通信情報保護學會誌
第2卷, 第1號, 1992. 3

連載特輯

公開키 暗號시스템에 關한 硏究

Study on the Public Key Cryptosystems

(3)

李 晩 榮*

第1卷,第2號에 이어 本稿에서는 非對稱暗號시스템에서의 認證(Authentication) 및 디지탈 署名(Digital Signature) 方式을 讀者의 理解를 돕기 위해 代表的인 몇가지 技法에 대해 分析한다.

다음號(第2卷, 第2號)에서는 對稱暗號시스템에서의 認證 및 署名方式을 다룰 豫定이나 讀者諸位의 呼應度가 낮을 경우 本號를 끝으로 連載를 마감할까 한다.

目 次

* 종신회원, 漢陽大學校 名譽教授, 本 學會 會長

6. 非對稱 暗號시스템에서의 認證 및 署名方式

6. 1 離散對數 문제를 기반으로 한 ElGamal의 認證 및 潛在署名方式

1) 認證方式

본절에서는 ElGamal의 認證方式에 대한 안전성은 p가 소수일때 유한체 GF(p)상의 離散 對數 문제를 푸는 것이 매우 어렵다는 사실에 기초한다. ElGamal 認證方式은 平文의 메세지와 署名文을 함께 수신자에게 보내어, 수신자가 平文과 署名文과의 대수학적 특성을 조사하여 타당성이 있을 경우 송신자를 인정하는 방법을 이용하고 있다.

X를 署名된 平文 메세지라 하자. 그러면 $X \in GF(p)$ 혹은 $0 \le X \le p-1$의 관계를 만족한다. 송신자는 GF(p)상의 원시원(primitive element) α를 선정한다. 단, 원시원 α는 α를 멱승하여 GF(p)상의 "0"를 제외한 모든 원소를 생성할 수 있는 GF(p)상의 임의의 원소이다. 그리고 다음 $r \in GF(p)$인 임의의 亂數 r를 선택한 후 다음 합동식을 이용하여 자신의 공개키 K를 계산한다.

$$K \equiv \alpha^r \bmod p \qquad (53)$$

K는 공개철안에 보관되어 있는 사용자 A의 공개키이다. 메세지 X인 署名文을 생성하기 위해서 송신자는 $\gcd(s, p-1)=1$의 관계를 만족하는 유한체 원소 $s(\in GF(p))$를 구한다. 그리고, 다음식을 이용하여 첫번째 署名文 W를 계산한다.

$$W \equiv \alpha^s \bmod p \qquad (54)$$

그리고 유클리드 알고리즘과 합동식을 이용하여 두번째 署名文 V를 계산한다.

$$X \equiv rW + sV \bmod (p-1) \qquad (55)$$

상기식에서 s가 $\gcd(s, p-1)=1$를 만족하면 임의의 V에 대해서 유일한 W가 결정될 수 있다. 이와 같은 과정을 통해 X, W, 및 V가 결정되면 송신자는 메시지 X와 認證者(authenticator)라 불리우는 비밀쌍(W, V), $0 \le W, V \le p-1$를 수신자에게 전송한다. 송신자에 의해 생성된 X, W, V는 다음의 합동식을 반드시 만족한다.

$$\begin{aligned} \alpha^X &\equiv K^W W^V \bmod p \\ \alpha^X &\equiv \alpha^{rW}\alpha^{sV} \bmod p \\ &\equiv \alpha^{rW+sV} \bmod p \end{aligned} \qquad (56)$$

暗號文(X, W, V)를 수신한 수신자는 공개키 디렉토리의 (K, α, p)를 이용하여 α^X와 α^{rW+sV} (mod p)를 각각 계산하여 같으면 비밀쌍(W, V)가 平文 메세지 X와 대수 특성이 만족하므로 일치하기 때문에 平文 X를 송신자가 보낸 진정한 메세지로 認證한다.

[例題 13] 식(55)를 증명해 보자. 일반적으로 $\beta = \gamma + k(p-1)$이면 $\beta \equiv \gamma \pmod{p-1}$ 관계를 만족한다. 그러면 $\alpha^\beta \equiv \alpha^\gamma \pmod p$이다. 만약 $\beta = X$이고 $\gamma = rW + sV$라 하면 $\alpha^X \equiv \alpha^{rW+sV} \pmod p$가 된다. 즉 $X \equiv rW + sV \pmod{p-1}$이다.

[例題 14] 유한체 GF(11)에서, 이 원시원 GF(11)의 집합은 {2, 6, 7, 8}이 된다. 이 중 임의의 원시원 $\alpha = 7$를 선정한다. 송신자가 $r=3$을 선택하면 $K \equiv 7^3 \pmod{11} = 2$를 얻을 수 있다. 위의 과정을 이용하여 송신자는 공개키 (K, α, p)=(2, 7, 11)를 구할 수 있다. 平文 메세지가 $X=6$이라 하자 송신자는 $\gcd(s, p-1) = \gcd(7, 10) = 1$이 되는 다른 亂數 $s=7$를 선택 한 후, $W \equiv \alpha^s \pmod p = 7^7 \pmod{11} = 6$를 계산하여 첫번째 署名文 W를 구한다. 그리고 송신자는 아래식을 이용하여 두번째 署名文 V를 구한다.

$$\begin{aligned} X &\equiv rW + sV \quad \bmod(p-1) \\ 6 &\equiv 3 \cdot 6 + 7V \quad \bmod 10 \end{aligned}$$

이식의 해 V=4이다. 그다음 송신자는 메세지와 署名文들로 구성된 暗號文 Y=(X, W, V)=(6, 6, 4)를 수신자에게 전송한다. 暗號文 Y는 비밀 認證者 (W, V)와 平文의 메세지 X로 구성 되어있다. 수신자는 다음과 같이 α^X, 와 $K^W W^V$ (mod p)를 각각 계산한다.

오른쪽 값 : $K^W W^V \pmod p = 2^6 \cdot 6^4 \pmod{11} = 82944 \pmod{11} = 4$

왼쪽 값 : $\alpha^X \pmod p = 7^6 \pmod{11} = 4$

양쪽 값이 같으므로 메세지 X=6은 진정한 송신자가 보낸 메세지인 것으로 認證한다.

2) ElGamal의 潛在署名方式

송신자는 p가 소수인 경우의 유한체 GF(p)를 구성한다. α는 GF(p)의 원시원이라 하면, 송신자는 α와 p는 공개한다. 송신자는 임의로 비밀키 r를 선정하여, 이를 고도의 비밀 채널을 통해 수신자에게 보내어 송신자와 수신자만이 r를 알고 있도록 한다. p와 서로소 관계인 平文 메세지를 X로 하자. 송신자가 다음식을 이용하여 첫번째 署名文 W를 계산한다.

$$W \equiv \alpha^X \bmod p \qquad (57)$$

그리고 송신자는 暗號文 Y를 gcd(Y, p)=1를 만족하는 임의의 수로 결정한다. 그리고 다음식을 이용하여 두번째 署名文 V를 구한다.

$$Y \equiv rW + XV \bmod(p-1) \qquad (58)$$

송신자는 暗號文과 署名文쌍 (Y, W, V)를 수신자에게 전송한다. (Y, W, V)를 수신한 수신자는 다음의 A를 계산한다.

$$A \equiv \alpha^{Y-XV} (\alpha^X)^V \bmod p \equiv \alpha^Y \bmod p \qquad (59)$$

수신자는 α^r를 계산한 후, A와 $\alpha^r \pmod p$가 같으면 暗號文 Y는 진정한 송신자가 보낸 暗號文으로 간주한다. 認證이 완료된 暗號文 Y와 식(58)을 이용하여 메세지 X는 다음과 같이 구해질수 있다.

$$X \equiv V^{-1} (Y - rW) \bmod(p-1) \qquad (60)$$

例題 14의 유한체 GF(11)에서, 원시원의 집합은 {2, 6, 7, 8}이다. 원시원 집합으로부터 임의의 원시원 α=7을 선택한다. (p, α)=(11, 7)을 공개하고 비밀키 r=7는 송신자와 수신자에 의하여 비밀키로 보관된다. 송신자가 gcd(X, p)=gcd(3, 11)=1인 메세지 X를 전송하기 위해 다음과 같이 계산한다.

$$W \equiv 7^3 \pmod{11} = 2$$

만약 송신자가 暗號文 Y=7로 설정하면, 다음과 같이 두번째 署名文 V를 계산한다.

$$7 \equiv (5)(2) + 3V \pmod{10}$$
$$3V \equiv 7 \pmod{10}$$

윗식의 해는 V=9이다. 송신자는 수신자에게 暗號文 및 署名文쌍 (Y, W, V)=(7, 2, 9)를 보낸다. (7, 2, 9)를 수신한 수신자는 아래와 같이 A와 α^Y를 각각 계산한다.

$$A \equiv (7^5)^2 \cdot 2^9 \pmod{11}$$
$$\equiv (10^2)(2^9) \pmod{11} = 6$$

그리고

$$\alpha^Y \pmod p \equiv 7^7 \pmod{11} = 6$$

따라서 $A = \alpha^Y = 6$에 일치하므로 暗號文 (7, 2, 9)이 받아드려지고 Y=7이 認證된다. 끝으로 平文 메세지 X는 다음과 같이 구해진다.

$$X \equiv 9^{-1}(7-5\cdot 2) \bmod 10$$
$$\equiv (9^{-1})(7) \bmod p=3$$

이렇게 하므로써 메세지 X=3은 완전히 복호될 수 있다. 두번째 ElGamal의 署名시스템의 특징은 첫번째 ElGamal의 署名시스템에서와는 달리 송신자와 수신자가 비밀키 r을 유지해야 하며 송신자와 수신자간의 정보에 平文의 메세지 X가 暗號文 Y로 바뀌어져 전송되므로서 임의의 暗號해독자가 平文의 X를 알 수 없는 특징이 있다.

6. 2 Quadratic congruence에 기반을 둔 Ong-Schnorr-Shamir 認證 및 潛在署名方式

1) 認證方式

Ong, Schnorr, 및 Shamir[3]는 다항식 방정식 $P(x_1, x_2, \cdots, x_k) \bmod n$을 이용한 署名方式을 1984년 제안했다. OSS署名方式은 1984년 이차 다항식 P를 이용하여 제안되었으며 당시 많은 관심을 끌었으나 J. M. Pollard[4]에 의해 깨지고 말았다.

이차방정식 OSS 시스템에서 공개키는 두 정수 n과 λ로 구성된다. 법 n은 몇개 큰소수의 결합수(composite number)이고, 이의 인수(factor)들은 비밀로 간직되며, λ는 n과 비슷한 크기의 수로서 다음의 과정을 만족하도록 설정된다. OSS署名方式에서는 메세지 M에 대한 署名文 쌍 (x, y)는 식(61)을 만족하도록 설정된다. 그러므로 메세지 M ($0<M<n$)에 대한 위조의 署名文쌍을 구하기 위해서는 다음식의 관계를 만족하는 署名文 쌍 (x, y)를 먼저 구해야 한다. 한편 공개키 중의 하나인 λ를 구하기 위하여 송신자는 먼저 gcd(k, n)=1을 만족하는 k를 선정한 후 k를 비밀스럽게 간직하고, 공개키 λ를 식(62)를 이용하여 계산한다.

$$x^2+\lambda y^2 \equiv M \pmod n \qquad (61)$$
$$\lambda \equiv -k^{-2} \pmod n \qquad (62)$$

따라서 OSS 署名方式에서의 공개키 쌍은 임의의 합성수 n과 식(62)에서의 λ로 구성된다. gcd(M, n)=1을 만족하는 메세지 M에 대한 認證은 다음의 과정을 통해 수행된다. 먼저 gcd(r, n)=1인 관계를 만족하는 임의의 r를 선택한 후, 식(63)을 이용하여 M에 대한 署名文쌍 (x, y)를 구한다. 그리고 (x, y)를 수신자에게 보낸다.

$$x \equiv \frac{1}{2}\left[\frac{M}{r}+r\right] \pmod n \qquad (63)$$
$$y \equiv \frac{k}{2}\left[\frac{M}{r}-r\right] \pmod n$$

署名文 쌍 Y=(x, y)를 수신한 수신자는, 메세지 M을 공개키 λ와 n을 참조하고 식(61)을 이용하여 구한다. 여기서 구해진 M이 정해진 규칙을 만족하면 수신자는 (x, y)를 M에 대한 유효한 署名文으로 간주하고, 그렇지 않을 경우 유효하지 않은 署名文으로 간주한다. OSS 署名시스템의 기본동작 원리는 [例題 15]의 결과에서 기인된다.

[例題 15] 식 (62)의 관계를 만족하는 λ와 식 (63)을 만족하는 (x, y)는 $x^2+\lambda y^2 \equiv M \pmod n$의 관계를 만족함을 증명하시오.

$$x^2+\lambda\, y^2=\left[\frac{1}{2}\left(\frac{M}{r}+r\right)\right]^2+\lambda\left[\frac{1}{2}k\left(\frac{M}{r}-r\right)\right]^2$$
$$=\frac{1}{4}\left[\left(\frac{M}{r}+r\right)^2-\left(\frac{M}{r}-r\right)^2\right]$$
$$=M$$

[例題 16] gcd(k, n)=gcd (5, 12)=1를 만족하는 OSS 시스템에서의 n=12와 k=5를 선택한다. 여기서 n은 OSS의 공개키 중 하나이고 k는 비밀키이다. 비밀키 k=5를 이용하여 OSS의 공개키 λ는 식 (62)를 이용하여 계산한다. 먼저 $k\cdot k^{-1}=1 \pmod{12}$를 만족하는 $k^{-1}=5$를 구한 후, $\lambda \equiv -(k^{-1})^2 \pmod{12}$에 대입하면 $\lambda \equiv -(5)(5) \pmod{12}$가 된다. 따라서 $\lambda \equiv -25 \pmod{12}=11 \pmod$

12)이다. 그러므로 OSS 署名方式에서의 공개키 (λ, n)=(11, 12)이고 비밀키 k=5이다. 만일 gcd (M, n)=gcd(7, 12)=1인 메세지 M=7에 대한 署名文쌍 (x, y)를 구하기 위하여 송신자는 gcd(r, n)=1을 만족하는 r=5를 선택한다. 그리고 $r \cdot r^{-1}$ =1을 만족하는 $r^{-1}=5 \bmod 12$를 계산한 후, 식 (63)을 이용하여 署名文 쌍 x와 y를 계산한다.

$$x \equiv \frac{1}{2}(7 \cdot 5+5) \pmod{12} \equiv 20 \pmod{12} = 8$$

$$y \equiv \frac{5}{2}(7 \cdot 5-5) \pmod{12} \equiv 75 \pmod{12} = 3$$

따라서 署名文 쌍 Y=(x, y)=(8, 3)을 수신한 수신자는 송신자가 보낸 메시지 M을 다음과 같이 공개키 n과 λ를 참조하고 식 (61)을 이용하여 복원한다.

$$M \equiv (8^2+(11)3^2) \pmod{12}$$
$$=7$$

OSS 시스템의 quadratic version은 다항식 $x^2+\lambda y^2=M$을 사용했다. 여기서 공개키중 하나는 $\lambda \equiv -k^{-2} \pmod n$인 정수 λ이고, 비밀키는 gcd(k, n)=1을 만족하는 임의의 亂數 k이다. OSS 署名方式은 곱셈에 기초하여 署名文쌍이 형성되므로, 만일 $x_1^2+\lambda y_1^2=M_1$과 $x_2^2+\lambda y_2^2=M_2$인 관계를 만족하는 (x_1, y_1, M_1)과 (x_2, y_2, M_2)을 구하면 이를 이용하여 새로운 署名文과 메세지 (x, y, M_1M_2)는 다음과 같은 관계식을 만족한다.

$$(x_1^2+\lambda y_1^2) \cdot (x_2^2+\lambda y_2^2)=M_1M_2$$

위 식의 좌변은 $(x_1x_2-\lambda y_1y_2)^2+\lambda(x_1y_2+x_2y_1)^2$이 되어 새로운 署名文 쌍은 $x=x_1x_2-\lambda y_1y_2$와 $y=x_1x_2+x_2y_1$이 된다.

Pollard는 quadratic과 cubic OSS 技法에 대해 暗號공격을 성공하여 OSS 署名技法의 안전성이 붕괴되었다.

2) 潛在署名方式

원래의 OSS 署名方式에서와 같이 gcd(k, n)=1인 비밀키 k를 선택한다. OSS 署名文方式에서의 공개키 n은 덧셈과 곱셈 모듈라 연산을 정의한다. 그리고 송신자는 비밀키 k를 수신자에게 고도의 비밀채널을 통해 전달하며, 송신자와 수신자가 공히 비밀키 k를 비밀로 보관한다. 만약 송신자가 메세지 M을 暗號文 Y를 이용하여 전송한다고 가정하자. 송신자는 먼저 gcd(M, n)=1, (M=1, 2, …, n−1)이고 gcd(Y, n)=1, (Y=1, 2, …, n−1)을 만족하는 메세지 M과 暗號文 Y를 결정하고 이에 대한 署名文 쌍 (x, y)를 식 (64)를 이용하여 구한다.

$$x \equiv \frac{1}{2}\left[\frac{Y}{M}+M\right] \pmod n \qquad (64)$$

$$y \equiv \frac{k}{2}\left[\frac{Y}{M}-M\right] \pmod n$$

이후 송신자는 세개로 구성된 暗號文과 署名文 쌍 (Y, x, y)를 수신자에게 전송한다. 暗號文 (Y, x, y)를 받은 수신자는 다음 합동식을 이용하여 Y′을 구하여, 수신된 (Y, x, y)의 타당성 여부를 조사한다.

$$Y' \equiv x^2-y^2/k^2 \pmod n \qquad (65)$$

수신자는 Y′=Y인지를 비교하여 Y′=Y일 경우 수신된 (Y, x, y)는 타당한 것으로 認證하고 (Y, x, y)를 받아 들인다. 그러나 Y′≠Y이면 수신된 (Y, x, y)는 타당하지 않은 것으로 간주한다. 일단 (Y, x, y)가 認證되었다고 간주되면 수신자는 메세지 M을 식 (66)을 이용하여 복원한다.

$$M \equiv \frac{Y}{x+K^{-1}y} \pmod n \qquad (66)$$

수정된 OSS 署名方式의 기본 동작은 식 (65)와 식 (66)에 기초하여 수행된다. 따라서, 식 (64)를 만

족하는 (Y, x, y)가 식 (65)와 식 (66)을 만족하는가는 例題 17에서 설명한다.

[例題 17] 식 (64)를 식 (65)에 대입하여 $Y' \equiv x^2 - y^2/k^2$으로 부터 구한 Y'이 Y'=Y인 관계식을 만족함을 증명하시오.

$$Y' = (1/4)[(Y/M)^2 + 2Y + M^2) - (1/4)[(Y/M)^2 - 2Y + M^2] = Y \pmod n$$

그리고 식 (64)를 식 (66)에 대입하여 $M \equiv \frac{Y}{x + k^{-1}y}$임을 증명해 보자.

$$\frac{Y}{x + k^{-1}y} = \frac{Y}{(1/2)(Y/M + M) + k^{-1}(k/2)(Y/M - M)} = M$$

(증명끝)

[例題 18] gcd(k, n)=gcd(2, 15)=1인 모듈라 n=15와 비밀키 k=2를 선택하자. $k \cdot k^{-1} \equiv 1 \pmod n$ 즉 $2k^{-1} = 1 \pmod{15}$인 $k^{-1}=8$을 계산한다. gcd(Y, n)=gcd(13, 15)=1인 暗號文 Y=13을 이용하여 메세지 M=7을 전송해 위해, 먼저 $7M^{-1} \equiv 1 \pmod{15}$에서 $M^{-1}(=13)$을 계산한다. 식 (64)를 이용하여 署名文쌍 x, y를 계산한다.

$$x \equiv (1/2)(13 \cdot 13 + 7) \pmod{15} \equiv 88 \pmod{15} = 13$$

$$y \equiv (2/2)(13/7 - 7) \pmod{15} \equiv (169 - 7) \pmod{15} = 12$$

(x, y)를 구한 송신자는 暗號文과 署名文 쌍 (Y, x, y)=(13, 13, 12)를 수신자에게 전송한다. (Y, x, y)를 받은 수신자는 비밀키 k=2를 이용하여 (Y, x, y)에 대한 認證을 식 (65)를 이용하여 수행한다.

$$Y' \equiv x^2 - y^2/k^2 \pmod n \equiv 133 \pmod{15} = 13$$

따라서 Y'=13=Y이므로 수신자는 수신된 (Y, x, y)가 정당한 것으로 認證하고 식 (66)를 이용하여 메세지 M을 복원한다.

$$M \equiv Y/(x + k^{-1}y) \pmod n \equiv 52 \pmod{15} = 7$$

6. 3 Knapsack 문제에 기반을 둔 Shamir의 認證方式

1) 認證方式

1978년 Shamir는 knapsack 문제에 기반을 둔 高速認證 技法을 제안하였다. Shamir의 高速認證 技法의 주요 특징은 첫째 송신자에 의해 생성이 수행되며, 둘째 비밀키는 송신자가 비밀리에 보관하며 공개키는 수신자가 수신된 暗號文을 認證하는데 이용된다는 점이다. 그리고, Shamir의 高速認證 시스템은 高速으로 동작될 수 있어서 認證과정이 S/W로 구성되었을 때도 수신자가 원래의 메세지를 빨리 복구할 수 있다는 점이다. Shamir의 高速認證 技法에 대한 暗號해독은 알고리즘이 knapsack 문제에 기반을 두고 있으므로 곱셈 knapsack 시스템에 대한 暗號해독 방법과 유사하다. 그러나 1984년에 Odlyzko[2]는 Shamir의 高速認證 技法을 깨는 방법들을 보였다. 본 절에서는 Shamir의 高速認證 技法을 분석하여, 실제 적용예를 제시하여 알고리즘의 타당성을 확인한다. 송신자는 무작위로 선정된 $n \times 2n$개의 $k_{ij} \in GF(2)$ (i=1, 2, …, n,

j=1, 2, …, 2n)들로 구성된 행렬 K를 만든다. 여기서 생성된 K는 비밀키로서 송신자만이 비밀리에 보관한다. 그리고, 송신자는 n이 平文의 길이일때 $p \geq 2^n - 1$의 관계를 만족하는 소수 p를 선택한다. 그리고, 공개키 중 하나인 벡터 $A=(a_1, a_2, \cdots, a_{2n})$, $a_i \in GF(p)$, (i=1, 2, …, 2n)를 구하기 위해 다음과 같은 행렬 합동(congruence) 시스템을 구성한다.

$$K_{n\times 2n} \times A^{T}_{2n\times 1} = \begin{bmatrix} 1 \\ 2 \\ \cdot \\ \cdot \\ \cdot \\ 2^{n-1} \end{bmatrix} \bmod p \qquad (67)$$

여기서, $A=(a_1, a_2, \cdots, a_{2n})$

식 (67)에서 발생 가능한 방정식은 n개이므로 미지수 2n개의 방정식을 풀기 위해서는 송신자는 A의 무작위로 n개의 원소 $(a_1, a_2, \cdots, a_n)$을 선택하고, 나머지는 식 (67)을 이용하여 $(a_{n+1}, a_{n+2}, \cdots, a_{2n})$을 계산한다. 여기서 구해진 (A, p)쌍을 공개키로 공개한다. 일반적으로 메세지 平文 $X \in GF(p)$를 이진수 $X=(x_1, x_2, \cdots, x_n)$, $x_i \in GF(2)$로 변환할 수 있다. 만일 이진 표현된 메세지 X를 재배열하면 $X=(x_n, x_{n-1}, \cdots, x_1)$, 즉 $X=x_nz^0+x_{n-1}z^1+\cdots, +x_1z^{n-1}$이 된다. X에 대응되는 暗號文 Y는 이제 다음처럼 결정된다.

$$Y=X \cdot K \bmod p \qquad (68)$$

즉,

$$(y_1, y_2, \cdots, y_{2n}) = (x_n, x_{n-1}, \cdots, x_1) \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1,2n} \\ k_{21} & k_{22} & \cdots & k_{2,2n} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ k_{n,1} & k_{n,2} & \cdots & k_{n,2n} \end{bmatrix}$$

따라서 Y의 각 구성요소 y_j(j=1, 2, …, 2n)는 다음과 같이 표현될 수 있다.

$$y_i = \sum_{i=1}^{n} x_{n-i+1}\, k_{ij} \bmod p \qquad (69)$$

수신 暗號文 Y를 수신한 수신자는 暗號文 Y와 공개키 (A, p)를 이용하여 다음과 같이 메세지 X를 계산할 수 있다.

$$X=Y \cdot A^{T} \pmod p \qquad (70)$$

즉,

$$D_k(Y)=(y_1, y_2, \cdots, y_{2n}) \cdot \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{2n} \end{bmatrix}$$

$$= \sum_{j=1}^{2n} y_j a_j \qquad (71)$$

식 (69)의 y_j를 식(71)에 대입하면,

$$D_k(Y)=\sum_{i=1}^{n} x_{n-i+1}\left(\sum_{j=1}^{2n} k_{ij}a_j\right) \qquad (72)$$

한편 식 (67)은 다음과 같이 다시 표현될 수 있다.

$$\begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1,2n} \\ k_{21} & k_{22} & \cdots & k_{2,2n} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ k_{n,1} & k_{n,2} & \cdots & k_{n,2n} \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{2n} \end{bmatrix} = \begin{bmatrix} 2^0 \\ 2^1 \\ \cdot \\ \cdot \\ \cdot \\ 2^{n-1} \end{bmatrix}$$

위의 관계식으로 부터 다음 식을 구할 수 있다.

$$\sum_{j=1}^{2n} k_{ij}a_j=2^{i-1},\ i=1,\ 2,\ \cdots,\ n \qquad (73)$$

식 (72)의 좌변의 오른쪽 항은 식 (73)의 좌변과 같으므로, 식 (73)의 결과를 식 (72)에 대입하면 다음과 같은 식을 구할 수 있다.

$$D_k(Y)=\sum_{i=1}^{n} x_{n-i+1}(2^{i-1}) \qquad (74)$$

일반적으로 메세지 X는 다음과 같이 표시된다.

$$X=x_n2^0+x_{n-1}2^1+x_{n-2}2^2+\cdots+x_12^{n-1}$$
$$=\sum_{i=1}^{n} x_{n-i+1}\,2^{i-1} \qquad (75)$$

식 (74)와 식 (75)를 비교하면 다음을 알 수 있다.

$$D_k(Y)=X=\sum_{i=1}^{n} x_{n-i+1}\,2^{i-1}\ (\mathrm{mod}\ p) \qquad (76)$$

식 (68)을 이용하여 생성된 Y는 공개키(A, p)를 이용하여 X를 생성할 수 있으므로, 보내온 메세지 M은 2n개의 선형방정식을 생성하므로, 이를 이용하여 비밀키 K를 구할 수 있다. 일반적으로 K에서의 n×2n개의 원소를 결정하기 위해서는 평균 n개의 메세지가 요구된다. 따라서 위에서 제안된 認證技法은 안전하지 않다.

[例題 19] 송신자가 p=7을 선택하여 GF(7)을 이용하여 메세지 認證을 위해 Shamir의 認證시스템을 생각해 보자. $p\geq 2^n-1$을 만족하는 메세지 길이 n은 3이 된다. 송신자에 의해 임의로 선택된 비밀키 K가 다음과 같다고 가정하자.

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

A의 6개의 $a_i \in GF(7)$ 원소 중에서 송신자는 a_1, a_2, a_3을 $a_1=2$, $a_2=5$, $a_3=6$이 되도록 임의로 선택했다면, A의 나머지 원소들 a_4, a_5, a_6은 식 (67)을 이용하여 결정할 수 있다.

$$\begin{bmatrix} 1&1&1&0&0&1 \\ 0&0&1&1&0&1 \\ 0&1&1&1&1&0 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 5 \\ 6 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} \quad (\mathrm{mod}\ 7)$$

$$2+5+6+a_6 \equiv 1 \pmod 7$$
$$6+a_4+a_6 \equiv 2 \pmod 7$$
$$5+6+a_4+a_5 \equiv 4 \pmod 7$$

이 합동 시스템으로부터, 우리는 $a_6=2$, $a_4=1$, 그리고 $a_5=6$을 얻을 수 있다. 따라서, 공개키 (A, p)를 $\mathbf{A}=(2, 5, 6, 1, 6, 2)$로 공개한다. 平文을 $\mathbf{X}=5 \in GF(7)$이라 가정하면, 이것을 이진수로 표현하면, $\mathbf{X}=(1\ 0\ 1)$이다. 식 (68)을 이용하면, 暗號文 **Y**는 다음과 같이 된다.

$$\mathbf{Y}=(1\ 0\ 1)\begin{bmatrix} 1&1&1&0&0&1 \\ 0&0&1&1&0&1 \\ 0&1&1&1&1&0 \end{bmatrix}=(1\ 2\ 2\ 1\ 1\ 1)$$

수신자에서는, 공개키 (**A**, p)를 이용하여 平文을 다음과 같이 다시 만들어낼 수 있다.

$$\mathbf{X}=(1\ 2\ 2\ 1\ 1\ 1)\begin{bmatrix} 2 \\ 5 \\ 6 \\ 1 \\ 6 \\ 2 \end{bmatrix}=2+10+12+1+6+2$$

$$=33 \pmod 7=5$$

따라서, 平文 $\mathbf{X}=5$는 완전하게 복원됐다.

2) 개량된 認證 方式

위에서 수행된 암호공격을 막기 위해서, Shamir는 각기 고유의 平文에 무작위요소(random factor)를 더하여 그가 제안한 認證技法을 더욱 안전하게 한 변경된 認證技法을 제안하였다. 송신자는 변형된 송신문을 다음과 같이 생성한다.

$$\mathbf{X}' \equiv \mathbf{X}-\mathbf{R}\mathbf{A}^T \pmod p \qquad (77)$$

여기서, **X**는 원래의 平文이고, $\mathbf{R}=(r_1, r_2, \cdots, r_{2n})$은 무작위 벡터로서 각 원소 $r_i \in GF(2)$는 무작위로 선택되며, 그리고 $\mathbf{A}=(a_1, a_2, \cdots, a_{2n})$ 공개키이다. 만약 변형된 平文 $\mathbf{X}'$이 $\mathbf{X}'=(x_n', x_{n-1}', \cdots x_1')$ 와 같이 첨자가 내림차순으로 배열되면, 이것의 다항식 형태는

$$X'=x_n'2^0+x_{n-1}'2^1+x_{n-2}'2^2+ \cdots +x_1'2^{n-1}$$

이다. 송신자는 먼저 초기 暗號文을 다음과 같은 식을 이용해서 구한다.

$$\mathbf{Y}' \equiv \mathbf{X}' \cdot \mathbf{K} \pmod p \qquad (78)$$

그리고 송신자는 전송할 최후의 暗號文을 다음 식을 이용하여 구한다.

$$\mathbf{Y} \equiv \mathbf{Y}'+\mathbf{R} \pmod p \qquad (79)$$

Y를 수신한 수신자에서는, 다음의 관계가 성립하는가 여부를 검사함으로서 수신자는 메세지에 대한 認證을 수행한다.

$$\mathbf{X} \equiv \mathbf{Y} \cdot \mathbf{A}^T \pmod p \qquad (80)$$

[例題 20] Shamir 고속 認證技法에서 $\mathbf{X} \equiv \mathbf{Y} \cdot \mathbf{A}^T \pmod p$임을 증명해보자.

(증명)

$$\mathbf{Y} \cdot \mathbf{A}^T=(\mathbf{Y}'+\mathbf{R})\mathbf{A}^T=\mathbf{Y}'\mathbf{A}^T+\mathbf{R}\mathbf{A}^T, \qquad (81)$$

식 (77)로 부터 $R\ A^T=X-X'$임을 알 수 있다.
식 (78)을 다음의 같은 형태로 다시 표현 할 수 있고 이로부터 y_j'를 다음과 같이 구할 수 있다.

$$(y_1', y_2', \cdots, y_{2n}') = (x_n', x_{n-1}', \cdots, x_1') \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1,2n} \\ k_{21} & k_{22} & \cdots & k_{2,2n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ k_{n,1} & k_{n,2} & \cdots & k_{n,2n} \end{bmatrix}$$

또는

$$y_j' = \sum_{i=1}^{n} x_{n-i+1}' k_{ij} \text{ for } j=1, 2, \cdots, 2n \quad (82)$$

한편 식 (81)의 우변의 첫번째 항은 다음과 같다.

$$\mathbf{Y}' \cdot \mathbf{A}^T = (y_1', y_2', \cdots, y_{2n}') \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{2n} \end{bmatrix}$$

$$= \sum_{j=1}^{2n} y_j' a_j \quad (83)$$

식 (82)의 결과를 식 (83)에 대입하면,

$$\mathbf{Y}' \cdot \mathbf{A}^T = \sum_{i=1}^{n} x_{n-i+1}' \sum_{j=1}^{2n} k_{ij} \cdot a_j$$

$$= \sum_{i=1}^{n} x_{n-i+1}' (2^{i-1}) = \mathbf{X}' \quad (84)$$

따라서, $\mathbf{Y}' \cdot \mathbf{A}^T = \mathbf{X}'$과 $\mathbf{R} \cdot \mathbf{A}^T = \mathbf{X} - \mathbf{X}'$ 관계식을 이용하여, 식 (81)로 부터 다음식을 얻을 수 있다.

$$\mathbf{Y}' \cdot \mathbf{A}^T = \mathbf{X}' + (\mathbf{X} - \mathbf{X}') \equiv \mathbf{X} \pmod{p} \quad \text{(증명끝)}$$

Shamir가 제안한 변경된 認證시스템의 구체적인 실행 예는 例題 21와 같다.

[例題 21] 송신자는 例題 19에서 사용된 n=3, p=7, X=5, **K**를 임의로 선택해 보자. 만약 n=3에 대하여 무작위 벡터 $\mathbf{R}=(r_1, r_2, \cdots, r_6)=(1\ 1\ 0\ 1\ 0\ 0)$을 취하면, 변형된 平文은 다음과 같다.

$$\mathbf{X}' \equiv \mathbf{X} - \mathbf{R}\ \mathbf{A}^T \pmod 7$$

$$\equiv 5 - (1\ 1\ 0\ 1\ 0\ 0) \begin{bmatrix} 2 \\ 5 \\ 6 \\ 1 \\ 6 \\ 2 \end{bmatrix} \pmod 7$$

$$\equiv 4 = (1\ 0\ 0)$$

변형된 平文 $\mathbf{X}'=4$가 이진 수열(1 0 0)으로 바뀌었고, 이것의 역은 (0 0 1)이다. 송신자는 식 (78)을 이용하여, 초기의 平文 $\mathbf{Y}'$을 계산한다.

$$\mathbf{Y}' \equiv \mathbf{X}' \cdot \mathbf{K} \pmod 7$$

$$\equiv (1\ 0\ 1) \begin{bmatrix} 1\ 1\ 1\ 0\ 0\ 1 \\ 0\ 0\ 1\ 1\ 0\ 1 \\ 0\ 1\ 1\ 1\ 1\ 0 \end{bmatrix} \pmod 7$$

$$\equiv (0\ 1\ 1\ 1\ 1\ 0) \pmod 7$$

따라서, 송신자는 전송될 최종의 暗號文을 다음과 같이 구한다.

$$\mathbf{Y} \equiv \mathbf{Y} + \mathbf{R} \pmod 7$$
$$\equiv (0\ 1\ 1\ 1\ 1\ 0) + (1\ 1\ 0\ 1\ 0\ 0) \pmod 7$$
$$\equiv (1\ 2\ 1\ 2\ 1\ 0) \pmod 7$$

수신자는 원래의 平文을 다음과 같이 복구한다.

$$\mathbf{X} \equiv \mathbf{Y} \cdot \mathbf{A}^T \pmod 7$$

$$\equiv (1\ 2\ 1\ 2\ 1\ 0) \begin{bmatrix} 2 \\ 5 \\ 6 \\ 1 \\ 6 \\ 2 \end{bmatrix} \pmod 7$$

$$\equiv 12 \pmod 7 = 5$$

그러므로, 平文 $\mathbf{X}=5$는 완전하게 공개키 $\mathbf{A}$를 사용하여 복원된다. 상기의 개선된 認證 방법도 1984년 Odlyzko에 의해 암호시스템의 안전성이 깨지고 말았다.

6. 4 Seberry-Jones 潛在署名方式

Jones와 Seberry는 1985년 Shamir의 고속 認證技法을 확장한 새로운 認證技法을 제안하였다. 6. 3절에서 분석된 바와같이, 송신자는 $n \times 2n$개의 원소로 구성된 k를 임의로 생성한 후, n개의 원소가 무작위로 선택되고 나머지 n개의 원소가 식 (67)에 의해 결정되는 A를 계산한다. 그리고 (A, p)를 공개키로 공개한다. 그후 송신자는 다음의 합동식을 이용하여 비밀 벡터 $B=(b_1, b_2, \cdots, b_{2n})$를 계산한다.

$$\mathbf{K}\ \mathbf{B}^T \equiv 0 \pmod p \qquad (85)$$

여기서 $\mathbf{B}$는 정보 송수신이 수행되기 이전에 송신자가 수신자에게 비밀리에 전달되어지는, 송신자와 수신자만의 비밀키이다. 여기서 송신자가 수신자에게 진실로 보내려고 하는 숨어 있는 메세지를 $X^* \in GF(p)$라 하면, 그 후 송신자는 $1 \times 2n$개의 원소 $r_i \in GF(2)$ $(i=1, 2, \cdots, 2n)$로 구성된 벡터 R을 식 (86)과 숨어 있는 메세지 $\mathbf{X}^*$을 이용하여 결정한다.

$$\mathbf{X}^* \equiv \mathbf{R}\ \mathbf{B}^T \pmod p \qquad (86)$$

여기서 $r_i \in GF(2)$ $(1 \le i \le 2n)$는 R의 원소들이다. Shamir가 제안했던 것처럼, 송시자는 다음과 같이 변형된 平文을 만든다.

$$\mathbf{X}' \equiv \mathbf{X} - \mathbf{R}\ \mathbf{A}^T \pmod p$$

$$\equiv \mathbf{X} - (r_1, r_2, \cdots, r_{2n}) \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{2n} \end{bmatrix} \pmod p \qquad (87)$$

여기서, $X \in GF(p)$는 송신자가 임의로 선택한 認證者(authenticator)이며 $X' \in GF(p)$는 변형된 平文을 표시하며 이 X'의 이진 표현 벡터 $(x'_n, x'_{n-1}, \cdots, x'_1)$는 다음의 관계식을 만족한다.

$$X' = \sum_{i=1}^{n} x'_{n-i+1}\ 2^{i-1}$$

$\mathbf{Y}' \equiv \mathbf{X}'\mathbf{K} \pmod p$을 이용하여 초기의 暗號文 $\mathbf{Y}'$을 구한후, $\mathbf{Y} \equiv \mathbf{Y}' + \mathbf{R} \pmod p$을 이용하여 수신자로 보낼 최종 暗號文 Y를 계산한다. 그리고 송신자는 認證쌍 $(\mathbf{X}, \mathbf{Y})$를 수신자에게 보낸다.

認證쌍 $(\mathbf{X}, \mathbf{Y})$ 수신한 수신자는 공개키 A와 p를 이용하여 $\mathbf{Y}\ \mathbf{A}^T \pmod p$를 먼저 계산한다. 만약 $\mathbf{Y}\ \mathbf{A}^T \pmod p = \mathbf{X}$이면, 認證쌍 $(\mathbf{X}, \mathbf{Y})$는 정당한 것으로 認證하고, 그러나 만약 $\mathbf{Y}\ \mathbf{A}^T \pmod p \neq \mathbf{X}$이면 정당하지 않은 것으로 간주한다. 그리고 숨어

있는 메세지 $\mathbf{X}^*$는 비밀키 $\mathbf{B}$를 이용하여 다음과 같이 복원할 수 있다.

$$\mathbf{X}^* \equiv \mathbf{Y}\ \mathbf{B}^T \pmod p \tag{88}$$

[例題 22] $\mathbf{X} \equiv \mathbf{Y}\ \mathbf{B}^T \pmod p$ 그리고 $\mathbf{X}^* \equiv \mathbf{Y}\ \mathbf{B}^T \pmod p$임을 증명하라.

$\mathbf{Y}\ \mathbf{A}^T \pmod p$는 다음과 같이 표현된다.

$$\mathbf{Y}\ \mathbf{A}^T = (\mathbf{Y}' + \mathbf{R})\ \mathbf{A}^T = \mathbf{Y}'\ \mathbf{A}^T + \mathbf{R}\ \mathbf{A}^T \tag{89}$$

식 (87)로 부터, 우리는 다음을 얻는다.

$$\mathbf{R}\ \mathbf{A}^T = \mathbf{X} - \mathbf{X}' \pmod p \tag{90}$$

그리고

$$\mathbf{Y}'\ \mathbf{A}^T = (y'_1,\ y'_2,\ \cdots,\ y'_{2n}) \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{2n} \end{bmatrix} = \sum_{j=1}^{2n} y'_j a_j \tag{91}$$

초기의 暗號文 $\mathbf{Y}' \equiv \mathbf{X}'\ \mathbf{K} \pmod p$이므로 이것은 다음과 같다.

$$(y'_1,\ y'_2,\ \cdots,\ y'_{2n}) = (x'_n,\ x'_{n-1},\ \cdots,\ x'_1) \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1,\,2n} \\ k_{21} & k_{22} & \cdots & k_{2,\,2n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ k_{n,\,1} & k_{n,\,2} & \cdots & k_{n,\,2n} \end{bmatrix}$$

여기서 j번째 열이 다음과 같다.

$$y'_j = \sum_{i=1}^{n} x'_{n-i+1}\ k_{ij},\quad 1 \le j \le 2n \tag{92}$$

식 (92)를 식 (91)에 치환하면

$$\mathbf{Y}'\ \mathbf{A}^T = \sum_{j=1}^{2n} y'_j \cdot a_j = \sum_{j=1}^{n} x'_{n-i+1} \sum_{j=1}^{2n} k_{ij} \cdot a_j \tag{93}$$

식 (90)과 (93)을 식 (89)에 치환하면 다음과 같다.

$$\mathbf{Y}\ \mathbf{A}^T \equiv \mathbf{X} \pmod p \tag{94}$$

한편 $\mathbf{Y}\mathbf{B}^T$은 다음과 같다.

$$\mathbf{Y}\ \mathbf{B}^T = (\mathbf{Y}' + \mathbf{R})\mathbf{B}^T = \mathbf{Y}'\ \mathbf{B}^T + \mathbf{R}\ \mathbf{B}^T = (\mathbf{X}'\ \mathbf{K})\mathbf{B}^T + \mathbf{R}\ \mathbf{B}^T$$

식 (85)로 부터 $\mathbf{K}\ \mathbf{B}^T = 0 \pmod p$이므로, 우리는 식 (86)을 이용하여 다음을 얻는다.

$$\mathbf{Y}\ \mathbf{B}^T \equiv \mathbf{X}^* \pmod p \tag{95}$$

(증명끝)

위에서 기술된 認證技法의 구체적인 동작은 例題 23에 나타나 있다.

[例題 23] 平文의 길이 n을 3이라 하고, $p \geq 2^3-1$을 만족하는 소수 p를 7이라 가정한다. 송신자는 3×6 행렬 K를 임의로 다음과 같이 선택한다.

$$K=\begin{bmatrix} 1&4&3&1&3&1 \\ 2&2&2&4&0&2 \\ 4&1&1&1&2&0 \end{bmatrix}$$

$$K\cdot A^T\equiv \begin{bmatrix} 1&4&3&1&3&1 \\ 2&2&2&4&0&2 \\ 4&1&1&1&2&0 \end{bmatrix}\cdot\begin{bmatrix} 3 \\ 2 \\ 1 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix}\equiv\begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} \pmod 7$$

윗 식으로부터 다음과 같은 선형 합동시스템을 얻는다.

$$\begin{aligned} 3+8+3+\ a_4+3a_5+\ a_6&\equiv 1 \pmod 7 \\ 6+4+2+4a_4+\ \ 2a_6&\equiv 2 \pmod 7 \\ 12+2+1+\ a_4+2a_5\ \ &\equiv 4 \pmod 7 \end{aligned}$$

또는

$$\begin{aligned} a_4+3a_5+\ a_6&\equiv 1 \pmod 7 \\ 4a_4+\ \ 2a_6&\equiv 1 \pmod 7 \end{aligned}$$

마지막 합동식은 다음과 같이 나타낼 수 있다.

$$a_4\equiv 3-2a_5 \pmod 7$$

처음 두 합동식에 이 a_4를 대입하면,

$$\begin{aligned} a_5+a_6&\equiv 5 \pmod 7 \\ -4a_5+a_6&\equiv 3 \pmod 7 \end{aligned}$$

을 얻는다. 이 마지막 세 합동식을 풀어서 각각 A의 나머지 세 원소 a_4, a_5, a_6을 $a_5=6$, $a_6=6$, $a_4=5$와 같이 구한다. 위의 과정을 통해 **A**=(3, 2, 1, 5, 6, 6)을 구한 후 (**A**, **P**)={(3, 2, 1, 5, 6, 6), 7} 수정완료를 공개키로 공개한다. 한편 송신자와 수신자만이 공유하는 비밀벡터 **B**는 식 (85)를 이용하여 계산한다.

$$\mathbf{K}\cdot\mathbf{B}^T\equiv\begin{bmatrix} 1&4&3&1&3&1 \\ 2&2&2&4&0&2 \\ 4&1&1&1&2&0 \end{bmatrix}\cdot\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b \\ b_6 \end{bmatrix}\equiv 0 \pmod 7$$

이 합동 시스템은 3개의 합동식과 6개의 미지수를 갖기 때문에 그중 3개를 $b_1=1$, $b_2=3$, $b_3=2$와 같이 임의로 결정한다. 남은 3개 원소는 다음과 같이 구할 수 있다.

$$\begin{aligned} 1+12+6+\ b_4+3b_5+\ b_6 &\equiv 0 \pmod 7 \\ 2+\ 6+4+4b_4+\quad 2b_6 &\equiv 0 \pmod 7 \\ 4+\ 3+2+\ b_4+2b_5 \quad &\equiv 0 \pmod 7 \end{aligned}$$

또는

$$\begin{aligned} b_4+3b_5+\ b_6 &\equiv 2 \pmod 7 \\ 4b_4+\quad 2b_6 &\equiv 2 \pmod 7 \\ b_4+2b_5 \quad &\equiv 5 \pmod 7 \end{aligned}$$

이 세개의 합동 시스템을 풀어서 $b_5=4$, $b_4=4$, $b_6=0$을 얻는다. 이것으로 부터 비밀키 **B**는 **B**=(1, 3, 2, 4, 4, 0)을 구할 수 있다.

B는 숨어 있는 메세지 **X**을 전송하기 전에 수신자에게 미리 비밀스럽게 보내져야 한다. 송신자가 지금 숨어 있는 메세지 $X=3\in GF(7)$을 송신한다고 가정한다. 송신자는 먼저 벡터 $\mathbf{R}=(r_1, r_2, r_3, r_4, r_5, r_6)$를 다음과 같이 계산한다.

$$\mathbf{X}^* \equiv \mathbf{R}\cdot\mathbf{B}^T$$

$$\equiv (r_1, r_2, r_3, r_4, r_5, r_6)\cdot\begin{bmatrix}1\\3\\2\\4\\4\\0\end{bmatrix} \pmod 7$$

$$=3$$

이 합동식을 만족할 수 있는 많은 해중 한 해는 **R**=(0 0 1 1 1 0)이다. 송신자는 **R**을 위 합동식을 만족하는 또다른 2진배열 **R**=(1 1 1 1 0 0)로 사용할 수 있다. 여기서 **R**은 $\mathbf{X}^*$의 전송자(carrier)라 불리워지기도 한다.

송신자는 숨어 있는 메세지 $\mathbf{X}^*$을 $\mathbf{X}'$을 이용하여 보낸다고 가정하면, 송신자는 임의로 메세지 $\mathbf{X}=6 \pmod 7$을 선택한다. 송신자는 변형된 메세지 $\mathbf{X}'$을 숨어 있는 메세지 $\mathbf{X}^*$와 위에서 구해진 **R**, 그리고 공개키 **A**를 이용하여 생성한다.

$$\mathbf{X}' \equiv \mathbf{X}-\mathbf{R}\ \mathbf{A}^T \pmod P$$

$$\equiv 6-(0\ 0\ 1\ 1\ 1\ 0)\cdot\begin{bmatrix}5\\2\\1\\5\\6\\6\end{bmatrix} \pmod 7$$

$$=6-5=1$$

2진 표현법으로 $\mathbf{X}'$을 나타내면 $\mathbf{X}'=(1\ 0\ 0)$이다. 그 다음 송신자는 초기 暗號文 $\mathbf{Y}'$을 다음과 같이 계산한다.

$$\mathbf{Y}' \equiv \mathbf{X}'\cdot\mathbf{K} \pmod P$$

$$\equiv (1\ 0\ 0)\cdot\begin{bmatrix}1&4&3&1&3&1\\2&2&2&4&0&2\\4&1&1&1&2&0\end{bmatrix} \pmod 7$$

$$=(1,\ 4,\ 3,\ 1,\ 3,\ 1)$$

송신자는 최종 暗號文 **Y**를 다음과 같이 계산한다.

$$\begin{aligned} \mathbf{Y} &\equiv \mathbf{Y}'+\mathbf{R} \pmod P \\ &\equiv (1,\ 4,\ 3,\ 1,\ 3,\ 1)+(0,\ 0,\ 1,\ 1,\ 1,\ 0) \pmod 7 \\ &\equiv (1,\ 4,\ 4,\ 2,\ 4,\ 1) \end{aligned}$$

송신자는 認證 쌍 (X, Y)={6, (1, 4, 4, 2, 4, 1)}을 수신자에게 송신한다. 수신자는 (X, Y)를 수신하면 먼저 $\mathbf{Y}\cdot\mathbf{A}^T$를 계산한다.

$$\mathbf{Y}\cdot\mathbf{A}^T\equiv(1,\ 4,\ 4,\ 2,\ 4,\ 1)\cdot\begin{bmatrix}3\\2\\1\\5\\6\\6\end{bmatrix}\ (\mathrm{mod}\ 7)\equiv 55\ (\mathrm{mod}\ 7)=6$$

$\mathbf{Y}\cdot\mathbf{A}^T=\mathbf{X}=6$이므로 (X, Y) 認證쌍은 認證된 것으로 간주한다. 마지막으로 식 (95)를 사용하여 숨어 있는 메세지 $\mathbf{X}^*$은 다음과 같이 복구된다.

$$\mathbf{X}^*\equiv\mathbf{Y}\cdot\mathbf{B}^T\ (\mathrm{mod}\ p)$$

$$\equiv(1,\ 4,\ 4,\ 2,\ 4,\ 1)\cdot\begin{bmatrix}1\\3\\2\\4\\4\\6\end{bmatrix}\ (\mathrm{mod}\ 7)\equiv 45\ (\mathrm{mod}\ 7)=3$$

따라서 숨어 있는 메세지 $\mathbf{X}^*$도 완전하게 복구될 수 있다.

7. 連載特講을 마치면서

본 연재특강에서는 公開키 암호시스템 및 署名시스템에 대해 주로 기술하였다. 여기서 기술한 硏究內容 이외에 현재 선진 각국에서 활발히 수행하고 있는 ID 기본암호 시스템 및 영지식 상호 증명시스템 등의 연구분야는 IC 카드 즉, 스마트 카드가 常用通信網에 널리 적용될 예정이므로 앞으로 국내에서도 활발히 연구가 수행되어야 할 분야이다. 따라서 이 분야에 대한 연재특강도 제시할 수 있으나, 본 學會誌의 근본 취지인 여러 硏究者들에게 지면을 할애해야 한다는 原則을 고려하여 기술할 수 없음을 유감으로 생각한다. 그러나 독자의 要求나 추후에 지면이 허용되면 연재할 것을 약속한다.

끝으로 여기서 記述된 內容이 이 분야의 응용 및 연구시 널리 活用될 수 있었음 하는 바램이다.

참 고 문 헌

1. ElGamal, T. : "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Inform. Theory, vol, IT-31, no. 4, pp.469-472, Junly 1985.

2. Odlyzko, A.M. : "Cryptanalytic Attacks on the Multiplicative Knapsack Cryptosystem and on Shamir's Fast Signature Scheme", IEEE Trans. Inform, Theory, vol. IT-30, no. 4. pp.594-601, July 1984.

3. Ong, H., C.P. Schorr, and A. Schamir, "An Efficient Signature Scheme Based on Quadratic Equations", Proc, of the 16th Symposium on the Theory of Computing. Washington, DC. April 1984.

4. Pollard, J.M. and C.P. Schnorr : "An Efficient Solution of the Congruence $x^2+ky^2\equiv m \pmod n$", IEEE Trans. Inform, Theroy, vol. IT-33, no. 5, pp.702-709, Sept. 1987.

5. Seberry, J. : "A Subliminal Channel in Codes for Authetication without Secrecy", Ars Combinatoria, vol. 19A, pp.337-342, 1985.

6. Seberry, J. and Pieprzyk : Cryptography : An Introduction to Computer Security, Prentice Hall, Sydeny, Australia, 1989.

□ 著者紹介

李 晩 榮(終身會員)

1924년 11月 30日生
漢陽大學校 名譽教授
韓國通信情報保護學會 會長
受 賞 : 大韓民國 學術院賞
著 書 : Error Correcting Coding Theory, McGraw-Hill, New York, 1989.