論文 84-21-3-6

MH 公開키 시스템의 Master Key

(A Master Key for MH Public Key Cryptosystem)

高 崙 碩*, 崔 炳 旭**

(Yun Seok Ko and Byung Uk Choi)

要 約

本 論文에서는, 複數의 使用者가 MH 公開키 시스템을 利用하는 경우, 複數의 個別키에 共通으로 摘用할 수 있는 마스터키를 새로이 提案하여 誘導하였다. 이러한 마스터키를 시스템內에 導入하면 個別키의 크기의 總和보다 작은 마스터키를 選擇하여 記憶容量을 節約시킬 수 있고, 디지탈署名에 依한 認證이 용이해진다. 또 RSA 公開키 시스템과 비교해 볼 때, 마스터키를 使用하더라도 個別키를 使用할 때에 比해서 處理時間에 큰 影響이 없음을 컴퓨터 시뮬레이션에 依해 立證하였다.

Abstract

The master key on the multiuser MH public key cryptosystem, can be substituted for multiple private keys, is proposed and derived.

Applying it to public key cryptosystem, it can be possible to save memory size by selecting the master key and easy to authenticate the truth of message and the identity of the sender. Using this master key, it is proved that the encryption time ratio of MH method is smaller than that of RSA's method.

Ⅰ. 序 論

最近 컴퓨터를 通한 情報處理가 社會的으로 急增하고 컴퓨터의 大量普及으로 因하여 데이타通信과 事務自動化 等이 發展함에 따라서 通信과 file의 情報에 對한 盜聽과 捏造를 防止하는 일이 重要하게 되었다. 資料의 保護와 신빙성을 보장하는 手段으로 컴퓨터를 利用한 Cryptosystem이 硏究되고 있으며,[10] 특히 키管理가 용이한 Public Key Cryptosystem(이하 PKS 로 표기)에 對한 硏究가 活潑히 進行되고 있다.[1][2][3] 最近의 cryptosystem은 알고리즘 自體는 公開되어 있고 키에 依하여 安全性이 左右되므로 키의 管理를 爲한 protocol이 必要하다.[4] PKS에서도 復號化키는 保護되어야 하므로 키의 管理法의 重要性에 對한 認識이 높아졌고 키管理法에 關한 硏究가 活潑히 進行되고 있다.[5][6] 만약 키가 適切한 方法으로 保護될 수 없다면 시스템의 安全性은 維持될 수 없다. 結果的으로 cryptographic algorithm의 有用性은 그것의 節次에 使用되는 키의 管理技術에 크게 依存한다. 本 論文에서는 PKS의 한 方法인 MH法[2]의 새로운 키管理法으로서 多數의 個別키에 共通으로 代置할 수 있는 마스터키를 誘導하고, 마스터키의 管理者를 通해서 digital signature에 依한 認證이 可能함을 보인다. 또 마스터키를 使用하더라도 RSA法[4]과는 달리 encryption(decryption)時間에 큰 影響이 없음을 computer simulation에 依해 立證한다.

*準會員, **正會員, 漢陽大學校 電子通信工學科

(Dept. of Electron. Telecommunication, Han Yang Univ.)

接受日字 : 1984年 1月 20日

Ⅱ. MH Algorithm

PKS의 槪念을 提案한 Merkle과 Hellman은 Knapsack function이라는 單方向性函數(one way function

를 利用한 algorithm을 發表하였다.[2] Knapsack function이란 무게가 각각 $a_1, a_2, \cdots, a_n$ 인 물건의 集合과 定量이 S인 knapsack이 있을 때, 適當한 물건을 選擇하여 그 總合이 正確하게 S가 되도록 하는 古典的인 問題이다. 여기서 물건의 集合을 n元 벡터 $\vec{a}$로 하고, 해당하는 물건의 存在有無를 2進 n元 벡터 $\vec{X}$라 하여

$$\vec{a} = (a_1, a_2, \cdots\cdots, a_n)$$
$$\vec{X} = (x_1, x_2, \cdots\cdots x_n)$$

으로 하면 S는 式(1)과 같다.

$$S = \vec{a} * \vec{X} = \sum_{i=1}^{n} a_i * x_i \qquad (1)$$

여기서 x_i는 0또는 1이고, $\vec{a}$를 이미 알려진 값이라 하면 S는 結果的으로 單方向性函數가 된다. 즉 x_i가 주어졌을 때 S는 간단히 구해지나, n이 큰 境遇 S로부터 x_i를 誘導하는 것은 NP完全問題로 至極히 어렵다.[1] 따라서 $\vec{a}$를 使用者의 public key로 公開하고 $\vec{X}$를 plain text로 하면 S는 結果的으로 ciphertext가 된다. 이 ciphertext에서 plaintext x_i를 解讀하는 것은 knapsack問題를 푸는 것으로 n이 커지면 事實上 計算이 不可能해진다. 그러나, 復號化키를 알고 있으면 n回의 計算으로 簡單하게 平文을 구할 수 있다. S로부터 平文 x_i를 구해내는 復號化過程은 아래와 같다. 復號化키 w^{-1}는 m을 利用하여 구한다. 여기서 w는 m보다 작고 m과 서로 소인 큰 임의의 양의 整數이다.

$$w * w^{-1} = 1 \pmod{m} \qquad (2)$$

w^{-1}을 구한 후 다음과 같이 knapsack 問題를 誘導한다.

$$\vec{a}' = \vec{a} * w^{-1} \pmod{m} \qquad (3)$$

$$S' = S * w^{-1} \pmod{m}$$
$$= \sum_{i=1}^{n} a_i * x_i * w^{-1} \pmod{m}$$
$$= \sum_{i=1}^{n} a_i' * w * x^1 * w^{-1} \pmod{m}$$
$$= \sum_{i=1}^{n} a_i' * x_i \pmod{m} \qquad (4)$$

(4)식으로부터 plaintext x_i를 구하는 過程은 아래와 같다.

```
Procedure decryption MH;
BEGIN.
  IF S'≥a'n THEN xn : = 1
  ELSE xn : =0
  FOR j : =n−1 DOWN TO 1 DO
  IF S'≥ Σ_{i=j+1}^{n} ai' *xi+a'j THENxj : = 1
  ELSE xj : = 0
END;
```

MH法에서 注意해야 할 點은 knapsack vector $\vec{a}'$는 $a'_1 < a'_2$, $a'_1 + a'_2 < a'_3$, ……, $a'_3 + a'_2 + \cdots\cdots + a'_{n-1} < a_n'$를 만족해야하고 m은 $m > w$, $m > \sum_{i=1}^{n} a_i$가 되도록 選擇해야 한다. 즉 $\vec{a}'$를 選擇한 後 (3)式을 利用하여 trapdoor knapsack vector $\vec{a}$를 구하여 公開한다.

Ⅲ. PKS에서의 마스터키

Conventional Crypto System(이하, C·C·S로 表記) PKS에서는 키의 保護 및 管理를 爲해서 마스터키를 導入할 수 있다. 그러나 두 시스템에서 사용되는 마스터키의 意味는 서로 다르다. 즉 CCS에서는 마스터키가 데이타암호화키를 다시 暗號化하여 保護하기 爲한 것이고,[4] PKS에서의 마스터키는 複數의 個別키에 共通으로 適用할 수 있도록 導出되어서, 複數의 個別키를 마스터키의 管理者가 一元的으로 管理할 수 있도록 만든 것[5]으로 그 意味는 完全히 區別되어야 한다. PKS에서의 마스터키와 個別키와의 關係는 그림 1과 같이 圖示된다.

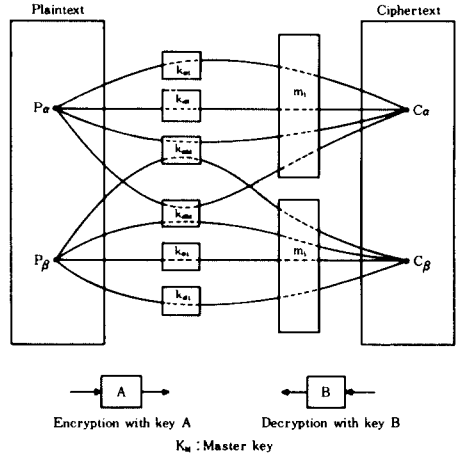

그림 1. PKS에서의 master key와 개별 key와의 관계
Fig. 1. Relation of master key with private keys in PKS.

PKS에서 user i의 encryption키를 K_{ei}, 그에 대한 마스터키를 K_{em}이라 하고, decryption키를 K_{di}, 그에 대한 마스터키를 K_{dM}이라 하면 마스터키의 存在條件은 다음 (5), (6), (7)式과 같다.[5]

i) j個의 모든 K_{ej}와 모든 plaintext P에 對해서
$$E_{keM}(p) = E_{kej}(p) \pmod{m_i} \qquad (5)$$

ii) j個의 모든 K_{dj}와 모든 ciphertext C에 對해서
$$D_{K\,dM}(C) = D_{Kdj}(c) \pmod{m_i} \qquad (6)$$

iii) 각 키의 크기를 絶對値로 表示하면

$$\left.\begin{array}{l} |K_{eM}| < \sum_{i=1}^{j} |K_{ei}| \\ |K_{dM}| < \sum_{i=1}^{j} |K_{di}| \end{array}\right\} \quad (7)$$

이다. (5)式과 (6)式에서 E와 D는 encryption과 decryption을 意味한다. 또 (7)式은 마스터키의 크기가 모든 個別키의 크기의 總和보다 작아야하는 性能條件을 나타낸다 즉 마스터키를 所有하는 쪽이 記憶容量을 節約시킬 수 있음을 意味한다.

Ⅳ. MH法의 마스터키

1. MH法의 마스터키의 存在條件

MH法에서 마스터키가 存在하는 技能的인 條件은 user i에 對해서

$$S = \vec{a_M} * \vec{x} = \vec{a_i} * \vec{X} \pmod{m_i} \quad (8)$$

$$S' = \vec{a'_M} * \vec{x} = \vec{a'_i} * \vec{X} \pmod{m_i} \quad (9)$$

와 같으며, (8), (9)式은 각각 (5), (6)式에 對應하며, (7)式은 물론 滿足되어야 한다.

2. 마스터키의 導出 알고리즘

前節의 條件에 依해 MH法의 마스터키를 導出하는 알고리즘을 보인다.[12] K_{Mn}을 n個의 個別키에 適用되는 마스터키로 하고 K_i를 個別키, K_{Mi}를 1項부터 i項까지의 個別키에 對한 마스터키로 하면

i) From(8), (9)

$$a_{Mn} = a_i \pmod{m_i} \quad (10)$$

$$w_{Mn}^{-1} = w_i^{-1} \pmod{m_i} \quad (11)$$

(For i = 1, 2, ……n − 1, n)

ii) $K_{Mi} = K_{M(i-1)} \pmod{m'_{i-1}}$ (12)

$$K_{Mi} = K_i \pmod{m_i} \quad (13)$$

(where $m'_{i-1} = \mathrm{LCM}(m_1, m_2, \cdots\cdots m_{i-1})$)

iii) From(12), (13)

$$K_{Mi} = K_{M(i-1)} + m'_{i-1} * \ell_{i-1} \quad (14)$$

$$K_{Mi} = K_i + m_i * \ell_i \quad (15)$$

(14)式과 (15)式에 依해서

$$K_{Mi} = f(K_{M(i-1)}, K_i, m_i, m'_{i-1}) \quad (16)$$

iv) FOR i = 2 To n

$$a_{Mi} = f(a_{M(i-1)}, a_i, m_i, m'_{i-1}) \quad (17)$$

$$w_{Mi}^{-1} = f(w_{M(i-1)}^{-1}, w_i^{-1}, m_i, m_{i-1}) \quad (18)$$

(where $a_{M1} = a_1$, $w_{M1}^{-1} = w^{-1}$)

(14)式에서 $\vec{K}_{M(i-1)}$, K_i, m'_{i-1}, m_i는 槪知數이므로 이式은 l_i와 l'_{i-1}에 關한 二元一次不定方程式이다. 그런데 $\vec{a} = (a_1, a_2, \cdots\cdots, a_n)$이므로 $\vec{a}_M$을 구하기 爲해서 (j−1)*n回의 計算이 必要하다. 安全性을 維持하기 爲해서 n값을 100以上으로 擇하므로 마스터키의 誘導에 상당히 많은 時間이 要求된다. 따라서 MH法에서 마스터키를 誘導하는데 修正을 가할 必要가 있다. (10)式에서 $a_{Mn} = a_i$로 놓으면 이 問題는 쉽게 解決된다.

이방법은 trapdoor knapsack vector의 마스터키가 각각의 個別키(TKV)와 同一하게 되지만 TKV는 公開키이므로 마스터키 管理者는 w^{-1}(w)에 對한 마스터키만을 所有하고도 複數의 個別키를 一元的으로 管理할 수 있다.

3. 마스터키의 導出例

3個의 個別키를 가진 MH algorithm에서 마스터키를 구해보자. 3個의 個別키를 각각 다음과 같이 가정하면,

$m_1 = 19$, $w_1^{-1} = 12$, $w_1 = 8$, $a_1 = (16, 5, 18)$

$m_2 = 23$, $w_2^{-1} = 8$, $w_2 = 3$, $a_2 = (9, 15, 10)$

$m_3 = 15$, $w_3^{-1} = 8$, $w_3 = 2$, $a_3 = (2, 6, 1)$

마스터키 w_M^{-1}은 다음과 같이 구해진다. (12), (13)式으로부터

$$\overline{w}_{M,3}^{-1} = \overline{w}_{M,2}^{-1} \pmod{437} \quad (19)$$

$$\overline{w}_{M,3}^{-1} = 8 \pmod{15} \quad (20)$$

이므로 우선 $\overline{w}_{M,2}^{-1}$을 구해야 한다.

$$\overline{w}_{M,2}^{-1} = 12 \pmod{19} \quad (21)$$

$$\overline{w}_{M,2}^{-1} = 8 \pmod{23} \quad (22)$$

(21), (22)을 行하면 $19\ell_1 + 12 = 23\ell_2 + 8$이된다. 윗式을 풀면 $\ell_1 = \ell_2 = 1$이므로 $\overline{w}_{M,2}^{-1} = 31$이 되고 이것을 (19)式에 代入하여 (19), (20)을 行하면 $437l_3 + 31 = 15\ell_3 + 8$이 된다. 이 式을 풀면 $l'_2 = 11$, $\ell_3 = 332$가되어 구하고자 하는 시스템의 마스터키는 $w_M^{-1} = 15 \times 332 + 8 = 4838$이 된다. 다음은 plaintext가 (1, 0, 1)일 때 각각의 個別키로 encryption한 것을 위해서 구한 마스터키로 decryption하여 本來의 plaintext가 發生됨을 證明하기로 한다.

$S_1 = 16 + 18 = 34$

$S_2 = 9 + 10 = 19$

$S_3 = 2 + 1 = 3$

S_1, S_2, S_3로 부터 plaintext를 구하기 위해서 $a'_{M,i}$와 S'_i를 구해야 한다. 각각의 $a'_{M,i}$는

$a'_{M,1} = (16 \times 4838, 5 \times 4838, 18 \times 4838) \pmod{19}$

$= (2, 3, 7)$

$a'_{M,2} = (9 \times 4838, 15 \times 4838, 10 \times 4838) \pmod{23}$

$= (3, 5, 11)$

$a'_{M,3} = (2 \times 4838, 6 \times 4838, 1 \times 4838) \pmod{15}$

$= (1, 3, 8)$

이고, S'_i는

$S'_1 = 34 \times 4838 \pmod{19}$

$= 9$

$S'_2 = 19 \times 4838 \pmod{23}$

$= 14$

$S_3' = 3 \times 4838 \pmod{15}$
$= 9$

이 된다. $S_i' = a_i' * S_i$이므로 $2x_1 + 3x_2 + 7x_3 = 9$, $3x_1 + 5x_2 + 11x_3 = 14$, $x_1 + 3x_2 + 8x_3 = 9$의 3個의 knapsack function이 나온다. 따라서 각각의 knapsack 問題를 풀면 모두 (1, 0, 1)의 plaintext가 發生하므로 $w_M^{-1} = 4838$의 마스터키를 所有하면 위와같은 시스템을 一元的으로 管理할 수 있다.

4. 마스터키를 利用한 認證

使用者間에 Data傳送을 할 境遇 傳文의 眞實性과 送受信者의 身分을 確認(認證)할 必要가 있다.[7]-[9] MH法에서는 마스터키를 導入함으로써 마스터키 管理者를 通해서 使用者間에 digital signature에 依한 認證이 간단해지며 그 關係를 그림 2에 보인다.

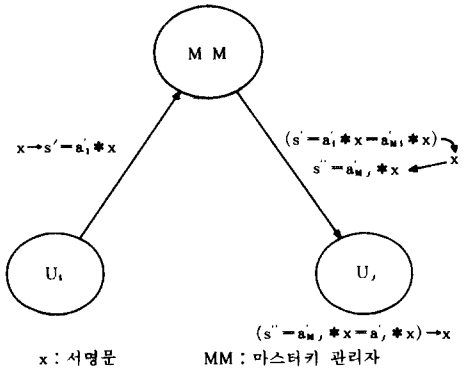

그림 2. 마스터키 관리자를 이용한 인증법
Fig. 2. Authentication using MM.

使用者 U_i와 U_j사이에 認證이 必要할 때 u_i는 自身의 祕密키 a_i'로 $s' = a_i' * x$를 發生시켜 마스터키 管理者에게 보내면 그는 自身의 master Knapsack vector (MKV)로 署名文 x를 回復시킨 後에 다시 MKV로 $S'' = a_{M_j}' * x$를 만들어 受信者 u_j에게 보낸다. u는 $a_{M_j}' * x$를 受信하여 그의 KV로 x를 回復시켜 u_j가 署名文을 確認할 수 있다. 이 境遇에 master key manager 를 除外하고는 u_i만이 署名文을 만들 수 있고 u_j만이 u_j의 의 署名文을 確認할 수 있어 利害關係가 있는 送受信者間에 摩擦을 제거할 수 있다.

5. 實驗 및 考察

複數의 使用者가 MH法에 依한 마스터키를 利用하는 境遇, RSA法과는 달리 알고리즘內에서 線形演算이 使用되므로 encryption(decryption)時間에 큰 影響을 주지 않는다. 표 1은 RSA法과 MH法에서 마스터키를 導入할 때 個別키에 對한 마스터키의 速度比를 나타낸다.

여기서 n의 자리수에 對한 Knapsack vector의 갯수는 RSA와 MH法에 있어서 同一한 work factor를 基準으로 定했다. 표 1에서는 RSA法의 경우 n의 자리수가 6, MH法의 경우 knapsack vector의 갯수가 17인 경우를 나타낸다. 本 硏究의 마스터키는 algorithm

표 1. 마스키를 導入할 때의 速度比
Table 1. Encryption (decryption) time ratio in using master key.

個別키의 數	RSA의 速度比	MH의 速度比
2	1.394	1.066
3	2.370	1.104
4	2.891	1.152
5	4.054	1.206
6	5.036	1.298
7	6.055	1.349

에서 이미 나타나 있지만 Knapsack vector의 數가 다른 경우에도 利用될 수 있다. 그러나 MH法에서는 RSA法과는 달리 알고리즘에 使用되는 m_i가 祕密키이므로 마스터키 管理者가 마스터키와 함께 m_i를 同時에 保管해야 하므로 RSA法에 比해 키管理面에서는 不利한 面도 있다.

V. 結 論

本 論文에서는 MH public key cryptosystem의 키의 安全하고 簡便한 管理를 爲해서 마스터키를 誘導하여 마스터키 管理者에 의해서 시스템을 一元的으로 管理할 수 있는 方法을 提案하였다.

그 結果 複數의 個別키 代身에 master key를 使用하여 一元的으로 入力시킬 수 있음과 個別키의 크기의 合보다 작은 마스터키를 選擇하여 記憶容量을 節約할 수 있음을 알았다. 또한 마스터키를 利用하여 MH法에서 問題點으로 指摘되고 있는 使用者間의 認證이 용이함을 보였고 master key를 使用할 때의 RSA法[5]과는 달리 encryption(decryption) time에 큰 影響을 주지 않음을 computer simulation에 依해 立證하였다.

끝으로 本 硏究에 있어서 많은 도움을 준 本 大學院生 유 수항君에게 感謝하는 바이다.

參 考 文 獻

[1] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystem", *C-ACM*, vol. 21, no. 2, pp.120-126, Feb. 1978.

[2] R.C. Merkle, M.E. Hellman, "Hiding information and signatures in trapdoor knapsacks", *IEEE Trans. Inf. Theory*, vol. IT-24, no.5, pp.525-530, Sep. 1978.

[3] M.E. Hellman "The Mathematics of public key cryptosystem," *Scientific American*, vol. 241, no.3, pp.130-139, 1979.

[4] W.F. Ehrsam, S.M. Matyas, C.H. Meyer, W.L. Tuckman, "A cryptographic key management scheme for implementing the data encryption standard", *IBM SYST J.*, vol. 17, no.2, pp.107-125, 1978.

[5] Kenji Koyama, "A master key for RSA public key cryptography," 日本電子通信學會論文誌, vol. J. 65-D, no. 2, pp.163-170, Feb. 1982

[6] Kenji Koyama "A cryptosystem using the master key for multi-address communication," 日本電子通信學會論文誌, vol. J. 64-D, no. 9, pp.1151-1158, Sep. 1982.

[7] S.G. AKI, *Digital Signatures : A Tutorial Survey*. Computer pp.51-24, Feb, 1983.

[8] Donald W. Davis, *Applying the RSA Digital Signature to Electronic Mail*. Computer, pp.27-35, Feb. 1983.

[9] W. Diffie, M.E. Hellman, "Privacy and authentication: An introduction to cryptography," *Proceedings of the IEEE*, vol. 67, no. 3, pp.397-427, Mar. 1979.

[10] C.H. Meyer, S.H. Matyas, *Cryptograph: A New Dimension in Computer Data Security*. John Wiley & Sons, New York, 1982.

[11] A.V. Aho, J.E. Hopcroft, J.D. Ullman, *The Design and Analysis of Computer Algorithms*. Addison-Wesley Pub. Company, pp.373-394, 1976.

[12] 高崙碩, 崔炳旭, "MH法에 있어서의 Master Key" 대한전자공학회 추계종합학술대회 논문집, vol. 6, no. 2, pp. 173-176, Nov. 1983.