韓國 OA學會 論文誌
第3卷 第2號, 1998. 6.

98-3-2-3-4

공개키 암호 시스템의 순수 마스터키에 관한 연구

이 지 영*

A Study on the Pure Master Key for the Public Key Cryptosystem

Jie-Young Lee*

요 약

본 논문은 다중 암호시스템에서 공용으로 사용 가능한 순수 마스터 키를 제안한다. 또한 이 연구는 Fermat 정리와 마스터 키 알고리즘을 사용한 RSA 공개키 암호계에 대한 마스터 키 조건을 제안한다.

Abstract

This paper proposes pure master key which can be commonly used in multi-cryptographic system. It also refer to master key condition for RSA public key cryptosystem using Fermat's theorem and master key algorithm as well.

---

* 세명대학교 컴퓨터과학과 부교수

논문접수 : 98. 4.13 심사완료 : 98.5.22

Ⅰ. 서 론

최근 컴퓨터와 통신의 발달로 말미암아 정보화 사회가 급속히 도래하고 있는 가운데 정보 통신의 역할은 필수 불가결한 것이라 할 수 있다. 이에 따라서 어떤 파일이나 정보를 통신할 때 제 3자가 불법추출내지는 개입을 방지하는 것이 중요하다. 이 때문에 기밀 보호와 그 정보의 신뢰성을 보증하는 방법으로 암호 방식이 널리 쓰이고 있다.[1,2] 특히 공개키 암호 방식에서는 암호화키는 공개하지만 복호화 키는 비밀로 간직하여야 하므로 키 관리의 연구도 활발히 진행되고 있다.[3] 고로 복수 개의 개별키에 공통으로 대체할 수 있는 마스터키의 존재는 매우 중요하다. 마스터키는 일원적 관리의 조직에서 신뢰할 수 있는 마스터 키 관리자가 각 개별 키를 사용하지 않고도 빨리 키입력이 되고, 개별 키의 파괴 및 분실에 대해 신뢰성이 있으며 키 관리 용량이 작은 장점이 있다. 이 마스터키를 순수 마스터키라 한다. 현재 암호화 분야에서의 마스터키는 안전성을 높이는데 목적이 있으며 개별키 암호화용의 마스터키이며 위의 순수 마스터키와는 다르다. 순수 마스터키는 개별 키의 요철 관계의 논리화에 의해 합성시킬 수 있다.

본 논문에서는 순수 마스터키(이하 그냥 마스터키라고 부른다)를 새롭게 제안하고 그 존재 조건과 도출법 및 그 적용성을 밝히고 암호 시스템으로서 유망한 RSA 공개키 암호법을 마스터키의 검토 대상으로 한다.[1,4]

Ⅱ. 암호 시스템의 마스터 키 존재 조건

암호 시스템에서의 마스터 키 존재 조건은 우선 암호관수 E, 복호관수 D를 갖는 암호 시스템을 가정하고 m개의 개별 키에 대한 마스터키를 검토한다. 암호화 개별 키를 kei(i= 1, ……, m), 복호화 개별 키를 kdi(i=1, ……, m)라 하고 암호화 마스터키를 keM, 복호화 마스터키를 kdM라 한다.

마스터키의 존재 조건은 다음 (i), (ii), (iii)의 조건을 만족하는 것으로 한다.

(i) m개의 모든 kei와 모든 평문 p에 대응하고

EkeM(p)=Ekei(p) (2-1)이 성립한다.

(ii) m개의 모든 kdi와 모든 암호문 C에 대응하고

DkdM(C)=Dkdi(C) (2-2)이 성립한다.

(iii) keM, kdM, kei, kdi 키의 크기(bit 수)를 각각 |keM|, |kdM|, |kei|, |kdi|로 하면 다음의 식을 만족하는 keM, kdM이 존재한다.

$$|K_{eM}| < \sum_{i=1}^{m} |K_{ei}|$$

$$|K_{dM}| < \sum_{i=1}^{m} |K_{di}|$$

위의 (i),(ii)는 어떤 평문(암호문)에 대해서도 임의의 암호화 개별키(복호화 개별키)에 의한 암호화(복호화)의 결과와 마스터키에 의한 암호화(복호화)의 결과가 일치하는 기능적인 조건이다.

(iii)은 마스터키의 크기가 모든 개별 키의 크기의 합계보다 작은 것을 나타내는 성능 조건을 나타낸다. 즉, 개별키 전체의 시스템을 유지하는 것보다 마스터키를 사용하는 것이 기억용량을 절약할 수 있다는 것을 의미한다. 위의 조건은 비대칭 암호계인 공개키 암호계 형태이며, DES와 같이 대칭 암호계인 관용 암호 방식에서는 암호화키와 복호화키가 동일하며 (i)과 (ii)의 조건을 하나로 줄일 수 있다.[4]

Ⅲ. RSA 암호 방식의 기본 원리

RSA 암호 방식은 임의의 상이한 2개의 큰 소수 p_i , q_i를 선택하고 $n_i = p_i \cdot q_i$를 계산한다. 그 다음 $((p_i-1),(q_i-1))$과 서로 소이며 그것보다 작은 임의의 정수 Kei를 선택한다. 그리고

$L_i = LCM(p_i-1, q_i-1)$이며

$Kei \cdot Kdi \equiv 1 (\bmod Li)$를 계산하고 Kdi를 구한다. Kei와 Kdi의 관계는

$Kei \cdot Kdi \equiv 1 (\bmod \phi(n_i)(=(p_i-1)(q_i-1)))$

이다.

RSA 암호 방식은 계산적 안전도가 높고 디지털 서명에 의한 인증이 가능하며 개인키의 배포가 용이하므로 마스터키의 존재 조건과 적용성을 검토 대상으로 한다.[1]

사용자가 공개화일에 등록한 암호화키 Kei는 (Kei, n_i)의 조합이며 대응하는 복호화키 Kdi는 (Kdi, n_i)의 조합이고, Kdi는 사용자 i만이 알 수 있다. 암호화 및 복호화 알고리즘은 다음과 같다.

$$C = E_{Kei}(P) = P^{Kei} (\mathrm{mod}\ n_i) \quad (3\text{-}1)$$

$$P = D_{Kei}(C) = C^{Kdi} (\mathrm{mod}\ n_i) \quad (3\text{-}2)$$

로 표현하며 P와 C는 0에서 $n_i - 1$사이의 정수이다.

$Kei \cdot Kdi \equiv 1 (\mathrm{mod}\ Li)$는

$M^{Kei\ Kdi} \equiv M (\mathrm{mod}\ n_i)$이 성립하기 위한 필요 충분조건이고

$Kei \cdot Kdi \equiv 1 (\mathrm{mod}\ \phi(n_i) (= (p_i - 1)(q_i - 1)))$

이 성립하기 위한 충분조건이다.

$M^{Kei \cdot Kdi} \equiv M (\mathrm{mod}\ n_i)$를 만족하는 $Kei \cdot Kdi$를 구한다.

$x_i = Kei \cdot Kdi - 1$로 놓으면,

$M^{Kei \cdot Kdi} \equiv M (\mathrm{mod}\ n_i)$는

$M(M^{x_i} - 1) \equiv 0 (\mathrm{mod}\ n_i)$으로 표현된다.

여기서 $M(M^{x_i} - 1) \equiv 0 \pmod{p_i}$

$M(M^{x_i} - 1) \equiv 0 \pmod{q_i}$ 인

두식과 비교하면 이 두식을 만족하고 동치가 되며 위의 식의 해는 각각

$x_i \equiv 0 \pmod{(p_i - 1)}$

$x_i \equiv 0 \pmod{(q_i - 1)}$

이 되며 이 두식을 동시에 만족하는 x_i의 필요 충분 조건

$x_i \equiv 0 \pmod{LCM(p_i - 1)(q_i - 1)}$이 되고

충분조건은 $x_i \equiv 0 \pmod{(p_i - 1)(q_i - 1)}$이 된다.

IV. RSA법의 순수 마스터키 존재 조건

순수 마스터키가 존재하는 기능적 조건은 식(2-1), (3-1), (3-2)식에 의하고, 모든 i, p, c에 대하여

$$p^{K_{eM}} \equiv p^{Kei} \pmod{n_i}$$

$$c^{K_{dM}} \equiv c^{Kdi} \pmod{n_i}$$

이 성립한다. 암호화와 복호화 관수는 n_i를 법으로 해서 어떤 정수를 멱승하는 의미로 同形이고 암호화키와 복호화키의 마스터키 조건은 전부 독립된 同様으로 볼 수 있다. 또한 Kei와 Kdi, KeM, KdM은 각각 Ki, KM으로 표시한다. 그러면, 위 식은

$$M^{K_M} \equiv M^{K_i} \pmod{n_i} \quad (1 \le i \le m) \quad (4\text{-}1)$$

$0 \le M \le n_i - 1$으로 표시된다.

식(4-1)을 보면 $n_i = p_i \cdot q_i$에서 p_i와 q_i는 서로 소이므로

$$M^{K_M} \equiv M^{K_i} \pmod{p_i} \quad (4\text{-}2)$$

$$M^{K_M} \equiv M^{K_i} \pmod{q_i} \quad (4\text{-}3)$$

이다. 0에서 $n_i - 1$까지의 정수를 요소로 하는 메시지 M의 집합을 p_i와 서로 소인 정수 집합 M(1), q_i와 서로 소인 정수 집합 M(2), M(1)과 M(2)의 적집합 M(3), M(1)과 M(2)의 和집합에 대한 M의 補집합 M(4)로 나눈다. 이때 M(4)는 0만을 요소로 갖는다.

이들 관계는

$$M = M^{(1)} \cup M^{(2)} \cup M^{(4)}$$

$$M^{(3)} = M^{(1)} \cap M^{(2)}$$

이 된다.

M(1)과 M(2)를 기본으로 식(4-1)이 성립하는 조건을 도입한다.

(i) $M \in M^{(1)}$ 일 때

p_i와 M이 서로 소, 즉 p와 M의 최대공약수가

1(GCD(M, p_i) = 1)일 때 식(4-2)은

$$M^{K_M - K_i} \equiv 1 (\mathrm{mod}\ p_i) \quad (4\text{-}4)$$

로 변형 가능하다. 지금

$$f_i = K_M - K_i$$

$$M^{f_i} \equiv 1 (\mathrm{mod}\ p_i) \quad (4\text{-}5)$$

로 놓자. M(1)의 요소는 $M_1^{(1)}, M_2^{(1)}$, ……, $M_K^{(1)}, M^{(1)}$(pi-1)qi와 첨자를 사용하여 구별한다. $M_K^{(1)}$일 때 식(4-5)을 만족하는 f_i의 최소 양의 정수를 $f_{k,i}$로 나타낸다. 모든 k에 대한 식(4-2)가 성립하는 조건은 연립방정식

$$K_M \equiv K_i \ (\mathrm{mod}\ f_{k,i}) \quad (4\text{-}6)$$

$$1 \le k \le (p_i - 1)q_i$$

이 성립하는 것이다.

식(4-6)이 모든 k에 대하여 성립하는 필요 충분 조건은 다음 식으로 표현할 수 있다.

$$z9K_M \equiv K_i \ (\mathrm{mod}\ LCM(f_{1,i},\ldots,f(\mathrm{pi-1})\mathrm{qi},i)) \quad (4\text{-}7)$$

Fermat 정리에 의해 식(4-5)는 $f_i = p_i - 1$로 성립한다.[6,7,8,9] 고로 각 $f_{k,i}$는 $p_i - 1$과 같거나 혹은 $p_i - 1$의 약수이다.

하지만 $f_{k,i}$는 $M_k^{(1)}$의 법 p_i에 관한 지수라 불려지고, 특히 소수 p_i를 법으로 하는 지수 $f_{k,i}$ $(1 \le k \le (p_i - 1)q_i)$중

$f_{k,i} = p_i - 1$이 되는 원시근 $\overline{M^{(1)}} \in M^{(1)}$이 반드시 존재하는 것이 증명되고 있다. 따라서

$$LCM(f_1, i, f_2, i, \ldots, f(\mathrm{pi-1})\mathrm{qi},i)) = p_i - 1 \quad (4\text{-}8)$$

이 된다. 따라서 $GCD(M, p_i) = 1$일 때 식(4-2)가 성립하는 조건은

$$K_M \equiv K_i \ (\mathrm{mod}\ (q_i - 1)) \quad (4\text{-}9)$$

이 된다. 위의 식(2-1),(2-2)에 따라 메시지 공간을 다음의 경우로 분류하여 마스터키 조건을 유도한다.

첫째, $M \in M^{(3)}$일 때

$GCD(M, p_i) = 1$ 단 $GCD(M, p_i) = 1$의 경우이다.

식(4-2)의 해 식 (4-6)과 식(4-3)의 해 식(4-6)을 동시에 만족하는 조건은

$$K_M \equiv K_i \ (\mathrm{mod}\ L_i) \quad (4\text{-}10)$$

으로 표시한다.

둘째, $M \in M^{(1)} - M^{(3)}$일 때

$GCD(M, p_i) = 1$ 단 $GCD(M, q_i) \neq 1$의 경우이다.

$GCD(M, q_i) \neq 1$에 의해 $M = sq_i$(s는정수)로 된다.

$K_M \neq 0, K_i \neq 0$ 이므로 식(4-3)은 항등적으로

$$M^{K_M} \equiv M^{K_i} \equiv 0 \ (\mathrm{mod}\ q_i)$$

이 되어 어떠한 K_M과 K_i에 있어서도 식(4-3)은 성립한다.

그러므로 식(4-2)와 (4-3)을 동시에 만족하는 해는

$$K_M \equiv K_i \ (\mathrm{mod}\ (p_i - 1)) \quad (4\text{-}11)$$

로 표현한다.

셋째, $M \in M^{(2)} - M^{(3)}$일 때

$GCD(M, p_i) \neq 1$ 단 $GCD(M, q_i) = 1$의 경우이다.

두 번째와 同樣으로써 식(4-2)와 (4-3)을 동시에 만족하는 식으로

$$K_M \equiv K_i \ (\mathrm{mod}\ (q_i - 1)) \quad (4\text{-}12)$$

이다.

넷째, $M \in M^{(4)}$일 때

$M = 0$의 경우이다. $K_M \neq 0$, $K_i \neq 0$가 되기 때문에

$$M^{K_M} \equiv M^{K_i} \equiv 0 \ (\mathrm{mod}\ p_i)$$

$M^{K_M} \equiv M^{K_i} \equiv 0 \pmod{q_i}$

가 된다. 이상에서 보면 개별키 K_i와 n_i에 관한 메시지 공간 전체에 대해서 마스터키가 존재하는 필요 충분조건은

$$K_M \equiv K_i \pmod{L_i} \tag{4-13}$$

이 된다. 따라서 m개의 개별키 K_i $(i=1, \ldots, m)$에 대하여 마스터키가 존재하는 필요 충분조건은 $i=1, \ldots, m$에 대한 식(4-13)의 연립 합동식을 만족하는 K_M, K_i가 존재하는 것이다. 식(4-3)의 임의의 두 식에 의해 K_M을 소거하면 1부터 m까지 상이하게 되는 정수 i, j로 대하고 mC_2개의 식이 유도된다.

즉, $$L_i \cdot l_i - L_j l_j = K_j - K_i \tag{4-14}$$

단 l_i, l_j는 정수이다.

m개의 개별키 K_i와 소수 p_i, q_i에 의해 유도되는 L_i가 이미 주어져 있는 경우 식(4-14)의 미지수는 l_i와 l_j가 된다. 순수 마스터키의 존재 조건은 mC_2개의 2원1차 부정방정식(4-14)가 정수해 l_i, l_j를 갖는 조건이 되고 그 조건은 정수론의 기본 정리에 의해 $K_j - K_i$가 L_i와 L_j의 최대공약수로 나누어 떨어진다 라는 것이다.

이상을 종합하면 m개의 개별키 K_i에 대한 마스터키 K_M이 어떤 평문이나 암호문에 대해서도 존재하는 필요 충분조건은

$$K_i \equiv K_j \pmod{GCD(L_i, L_j)} \tag{4-15}$$

$(i \neq j,\ 1 \leq i,\ j \leq m)$

이 성립하는 것이다. 따라서 K_M가 존재한다면 K_M는 $LCM(L_1, L_2, \ldots, L_M)$을 법으로 단지 1개 존재한다.

이상에서 순수 마스터키가 존재하는 조건을 암호화키와 복호화 키로써 독립적으로 구해 보았다.

즉, $g_{ij} = GCD(L_i, L_j)$

로 놓으면 암호화키의 존재 조건은

$K_{ei} \equiv K_{ej} \pmod{g_{ij}}$

가 성립하는 것이고 복호화키의 조건은

$K_{di} \equiv K_{dj} \pmod{g_{ij}}$

이 성립하는 것이다.

그런데 RSA 법으로는 $Kei \cdot K_{di} \equiv 1 \pmod{L_i}$로 나타난 방법으로 암호화키와 복호화키 에서는 관계가 있다. 그러므로 어느 것이나 보통의 마스터키의 존재 조건이 만족되는 경우에, 보통의 마스터키에 대한 존재 조건도 동시에 만족함을 검토한다.

우선 암호화 마스터키 K_{eM}이 존재하는 경우에 복호화 마스터키 K_{dM}도 존재하며 그 역도 성립한다. 그러므로

$K_{eM} \cdot K_{dM} \equiv 1 \pmod{L}$

이 된다. 단 $L = LCM(L_1, L_2, \ldots, L_m)$

V. 순수 마스터키의 도출 알고리즘

IV절의 순수 마스터키 존재 조건을 만족하는 개별키가 주어진 경우에 순수 마스터키의 도출 알고리즘을 살펴보면 암호화키와 복호화 키는 도출 알고리즘이 同樣이므로 개별키를 K_i $(1 \leq i \leq m)$, m개의 개별키에 대한 마스터키를 K_M으로 표시한다.

K_M의 도출은 $K_M \equiv K_i \pmod{L_i}$의 연립 합동식을 푸는 것에 대응한다. 편의상 1부터 i번째까지의 개별 키에 대한 순수 마스터키를 $\overline{K}_{M,i}$로 표시한다.

이때 $\overline{K}_{M,1} = K_1$, $\overline{K}_{M,m} = K_M$이 된다.

일반적으로 $\overline{K}_{M(i-1)}$에서 $\overline{K}_{M,i}$를 구하는 알고리즘의 구조 원리를 보면 $i=2, \ldots, m$일 때

$$\overline{K}_{M,i} \equiv K_{M,(i-1)} \pmod{\overline{L}_{i-1}} \tag{5-1}$$

$$\overline{K}_{M,i} \equiv K_i \pmod{L_i} \tag{5-2}$$

이 성립한다. 단

$\overline{L}_i = LCM(L_1, L_2, \ldots, L_i)$, $i \geq 2$, $\overline{L}_1 = L_1$

이다.

식(5-1), (5-2)에서 $\overline{K}_{M,i}$를 소거하면

$$\bar{l}_{i-1} \cdot \overline{L}_{i-1} - \bar{l}_i \cdot L_i = K_i - \overline{K}_{M,(i-1)}$$

를 얻는다. 단 $\bar{l}_{i-1}, l_i$는 정수이다. 여기서 L_{i-1}, $\overline{L}_i, K_i$, $\overline{K}_{M,(i-1)}$은 이미 알고 있으므로 $\bar{l}_{i-1}, l_i$에 관한 2원 1차 부정 방정식이 된다. 이 방법을 유크리드의 호제법등을 사용하여 $\bar{l}_{i-1}$ 또는 l_i를 구하면 $\overline{K}_{M,i}$ 가 구해진다. $\overline{K}_{M,i}$로부터 $\overline{K}_{M,m}$까지 순차적으로 해석하면 K_M이 구해진다.

이 알고리즘은 다음과 같다.

input { m, K_i, p_i, q_i, $(i=1, \ldots, m)$ }
for $i=1$ *step* 1 *until* m
begin
Li = {least common multiple of
$((p_i-1),(q_i-1))$}
end
$\overline{K}_{M,1} = K_1$
for $i=1$ *step* 1 *until* $m-1$
begin
$\overline{L}_i$ = { least common multiple of
$(L_1, L_2, \ldots L_i)$ }
$\bar{l}_i, l_{i+1}$ ←{solve an indeterminate equation :
$\bar{l}_i \cdot \overline{L}_i - l_{i+1} \cdot L_{i+1} = K_{i+1} - \overline{K}_{M,i}$ }
$\overline{K}_{M,(i+1)} \leftarrow K_{i+1} + l_{i+1} \cdot L_{i+1}$
end
$K_M = \overline{K}_{M,m}$
output K_M

VI. 결 론

본 논문에서는 일반적인 마스터키의 존재 조건과 RSA법의 순수 마스터키의 존재 조건과 마스터키의 도출 알고리즘을 새롭게 제안하였으며 암호화 개별 키와 복호화 마스터 키, 암호화 마스터키와 복호화 개별 키, 암호화 마스터키와 복호화 마스터키의 모든 조합이 가능함을 보였다. 향후 각 개별 키의 생성자, 비밀 정보의 소유자, 마스터키의 설정치 등을 다르게 함으로써 비밀키의 안전성이 어떻게 달라지는가와 마스터키의 크기에 따라서 암호 속도가 어떻게 되는가 등의 연구가 진행되어야 할 것이다.

References

[1] Rivest, R.L., Shamir, A. and Adleman, L., " A method for obtaining digital signature and public key cryptosystem ", Comm.ACM, 21, 2 .pp.120-126, 1978

[2] Rivest, R.L., " A description of a single chip cryptosystem ", National Telecom.Conf.(NTC), 3~4, 49, 2.1, 1980

[3] Matyas, S.M. and Meyer,C.H, " Generation, distribution and installation of cryptographic keys ", IBM Sys.J., 17, 2, pp.126-137, 1978

[4] Meyer C.H and Matyas, S.M, " Cryptography :A new dimension in computer data security", 1982

[5] Popek, G.J. and Kline, C.S, " Encryption and secure computer network ", ACM Computing Surveys, 11, 4, pp.331-356, 1979

[6] 宮口, 水田, 古家, 水田, "暗號處理用 合同式 演算 回路", 第22回 情報處理學會全大, pp.141-142, 昭56.

[7] 高木貞治, " 初等 整數論 講義 " , 共立出版, 1971

[8] 廣瀨建 , " 情報數學 ", 昭和 60

[9] 金應泰, 朴勝安, " 整數論 "

[10] 金應泰, 朴勝安, " 現代 代數學", 1985

● 저자소개

이 지 영

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