韓國 OA學會 論文誌
第3卷 第2號, 1998. 6.

98-3-2-3-5

정수론에 근거한 확장 RSA 공개키 암호 방식에 관한 연구

류 재 관* 이 지 영**

A Study on the Extended RSA Public Key Cryptosystem Based on the Integral Number Theory

Jae-kwan Ryu* Jie-Young Lee**

요 약

본 논문은 기존의 RSA 공개키 암호방식을 확장한 확장 RSA공개키 암호 방식을 제안하였다. RSA 암호방식의 법 파라메타 p, q를 확장하여 승산 횟수를 증가시켰다. 그 결과 암호해독에 필요한 계산량이 증가되었고 정수론에 기초한 증명을 통하여 RSA 공개키 암호의 강도를 개선할 수 있었다.

Abstract

This paper proposes an extended RSA public-key cryptosystem which extends a conventional one.

The number of multiplication times has been increased by extending the modulus parameters p, q. This result shows the increase of computational complexity which required in cryptanalysis. It also improves the strength of RSA public key cryptosystem through this proof which is based on integral number theory.

* 세명대학교 컴퓨터과학과 강사

** 세명대학교 컴퓨터과학과 부교수

논문접수 : 98. 4.20 심사완료 : 98.5.27

Ⅰ. 서 론

최근 정보통신의 발달로 정보의 축적, 처리, 전송이 고도화 및 다양화되어 감에 따라 중요한 정보들은 보안을 요구하며 정보시스템 내에서의 정보 보호는 정보의 분실이나 불법도청 등으로부터 정보의 변형 또는 누출을 방지한다. 최근 각종 종합정보통신망, 전자우편, 데이터베이스 등에서 사용하는 고가의 정보를 불법 사용하는 등의 문제를 해결하고 비밀정보 등을 보호하기 위하여 암호화 기법을 사용하고 있다.[1~5]

암호기술은 키의 공개 유무에 따라 관용암호방식과 공개키 암호방식으로 나눌 수 있다. 관용암호방식은 암호화 및 복호화 키가 동일한 방식으로서 대표적인 것이 미국 상무성 표준국에서 암호를 정량적으로 표시할 수 있는 방법인 DES(Data Encryption Standard)이다.[1]

공개키 암호방식은 RSA암호방식[2], Rabin의 암호방식[3], Knapsack 문제를 이용한 M-H 암호계[4], 또한 선형오차 수정부호를 일반적으로 복호화하는데 문제의 어려움이 있는 것을 이용한 McEliece 암호계[5]등이 제안되고 있다. 특히 RSA 방식은 디지털 서명이 가능하고 계량적인 안전도가 뛰어나 최근에도 유망한 공개키 암호 방식이다.

RSA 방식은 각자가 암호화키에 대응하는 복호화키를 구하고 암호화키는 공개하고 복호화키는 비밀리에 보관한다. 제3자는 공개된 암호화키로 부터 복호화 키를 구하는 것이 불가능하지만 암호화키 작성자는 암호화키로 부터 복호화 키를 구할 수 있다. 이 방식은 법 파라메타(Modulus Parameter) n을 크게 하여 암호의 강도를 높이는데 n값이 너무 커지므로 소수의 분포가 적어져 사용자가 많을 경우 소수의 선택의 폭이 적어지고 처리속도가 늦어지는 단점이 있다. 본 논문에서는 기존의 RSA 방식을 확장한 RSA방식을 제안하였다.

RSA방식의 실제 응용 면에서 $n = p \cdot q$ 이므로 제한된 소수로 n을 구할 때 가입자가 선택해야 할 소수의 수가 제한되고 있으므로 n을 여러 개의 소수로 선택할 경우 가입자가 얻을 수 있는 n 값이 많아진다. 그러므로 파라메타 $p \cdot q$ (단 p와 q는 소수)를 확장하고 크기 조정이 가능한 n을 만족할 만하게 선택한 후 그 증명을 통해 파라메타 추출이 더욱 어렵도록 하였다. 결국 승산 횟수가 늘어나 암호해독에 요구되는 계산량이 증대되었으며 결과적으로 암호의 강도를 개선할 수 있었다.

Ⅱ. 공개키 암호시스템

암호방식에는 관용암호 방식과 공개키 암호 방식이 있다. 관용암호방식은 암호화 및 복호화키가 동일한 방식이며 키 배송문제의 어려움이 있다. 송신자는 암호문을 전달하기전에 난수열로부터 얻은 키 e를 비밀 통신을 원하는 특정수신자 Y에게 미리 전달한 후 그 다음 그 키를 사용하여 메시지를 암호문 C로 변환하여 수신자 Y에게 전달한다. 수신자 Y는 송신자로부터 받은 키를 사용하여 암호문 C를 복호화하여 메시지를 얻는다. 이와 같이 관용암호방식은 키를 미리 전달해야 하는 불편함과 어려움이 있다. 이것에 비해 공개키 암호방식은 키 배송이 불필요한 방식이다. 공개키 암호방식은 암호화 할 때 사용하는 키(공개키)와 복호화 할 때 사용하는 키(비밀키)를 다르게 작성하여 공개키는 공개하고 비밀키는 비밀로 간직하는 방식이다.

그림 2.1은 공개키 암호 시스템을 나타낸다.

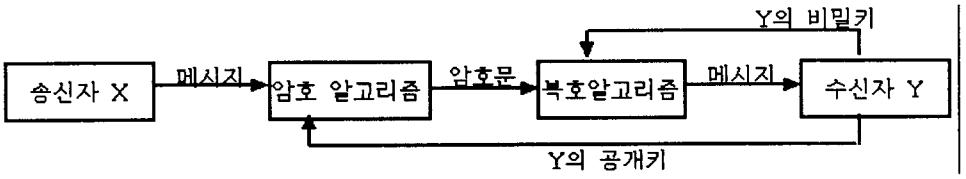

그림 2.1 공개키 암호 시스템
Fig 2.1 Public Key Cryptosystem

비밀통신을 하고자 하는 송신자 X가 메시지를 수신자 Y에게 보내고자 할 때 공개 파일에서 Y의 공개키를 사용하여 메시지를 암호화 하였다.

Y는 송신자 X에게서 온 암호문 C를 자신의 비밀키를 사용하여 복호화하여 메시지를 구한다. Y가 공개한 공개키를 가지고 Y에게 메시지를 암호화하여 보낼 수는 있지만 수신자 Y는 복호화키를 자신만이 비밀리에 보관하고 있기 때문에 Y 이외의 어느 누구도 암호문을 복호화하여 메시지를 얻을 수 없다.

Ⅲ. RSA 공개키 암호 시스템

3-1 RSA 암호방식의 기본원리[2]

i, k를 양의 정수로 하였을 때 i를 k로 나눈 나머지를 i mod k 로 표현하자. RSA 암호방식은 메시지 $M(0 \le M \le n-1)$에 대하여 암호문 $C = M^e \bmod n$을 대응시킨 암호법이다. 키를 만들기 위하여 우선 임의의 서로 다른 10100 정도의 크기의 큰 소수를 선택하고 그 두수의 곱을 법 파라메타 n이라 하자

그러면

$n = p * q$ (단 p, q 는 서로 소) (1)

그 다음 Euler 함수 값

$\phi(n)=(p-1)*(q-1)$ (2)

과 서로 소가 되는 Ke를 계산한다. 이때 Ke는 암호화키로

$L = LCM(p-1, q-1)$ (3)

$\phi(n)$의 최소공배수 값 L을 생성한다.

$Ke * Kd \equiv 1 \pmod{L}$, $(o<Ke, Kd \le L-1)$ (4)

에 의하여 Kd 값을 생성한다. 이때 Kd는 복호화키 이다.

즉, 암호화 및 복호화는 다음과 같다.

$C = MKe \pmod{n}$ (5)

$M = CKd \pmod{n}$ (6)

3-2. 확장 RSA암호 시스템

RSA암호방식의 확장은 기존의 RSA암호방식과 같이 극비의 데이터를 더욱 안전하게 전송하는데 그 목적이 있다. 즉 비밀통신에서 사용하는 키배송의 안전성을 고려하여 여러개의 소수를 사용하는 방법이다.

여러 가지 큰 소수의 곱에 기인한 법 파라메터 n은 커질수록 좋지만 큰 수의 소수는 제한되어 있으므로 소수의 개수가 늘어남에 따라 어려움도 증가하게 된다. 즉 기존의 RSA암호방식에서는 서로 소인 두 개의 큰 소수 p와 q를 임의로 선택하여 그 곱인 n값을 가능한 크게 하여 암호 강도를 높이는 방법을 사용하였다. 그러나 p, q값이 커지면 소수의 분포가 적어져 p, q값 선택의 폭이 좁아지고 암호 파라메터들의 크기가 커짐으로써 암호화 및 복호화의 처리 속도가 느려지는 단점이 있다. 즉 소인수분해의 어려움을 이용한 방식으로 이러한 암호 통신 방식은 어느것이나 RSA알고리즘에 따라서 행하여진다.

결국 암호 계산은 더욱 복잡하여지고 시간도 증가하게 된다. 또한 RSA암호 방식처럼 서로 소인 두 개의 큰 수의 곱과 크기가 비슷한 법파라메터 n을 가지고도 충분히 계산을 복잡하게 만드는 효과를 가져온다. 우선 법 파라메터 n을 8개의 소수 p, q, r, s, t, u, v, w의 곱이라 하자. 그러면 확장 RSA알고리즘의 방법 및 증명은 다음과 같다.

3-3. 확장 RSA 알고리즘의 방법 및 증명

법파라메터 $n=p \cdot q \cdot r \cdot s \cdot t \cdot u \cdot v \cdot w$(단, p, q, r, s, t, u, v, w는 서로소) (7)

이며 p, q, r, s, t, u, v, w는 소수이다.

또한

$L=LCM(p-1, q-1, r-1, s-1, t-1, u-1, v-1, w-1)$ (8)

$GCD(e, L) = 1$

$e * d \bmod L = 1$

여기서 $e * d = aL + 1$

$$= ab(p-1) + 1 \quad (9)$$
$$= ac(q-1) + 1 \quad (10)$$
$$= ad(r-1) + 1 \quad (11)$$
$$= ae(s-1) + 1 \quad (12)$$
$$= af(t-1) + 1 \quad (13)$$
$$= ag(u-1) + 1 \quad (14)$$
$$= ah(v-1) + 1 \quad (15)$$
$$= ai(w-1) + 1 \quad (16)$$

으로 쓸 수 있다. 따라서 다음식이 성립한다.

$$Cd = (Me)d = Me \cdot d \quad (17)$$

이 식 (17)에 식 (9)~(16)을 대입한다.

$Mab(p-1)+1 \bmod p = M$
$Mac(q-1)+1 \bmod q = M$
$Mad(r-1)+1 \bmod r = M$
$Mae(s-1)+1 \bmod s = M$
$Maf(t-1)+1 \bmod t = M$
$Mag(u-1)+1 \bmod u = M$
$Mah(v-1)+1 \bmod v = M$
$Mai(w-1)+1 \bmod w = M$

이므로 $Me \cdot d \equiv M \bmod n$ ($n = p \cdot q \cdot r \cdot s \cdot t \cdot u \cdot v \cdot w$)임을 알 수 있다. (증명 완료)

Ⅳ. 확장 RSA의 계산량

4-1. 복호화 과정 및 계산량 비교

기존의 RSA 방법에서 $M \equiv Cd \pmod n$을 직접 계산하지 않고 그대신 개선된 확장 RSA방법은 중국인의 잉여정리(Chinese remainder theorem)을 이용한다. 쌍마다 서로 소인 p,q,r,s,t,u,v,w에 대해 연립 방정식

$M1 \equiv Cd \pmod p$
$M2 \equiv Cd \pmod q$
⋮
$M8 \equiv Cd \pmod w$ 는

중국인의 잉여정리에 의해 메시지 M ($0 \le M < n$)이 일의적으로 구해진다.

간단한 예를 들어보자.

P=2, q=3, r=5, s=7, t=11, u=13, v=17, w=19이면

$n = p \cdot q \cdot r \cdot s \cdot t \cdot u \cdot v \cdot w$
$= 9699690$

$L = LCM(p-1, q-1, r-1, s-1, t-1, u-1, v-1, w-1)$
$= 720$

여기서 e 즉 Ke를 7, 메시지 $M(0 \le M < n) = 54321$이라 하면 암호문 C는

$C = (54321)7 \pmod{9699690}$
$= 9394911$

이 되며 $L = LCM(1, 2, 4, 6, 10, 12, 16, 18) = 720$으로부터 e 즉 Ke의 역수, 복호화키

Kd = 103을 얻을 수 있다.

즉 복호화알고리즘은

$M = (9394911)103 \pmod{9699690}$
$= 54321$

위의 증명에서 알 수 있는 바와 같이 각각의 법 파라메터를 사용하였을 때에도 마찬가지의 결과를 얻을 수 있다.

기존의 RSA방법을 사용하면 우선 M1, M2를 구한다. 서로 소인 p, q를 공통으로 2진 m비트라 하고 이것을 법으로 하는 승산을 2log2di회(di ≡ d (mod (p 또는 q-1))) 행하면 된다. di도 약 m비트와 견주어 보면 승산회수는 p, q에 대해 각각 2m회 된다. 동시에 4m회의 p, q를 법으로 하는 승산이 필요하다. 다음 M을 구한다.

중국인 잉여정리에 의해 식(15)를 구할수 있다.

$$M = M1P + M2Q \pmod{pq} \quad (15)$$

단 p, q는

$P \equiv 1 \pmod p$, $P \equiv 0 \pmod q$
$Q \equiv 1 \pmod q$, $Q \equiv 0 \pmod p$

를 만족한다.

위의 p, q에서

$P = Qp-1$
$Q = Pq-1$이다 (Fermat 정리)

이렇게 P, Q를 구해놓고 임의의 M1, M2(m 비트)에 P, Q(2m 비트)를 각각 곱해서 메시지 M을

구한다. 이때 승산 횟수는 2회이다. 확장된 RSA방법을 보면 우선 M1, M2, M3, M4, M5, M6, M7, M8을 구한다. 소수 p, q, r, s, t, u, v, w를 2진 m′ 비트라 하면 이 소수를 법으로 하는 승산은 16m′회 필요하다. 다음 M을 구한다. 이것 역시 기존의 RSA방법과 같이 평문 M이 구해지기 때문에 승산 횟수는 8회면 된다.(중국인 잉여정리이용)

$$M \equiv M1P + M2Q + M3R + M4S + M5T + M6U + M7V + M8W \pmod{p \cdot q \cdot r \cdot s \cdot t \cdot u \cdot v \cdot w}$$

즉,

$P \equiv 1 \pmod{p}$,
$P \equiv 0 \pmod{q, r, s, t, u, v, w}$

$Q \equiv 1 \pmod{q}$,
$Q \equiv 0 \pmod{p, r, s, t, u, v, w}$

$R \equiv 1 \pmod{r}$,
$R \equiv 0 \pmod{p, q, s, t, u, v, w}$

$S \equiv 1 \pmod{s}$,
$S \equiv 0 \pmod{p, q, r, t, u, v, w}$

$T \equiv 1 \pmod{t}$,
$T \equiv 0 \pmod{p, q, r, s, u, v, w}$

$U \equiv 1 \pmod{u}$,
$U \equiv 0 \pmod{p, q, r, s, t, v, w}$

$V \equiv 1 \pmod{v}$,
$V \equiv 0 \pmod{p, q, r, s, t, u, w}$
$W \equiv 1 \pmod{w}$,
$W \equiv 0 \pmod{p, q, r, s, t, u, v}$

표 1은 종래의 RSA방법과 확장된 RSA방법과의 승산회수를 비교한 것이다.

표 1. RSA방법과 확장된 RSA방법과의 승산회수 비교.
Table 1. A Comparison of the number of multiplication times between RSA and Extended RSA.

계산 / 방식	Mi 계산	M 계산
RSA	4m회 (p, q를 m 비트로 가정)	2회
확장 RSA	16m′회 (p, q, r, s, t, u, v, w를 m′비트로 가정)	8회

위의 과정에서 확장된 RSA 암호방식의 계산량이 훨씬 복잡하고 증대된 것을 알수 있다. 기존의 RSA방법과 확장 RSA방법의 계산량을 비교할 때 기존의 RSA방식에서 법 파라메터 p, q를 각각 2진 300비트 정도(약 10100)로 한다. 또한 확장 RSA방법에서 법 파라메터 p, q, r, s, t, u, v, w를 각각 2진 75비트 정도로 취한다. 그러면 n비트수를 공히 600비트로 해서 비교한다. 그 결과 $m : m' = 300 : 75$로 하면 확장 RSA의 계산량은 종래 RSA의 계산량의 $\frac{2}{8}$이면 족하다. 하지만 n이 두소수의 곱인 경우와 여러개의 소수의 곱일 경우 n의 비트수가 동일하다고 가정할 경우에는 인수분해가 용이해지나 각각의 소수의 크기가 같다고 가정할 경우에는 여러개의 소수의 곱인 n이 계산량이 훨씬 많아진다.

이 두 방식에서 각 법 파라메터의 비트수를 동일하게한 계산량은 RSA가 600비트이고 확장 RSA는 2400비트가 되어 계산량은 확장 RSA가 4배 많다. 또한 n비트 * n비트에서 n비트의 소수를 법으로하는 승산시간은 O(n)로 한다. 이것은 n 비트의 정수 승산 및 제산이 O(n)로 행해지는 것에 의한다.

실제 암호 해독을 위한 계산에 있어서 메시지의 길이를 n비트라하면 메시지의 종류는 2n으로 유한개의 수가 되기 때문에 메시지의 수가 적을 때 전부 메시지로 변환한 대응표를 만들면 간단히 해독가능 하지만 메시지의 길이가 100비트 정도면 메시지의 종류는 1033정도가 되므로 변환표를 만들려해도 사실상 불가능하다.

하지만 복호화 키를 알고 있는 수신자는 쉽게 암호문을 해독하여 메시지 M을 구할 수 있다.

V. 결 론

본 연구에서는 서로 다른 8개의 큰 소수를 사용하여 암호화키를 구하는데 더욱 복잡한 과정을 거쳐야함을 알 수 있었다. 결국 암호해독을 위한 계산량의 증가로 말미암아 해독의 강도를 개선할 수 있음을 알았다. 또한 n과 e 자체만으로 확장 RSA 암호문을 해독하는 것은 n을 소인수 분해하는것과 같은 정도로 난해하며 n의 행수가 아주 클 때 n을 소인수 분해하는 것은 현재 알려져 있는 것 중 가장 우수한 알고리즘을 사용하여도 계산량이 엄청나다.

또한 이 확장 RSA방법은 법 파라메터 n이 몇 개

의 소수의 곱인가를 알 수 없다. n이 10200정도의 수라면 이 확장된 암호문을 해독하려면 고속의 새로운 알고리즘이 개발되어야 할 것이다.

References

[1] Data Encryption Standard, Federal Information Processing Standard (FIPS) publication 46, National Bureau of Standards, U.S.Department of Commerce, Washington, DC · Jan.1977

[2] R.V.Rivest, A. Shamir and L. Adleman : "A method for Obtaining Digital Signatures and Public Key Cryptosystem." Comm.ACM, 21, 2, pp. 120-126. 1978

[3] M.O.Rabin, "Probabilistic algorithms", In J.F. Tran, Ed., Algorithms and Complexity, Academic Press, New York, pp. 21-40. 1976

[4] R.C.Merkle and M.E.Hellman, "Hiding information and signatures in trapdoor Knapsacks," IEEE Trans Inform. Theory. vol. IT-24, pp. 524-530, Sept. 1978

[5] R.J.McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory", Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, DSN Progress Report, pp. 42-44, pp. 144-116, Jan-Feb. 1978

[6] 高木貞治, "初等整數論 講義第 2版." 共立出版, 昭和 60年

[7] 一松信, "暗號の 數理" pp. 126-144. 講談社

[8] W.Diffie and M.Hellman, "New directions in cryptography", IEEE Trans. Inform. Theory, vol. IT-22, pp. 644-656, 1976

[9] C.H Meyer and S.M.Matyas. "Cryptography : A new dimension in computer data security", John Wiley & Sons, 1982.

[10] 한국전자통신연구소편저, "현대암호학", pp. 1-156, 1982.

[11] 이만영, "공개키 암호 시스템에 관한 연구 (2)", 한국통신정보 보호학회지, vol. 1, no.2, pp 63-75, Aug, 1991.

[12] 류재관, "확장 RSA 공개키 암호시스템에 관한 연구", 세명대학교 대학원 석사학위 논문, 1998

● 저자소개

류 재 관

1992년 ~ 1996년 : 세명대학교 전자계산과 (공학사)
1996년 ~ 1998년 : 세명대학교 전산정보대학원 (공학석사)
1998년 ~ 현재 : 세명대학교 컴퓨터과학과 강사

이 지 영

1988년 : 성균관대학원 전자공학과 (공학박사)
1988년 ~ 1992년 : 해군사관학교 전자공학과 부교수
1992년 ~ 현재 : 세명대학교 컴퓨터과학과 부교수
관심분야 : 정보이론, 암호이론, 고속연산알고리즘