論 文

"컴퓨터 통신 NETWORK를 위한 공개키 암호 시스템"에 관한 고찰

正會員 權 蒼 英* 正會員 張 靑 龍** 正會員 元 東 豪***

A Study on "A Public Key Cryptosystem for Computer Communication Networks"

Chang Young Kwon*, Chung Ryong Jang**, Dong Ho Won*** *Regular Members*

要 約

한국통신학회 논문지('92-3 Vol.17 No.3) "컴퓨터 통신 NETWORK를 위한 공개키 암호 시스템에 관한 연구(논문번호 92-22)"에서 다변수 다항식을 이용하여 공개키 암호 시스템을 제안하였는 바 제안한 프로토콜은 공개정보를 아는 임의의 제3자가 비밀문에서 평문을 쉽게 해독할 수 있는 문제점이 있으며, 몇 가지 고려하여야 할 사항이 있어 지적한다.

ABSTRACT

This paper points out some weakpoints in the "A Study on Public Key Cryptosystem for Computer Communication Networks" proposed by Gi Jun Ku at KICS 92-22('92-3 Vol.17 No.3). This public key cryptosystem based on polynomials over finite rings is not strong against cipertext-only-attack. This paper indicate the insecureness of the proposed a public key cryptosystem.

I. 서 론

국내의 다변수 다항식을 이용한 공개키 암호 시스템에 대한 연구[1,2,3] 중 KISC 92-22 "컴퓨터 통신 Network를 위한 공개키 암호 시스템에 관한 연구"에서 제안된 다변수 다항식을 이용한 공개키 암호 시스템[1]은 공개정보인 f(x,y,z), h(x,y,z)와 비밀문을 이용하여 제3자가 비밀문에서 평문을 해독할 수 있는 문제점이 있으며 몇가지 고려하여야 할 사항이 있어 본고를 작성하였다.

* 大宥工業專門大學 事務自動化科
Dept. of Office Automation, Dae Yeu Technical Junior College
** 韓國通信 研究開發團
Korea Telecom Research Center
*** 成均館大學校 情報工學科
Dept. of Information Engineering, Sung Kyun Kwan Univ.

論文番號 : 93-108

II. KLS 공개키 암호 시스템

논문 KISC 92-22 "컴퓨터 통신 Network를 위한 공개키 암호 시스템에 관한 연구"[이하 KLS 방식]의 "III. 데이타 보안성을 위한 공개키 암호" 내용을 요약 정리하면 다음과 같다.

II.1. 공개 정보 생성 방법

gcd(3, p-1) = 1이 만족되는 소수 p를 생성하고, 3변수 x, y, z에 대하여 적당한 값 3개를 생성한다.

$$0 < x_i, y_i, z_i < p \quad 단, i = 1, 2, 3 \tag{1}$$

또한 z_i의 GF(p) 상에서의 승산 역원 z_i^{-1}을 구하고 식(2)를 만족하는 a_j, b_j를 선택하고, 식(3)으로 r_i를 계산한 후 식 (4), (5)로 공개키 f(x,y,z), h(x,y,z)를 구하여 공개한다.

$$0 < a_j,\ b_j < p \qquad \text{단, } j = 1, 2, 3, 4, 5, 6 \tag{2}$$

$$r_i = -(a_i \cdot x_i + b_i \cdot y_i) z_i^{-1} \tag{3}$$
$$r_{i+3} = -(a_{i+3} \cdot x_i + b_{i+3} \cdot y_i) z_i^{-1} \qquad \text{단, } i = 1, 2, 3$$

$$f(x,y,z) = \prod_{j=1}^{3} (a_j \cdot x + b_j \cdot y + r_j \cdot z) \tag{4}$$

$$h(x,y,z) = \prod_{j=4}^{6} (a_j \cdot x + b_j \cdot y + r_j \cdot z) \tag{5}$$

식 (6)을 만족하는 d를 계산하고, 위에서 선택한 x_i, y_i, z_i(i=1,2,3)을 이용하여 식 (7), (8)이 만족되는 $T_1T_2 - T_3T_4$의 승산 역원 및 T_4의 승산 역원을 계산하여 자신의 비밀키로 한다.

$$3 \cdot d \equiv 1 \pmod{p-1} \tag{6}$$

$$(T_1T_2 - T_3T_4)(T_1T_2 - T_3T_4)^{-1} \equiv 1 \pmod{p} \tag{7}$$

$$T_4T_4^{-1} \equiv 1 \pmod{p} \tag{8}$$

단, $T_1 = x_1z_2 - x_2z_1 = \begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix}$

$T_2 = y_1z_3 - y_3z_1 = \begin{vmatrix} y_1 & z_1 \\ y_3 & z_3 \end{vmatrix}$

$T_3 = x_1z_3 - x_3z_1 = \begin{vmatrix} x_1 & z_1 \\ x_3 & z_3 \end{vmatrix}$

$T_4 = y_1z_2 - y_2z_1 = \begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix}$

Ⅱ.2. 암호화 과정

KLS 방식의 암호화 과정을 단계별로 나타내면, 아래와 같다.

단계 1. 3개의 평문 블럭 M_1, M_2, M_3을 식 (9)의 다항식 형태로 나타낸다.

$$M(x,y,z) \equiv M_1x + M_2y + M_3z \pmod{p} \tag{9}$$

단계 2. 임의의 수 a, b(0<a, b<p)를 이용하여 비밀 다항식을 생성한다.

$$C(x,y,z) \equiv M(x,y,z)^3 + af(x,y,z) + bh(x,y,z) \pmod{p} \tag{10}$$

비밀 다항식의 계수 C_i(i=1,...,10)를 수신자에게 전송한다.

Ⅱ.3. 복호화 과정

KLS 방식의 복호화 과정을 단계별로 나타내면, 아래와 같다.

단계 1. 10개의 비밀문 블럭 C_i를 이용하여 식 (10)의 다항식 형태로 나타낸다.

단계 2. $C(x,y,z)$에 f(x,y,z), h(x,y,z)의 근 x_i, y_i, z_i(i=1,2,3)을 대입하여 af(x,y,z) 및 bh(x,y,z)의 항이 소거된 다항식 3개를 계산한다.

$$C(x_1, y_1, z_1) \equiv M(x_1, y_1, z_1)^3 \equiv D_1(x_1, y_1, z_1) \pmod{p} \tag{11}$$

$$C(x_2, y_2, z_2) \equiv M(x_2, y_2, z_2)^3 \equiv D_2(x_2, y_2, z_2) \pmod{p} \tag{12}$$

$$C(x_3, y_3, z_3) \equiv M(x_3, y_3, z_3)^3 \equiv D_3(x_3, y_3, z_3) \pmod{p} \tag{13}$$

단계 3. $D_i(x_i, y_i, z_i)$(i=1,2,3)을 비밀키 d로 각각 멱승하여 아래의 다항식 3개를 구한다.

$$D_1(x_1, y_1, z_1)^d \equiv M(x_1, y_1, z_1) \equiv M_1x_1 + M_2y_1 + M_3z_1 \pmod{p} \tag{14}$$

$$D_2(x_2, y_2, z_2)^d \equiv M(x_2, y_2, z_2) \equiv M_1x_2 + M_2y_2 + M_3z_2 \pmod{p} \tag{15}$$

$$D_3(x_3, y_3, z_3)^d \equiv M(x_3, y_3, z_3) \equiv M_1x_3 + M_2y_3 + M_3z_3 \pmod{p} \tag{16}$$

단계 4. 3원 1차 연립방정식 $M(x_i, y_i, z_i)$(i=1,2,3)의 해 M_1, M_2, M_3를 구하여 평문을 획득한다.

Ⅲ. 문 제 점

Ⅲ.1. KLS 방식의 해독

a, b가 어떠한 경로로 알려졌을 경우(논문 KISC 92-22의 "그림 3"에서 처럼 a, b를 공개키로 하였을 경우 또는 공격자가 모종의 방법으로 a, b를 알았을 경우) KLS 방식의 암호화 과정에서 af(x,y,z)와 bh(x,y,z)를 더하는 행위는 제안한 방식의 안전성을 전혀 보장하여 주지 못하여 암호화 과정의 계산량만 증가시키는 결과를 초래한다. 왜냐하면, 누구나 알 수 있는 공개 정보를 이용하여 아래와 같은 방법으로 해독과정을 거치면, 비밀문에서 평문을 해독할 수 있다.

해독 알고리즘 1.

단계 1. 공개 정보 a, b, f(x,y,z), h(x,y,z)를 이용하여 아래와 같은 계산을 한다.

$$C(x,y,z) - af(x,y,z) - bh(x,y,z) \equiv M(x,y,z)^3 \pmod{p} \quad (17)$$

즉, 식 (17)의 결과인 다항식중 x^3, y^3, z^3의 계수는 M_1^3, M_2^3, M_3^3이다.

단계 2. mod p−1상에서의 식(18)이 성립하는 d를 Euclid 알고리즘으로 계산한다.

$$3 \cdot d \equiv 1 \pmod{p-1} \quad (18)$$

단계 3. 단계 1의 결과 다항식의 x^3, y^3, z^3항의 계수를 각기 mod p 상에서 d승을 취하여, 평문 M_1, M_2, M_3을 획득한다.

a, b가 알려졌을 경우, KLS 방식은 실제로 해독 가능하다는 것을 입증하기 위하여, 논문 KISC 92-22에서 시뮬레이션한 자료를 그대로 이용하여 해독한 결과를 제시하였다. 이 과정은 IBM-PC에서 시뮬레이션한 결과이다.

그러므로 a, b가 어떠한 경로로 알려졌을 경우, KLS 방식의 암호화 과정 중 af(x,y,z)항과 bh(x,y,z)항을 더하는 행위는 제안한 방식의 안정성에는 도움을 주지 못하며, 암호화 과정의 계산량만 증가시키는 결과를 초래한다. 또한, mod p 상에서의 공개키와 비밀키의 쌍(e, d)의 적용은 공개키 e로부터 비밀키 d를 Euclid 알고리즘으로 계산 가능하므로 안전성이 없는 방식이다. KLS 방식은 e=3인 특별한 경우이므로 비밀키 d를 Euclid 알고리즘으로 계산 가능하므로 안정성이 없는 방식이다.

Ⅲ.2. KLS 방식의 일반적인 해독

KLS 방식에서 a, b를 공개하지 않은 상태에서는 앞절에서 언급한 해독 방법으로는 해독되지 않으며, 이 경우 KLS 방식의 안전성은 공개키인 다항식 f(x,y,z), h(x,y,z)를 동시에 만족하는 임의의 근 x_i, y_i, z_i(i=1, 2, 3) 3개를 구하는 문제로 귀착(reduce)된다.

즉, 2개의 3변수 다항식 f(x,y,z), h(x,y,z)에서 근 x_i, y_i, z_i(i=1, 2, 3)를 구하는 문제인 mod p 상에서의 부정방정식의 해를 구하는 문제로 귀착된다.

그러나, 본고에서는 아래의 10개 식을 이용하여 "a, b를 찾는 문제" 또는 "a, b, M_1, M_2, M_3을 찾는 문제"로 귀착시켜 해독하는 방법을 제시하고자 한다.

표 1. KLS 공개키 암호 시스템의 해독(mod 29, a=6, b=25)

Table 1. Cryptanalysis of KLS Public Key Cryptosystem

항	수치화	암호화	공개정보활용				해독 1	해독 3
	평문	비밀문	f(x,y,z)	h(x,y,z)	a*f(x,y,z)	b*f(x,y,z)	$M(x,y,z)^3$	M_i
x^3	P(16)	27	6	4	7	13	7	16(P)
y^3	U(21)	10	24	7	28	1	10	21(U)
z^3	B(2)	18	28	25	23	16	8	2(B)
x^2y		8	0	28	0	4	4	
x^2z		13	21	28	10	4	28	
xy^2		9	17	1	15	25	27	
y^2z		5	7	11	13	14	7	
xz^2		10	7	27	13	8	18	
yz^2		12	28	15	23	27	20	
xyz		21	4	1	24	25	1	

$$
\begin{aligned}
C_1 &= M_1^3 + a f_1 + b h_1 \\
C_2 &= M_2^3 + a f_2 + b h_2 \\
C_3 &= M_3^3 + a f_3 + b h_3 \\
C_4 &= 3M_1^2 M_2 + a f_4 + b h_4 \\
C_5 &= 3M_1^2 M_3 + a f_5 + b h_5 \\
C_6 &= 3M_1 M_2^2 + a f_6 + b h_6 \\
C_7 &= 3M_2^2 M_3 + a f_7 + b h_7 \\
C_8 &= 3M_1 M_3^2 + a f_8 + b h_8 \\
C_9 &= 3M_2 M_3^2 + a f_9 + b h_9 \\
C_{10} &= 6M_1 M_2 M_3 + a f_{10} + b h_{10}
\end{aligned} \tag{19}
$$

Ⅲ.2.1. 선형연립방정식 문제로 귀착

식 (19)로 표시되는 10개의 C_i는 비보호 통신로를 이용하여 전송되는 비밀문이므로 제 3자가 도청이 가능하며, f_i 및 h_i는 공개정보이므로 암호해독자는 M_1, M_2, M_3을 미지수로 하는 연립방정식을 풀려고 여러 가지 방법으로 시도할 것이다.

본고에서는 선형연립방정식의 해를 구하는 방법을 이용하기 위하여 식 (19)를 이항정리하여 식 (20)으로 변형한다.

$$
\begin{aligned}
M_1^3 &= C_1 - a f_1 - b h_1 \\
M_2^3 &= C_2 - a f_2 - b h_2 \\
M_3^3 &= C_3 - a f_3 - b h_3 \\
3M_1^2 M_2 &= C_4 - a f_4 - b h_4 \\
3M_1^2 M_3 &= C_5 - a f_5 - b h_5 \\
3M_1 M_2^2 &= C_6 - a f_6 - b h_6 \\
3M_2^2 M_3 &= C_7 - a f_7 - b h_7 \\
3M_1 M_3^2 &= C_8 - a f_8 - b h_8 \\
3M_2 M_3^2 &= C_9 - a f_9 - b h_9 \\
6M_1 M_2 M_3 &= C_{10} - a f_{10} - b h_{10}
\end{aligned} \tag{20}
$$

식 (20)은 일반적으로 그 해가 존재하나 본고에서는 KLS 방식에서 시뮬레이션한 결과를 실제로 해독한 근거를 제시하기 위하여 mod 29 상에서 수식을 전개하였다. 3 및 6의 mod 29 상의 승산 역원 10, 5를 이용하면, 아래와 같은 10개의 식을 얻을 수 있다.

$$
\begin{aligned}
M_1^3 &= C_1 - a f_1 - b h_1 \\
M_2^3 &= C_2 - a f_2 - b h_2 \\
M_3^3 &= C_3 - a f_3 - b h_3 \\
M_1^2 M_2 &= 10C_4 - 10a f_4 - 10b h_4 \\
M_1^2 M_3 &= 10C_5 - 10a f_5 - 10b h_5 \\
M_1 M_2^2 &= 10C_6 - 10a f_6 - 10b h_6 \\
M_2^2 M_3 &= 10C_7 - 10a f_7 - 10b h_7 \\
M_1 M_3^2 &= 10C_8 - 10a f_8 - 10b h_8 \\
M_2 M_3^2 &= 10C_9 - 10a f_9 - 10b h_9 \\
M_1 M_2 M_3 &= 5C_{10} - 5a f_{10} - 5b h_{10}
\end{aligned} \tag{21}
$$

위의 10개 식을 이용하여 아래와 같은 3종류의 관계식을 얻을 수 있다.

$$M_1/M_2 \tag{22}$$

$$
\begin{aligned}
&= M_1^3/M_1^2 M_2 = (C_1 - a f_1 - b h_1)(10C_4 - 10a f_4 - 10b h_4) \\
&= M_2^2 M_1/M_2^3 = (10C_6 - 10a f_6 - 10b h_6)(C_2 - a f_2 - b h_2) \\
&= M_1^2 M_3/M_1 M_2 M_3 = (10C_5 - 10a f_5 - 10b h_5)(5C_{10} - 5a f_{10} - 5b h_{10}) \\
&= M_1 M_2 M_3/M_2^2 M_3 = (5C_{10} - 5a f_{10} - 5b h_{10})(10C_7 - 10a f_7 - 10b h_7)
\end{aligned}
$$

$$M_2/M_3 \tag{23}$$

$$
\begin{aligned}
&= M_2^3/M_2^2 M_3 = (C_2 - a f_2 - b h_2)(10C_7 - 10a f_7 - 10b h_7) \\
&= M_3^2 M_2/M_3^3 = (10C_9 - 10a f_9 - 10b h_9)(C_3 - a f_3 - b h_3) \\
&= M_1 M_2^2/M_1 M_2 M_3 = (10C_6 - 10a f_6 - 10b h_6)(5C_{10} - 5a f_{10} - 5b h_{10}) \\
&= M_1 M_2 M_3/M_1 M_3^2 = (5C_{10} - 5a f_{10} - 5b h_{10})(10C_8 - 10a f_8 - 10b h_8)
\end{aligned}
$$

$$M_3/M_1 \tag{24}$$

$$
\begin{aligned}
&= M_1^2 M_3/M_1^3 = (10C_5 - 10a f_5 - 10b h_5)(C_1 - a f_1 - b h_1) \\
&= M_3^3/M_1^2 M_1 = (C_3 - a f_3 - b h_3)(10C_8 - 10a f_8 - 10b h_8) \\
&= M_1 M_2 M_3/M_1^2 M_2 = (5C_{10} - 5a f_{10} - 5b h_{10})(10C_4 - 10a f_4 - 10b h_4) \\
&= M_2 M_3^2/M_1 M_2 M_3 = (10C_9 - 10a f_9 - 10b h_9)(5C_{10} - 5a f_{10} - 5b h_{10})
\end{aligned}
$$

위 3식에서 M_1/M_2, M_2/M_3, M_3/M_1을 각각 K_1, K_2, K_3로 놓고 정리하면, 아래 식을 얻을 수 있다.

$$
\begin{aligned}
af_1 + bh_1 + K_1(10C_4 - 10af_4 - 10bh_4) &= C_1 \\
10af_6 + 10bh_6 + K_1(C_2 - af_2 - bh_2) &= 10C_6 \\
10af_5 + 10bh_5 + K_1(5C_{10} - 5af_{10} - 5bh_{10}) &= 10C_5 \\
5af_{10} + 5bh_{10} + K_1(10C_7 - 10af_7 - 10bh_7) &= 5C_{10}
\end{aligned}
\tag{25}
$$

$$
\begin{aligned}
af_2 + bh_2 + K_2(10C_7 - 10af_7 - 10bh_7) &= C_2 \\
10af_9 + 10bh_9 + K_2(C_3 - af_3 - bh_3) &= 10C_9 \\
10af_6 + 10bh_6 + K_2(5C_{10} - 5af_{10} - 5bh_{10}) &= 10C_6 \\
5af_{10} + 5bh_{10} + K_2(10C_8 - 10af_8 - 10bh_8) &= 5C_{10}
\end{aligned}
\tag{26}
$$

$$
\begin{aligned}
10af_5 + 10bh_5 + K_3(C_1 - af_1 - bh_1) &= 10C_5 \\
af_3 + bh_3 + K_3(10C_8 - 10af_8 - 10bh_8) &= C_3 \\
5af_{10} + 5bh_{10} + K_3(10C_4 - 10af_4 - 10bh_4) &= 5C_{10} \\
10af_9 + 10bh_9 + K_3(5C_{10} - 5af_{10} - 5bh_{10}) &= 10C_9
\end{aligned}
\tag{27}
$$

또한, 위 식을 a, b, K_1, K_2, K_3와 aK_1, aK_2, aK_3 및 bK_1, bK_2, bK_3를 미지수로 보고 정리하면, 변수가 5개이고 방정식이 4개인 연립방정식 3쌍을 얻을 수 있다.

$$
\begin{aligned}
f_1 a + h_1 b + 10C_4 K_1 - 10f_4 aK_1 - 10h_4 bK_1 &= C_1 \\
10f_6 a + 10h_6 b + C_2 K_1 - f_2 aK_1 - h_2 bK_1 &= 10C_6 \\
10f_5 a + 10h_5 b + 5C_{10} K_1 - 5f_{10} aK_1 - 5h_{10} bK_1 &= 10C_5 \\
5f_{10} a + 5h_{10} b + 10C_7 K_1 - 10f_7 aK_1 - 10h_7 bK_1 &= 5C_{10}
\end{aligned}
\tag{28}
$$

$$
\begin{aligned}
f_2 a + h_2 b + 10C_7 K_2 - 10f_7 aK_2 - 10h_7 bK_2 &= C_2 \\
10f_9 a + 10h_9 b + C_3 K_2 - f_3 aK_2 - h_3 bK_2 &= 10C_9 \\
10f_6 a + 10h_6 b + 5C_{10} K_2 - 5f_{10} aK_2 - 5h_{10} bK_2 &= 10C_6 \\
5f_{10} a + 5h_{10} b + 10C_8 K_2 - 10f_8 aK_2 - 10h_8 bK_2 &= 5C_{10}
\end{aligned}
\tag{29}
$$

$$
\begin{aligned}
10f_5 a + 10h_5 b + C_1 K_3 - f_1 aK_3 - h_1 bK_3 &= 10C_5 \\
f_3 a + h_3 b + 10C_8 K_3 - 10f_8 aK_3 - 10h_8 bK_3 &= C_3 \\
5f_{10} a + 5h_{10} b + 10C_4 K_3 - 10f_4 aK_3 - 10h_4 bK_3 &= 5C_{10} \\
10f_9 a + 10h_9 b + 5C_{10} K_3 - 5f_{10} aK_3 - 5h_{10} bK_3 &= 10C_9
\end{aligned}
\tag{30}
$$

즉, 최초의 10개 식을 이용하여 "a, b를 찾는 문제" 또는 "a, b, M_1, M_2, M_3을 찾는 문제"는 a, b, K_1, K_2, K_3와 aK_1, aK_2, aK_3 및 bK_1, bK_2, bK_3를 미지수로 보면, 변수가 5개이고 방정식이 4개인 연립방정식 3쌍을 동시에 만족하는 선형연립방정식의 해를 구하는 문제로 귀착(reduce)된다.

Ⅲ.2.2. 선형연립방정식의 풀이

앞 절에서 획득한 4개 연립방정식 (28), (29), (30) 각각은 5개의 미지수를 갖는 4개의 선형 연립방정식 형태로 변형 가능하다.

$$
\begin{aligned}
a_{11} x_1 + a_{12} x_2 + a_{13} x_3 + a_{14} x_4 + a_{15} x_5 &= b_1 \\
a_{21} x_1 + a_{22} x_2 + a_{23} x_3 + a_{24} x_4 + a_{25} x_5 &= b_2 \\
a_{31} x_1 + a_{32} x_2 + a_{33} x_3 + a_{34} x_4 + a_{35} x_5 &= b_2 \\
a_{41} x_1 + a_{42} x_2 + a_{43} x_3 + a_{44} x_4 + a_{45} x_5 &= b_4
\end{aligned}
$$

단, $x_1 = a$, $x_2 = K_1$, $x_3 = aK_1$, $x_4 = bK_1$, $x_5 = b$

(31)

선형연립방정식의 해를 구하는 방법에는 행렬식을 이용한 Cramer의 법칙을 이용하는 방법이 있으나, 이 방법은 $n = 2$인 경우에 매우 좋고, $n = 3$인 경우에는 유용한 정도이나, $n \geq 4$인 경우에 대해서는 Gauss-Jordan 방법이 보다 효과적이다[4].

특히, Gauss-Jordan 방법은 계수행렬이 정칙(non-singular)일 필요도 없으며 하나 이상의 해가 존재할 때에도 모든 해를 구할 수 있는 장점이 있다. 그러므로 본 논문에서는 Gauss-Jordan 방법을 이용하여 KLS 방식을 공격하는 방법을 모색하여 보기 위하여 관련된 이론을 간단히 언급하겠다.

제차 선형연립방정식(homogenious equation) 및 비제차 선형연립방정식(non-homogenious equation)은 모두 행렬을 이용하여 해를 구할 수 있으나, 보다 일반적인 비제차 선형연립방정식에 대하여 언급하겠다.

비제차 선형연립방정식을 계수 행렬(matrix of coefficient)을 이용하여 나타내면, 아래와 같은 형태로 쓸 수 있다.

$$AX = B \tag{32}$$

단, $A=\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \end{bmatrix}$ $X=\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}$ $B=\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}$

즉, 행렬 A의 행의 수는 방정식의 갯수이고, 행렬 A의 열의 수는 미지수의 갯수이다.

임의의 행렬은 기본 행연산(elementary row operations)을 취하여 자신과 행동치(row-equivalent)인 유일한 축소된 형렬(reduced form)을 얻을 수 있다. 또한, 행렬의 계수(rank)는 선형연립방정식의 해를 구하는데 중요한 역할을 하는데 행렬을 벡터 공간(vector space)으로 보면, 임의의 n행의 행렬 A는 R^n의 부분공간(sub space)이고, A의 계수는 A의 행공간(row space)의 차원을 의미한다. 행공간의 차원은 일차 독립인 행공간의 기저를 이루는 행의 갯수를 의미한다.

비제차 선형연립방정식의 해를 구할 때는 제차 선형연립방정식의 해를 구할 때와는 다르게 첨가행렬(augmented matrix) [A|B]을 이용한다.

여기서 행렬 A의 4개의 행벡터(row vecter)들이 정수링 상에서 선형 독립(linearly independent)이라고 가정하면, 첨가 행렬에서 기본 행연산을 취하면, 아래와 같은 형태의 축소된 행렬을 얻을 수 있으며 첨가 행렬 [A B]의 계수(rank)는 4이다.

$$[A|B]=\left[\begin{array}{cccc|c} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & b_1 \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & b_2 \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & b_3 \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & b_4 \end{array}\right] \tag{33}$$

$$[A|B]_R=\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & a_{15}' & b_1' \\ 0 & 1 & 0 & 0 & a_{25}' & b_2' \\ 0 & 0 & 1 & 0 & a_{35}' & b_3' \\ 0 & 0 & 0 & 1 & a_{45}' & b_4' \end{array}\right] \tag{34}$$

축소 행렬로 부터 변수 5개 중 2개로 구성되는 2원 연립방정식 4개를 얻을 수 있다. 이중에서 1번째 row에서 얻은 2원 연립방정식은 a와 b의 합동식이다.

이와 같은 방법을 앞 절에서 획득한 4개 연립방정식 각 쌍에 적용하면, a와 b의 합동식 3개를 얻을 수 있다. 이 연립합동방정식을 이용하면, 암호해독자는 a, b를 쉽게 계산할 수 있다. 암호해독자가 a, b를 성공적으로 구할 수 있으므로 KLS 방식은 해독 알고리즘 1로 쉽게 해독된다.

Ⅲ.3. 구체적인 예

앞 절에서 언급한 내용의 실제적 근거를 제시하기 위하여 KLS 논문에서의 시뮬레이션 데이타를 그대로 이용하여 해독하여 보도록하겠다.

표 2의 10개의 식을 이용하여 변수가 5개이고 방정식이 4개인 연립방정식 3쌍을 얻을 수 있으며, 그 첫번째 연립방정식을 풀기위하여 첨가행렬 [A|B]을 만들면 아래와 같으며, 그 첨가행렬의 축소행렬을 구하면 아래와 같다.

$$\left|\begin{array}{cccc|c} 6 & 22 & 0 & 10 & 4 & 27 \\ 25 & 10 & 5 & 22 & 10 & 3 \\ 7 & 18 & 9 & 24 & 19 & 14 \\ 20 & 21 & 17 & 6 & 5 & 18 \end{array}\right| \equiv \left|\begin{array}{cccc|c} 1 & 23 & 0 & 21 & 20 & 19 \\ 0 & 15 & 5 & 19 & 3 & 21 \\ 0 & 2 & 9 & 22 & 24 & 26 \\ 0 & 25 & 17 & 21 & 11 & 15 \end{array}\right| \equiv$$

$$\left|\begin{array}{cccc|c} 1 & 0 & 2 & 17 & 27 & 10 \\ 0 & 1 & 10 & 9 & 6 & 13 \\ 0 & 0 & 18 & 4 & 12 & 0 \\ 0 & 0 & 28 & 28 & 6 & 9 \end{array}\right| \equiv \left|\begin{array}{cccc|c} 1 & 0 & 0 & 23 & 16 & 10 \\ 0 & 1 & 0 & 10 & 9 & 13 \\ 0 & 0 & 1 & 26 & 20 & 0 \\ 0 & 0 & 0 & 25 & 26 & 9 \end{array}\right| \equiv$$

$$\left|\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 6 & 11 \\ 0 & 1 & 0 & 0 & 16 & 21 \\ 0 & 0 & 1 & 0 & 15 & 15 \\ 0 & 0 & 0 & 1 & 8 & 5 \end{array}\right| \tag{35}$$

즉, 축소행렬의 첫번째 행에서 식 (36)를 얻을 수 있다.

$$a + 6b \equiv 11 \pmod{29} \tag{36}$$

또한, 3쌍 중 2번째 4개의 연립방정식을 동일한 방법을 행하면, 아래와 같으며, 축소행렬의 첫번째 행에서 식 (38)을 얻을 수 있다.

$$\left|\begin{array}{cccc|c} 24 & 21 & 17 & 6 & 7 & 10 \\ 19 & 18 & 1 & 4 & 5 & 4 \\ 25 & 18 & 9 & 24 & 10 & 3 \\ 20 & 13 & 17 & 20 & 5 & 18 \end{array}\right| \equiv \left|\begin{array}{cccc|c} 1 & 19 & 14 & 22 & 16 & 27 \\ 0 & 5 & 25 & 21 & 20 & 13 \\ 0 & 7 & 7 & 25 & 16 & 24 \\ 0 & 10 & 27 & 15 & 4 & 0 \end{array}\right| \equiv$$

표 2. KLS 공개키 암호 시스템의 비밀문(mod 29)
Table 2. Cipertext of KLS Public Key Cryptosystem (mod 29)

항	수치화	암호화	비 밀 문 의 의 미
	평문	비밀문	$C(x,y,z) \equiv M(x,y,z)^3 + a * f(x,y,z) + b * h(x,y,z)$
x^3	P(16)	27	$27 \equiv M_1^3 + 6a + 4b$
y^3	U(21)	10	$10 \equiv M_2^3 + 24a + 7b$
z^3	B(2)	18	$18 \equiv M_3^3 + 28a + 25b$
x^2y		8	$8 \equiv 3M_1^2M_2 + 28b$
x^2z		13	$13 \equiv 3M_1^2M_3 + 21a + 28b$
xy^2		9	$9 \equiv 3M_1M_2^2 + 17a + 1b$
y^2z		5	$5 \equiv 3M_2^2M_3 + 7a + 11b$
xz^2		10	$10 \equiv 3M_1M_3^2 + 7a + 27b$
yz^2		12	$12 \equiv 3M_2M_3^2 + 28a + 15b$
xyz		21	$21 \equiv 6M_1M_2M_3 + 4a + 1b$

$$\left|\begin{array}{rrrrr:r} 1 & 0 & 6 & 6 & 27 & 24 \\ 0 & 1 & 5 & 10 & 4 & 20 \\ 0 & 0 & 1 & 13 & 17 & 0 \\ 0 & 0 & 6 & 2 & 22 & 3 \end{array}\right| \equiv \left|\begin{array}{rrrrr:r} 1 & 0 & 0 & 15 & 12 & 24 \\ 0 & 1 & 0 & 3 & 6 & 20 \\ 0 & 0 & 1 & 13 & 17 & 0 \\ 0 & 0 & 0 & 11 & 7 & 3 \end{array}\right| \equiv$$

$$\left|\begin{array}{rrrrr:r} 1 & 0 & 0 & 0 & 13 & 12 \\ 0 & 1 & 0 & 0 & 12 & 6 \\ 0 & 0 & 1 & 0 & 14 & 7 \\ 0 & 0 & 0 & 1 & 27 & 24 \end{array}\right| \qquad (37)$$

$$a + 13b \equiv 12 \qquad (\text{mod } 29) \qquad (38)$$

식 (36)와 식 (38)를 연립하여 풀면, a=6, b=25를 쉽게 구할 수 있다.

또한, 3쌍 중 3번째 4개의 연립방정식을 동일한 방법을 행하면, 아래와 같으며, 축소행렬의 첫번째 항에서 식 (40)을 얻을 수 있다.

$$\left|\begin{array}{rrrrr:r} 28 & 13 & 17 & 20 & 25 & 18 \\ 7 & 27 & 23 & 25 & 19 & 14 \\ 19 & 18 & 9 & 24 & 5 & 4 \\ 20 & 22 & 0 & 10 & 5 & 18 \end{array}\right| \equiv \left|\begin{array}{rrrrr:r} 1 & 16 & 12 & 9 & 4 & 11 \\ 0 & 2 & 26 & 20 & 20 & 24 \\ 0 & 4 & 13 & 27 & 16 & 27 \\ 0 & 21 & 21 & 4 & 12 & 1 \end{array}\right| \equiv$$

$$\left|\begin{array}{rrrrr:r} 1 & 0 & 7 & 23 & 18 & 22 \\ 0 & 1 & 13 & 10 & 10 & 12 \\ 0 & 0 & 19 & 16 & 5 & 8 \\ 0 & 0 & 9 & 26 & 5 & 10 \end{array}\right| \equiv \left|\begin{array}{rrrrr:r} 1 & 0 & 0 & 11 & 7 & 16 \\ 0 & 1 & 0 & 25 & 2 & 5 \\ 0 & 0 & 1 & 10 & 14 & 5 \\ 0 & 0 & 0 & 23 & 24 & 23 \end{array}\right| \equiv$$

$$\left|\begin{array}{rrrrr:r} 1 & 0 & 0 & 0 & 22 & 5 \\ 0 & 1 & 0 & 0 & 15 & 9 \\ 0 & 0 & 1 & 0 & 25 & 24 \\ 0 & 0 & 0 & 1 & 25 & 1 \end{array}\right| \qquad (39)$$

$$a + 22b \equiv 5 \qquad (\text{mod } 29) \qquad (40)$$

즉, a, b를 구하는 데 있어서 식 (36), 식 (38), 식 (40) 중 2개만을 이용하면 되며 암호해독자는 a, b를 쉽게 구할 수 있으므로 KLS 방식은 해독 알고리즘 1로 쉽게 해독된다.

Ⅳ. 결 론

KLS 방식은 앞에서 언급한 해독 방법에 의해서 임의의 난수 a, b를 공개키 및 비밀문을 이용하여 계산할 수 있으므로 mod p 상에서의 안전성은 없다. 또한, "n=pq로하면 RSA 암호의 안전성에 다항식의 소인수 분해의 어려움을 더한 효율적인 보안성을 가진 공개키 암호 시스템 기법이다."라고 주장하였으나, KLS 방식은 RSA 방식에서 공개키를 e=3으로 적용한 방법의 안전성과 동일한 정도의 안전성을 제공할 뿐이다.

즉, KLS 방식은 e=3으로 적용한 RSA 방식과 동일한 방식이며, 다변수 다항식을 결합함으로써 의미없는 계산량이 많아졌으며 암호문의 길이가 평문의 길이의 약 3.33배 정도가 되는 결과를 초래하였다.

참 고 문 헌

1. 구 기준, 이 영노, 심 수보 "컴퓨터 통신 Network를 위한 공개키 암호 시스템에 관한 연구," 한국통신학회논문지 '92-3 Vol.17, No.3, pp.206-211, 1992.4.
2. 임 환주, 이 민수, 이 만영 "다변수 다항식의 초증가성을 이용한 공개키 암호 시스템에 관한 연구,"

'91 KIISC Proceeding, pp.72-84, 1991.11.
3. 이 영노, 신 인철, "컴퓨터 통신의 안전을 위한 공개키 배낭 암호계 알고리즘," 한국통신학회논문지 '91-9 Vol.16, No.9, pp.894-900, 1991.9.
4. P.V.O'Neil, Advanced Engineering Mathmatics, 2-nd Edition, Wadsworth Publishing Co., Belmont, California, 1990.

權 蒼 英(Chang-Young Kwon) 正會員
1957년 4월 22일생
1983년 2월 : 성균관대학교 수학교육과 졸업(이학사)
1991년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학석사)
1991년 3월 ~ 현재 : 성균관대학교 대학원 정보공학과 박사과정 재학중
1982년 12월 ~ 1988년 9월 : (주)KOLON 정보 SYSTEM 실 팀장
1993년 3월 ~ 현재 : 대유공업전문대학 사무자동화과 전임강사
※주관심분야 : 암호이론, 정보이론, 정보관리

元 東 豪(Dong-Ho Won) 正會員
1949년 9월 23일생
1976년 2월 : 성균관대학교 전자공학과 졸업(공학사)
1978년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학석사)
1988년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학박사)
1978년 4월 ~ 1980년 3월 : 한국전자통신연구소 연구원
1985년 9월 ~ 1986년 8월 : 일본 동경 공대 객원연구원
1982년 3월 ~ 현재 : 성균관대학교 공과대학 정보공학과 교수
※주관심분야 : 암호이론, 정보이론

張 靑 龍(Chung-Ryong Jang) 正會員
1957년 5월 27일생
1980년 2월 : 성균관대학교 전자공학과 졸업(공학사)
1986년 8월 : 연세대학교 대학원 전자공학과 졸업(공학석사)
1979년 12월 ~ 1983년 12월 : 한국전자통신연구소 연구원
1984년 1월 ~ 현재 : 한국통신 연구개발단 선임연구원
※주관심분야 : 암호이론, 정보보호기술