\ 0\ 0]=[0\ 0\ 1\ 1\ 0\ 0\ 0]\end{aligned}$$

을 계산하여 암호문

$$(b_1,b_2,b_3,\cdots,b_7)=(0,0,1,1,0,0,0)$$

을 A에게 전송한다.

(4) 수신자 A는 수신된 암호문과 자신의 비밀 열쇠 P를 이용하여

$$P^{-1}=P^T=\begin{bmatrix}0&1&0&0&0&0&0\\0&0&0&1&0&0&0\\1&0&0&0&0&0&0\\0&0&0&0&0&0&1\\0&0&1&0&0&0&0\\0&0&0&0&0&1&0\\0&0&0&0&1&0&0\end{bmatrix}$$

를 구하고

$$[y_1\ y_2 \cdots y_7] = [b_1\ b_2 \cdots b_7]P^{-1}$$
$$= [0\ 0\ 1\ 1\ 0\ 0\ 0]P^{-1} = [1\ 0\ 0\ 0\ 0\ 0\ 1]$$

을 계산하여 $w = (y_1, y_2, \cdots, y_7) = (1,0,0,0,0,0,1)$ 를 구한다.

이 때, w 의 신드롬 $S(w)$ 를 구하면

$$S(w) = H\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

이고 이것이 행렬 H의 제 3 열과 일치한다. 따라서 오류벡터 e' 을

$$e' = (c_1', c_2', \cdots, c_7') = (0,0,1,0,0,0,0)$$

으로 놓으면, w는 다음과 같은 부호어 v로 복호된다.

$$v = (x_1, x_2, \cdots, x_7) = w - e'$$
$$= (1,0,0,0,0,0,1) - (0,0,1,0,0,0,0) = (1,0,1,0,0,0,1)$$

(5) 수신자 A 는 자신의 비밀 열쇠 G가 $G = [I_4 \mid D]$ 의 꼴이므로

$$[a_1\ a_2\ s_3\ a_4] = [x_1\ x_2\ x_3\ x_4]S^{-1}$$
$$= [1\ 0\ 1\ 0]\begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [0\ 1\ 0\ 0]$$

이고 따라서 평문은 $(a_1, a_2, a_3, a_4) = (0,1,0,0)$ 이다.

여기서, S의 역행렬 S^{-1}는 다음과 같이 구한다(보기 6.1.1 참조).

$$[S \mid I_4] = \left[\begin{array}{cccc:cccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{cccc:cccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

$$\longrightarrow \left[\begin{array}{cccc:cccc} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{cccc:cccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right]$$
$$= [I_4 \mid S^{-1}]$$