通信情報保護學會誌
第1卷, 第2號, 1991. 8

招請特輯

# 公開 키 暗號 시스템에 關한 硏究
# Study on the Public Key Cryptosystems
# (2)

李 晩 榮*

創刊號에 이어 本稿에서는 公開 키 暗號시스템(public key cryptosystem)中 Merkle-Hellman Knapsack 暗號시스템의 Multiplicative knapsack 方法, Multiple iterative knapsack 方法과 RSA 公開 키 暗號시스템 그리고 McEliece 公開키 暗號시스템에 對한 詳細한 分析을 記述하고자 한다.

目 次



* 종신회원, 漢陽大學校 名譽教授, 本學會 會長

[例題 6] gcd(w, m)=1이 되도록 서로素인 w와 m, m>w의 값을 選擇한다. 于先 w=2550과 m=8443을 選定했을 때 서로素인가를 보이고자 한다.

$$8443=(2550)3+793$$
$$2550=(793)3+171$$
$$793=(171)4+109$$
$$171=(109)1+62$$
$$109=(62)1+47$$
$$62=(47)1+15$$
$$47=(15)3+2$$
$$15=(2)7+1$$
$$2=(1)2$$

따라서, gcd(2550, 8443)=1 이므로 w와 m는 서로素인 祕密키(w, m)를 形成한다. 다음에 knapsack 벡터를 $K_p'=(171, 196, 457, 1191, 2410)$로 選定하면 式(13)의 $K_i\equiv 2550K_i'(\text{mod } 8443)$, $1\leq i\leq 5$와 같은 關係式으로부터 Trapdoor knapsack 벡터 $K_p$는 다음과 같이 求해진다. 即,

$$K_1=(2550)171-(8443)51=5457$$
$$K_2=(2550)196-(8443)59=1663$$
$$K_3=(2550)457-(8443)138=216$$
$$K_4=(2550)1191-(8443)359=6013$$
$$K_5=(2550)2410-(8443)729=7439$$

따라서, 公開 키인 Trapdoor knapsack 벡터 $K_p$는

$$K_p=(5457, 1663, 216, 6013, 7439)$$

와 같이 된다.

$m=8443$이고 $\sum_{i=1}^{5} k_i'=171+196+457+1191+2410=4425$ 이므로 $8443>4425$ 即 $m>\sum_{i=1}^{5} k_i'$인 條件을 滿足함을 알 수 있다. Euclid 알고리즘 gcd(w, m)=vw+um을 利用하여 $v=w^{-1}$의 값을 求해보자.

$$1=15-(2)7$$
$$1=(15)22-(47)7$$
$$1=(62)22-(47)29$$
$$1=(62)29-(109)7$$
$$1=(171)29-(109)36$$
$$1=(171)173-(793)36$$
$$1=(2550)173-(793)555$$
$$1=(2550)1838-(8443)555$$

여기서 最終의 方程式을 살펴보면 $1\equiv(2550)1838 \pmod{8443}$와 같이 合同式(congruence)으로 表示되므로 v의 값 v=1838은 w의 값 w=2550의 乘算逆元이다. 平文을 X=(01011)이라하면 暗號文은 $Y=K_pX=1663+6013+7439=15115$가 된다. 따라서 變換暗號文은 $Y'=vY \pmod m$이므로

$$Y'\equiv(1838)(15115) \bmod 8443=3900$$

이와 같이 해서 平文 X를 復元하면 아래 表와 같다.

| i | $y_i'$ | | $k_i'$ | $x_i$ |
|---|---|---|---|---|
| 5 | 3900 | > | 2410 | 1 |
| 4 | 1490 | > | 1191 | 1 |
| 3 | 299 | < | 457 | 0 |
| 2 | 299 | > | 196 | 1 |
| 1 | 103 | < | 171 | 0 |

따라서 平文벡터 X는 X=(01011)가 되므로 위에서 設定한 X의 값과 一致한다.

### 3.2 Multiplicative knapsack 方法

Multiplicative knapsack 알고리즘은 또다른 形態의 Merkle-Hellman 暗號시스템이다. 이 multiplicative knapsack은 對數(logarithm)를 취하여 덧셈 knapsack으로 變換하는 方式이다. 設計者는 각 要素들이 서로素인 knapsack 벡터 $K_p'=(k_1', k_2', \cdots, k_n')$을 選擇하고, 다음 式을 滿足하는 素數 q를 選定한다.

$$q>\prod_{i=1}^{n} k_i' \qquad (16)$$

β가 有限體 GF(q)의 原始元이라 하자. 그러면 式(17)에서와 같이 基底 β인 離散對數를 取함으로서 公開 키 $k_i$를 決定해야 한다.

$$k_i'\equiv\beta^{k_i} \pmod q \qquad (17)$$

여기서 q, β와 $k_i'$, $1\leq i\leq 5$, 은 trapdoor 情報들이다.

傳送하려는 暗號文은 다음 式처럼 計算된다.

$$Y=\sum_{i=1}^{n} k_i x_i \qquad (18)$$

Trapdoor 情報 q, β와 $k_i'$을 알고 있으므로, 다음 式을 計算할 수 있다.

$$Y'\equiv \beta^{Y} \pmod q \qquad (19)$$

여기서

$$\begin{aligned}\beta^{Y}&=\beta^{(\Sigma k_i x_i)}\\&=\beta^{k_1x_1}\cdot\beta^{k_2x_2}\cdots\beta^{k_nx_n}\\&=\prod_{i=1}^{n}(\beta^{k_i})^{x_i}\\&=\prod_{i=1}^{n}(k_i')^{x_i} \pmod q\end{aligned} \qquad (20)$$

그리고 q는 式(16)을 滿足해야 한다.

公開 키 $k_i$를 決定하기 위해 다음 벡터로 表現되는 中國人의 剩餘定理를 사용한다.

$$k_i\equiv[\beta_1(\bmod q_1),\ \beta_2(\bmod q_2),\cdots,\beta_n(\bmod q_n)] \qquad (21)$$

따라서 $k_i$를 求하기 爲해서는 $\beta_i$, $i=1,2,\cdots,n$,를 計算함으로써 成就할 수 있다. $\beta_i$를 求하기 위해, 먼저 다음 式을 計算한다.

$$z_i=k_i'^{(q-1)/q_i}=(\beta^{k_i})^{(q-1)/q_i}=[\beta^{(q-1)/q_i}]^{k_i} \qquad (22)$$

$\gamma_i=\beta^{(q-1)/q_i}$로 놓으면 $k_i=\beta_i$가 되기위해 $z_i$는 數列 $\gamma_i^0=1,\ \gamma_i^1,\ \gamma_i^2,\cdots,\gamma_i^{q-1}$의 한 元素이다. 따라서 이제는 $z_i=\gamma^{\beta_i}$, $0\leq\beta_i\leq q_i-1$, 인 $\beta_i$를 찾아야 한다. 이 技法은 例題 5에서 볼 수 있다.

다음 例題를 통해 簡單한 Multiplicative knapsack 問題를 살펴보자.

[例題 5] $n=3$, $K_p'=(2,3,5)$ 그리고 $q=31>\prod_{i=1}^{n} K_p'=(2)(3)(5)=30$을 滿足하는 q를 利用하여 GF(q)를 定하고 對數基底가 $\beta=24$로 設定하자. 이 條件下에서 n=3인 2進 n벡터 $X=(x_1, x_2, x_3)=(1, 1, 1)$에 대한 Multiplicative knapsack 問題를 풀어보자.

Pohlig과 Hellman 등이 發表한 알고리즘을 使用하여, q가 素數인 GF(q)상의 離散알고리즘을 計算한다. $q-1=q_1 q_2\cdots q_k$, 여기서 $q_i<q_{i+1}$, $i=1, 2,\cdots,k$을 $q-1$의 素因數分解라 하고, $q_i$는 서로 다른 素數이다. Trapdoor 情報 $q=31$, $\beta=24$, $k_1'=2$를 알고 있으므로, 公開 키 $k_1$은

$$2\equiv 24^{k_1} \pmod{31}$$

에 依해 決定된다. $q-1=q_1q_2q_3=30=(2)(3)(5)$이므로 素因數分解 결과는 $q_1=2$, $q_2=3$, $q_3=5$이다. $\beta_i$의 計算은 다음 節次에 따라 행해진다. $q_1=2$에 대해

$$\gamma_1\equiv\beta^{(q-1)/q_1}=24^{15} \pmod{31}$$

를 計算한다. $24^2=576=18 \pmod{31}$이므로 $24^4=324 \pmod{31}\equiv 14 \pmod{31}$이고 $24^8\equiv 14^2 \pmod{31}=196 \pmod{31}\equiv 10 \pmod{31}$이 된다. 따라서 $24^{15}=(24)^8(24)^4(24)^2(24)=10\cdot 14\cdot 18\cdot 24 \pmod{31}=30 \pmod{31}=-1 \pmod{31}$이 된다. 따라서 $\gamma_1=-1 \pmod{31}$이 되고 그러므로 $\gamma_1^0=1$이고 $\gamma_1^1=-1$이 된다.

한편 $z_1=k_1'^{(q-1)/q_1}$으로부터 $z_1=2^{15}\equiv 1 \pmod{31}$이 된다. 數列$(\gamma_1^0,\gamma_1^1)=(1,-1)$로부터 $z_1$과 같은 한 元素를 選擇한다. 이것은 $\gamma_1^0=1=z_1$이고, 그러므로 $\beta_1=0$이다.

$q_2=3$에 대해

$$\gamma_2=\beta^{(q-1)/q_2}=24^{10} \pmod{31}$$

을 計算한다. $24^2\equiv 18 \pmod{31}$과 $24^8\equiv 10 \pmod{31}$를 利用하면 $\gamma_2=(24)^8(24)^2\equiv 180 \pmod{31}\equiv 25 \pmod{31}$이 된다. 따라서 $\gamma_2^0=1$이고 $\gamma_2^1=25$ 그리고 $\gamma_2^2=(25)^2 \pmod{31}\equiv 5 \pmod{31}$이 된다.

$z_2=k_1'^{(q-1)/q_2}=2^{10}=1024\equiv 1 \pmod{31}$과 數列 $(\gamma_2^0,\ \gamma_2^1,\ \gamma_2^2)=(1,\ 25,\ 5)$를 比較하면 $\beta_2=0$을 얻는다.

$q_3=5$에 대해

$$\begin{aligned}\gamma_3&=\beta^{(q-1)/q_3}=24^6=(24)^4(24)^2\\&\equiv(14)\ (18) \pmod{31}\equiv 4 \pmod{31}\end{aligned}$$

를 計算한다. 따라서 數列은 $\gamma_3^0=1$, $\gamma_3^1=4$, $\gamma_3^2=16$, $\gamma_3^3=2$, 그리고 $\gamma_3^4=8 \pmod{31}$이 된다. 다음에는 $z_3=2^6=64\equiv 2 \pmod{31}$와 같이 求해지므로

$z_3$와 元素 $\gamma_3^i$를 比較하면 $z_3=2\equiv\gamma_3^3$이 된다. 따라서 $\beta_3=3$을 얻는다. 結局, 公開 키 $k_1$은 다음과 같이 決定된다.

$$k_1=[0\ (\mathrm{mod}\ 2),\ 0\ (\mathrm{mod}\ 3),\ 3\ (\mathrm{mod}\ 5)]$$
$$\equiv 18\ (\mathrm{mod}\ 31)$$

$k_1=18$은 다음에 보는 것처럼 $2\equiv 24^{k_1}(\mathrm{mod}\ 31)$로부터 구할 수 있음을 쉽게 알 수 있다.

$$24^{18}=(24)^8(24)^8(24)^2\equiv(10)(10)(18)\ (\mathrm{mod}\ 31)\equiv 1800\ (\mathrm{mod}\ 31)\equiv 2\ (\mathrm{mod}\ 31)$$

公開 키 $k_2$를 $3\equiv 24^{k_2}(\mathrm{mod}\ 31)$로부터 求해보자.

$q_1=2$, $\beta=24$, $k_2'=3$에 대해

$$\gamma_1=\beta^{(q-1)/q_1}=24^{15}\ (\mathrm{mod}\ 31)\equiv -1\ (\mathrm{mod}\ 31)$$

가 求해짐으로 $\gamma_1^0=1$이고 $\gamma_1^1=-1$이다.

$z_1=(k_2')^{(q-1)/q_1}=3^{15}$를 利用하면, $z_1=(3)^8(3)^4(3)^3=(20)(19)(-4)\ (\mathrm{mod}\ 31)\equiv -1520\ (\mathrm{mod}\ 31)=-1\ (\mathrm{mod}\ 31)$이 되고, $z_1\equiv -1\ (\mathrm{mod}\ 31)$, $z_1=-1=\gamma_1^1$이므로 $\beta_1=1$이 된다.

$q_2=3$인 경우에도 앞에서처럼 計算하면 $\gamma_2=(24)^{10}\ (\mathrm{mod}\ 31)\equiv 25\ (\mathrm{mod}\ 31)$이 된다. 따라서 $\gamma_2^0=1$, $\gamma_2^1=25$, $\gamma_2^2\equiv 5\ (\mathrm{mod}\ 31)$이고, $3^4=81\equiv 19\ (\mathrm{mod}\ 31)$ 이므로

$$z_2=(k_2')^{(q-1)/q_2}=3^{10}\ (\mathrm{mod}\ 31)$$
$$=(9)(19)(19)\ (\mathrm{mod}\ 31)\equiv 25\ (\mathrm{mod}\ 31)$$

$z_2$와 $\gamma_2^i$元素들을 比較하면 $z_2=25=\gamma_2^1$이므로 $\beta_2=1$이다.

$q_3=5$인 경우에는 $\gamma_3=4\ (\mathrm{mod}\ 31)$이다. 따라서 數列은 다음처럼 된다.

$$(\gamma_3^0,\gamma_3^1,\gamma_3^2,\gamma_3^3,\gamma_3^4)=(1,4,16,2,8)$$

$z_3=(k_2')^{(q-1)/q_3}=3^6=729\equiv 16\ (\mathrm{mod}\ 31)$이므로 $z_3=16=\gamma_3^2$이 된다. 따라서, $\beta_3=2$로 定해지고 公開 키 $k_2$는 다음처럼 決定된다.

$$k_2=[1\ (\mathrm{mod}\ 2),\ 1\ (\mathrm{mod}\ 3),\ 2\ (\mathrm{mod}\ 5)]$$
$$\equiv 7\ (\mathrm{mod}\ 31)$$

마지막으로 $5\equiv 24^{k_3}(\mathrm{mod}\ 31)$로부터 公開 키 $k_3$를 決定해 보자.

$q_1=2$에 대해 $\gamma\equiv -1\ (\mathrm{mod}\ 31)$이므로 $\gamma_1^0=1$, $\gamma_1^1=-1$이 된다. $5^4\ (\mathrm{mod}\ 31)\equiv 5$, $5^8\ (\mathrm{mod}\ 31)\equiv 25$, $5^3\ (\mathrm{mod}\ 31)\equiv 1$ 이므로

$$z_1=5^{15}\ (\mathrm{mod}\ 31)=(5^8)(5^4)(5^3)\ (\mathrm{mod}\ 31)$$
$$\equiv(25)(5)(1)\ (\mathrm{mod}\ 31)$$
$$\equiv 125\ (\mathrm{mod}\ 31)\equiv 1$$

따라서 $z_1=1=\gamma_1^0$, 그러므로 $\beta_1=0$이 된다.

$q_2=3$에 대해 $\gamma_2\equiv 25\ (\mathrm{mod}\ 31)$이므로 $\gamma_2^0=1$, $\gamma_2^1=25$, $\gamma_2^2=5$를 얻는다. $5^2=25\equiv -6\ (\mathrm{mod}\ 31)$을 알고 있으므로, $5^4\equiv 36\ (\mathrm{mod}\ 31)\equiv 5\ (\mathrm{mod}\ 31)$이 된다. 따라서

$$z_2=5^{10}\ (\mathrm{mod}\ 31)=(5)(5)(25)\ (\mathrm{mod}\ 31)$$
$$=625\ (\mathrm{mod}\ 31)\equiv 5$$

$z_2$와 $\gamma_2^i$元素들을 i=0,1,2에 대해 比較하면 $z_2=5=\gamma_2^2$이므로 $\beta_2=2$이다.

$q_3=5$인 경우, 앞에서 計算한 것처럼 $\gamma_3=4\ (\mathrm{mod}\ 31)$이고 $\gamma_3^0=1$, $\gamma_3^1=4$, $\gamma_3^2=16$, $\gamma_3^3=2$, $\gamma_3^4=8$ 이다. $z_3=5^6=(5^4)(5^2)=125\equiv 1\ (\mathrm{mod}\ 31)$이므로 $z_3=1=\gamma_3^0$이 되고 $\beta_3=0$이 된다. 結局 公開 키 $k_3$는 다음과 같다.

$$k_3=[0\ (\mathrm{mod}\ 2),\ 2\ (\mathrm{mod}\ 3),\ 0\ (\mathrm{mod}\ 5)]$$
$$\equiv 20\ (\mathrm{mod}\ 31)$$

따라서 公開 키 벡터 $K_P$는 다음처럼 된다.

$$K_P=(k_1,k_2,k_3)=(18,\ 7,\ 20)$$

式(18)을 使用하면 전송되는 暗號文 Y는 다음과 같다.

$$Y=k_1x_1+k_2x_2+k_3x_3$$

그러나 $X=(x_1,\ x_2,\ x_3)=(1\ 1\ 1)$이므로 $Y=k_1+k_2+k_3=18+7+20=45$가 된다. 式(19)를 利用하면

$$Y'\equiv\beta^Y=24^{45}\ (\mathrm{mod}\ 31)$$

를 얻을 수 있다. 여기서 $\beta=24$, $Y=45$이다. 앞에서 본 것처럼 $24^{15}\ (\mathrm{mod}\ 31)\equiv 30\ (\mathrm{mod}\ 31)\equiv -1\ (\mathrm{mod}\ 31)$이다. 따라서 다음처럼 하면 期待했던 대로 $X=(1\ 1\ 1)$을 얻는다.

$$Y' = (24)^{15}(24)^{15}(24)^{15} \pmod{31}$$
$$= (-1)(-1)(30) \pmod{31} \equiv 30$$
$$= (2^1)(3^1)(5^1)$$

### 3.3 Multiple iterative knapsack 方法

Merkle-Hellman knapsack 알고리즘의 세번째 形態는 모듈로 곱셈에 基礎한 反復 knapsack 方式이다. 公開 暗號化 키를 다음처럼 놓자.

$$K_P = (k_1, k_2, \cdots, k_n)$$

祕密復元 키 $K_S$는, $K_P$를 簡單한 knapsack으로 變形시키는 方法을 利用해서 求할 수 있다. 그리고 $K_S$는 $1 \leq i \leq n$에 대해서 $k_i' > \sum_{j=1}^{i-1} k_j'$, $1 \leq i \leq n$, 를 滿足하는 超增加數列인 n개의 陽의 整數 벡터이다.

$$K_S = (k_1', k_2', \cdots, k_n')$$

暗號化는 $Y = \sum_{i=1}^{n} k_i x_i$ 이고 復號化는 knapsack $k_1, k_2, \cdots, k_n$과 合 Y를 利用한 knapsack 問題를 푸는 것이다.

祕密 키 $K_s$를 다음 式과 같이 反復的으로 生成하는 키, 即 $1 \leq k \leq j$에 대응하는 $K_s^k$라 정의하자.

$$\begin{aligned} K_s^0 &= (k_0^1, k_0^2, \cdots, k_0^n) \\ K_s^1 &= (k_1^1, k_1^2, \cdots, k_1^n) \\ K_s^2 &= (k_2^1, k_2^2, \cdots, k_2^n) \\ &\vdots \\ K_s^j &= (k_j^1, k_j^2, \cdots, k_j^n) = K_P \end{aligned} \tag{23}$$

여기서 $1 \leq i \leq n$과 $0 \leq m \leq j$에 대해 $k_m^i > \sum_{\lambda=1}^{i-1} k_m^\lambda$ 이다.

設計者는 $0 \leq i \leq j-1$에 대해 $m_i > \sum_{\lambda=1}^{n} k_i^\lambda$와 $\gcd(w_i, m_i) = 1$을 滿足하는 두개의 큰 祕密整數 $m_i$와 $w_i$를 선택해야 한다. $K_S^j$를 計算하기 위해 다음의 過程을 밟아야 한다. i=0인 경우 $m_0 > \sum_{\lambda=1}^{n} k_0^\lambda$이고 $\gcd(w_0, m_0) = 1$이다.

$$\begin{aligned} k_1^1 &\equiv w_0 k_0^1 \pmod{m_0} \\ k_1^2 &\equiv w_0 k_0^2 \pmod{m_0} \\ &\vdots \\ k_1^n &\equiv w_0 k_0^n \pmod{m_0} \end{aligned} \tag{24}$$

i=1인 경우 $m_1 > \sum_{\lambda=1}^{n} k_1^\lambda$이고 $\gcd(w_1, m_1) = 1$이다.

따라서

$$\begin{aligned} k_2^1 &\equiv w_1 k_1^1 \pmod{m_1} \\ k_2^2 &\equiv w_1 k_1^2 \pmod{m_1} \\ &\vdots \\ k_2^n &\equiv w_1 k_1^n \pmod{m_1} \end{aligned} \tag{25}$$

같은 방법으로 i=j−1에 대해 $m_{j-1} > \sum_{\lambda=1}^{n} k_{j-1}^\lambda$와 $\gcd(w_{j-1}, m_{j-1}) = 1$이므로

$$\begin{aligned} k_j^1 &\equiv w_{j-1} k_{j-1}^1 \pmod{m_{j-1}} \\ k_j^2 &\equiv w_{j-1} k_{j-1}^2 \pmod{m_{j-1}} \\ &\vdots \\ k_j^n &\equiv w_{j-1} k_{j-1}^n \pmod{m_{j-1}} \end{aligned} \tag{26}$$

祕密 키와 公開 키는 다음과 같이 決定된다.

$$\begin{aligned} K_s^0 &= (k_0^1, k_0^2, \cdots, k_0^n) \quad \text{(祕密復號化 키)} \\ K_P &= k_s^j = (k_j^1, k_j^2, \cdots, k_j^n) \quad \text{(公開暗號化 키)} \\ &\{(w_0, m_0), (w_1, m_1), \cdots, (w_{j-1}, m_{j-1})\} \\ &\text{(祕密키 偏差)} \end{aligned}$$

平文 X를 公開 키 $K_P$로 暗號化하면 暗號文 Y는 $Y = K_P X$로 얻어진다. Y로부터 X를 復元하기 위해 $Y' \equiv vY \pmod{m}$이 되도록 w의 乘算逆元(multiplicative inverse)인 v를 利用하여 Y를 Y'로 變換하는 것이다. 여기서 $v = w^{-1}$이고 $ww^{-1} = 1$이다. 따라서 다음 式이 成立된다.

$$\begin{aligned} w_0 w_1^{-1} &\equiv 1 \pmod{m_0} \\ w_1 w_1^{-1} &\equiv 1 \pmod{m_1} \\ &\vdots \\ w_{j-1}^{-1} w_{j-1} &\equiv 1 \pmod{m_{j-1}} \end{aligned} \tag{27}$$

平文벡터가 $X = (x_0, x_1, \cdots, x_n)$이고 公開 키가 $K_P = (k_0, k_1, \cdots, k_n)$라 할 때 暗號文 Y는 다음과 같이 얻어진다.

$$\begin{aligned} Y = K_P X &= \sum_{i=1}^{n} k_i x_i \\ &= k_1 x_1 + k_2 x_2 + \cdots + k_n x_n \end{aligned}$$

復元過程을 위한 反復變換을 다음에 說明하기로 하자. 暗號文 Y를 받은 후 다음 式처럼 $w_{j-1}^{-1}$과 Y를 곱하여 $Y^{(1)}$를 구한다.

$$Y^{(1)} = w_{j-1}^{-1} Y \pmod{m_{j-1}} \quad (28)$$

式(23)을 觀察하건데 $k_i = k_j^i$로 놓을 수 있으므로 $Y = \sum_{i=1}^{n} k_i^i x_i$가 된다. 따라서 式(28)은 다음과 같이 表現된다.

$$Y^{(1)} = w_{j-1}^{-1} \sum_{i=1}^{n} w_{j-1} k_{j-1}^i x_i \pmod{m_{j-1}}$$
$$= \sum_{i=1}^{n} k_{j-1}^i x_i \pmod{m_{j-1}} \quad (29)$$

같은 方法으로 두번째 變換은 다음과 같다.

$$Y^{(2)} = w_{j-2}^{-1} Y^{(1)} \pmod{m_{j-2}} \quad (30)$$

式(26)에 依하면 $k_{j-1}^i = w_{j-2} k_{j-2}^i$이므로 $Y^{(2)}$는 다음과 같이 된다.

$$Y^{(2)} = w_{j-2}^{-1} \sum_{i=1}^{n} w_{j-2} k_{j-2}^i x_i \pmod{m_{j-2}}$$
$$= \sum_{i=1}^{n} k_{j-2}^i x_i \quad (31)$$

여기서 $w_{j-2}^{-1} w_{j-2} = 1$이다. 變換을 두번 해본 結果로 보아 變換을 j번 해도 無妨하다. 고로 이 過程을 必要한만큼 反復할 수 있다는 것이 明白하다. 즉 各各 連續的으로 變換함으로써 公開키 $K_P$의 構造는 더욱더 알기 어렵게 될 것이다. 그래서 j번째 變換인 $Y^{(j)}$는 다음과 같이 計算된다.

$$Y^{(j)} \equiv w_0^{-1} Y^{(j-1)} \pmod{m_0}$$
$$\equiv w_0^{-1} \sum_{i=1}^{n} k_i x_i^i \pmod{m_0}$$
$$\equiv w_0^{-1} \sum_{i=1}^{n} (w_0 k_0^i) x_i \pmod{m_0}$$

式(27)을 使用하면 다음과 같다.

$$Y^{(j)} = \sum_{i=1}^{n} k_0^i x_i \quad (32)$$

다음 例題는 위 反復方法을 理解하는 데 도움을 주는 技法을 說明하기 위해서이다.

[例題 6] 祕密 키 $k_s^0 = (k_0^1, k_0^2, k_0^3) = (5, 10, 20)$를 式 $k_0^i > \sum_{n=1}^{n} k_0^j$에 合當하게 選擇되었다고 假定하고, 反復키 $k_s^1$와 $k_s = k_P^2$(公開 키)를 計算하자. 두數 w와 m은 w가 法m에 대해 逆元이 있고 $\gcd(w, m) = 1$이 되도록 選擇한다. $w_0 = 17$과 $m_0 = 47 > \sum_{\lambda=1}^{3} k_1 = 5+10+20 = 35$를 擇하면 $\gcd(w_1, m_0) = \gcd(17, 47) = 1$가 된다. 첫번째 反復키 $k_s = (k_1^1, k_1^2, k_1^3)$를 다음과 같이 計算한다.

$$k_1^1 \equiv w_0 k_0^1 \pmod{m_0}$$
$$\equiv 17 \cdot 5 \pmod{47} \equiv 38$$
$$k_1^2 \equiv w_0 k_0^2 \pmod{m_0}$$
$$\equiv 17 \cdot 10 \pmod{47} \equiv 29$$
$$k_1^3 \equiv w_0 k_0^3 \pmod{m_0}$$
$$\equiv 17 \cdot 20 \pmod{47} \equiv 11$$

따라서 $k_s = (38, 27, 11)$이 구해진다.

$w_1 = 3$와 $m_1 = 89 > \sum_{\lambda=1}^{n} k_1^\lambda = 38+29+11 = 78$이 되도록 $w_1$과 $m_1$을 擇하면 $\gcd(w_1, m_1) = \gcd(3, 89) = 1$이 된다. 正確하게 公開키 $k_P = (k_1, k_2, k_3)$와 같은 두번째 反復키 $k_s = (k_2^1, k_2^2, k_2^3)$를 計算한다. 그러므로 $k_P$의 成分들은 다음과 같다.

$$k_1 \equiv w_1 k_1^1 \pmod{m_1}$$
$$\equiv 3 \cdot 38 \pmod{89} \equiv 25$$
$$k_2 \equiv w_1 k_1^2 \pmod{m_1}$$
$$\equiv 3 \cdot 29 \pmod{89} \equiv 87$$
$$k_3 \equiv w_1 k_1^3 \pmod{m_1}$$
$$\equiv 3 \cdot 11 \pmod{89} \equiv 33$$

따라서 公開키는 $k_P \equiv (25, 87, 33)$이다.

Euclid 알고리즘을 使用하여 $w_0^{-1}$는 다음과 같이 變數 $w_0 = 17$와 $m_0 = 47$로부터 決定한다.

$$47 = (17)2 + 13$$
$$17 = (13)1 + 4$$
$$13 = (4)3 + 1$$
$$4 = (4)1$$

따라서 $\gcd(17, 47) = 1$이다. 이제 $w_0 \pmod{m_0}$의 逆元을 다음과 같이 計算할 수 있다.

$$13 = 47 - (17)2$$
$$4 = 17 - (13)1 = (17)3 - 47$$
$$1 = 13 - (4)3 = (47)4 - (17)11$$

마지막 式이 $1 \equiv (-11)17 \pmod{47}$로 表現될 수 있으므로 $w_0^{-1} = -11 \pmod{47} = (-11+47) \pmod{47} \equiv 36$을 얻는다. 같은 方法으로 $w_0^{-1}$는 $w_1 = 3$과

$m_1=89$를 사용하여 다음과 같이 計算한다.

$$89=(3)29+2$$
$$3=(2)1+1$$
$$2=(2)1$$

위 式은 gcd(3,89)=1이라는 것을 보여준다. 위 方程式들을 사용하면 다음과 같이 計算된다.

$$2=89-(3)29$$
$$1=3-(2)1=3-(89-3\times 29)$$
$$=(3)30-89$$

마지막 式은 $1=(3)30 \pmod{89}$로 表現된다. 따라서 $w_1=3$의 乘算逆元은 $w_1=30$이다. 暗號化되어질 平文이 X=(101)이라 假定하자. 그러면 暗號文은 다음과 같이 얻을 수 있다.

$$Y=X\cdot K_P=\sum_{i=1}^{3}k_ix_i=25+33=58$$

다음은 復元化 過程을 생각하자. 暗號文 Y=58를 받았을 때, 乘算逆元 $w_0^{-1}=36$과 $w_0^{-1}=30$下에서 祕密 키 $k_s=(5,10,20)$을 가지고 平文 X를 復元해야 한다. 여기서 $m_0=47$와 $m_1=89$이다. Y를 $w_1^{-1}$로 곱하면 $Y^{(1)}$는 다음과 같이 얻어진다.

$$Y^{(1)}\equiv w_1^{-1}Y \pmod{m_1}$$
$$\equiv (30)(58) \pmod{89}=49$$

$Y^{(1)}=w_0^{-1} \pmod{m_0}$를 곱하면 다음과 같은 結果가 된다.

$$Y^{(2)}\equiv w_0^{-1}Y^{(1)} \pmod{m_1}$$
$$\equiv (36)(49) \pmod{47}=25$$

따라서, $Y^{(2)}=25=5+20$이므로 復元된 平文은 X=(101)이다.

Merkle-Hellman시스템은 Multiplicative knapsack方式과 Iterative knapsack方式에서 言及했던 것처럼 Knapsack 問題에 根據를 두었다. 특히, Iterative knapsack方式은 單純 Knapsack을 강추기 위해 Additive knapsack과 Multiplicative knapsack 方式의 安全과 有用性을 改善하기 위해 처음으로 紹介되었다. 그러나 Shamir(1984)가 基礎的인 Knapsack暗號方式이 不安定하다는 論文을 發表했다. 追加로 Adleman(1983)과 Brickell(1985)이 反復暗號方式의 不安定을 證明했다.

## 4. RSA 公開 키 暗號시스템

Diffie와 Hellman이 公開 키 暗號시스템을 紹介한 後 곧 Rivest, Shamir와 Adleman(RSA)는 가장 有望한 公開 키 暗號시스템을 提案했다. RSA方式의 완벽한 說明을 이번 절에서 紹介한다.

暗號시스템은 各各 자기자신의 暗號 키와 復元 키를 가지는 使用者들의 集合으로 構成된다. 暗號키(公開)는 整數 r과 $k_p$로 構成하고 復元 키(祕密)는 整數 $k_s$이다. 이 方式에서 r은 주의깊게 選擇된 두개의 큰 素數 p와 q를 곱한 整數이다. 즉 r=pq이다. $k_p$는 公開 키를 나타내고 $k_s$는 祕密 키를 表示한다. $k_s$와 $k_p$는 各 키가 $\phi(r)$에 서로素가 되도록 選擇해야 한다. 여기서 $\phi(r)=(p-1)(q-1)$은 Euler의 totient 函數라고 한다.

暗號文 Y는 平文 X, $0\leq X\leq r-1$,를 $k_p \pmod r$ 乘한 것이고 反面에 復元은 아래式처럼 暗號文 Y를 $k_s \pmod r$乘하여 얻는다.

$$E_{K_p}(X)=Y=X^{K_p} \pmod r \quad (33)$$
$$D_{K_s}(Y)=Y^{K_s} \pmod r.$$
$$=X^{K_pK_s} \pmod r=X \pmod r \quad (34)$$

여기서 $0\leq X\leq r-1$과 gcd(X,r)=1이다.

定理 2.6을 參照하면 Euler의 公式은 gcd(a,r)=1에 대해 $a^{\phi(r)}=1 \pmod r$이다. a=X를 平文이라 하자. 그러면 Euler의 公式은 다음과 같이 된다.

$$X^{\phi(r)}=1 \pmod r \quad (35)$$

여기서 gcd(X,r)=1이다. 즉, 平文 X는 r에 서로素이다. 定理 2.3 즉, $a=b \pmod r$이면 어떤 陽의 整數 λ에 대해서 $a^\lambda=b^\lambda \pmod r$를 使用하면 式(36)은 다음 式과 같이 된다.

$$X^{\lambda\phi(r)}=1 \pmod r \quad (36)$$

$a=b \pmod r$이면 어떤 整數 μ에 대해 $a\mu=b\mu \pmod r$이므로 式(36)은 다음과 같이 된다. 즉,

$$X^{\lambda\phi(r)}\cdot X=X \pmod r$$

또는

$$X^{\lambda\phi(r)+1}=X \pmod r \qquad (37)$$

$\lambda\phi(r)+1=K_pK_s$와 같이 選擇하면 公開 키 $K_p$와 秘密 키 $K_s$는 式(38)을 滿足하도록 選擇할 수 있다.

$$K_pK_s=1 \pmod{\phi(r)} \qquad (38)$$

따라서, 式(37)은 다음과 같이 再表現할 수 있다.

$$X^{K_pK_s}=X \pmod r \qquad (39)$$

여기서 $\gcd(X,r)=1$이면 어떤 平文 X에 대해서도 成立한다. 式(39)는 또한 復元變換을 나타내는 $Y^{K_s}=X \pmod r=D_{K_s}(Y)$로 表示한다. 여기서 暗號文은 $Y=X^{K_p} \pmod r$이다.

[例題 7] 두 素因數 3과 7을 갖는 合成數 21에 대해 Euler의 totient 函數를 구하라. $\phi(21)=(3-1)(7-1)=12$개 整數들이 21에 서로素이어야 하기 때문에 그것들은 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20이다.

키의 雙 즉, $K_p$(公開 키)와 $K_s$(秘密 키)들을 만들기 위해 다음 過程을 생각하자.

1. 두 秘密 素數 p와 q를 選擇한다. 여기서 $p \neq q$이다.
2. 公開法인 곱 $r=pq$를 計算한다. 여기서 p와 q는 無作爲로 選擇한다.
3. 秘密 整數들인 Euler의 $\phi$-函數 $\phi(r)=(p-1)(q-1)$를 計算한다.
4. $K_pK_s=1 \pmod{\phi(r)}$임을 滿足하도록 $K_p$와 $K_s$를 選擇한다. 이것들은 $\phi(r)$에 서로素이다.
5. Euclid의 알고리즘을 사용하여 $K_p$ 또는 $K_s$ 法 r의 乘算逆元을 計算한다.

이제, 이들 必要條件을 滿足하는 $K_p$와 $K_s$를 選擇하는 일이 남아 있다.

단지 $d \mid b$이면 線形合同 $az=b \pmod n$는 正確하게 d개의 解를 갖는다. 여기서 $d=\gcd(a,n)$이다. 그러나 $a=K_s$, $b=1$ 그리고 $n=\phi(r)$이라 놓으면 $\gcd(K_s, \phi(r))=1$이라는 條件에 의해 $K_s$는 $\phi(r)$에 서로素이고 結論的으로 $\gcd(K_s, \phi(r))=1$은 1을 나눈다. 따라서 $z=K_p$를 選擇할 때 合同 $K_sz=1 \pmod{\phi(r)}$은 式(38)인 $K_pK_s=1 \pmod{\phi(r)}$이 된다. 이 合同은 $K_p$와 $K_s$를 求하는데 效率的인 方法을 제공한다. $K_pK_s=1 \pmod{\phi(r)}$를 滿足하는 $K_p$와 $K_s$를 求하기 위한 方法은 다음의 네번째 例題에서 檢討한다.

充分하게 큰 集合에서 秘密素數들을 選擇할 것과 그것들을 計算할 때에 效率的으로 計算하기를 推薦한다. 가장 큰 素數表가 充分한 安定性을 주기 위해 p와 q를 選擇하기 위해 必要하다. 보다 仔細한 說明을 위해 아래에 1부터 100까지의 素數를 보였다. 그러나 勿論 그것들은 實際 使用하기에는 매우 작은 素數이다. 100以下의 素數는 아래에서 보여주는 것처럼 25개이다.

[例題 8] 素數 p=41과 q=59를 選擇하자. 이때 $r=pq=2419$이고 $\Phi(r)=(p-1)(q-1)=2320$이다. $K_s=151$을 秘密 키라 할때, $k_s=151$에 對應되는 公開 키 $K_p$인 151 (mod 2320)의 乘算逆元을 찾아라. $\gcd(K_S, \Phi(r))=\gcd(151, 2320)=1$은 Euclid 알고리즘에 의해 證明할 수 있으므로, $K_P$의 값은 다음과 같이 計算된다.

$2320=(151)15+55$
$151=(55)2+41$
$55=(41)1+14$
$41=(14)2+13$
$14=(13)1+1$ (零이 아닌 마지막 나머지)
$13=(1)13$

零이 아닌 마지막 나머지가 1이므로 $\gcd(151, 2320)=1$이 된다. 따라서 두 整數 151과 2320은 서로素이다. 이제 $\gcd(K_S, \phi(r))=a\,K_S+b\,\phi(r)$인 關係에 의해 2320과 151의 線形結合으로 1을 表現할 수 있고 다음과 같다.

$1=14-(13)1$
$1=14-(41-14\times2)=(14)3-41$
$1=(55-41)3-41=(55)3-(41)4$
$1=(55)3-(151-(55)2)4=(55)11-(151)4$
$1=(2320-151\times15)11-(151)4$
$1=(2320)11-(151)169$ (40)

여기서 a=169=$K_P$이고 b=11이다. 또한, 式(40)은 1=−(151)(169) (mod 2320)으로 再表現할 수 있다. 따라서 公開 키 $K_p$=169가 祕密 키 $K_s$=151 (mod Φ(r)=2320)의 乘算逆元이 아니라는 것을 알 수 있다.

[例題 9] r=pq이고 α가 集合 {0, 1, 2, ⋯, r−1}內로 制限되어 있을때 어떠한 整數 α에 대해서도 $\alpha^{\Phi(r)+1}=\alpha$가 成立함을 보여라. Euler의 定理에 의해, $\alpha^{\Phi(r)}=1$ (mod r)은 集合 {0, 1, 2, ⋯, r−1} 內에 있는 모든 α 값에 대해 成立한다. p=3과 q=5인 境遇에 대하여 考察하자. 이때 r=pq=15이고, r에 대한 Euler의 totient 函數는 φ(r)=(p−1)(q−1)=8이다. 이것은 r=15와 서로素인 數가 8個임을 가리킨다. 集合 {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14}을 考慮해보자. 여기서 r=15와 서로素인 α의 集合은 {1, 2, 4, 7, 8, 11, 13, 14}이다. 集合 {0, 1, 2, ⋯, 12, 13, 14} 內의 모든 α값에 대해 $\alpha^{\phi(r)+1}=\alpha$ (mod r)를 計算하면 아래와 같다. 여기서 r=15이고 φ(r)=8이므로, φ(15)+1=9가 된다.

| α | $\alpha^{\phi(15)+1}$ (mod 15) |
|---|---|
| 1 | 1 |
| 2 | $2^9$ (mod 15)=512 (mod 15)=2 |
| 3 | $3^9$ (mod 15)=19683 (mod 15)=3 |
| 4 | $4^9$ (mod 15)=262144 (mod 15)=4 |
| 5 | $5^9$ (mod 15)=1953125 (mod 15)=5 |
| ⋮ | ⋮ |
| 13 | $13^9$ (mod 15)=10604499373 (mod 15)=13 |
| 14 | $14^9$ (mod 15)=20661046784 (mod 15)=14 |

結局, r=pq에 대해, 集合 {1, 2, ⋯, r−1}內의 어떠한 α값에 대해서도 $\alpha^{\phi(r)+1}=\alpha$ (mod r)가 成立함을 보였다.

$K_PK_S=1$ (mod φ(r))를 滿足하는 $K_p$와 $K_s$, 그리고 gcd(X, r)=1이 되는 集合 (0, 1, 2, ⋯, r−1) 內의 平文 X가 주어지면, $X^{k_pk_s}=X$ (mod r)이 됨을 알았다. 이제, $K_PK_S=1$ (mod φ(r))은 어떤 整數 m에 대하여 $K_PK_S=m\ \phi(r)+1$임을 意味한다. 따라서 $X^{k_pk_s}=X^{m\phi(r)+1}=X\cdot X^{m\phi(r)}=X(X^{\phi(r)})^m=X(1)^m$ (mod r) 即, $X^{k_pk_s}=X$ (mod r)이 成立한다. $K_PK_S=K_SK_P$이므로, 暗號化 및 復號化는 對稱的으로 交換이 可能하다. 이러한 對稱性 때문에 RSA 技法은 公開 키 시스템에서 디지틀 署名과 認證에 利用될 수 있다.

平文 메세지 X를 暗號化하기 위해서는 1<n<r−1인 一連의 n 디지트 各各에 平文 메세지를 집어넣는다. 文字는 一般的으로 8 비트인 ASCII 코드로 表現되나, 여기서는 簡單하게 하기 위해서 아래와 같이 平文의 各 文字에 대해 두자리 數를 使用하여 表現한다.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Blank | 00 | E | 05 | J | 10 | O | 15 | T | 20 | Y | 25 |
| A | 01 | F | 06 | K | 11 | P | 16 | U | 21 | Z | 26 |
| B | 02 | G | 07 | L | 12 | Q | 17 | V | 22 | | |
| C | 03 | H | 08 | M | 13 | R | 18 | W | 23 | | |
| D | 04 | I | 09 | N | 14 | S | 19 | X | 24 | | |

[例題 10] p=41과 q=59를 選擇하자. 여기서 r=(41)(59)=2419이고 φ(r)=(40)(58)=2320이다. $K_s$=151이라 놓으면 $K_p$=169가 된다. 平文 "PUBLIC KEY CRYPTOGRAPHY"는 4자리 숫자의 블럭으로 다음과 같이 各各 表現된다.

| | | | | | |
|---|---|---|---|---|---|
| 1621 | 0212 | 0903 | 0011 | 0525 | 0003 |
| 1825 | 1620 | 1507 | 1801 | 1608 | 2500 |

첫 블럭인 1621은 $K_p$=169를 冪乘하고 r=2419로 나눈 나머지 1757을 暗號文 Y의 첫째 블럭으로 擇함으로서 暗號化된다. 即, $1621^{169}$ (mod 2419)=1757이다. 따라서, 全體 平文 X는 다음과 같이 暗號化된다.

| | | | | | |
|---|---|---|---|---|---|
| 1757 | 0874 | 1272 | 1447 | 0241 | 1315 |
| 1843 | 2376 | 1931 | 1842 | 0788 | 1393 |

같은 方法으로, 暗號文 Y의 첫째 블럭 1757은 $K_s$=151을 冪乘하고, r=2419로 나눈 나머지 1258을 復元된 平文 X의 첫째 블럭으로 擇함으로서 復號된다.

| | | | | | |
|---|---|---|---|---|---|
| 1259 | 1974 | 1026 | 0220 | 2055 | 1613 |
| 1519 | 0330 | 0496 | 2282 | 2246 | 1150 |

그러나, 이것은 $K_PK_S=-1$ (mod φ(r))이라는 잘못된 關係 때문에 元來의 平文과는 完全히 다른

結果로 나타났다. 따라서 復號는 事實上 正確하게 된 것이 아니다. 그러므로 우리는 이러한 어려움을 克服하기 위하여 또다른 '方法을' 찾아야 한다.

式 (28)은

$$1=c\ \phi(r)-K_sK_P \qquad (41)$$

인 形態를 갖는다. 여기서 c=11, $\phi(r)=2320$, $K_S=151$, 그리고 $K_P=169$이다. 萬一, 式(29)에서 $K_S$가 $\phi(r)-K_S$로 代置된다면,

$$1=(c-K_P)\ \phi(r)+K_sK_P \qquad (42)$$

로 주어진다. 여기서 $c-K_P$는 整數이다. 式(30)은 式(29)에서의 $K_s$를 $\phi(r)-K_s$로 代置하면

$$1=K_SK_P\ (\mathrm{mod}\ \phi(r))$$

으로 再表現된다. 새로운 祕密 키는 $K'=\phi(r)-K_S=2169$이므로, 復元된 平文 블럭 $x_i$, $1\leq i\leq 12$는 各各 $1757^{2169}\ (\mathrm{mod}\ 2419)=1621$, $0874^{2169}\ (\mathrm{mod}\ 2419)=0121$ 等으로 얻어진다. 따라서, 이 例題의 다시 만들어진 正確히 復元된 平文은 다음과 같다.

| | | | | | |
|---|---|---|---|---|---|
| 1621 | 0212 | 0903 | 0011 | 0525 | 0003 |
| 1825 | 1620 | 1507 | 1801 | 1608 | 2500 |

[例題 11] 祕密 素數 p=41과 q=59를 다시 利用하자. 앞의 例에서와 같이 $r=pq=2419$, $\phi(r)=(p-1)(q-1)=2320$이나, 祕密 키를 $K_S=157$로 選擇한다. Euclid 알고리즘을 利用하여, $K_S$가 $\phi(r)$과 서로素 與否, 即, $\gcd(K_S,\ \phi(r))=\gcd(157,2320)=1$인가를 檢査할 수 있고 다음과 같다.

$$2320=(157)14+122$$
$$157=(122)1+35$$
$$122=(35)3+17$$
$$35=(17)2+1$$
$$17=(1)17$$

따라서, $\gcd(157,2320)=1$임이 證明된다. 다음으로, $K_S=157$의 乘算逆元인 $K_p$를 計算하면 다음과 같다.

$$1=35-(17)2$$
$$1=(35)7-(122)2$$
$$1=(157)7-(122)9$$
$$1=(157)133-(2320)9$$

이것은 $K_s=157$과 $K_P=133$에 대해 $1=(157)(133)\ (\mathrm{mod}\ 2320)=K_SK_P\ (\mathrm{mod}\ \phi(r))$ 임을 나타낸다.

公開 키 $K_P=133$을 利用하면, 平文 "PUBLIC KEY CRYPTOGRAPHY"는 다음과 같이 暗號文 블럭으로 暗號化된다.

| | | | | | |
|---|---|---|---|---|---|
| 2362 | 0299 | 0821 | 0663 | 0555 | 1022 |
| 1153 | 0251 | 1460 | 0823 | 2100 | 1229 |

祕密 키 $K_S=157$을 利用하면, 暗號文 Y의 첫째 블럭은 $2363^{157}\ (\mathrm{mod}\ 2419)=1621$로 復號되어 復元된 平文의 첫째 블럭이 된다. 같은 方法으로, 暗號文의 全體 블럭을 復號化 할 수 있고 블럭 對 블럭 復號化로 全體 復元된 平文을 얻을 수 있다.

## 5. McEliece의 公開 키 暗號시스템

1978년에 McEliece는 誤謬訂正코드에 基礎를 둔 公開 키 暗號시스템을 제안했다. 그의 暗號시스템이 生成行列 **G**인 Goppa符號를 利用한 **G** 行列을 公開 키 시스템의 公開 키 **G'**로 變形하였다. 본 公開 키 暗號시스템은 情報벡터 **m**을 **G'**로 곱한 符號語(code word) **c**에, 길이가 n이고 重(weight)이 t인 誤謬形態 **e**를 더하여 暗號文 **c**를 生成한다. 그리고 受信段에서는 Goppa符號에 대한 復號알고리즘을 適用함으로써 復元할 수 있다.

優先 McEliece 暗號시스템을 記述하기 전에 誤謬訂正方法을 간단히 紹介한다. k-bit 情報文을 $\mathbf{m}=(m_0, m_1, \cdots, m_{k-1})$라 하자. 符號語 $\mathbf{c}=(c_0, c_1, \cdots, c_{n-1})$는 $(k\times n)$ 生成行列 $\mathbf{G}=[\mathbf{P}_{k\times(n-k)}:\mathbf{I}_k]$에 **m**을 곱하여 다음과 같이 生成된다.

$$\mathbf{c}=\mathbf{m}\cdot\mathbf{G} \qquad (43)$$

여기서 $\mathbf{c}=(\gamma_0, \gamma_1, \cdots, \gamma_{n-k-1}, m_0, m_1, \cdots, m_{k-1})$은 (n, k) 線形組織形符號의 符號이고 **c**의 成分중 $(\gamma_0, \gamma_1, \cdots, \gamma_{m-k-1})$은 페리티檢査비트이다. 符號語 **c**가 線路를 통해 傳送되는 동안 誤謬形態 $\mathbf{e}=(e_0, e_1, \cdots, e_{n-1})$가 附加된다. 따라서 受信語 $\mathbf{r}=(r_0, r_1, \cdots, r_{n-1})$은 **c**와 **e**의 벡터合으로 만들어 진다.

$$\mathbf{r}=\mathbf{c}+\mathbf{e} \tag{44}$$

**r**을 受信한 復號機는 먼저 誤症을 求한 후, 復號 알고리즘을 利用하여 이에 대한 誤謬形態 **e**를 求해야 한다. 誤謬形態 **e**가 일단 求해지면 벡터 **r**+**e**는 受信符號語 $\hat{\mathbf{c}}$가 된다. 即,

$$\hat{\mathbf{c}}=\mathbf{r}+\mathbf{e} \tag{45}$$

이와 같은 방법으로 **r**에 포함된 **e**는 訂正되어, **m**을 求할 수 있다.

McEliece의 公開 키 暗號시스템은 다음과 같다. **G**를 線形符號의 t-誤謬訂正(k×n) 生成行列이라 하자. McEliece의 暗號시스템은 任意의 (k×k) 比特異(non-singular) 行列인 스크램블行列 **S**와 任意의 (n×n) 置換行列 **P**를 利用하여 **G**를 다음과 같은 式을 利用하여 **G'**으로 變換한다.

$$\mathbf{G}'=\mathbf{S}\,\mathbf{G}\,\mathbf{P} \tag{46}$$

**G'**은 **G**에 의하여 生成되는 符號와 같은 符號化率 k/n과 最少거리 $d_{min}$을 갖는 새로운 線形符號를 生成한다. **G'**을 (k×n) 公開生成行列(public generator matrix)이라 定意하자. **G'**을 暗號化키로 公開하고 그 成分行列 **G**, **S**, **P**는 모두 祕密로 保管한다. $\mathbf{G}=\mathbf{S}\cdot\mathbf{G}\cdot\mathbf{P}$로부터 $\mathbf{G}'=\mathbf{S}^{-1}\mathbf{G}'\mathbf{P}^{-1}$을 求할 수 있다. 送信者는 K-bit의 平文을 다음 式에 의해 n-bit의 暗號文으로 暗號化한다.

$$\begin{aligned}\mathbf{c}&=\mathbf{m}\,\mathbf{G}'+\mathbf{e}\\&=\mathbf{m}\,\mathbf{S}\,\mathbf{G}\,\mathbf{P}+\mathbf{e}\end{aligned} \tag{47}$$

**c**를 受信한 受信段는 다음 式을 利用하여 **c'**을 求한다.

$$\mathbf{c}'=\mathbf{c}\,\mathbf{P}^{-1}=(\mathbf{m}\,\mathbf{S})\mathbf{G}+\mathbf{e}' \tag{48}$$

여기서 $\mathbf{e}'=\mathbf{e}\cdot\mathbf{P}^{-1}$이다. 元來 線形符號의 復號알고리즘을 이용하여 誤謬벡터 **e'**을 求한 후, **c'**으로부터 **e'**을 除去하여 벡터 $\mathbf{m}\cdot\mathbf{S}$를 求할 수 있다. 따라서, 平文 **m**은 다음 式에 의해 쉽게 求할 수 있다.

$$\mathbf{m}=(\mathbf{m}\,\mathbf{S})\mathbf{S}^{-1} \tag{49}$$

따라서 본 公開 키 暗號시스템은 k와 t의 選擇에 따라 計算의 複雜性을 最大로 할 수 있고 暗號文 攻擊에 效率的으로 對處할 수 있다.

이 시스템에의 攻擊은 行列 **G'**의 k행을 任意로 찾음으로써 修行할 수 있다. **m**은 k 비트 情報이기 때문에 式(47)은 다음과 같이 바꾸어 쓸 수 있다.

$$\mathbf{c}_k=\mathbf{m}\,\mathbf{G}_k'+\mathbf{e}_k \tag{50}$$

여기서 $\mathbf{c}_k$, $\mathbf{G}_k'$, 그리고 $\mathbf{e}_k$는 이들 k행에 限定된 것이다. 式(50)은 다음과 같은 式으로 變形될 수 있다.

$$\mathbf{c}_k+\mathbf{e}_k=\mathbf{m}\,\mathbf{G}_k'$$

혹은,

$$\mathbf{m}=(\mathbf{c}_k+\mathbf{e}_k)(\mathbf{G}_k')^{-1} \tag{51}$$

이 된다. 만약 $\mathbf{e}_k=0$이면, 式(51)은 式(52)와 같이 된다.

$$\mathbf{m}=\mathbf{c}_k(\mathbf{G}_k')^{-1} \tag{52}$$

따라서 $\mathbf{G}_k'$이 決定되면, **m**은 式(42)를 利用하여 쉽게 求할 수 있다.

McEliece는 블럭길이 $n=2^m=2^{10}=1024$, $t=50$으로 된 Goppa符號를 利用했으므로 平文 블럭은 $k=n-mt=524$이고, 符號化率 $k/n=0.5$이다. $n=1024$, $t=50$일 때 上記의 攻擊이 成功할 때까지 豫想되는 演算의 수는 $2^{80.7}$이다. 한편, Adams와 Mieger는 $n=1024$와 $t=37$의 變數값이 上記의 攻擊에 對處할 수 있는 最適값이고, 이 때 豫想되는 演算의 演算水는 $2^{84.1}$이라는 것을 보였다.

다음에는 간단한 線形符號를 택하여 McEliece 작업을 證明하는 방법을 밝힐 것이다.

[例題 12] 最少거리 $d_{min}=3$을 갖는 單一誤謬訂正 (7,4) BCH Code에 대하여 考察하자. 生成行列 **G**, 스크램블行列 **S**, 置換行列 **P**가 각각 다음과 같이 주어졌다고 假定하자.

$$\mathbf{G}=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\1&1&1&0&0&1&0\\1&0&1&0&0&0&1\end{bmatrix}\quad \mathbf{S}=\begin{bmatrix}1&1&1&0\\1&0&1&0\\0&1&1&0\\1&0&1&1\end{bmatrix}\quad \mathbf{P}=\begin{bmatrix}0&0&1&0&0&0&0\\1&0&0&0&0&0&0\\0&0&0&0&1&0&0\\0&1&0&0&0&0&0\\0&0&0&0&0&0&1\\0&0&0&0&0&1&0\\0&0&0&1&0&0&0\end{bmatrix}$$

式(46)을 利用하여, 公開 暗號키 $\mathbf{G}'$을 다음과 같이 計算한다.

$$\mathbf{SG}=\begin{bmatrix}0&1&0&1&1&1&0\\0&0&1&1&0&1&0\\1&0&0&0&1&1&0\\1&0&0&1&0&1&1\end{bmatrix}$$

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

平文을 $\mathbf{m}=(0100)$, 傳送중에 發生하는 誤謬形態를 $\mathbf{e}=(0000100)$라고 하자. 그러면, 式(47)로부터 暗號文은 다음과 같음을 알 수 있다.

$$\mathbf{c}=\mathbf{mG}'+\mathbf{e}$$

$$=(0\,1\,0\,0)\begin{bmatrix}1&1&0&0&0&1&1\\0&1&0&0&1&1&0\\0&0&1&0&0&1&1\\0&1&1&1&0&1&0\end{bmatrix}+(0000100)$$

$$=(0\,1\,0\,0\,1\,1\,0)+(0\,0\,0\,0\,1\,0\,0)$$

$$=(0\,1\,0\,0\,0\,1\,0)$$

式(48)을 利用하면, 受信된 暗號문 $\mathbf{c}'=\mathbf{cP}^{-1}$는 다음과 같이 計算된다: 置換行列 $\mathbf{P}$로부터 行列式 $|\mathbf{P}|$를 計算하면 $|\mathbf{P}|=1$이다. 正方行列 $\mathbf{P}$의 余因子(cofactor)들을 計算한 다음, $\mathbf{P}$의 逆行列은 $\mathbf{P}$의 余因子들을 轉置(transpose)시켜 만든다. 그래서 $\mathbf{P}^{-1}$는 다음과 같이 計算된다.

$$\mathbf{P}^{-1}=\frac{[\text{余因子 } P_{ij}]^T}{|\mathbf{P}|}$$

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

같은 방법으로 스크램블行列 $\mathbf{S}$의 逆行列 $\mathbf{S}^{-1}$를 計算할 수 있다. 行列式이 $|\mathbf{S}|=1$이므로 다음을 얻는다.

$$\mathbf{S}^{-1}=\begin{bmatrix}1&0&1&0\\1&1&0&0\\1&1&1&0\\0&1&0&1\end{bmatrix}$$

$\mathbf{c}'$의 誤症 $\mathbf{s}$는 다음과 같은 3-tuple 행벡터로 정의된다.

$$\mathbf{s}=\mathbf{c}'\cdot\mathbf{H}^T=(s_0,s_1,s_2)$$

여기서, $\mathbf{H}^T$는 검사行列 $\mathbf{H}$의 轉置行列로 $\mathbf{G}$로부터 쉽게 얻어진다. $\mathbf{H}$를 計算하면

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

이므로 轉置行列 $\mathbf{H}^T$는

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

이다. 따라서 誤症은

$$\mathbf{s}=(0\,0\,0\,1\,0\,1\,0)\begin{bmatrix}1&0&1\\0&1&0\\0&0&1\\1&1&0\\0&1&1\\1&1&1\\1&0&1\end{bmatrix}=(0\,0\,1)$$

이다. 그러면 誤謬벡터 $\mathbf{e}'$은 다음과 같이 計算된다.

$$\mathbf{e}'=\mathbf{e}\mathbf{P}^{-1}=(0\,0\,0\,0\,1\,0\,0)\begin{bmatrix}0&1&0&0&0&0&0\\0&0&0&1&0&0&0\\1&0&0&0&0&0&0\\0&0&0&0&0&0&1\\0&0&1&0&0&0&0\\0&0&0&0&0&1&0\\0&0&0&0&1&0&0\end{bmatrix}$$

$$=(0\,0\,1\,0\,0\,0\,0)$$

$\mathbf{c}'$과 $\mathbf{e}'$ 合하면 오른쪽 4개의 디지트가 $\mathbf{m}'=\mathbf{m}\mathbf{S}=(1\,0\,1\,0)$인 다음 式을 얻을 수 있다.

$$\mathbf{c}'+\mathbf{e}'=(0\,0\,1\,1\,0\,1\,0)$$

式(49)를 利用하면 결국 平文은 다음과 같이 復元시킬 수 있다.

$$(\mathbf{m}\mathbf{S})\mathbf{S}^{-1}=(1\,0\,1\,0)\begin{bmatrix}1&0&1&0\\1&1&0&0\\1&1&1&0\\0&1&0&1\end{bmatrix}=(0\,1\,0\,0)$$

McEliece 暗號시스템은 公開키의 크기가 매우 크다는 缺點이 있다. 例를 들어 McEliece는 公開키의 크기를 $2^{19}$비트로 提案하였다. 매우 큰 公開키는 傳送되어야 할 情報量을 增加시킨다. 또한 一般的으로 暗號문의 길이는 平文의 2배 정도가 된다는 短點이 있다. 또한 本 公開키 暗號시스템은 완전히 比對稱이며 一對一 對應이 아니기 때문에 디지틀 署名분야에의 適用이 어렵다.

(다음 號에 계속)

(著者紹介는 p.27 參照)

---

지난 號의 誤記를 아래와 같이 바로 잡습니다.

| 面 段 行 | 誤 | 正 |
|---|---|---|
| 96 右 2 | 幕 | 冪 |
| 97 右 7 | $y_1=y_2-k_2=151=k_1=2412$ | $y_1=y_2-k_2=151=k_1$ |
| 97 右 25 | $Y'_1$ | $Y'$ |
| 98 左 24 | $\sum_{i=1}^{5} k'_p$ | $\sum_{i=1}^{5} k'_i$ |
| 99 左 9 | $K=(1979,\ 2726,\ 1914,\ 3016,.$ | $K_p=(1979,\ 2726,\ 1914,\ 3016,.$ |
| 99 左 18 | $Y'_i\ K'_i\ X_i$ | $y'_i\ k'_i\ x_i$ |
| 99 左 19 | 1867<1091 | 1867>1091 |
| 99 左 21 | 776>187 | 350>187 |
| 99 左 22 | 589>151 | 163>151 |