韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

招請特輯

公開 키 暗號 시스템에 關한 硏究
Study on the Public-Key Cryptosystems
(1)

李 晩 榮*

公開 키 暗號 시스템(public key cryptosystem)의 各種 方式을 說明하고 深度있는 理論的 解釋과 例題를 通한 各 暗號 시스템의 妥當性을 立證한다. 또한, 對稱暗號 시스템(private-key cipher systems)과 非對稱 暗號시스템(public-key cryptosystems)別로 나누어 認證(authentication) 및 디지탈 署名(digital signature)에 관한 問題들을 다음 목차에 따라 連載로 詳細히 記述하고자 한다.

目 次

* 정회원, 漢陽大學校 名譽教授, 本 學會 會長

1. 序 論

1970年初만 해도 暗號 시스템은 古典的인 對稱 暗號 시스템만이 알려져 있어 商用 暗號 시스템으로서는 그리 利用價値가 없었다. 그러나 1970年代 後半으로 접어들면서 事情은 극적으로 달라졌다. 當時 Stanford大의 Diffie와 Hellman 그리고 MIT의 Rivest, Shamir, Adleman 등이 考案한 公開 키 暗號 시스템의 發明은 慣用 暗號 시스템이 갖는 키 分配나 暗號强度 등과 같은 問題點을 補完한 劃期的인 暗號方式으로 情報 保安側面에서 商用化에 寄與할 수 있는 轉機를 마련한 唯一한 시스템이다. 그 後 暗號解讀에 必要한 數學的 接近方法도 폭넓게 開發되어서 暗號 및 그 應用分野의 새로운 章을 열었고 從來의 것과 全然 다른 새로운 暗號 시스템의 出發을 導出하게 된 것이다.

一般的으로 公開 키 暗號 시스템은 暗號化에 必要한 公開 키(public key) K_p와 情報 復元에 必要한 祕密 키(secret key) K_s를 使用한다. 暗號化 後 復號 또는 復號後 暗號化하는 節次에 無關하게 元來의 平文을 還元하는데는 다음과 같은 式에 의해 이루어진다.

$$D_{K_s}(E_{K_p}(X))=E_{K_p}(D_{K_s}(X))=X$$

公開 키 알고리즘은 復號施行時 暗號化 過程이 露出되지 않도록 設計되어야 한다. 旣存의 DES 알고리즘은 매우 複雜해서(特히, S-box 解析) 그의 作動의 數學的 表現을 完璧하게 解釋하기란 거의 不可能하다. 反面 公開 키 알고리즘은 數學的 表現은 容易하나 그 解析 亦是 쉽지는 않다. 暗號保安側面에서 完璧한 시스템이라 믿어지는 公開 키 暗號 시스템도 왕왕 暗號解讀이 可能해서 깨지는 경우가 많다. 또한 非公開 키(private key)와 公開 키(public key) 暗號 시스템과의 差異點은 키(鍵) 生成과 用途面에서 찾아 볼 수 있다. 慣用 DES의 경우 暗號化 키와 復號化 키가 서로 同一함으로 對稱暗號 시스템(symmetric cryptosystem)이라 부르나 公開 키 暗號 시스템은 公開 키(public key)와 祕密 키(secret key) 두個의 키를 使用하므로 非對稱 暗號 시스템(asymmetric cryptosystem)이라 부른다. 本 連載內容은 1970年代 後半에 發表된 Diffie의 公開 키 分配法(1976), RSA 公開 키 暗號 시스템(1978), Merkle과 Hellman의 Knapsack 暗號 公開 시스템(1978), McEliece의 暗號 시스템(1978) 및 1980年代에 發表된 補完 乃至 改善된 公開 키 알고리즘 그리고 認證(authentication)과 디지탈 署名(digital signature) 등을 順次的으로 記述해 나가도록 하겠다.

2. 公開 키 分配 시스템 (Public Key Distribution System)

有限體 GF(q)上의 演算 알고리즘에 있어서 그 解讀이 不可能 할때 暗號 시스템은 完璧하다고 한다. Diffie와 Hellman(1976)은 GP(q)上의 對數(logarithm) 演算이 그 當時 知識으로서는 大端히 어렵다고 생각되어 GF(q)上에서 冪乘의 可換性과 離散對數問題를 公開 키 알고리즘에 導入하는 方法을 提案하였다. 먼저 다음 한 雙의 逆函數를 생각해 보자.

$$Y \equiv \alpha^X \pmod q \qquad (1)$$

$$X \equiv \log_\alpha Y \text{ over } GF(q) \qquad (2)$$

여기서 X, Y는 各各 平文 및 暗號文이며 그 범위는 $1 \leq X,\ Y \leq q-1$이다. 그리고 q는 素數이며 α는 有限體 GF(q)의 한 原始元素이다. 平文 X를 알고 暗號文 Y를 計算하는 것은 쉬우나 Y로부터 X를 알아내는 일은 그리 쉽지 않다. 왜냐하면 基底 α로 Y의 對數를 취해 計算하는 일이 어렵기 때문이다. 事實 Diffie-Hellman의 키 交換 프로토콜에서 GF(q)上에서 指數의 逆프로세스인 離散對數를 취해서 計算해야 하는 難點이 暗號 시스템의 完璧을 立證하기 때문이다. 實際로 計算複雜度와 알고리즘 分析이 모든 暗號 시스템의 安全度(security)를 測定하는 尺度가 된다.

公開 키 分配 시스템은 한 키를 交換코자 하는 兩使用者 i와 j 間에 共用 키(common key)를 얻어낼때까지 反復해서 送受信해야 한다. 使用者 i는 集合 {1, 2,…, q−1}로부터 均等하게 獨立無作爲

變數 X_i를 選出한다고 하자. 使用者 i는 X_i를 必要로 하고

$$Y_i \equiv \alpha^{X_i} \pmod q \qquad (3)$$

는 公開한다. 두 使用者 i와 j가 隱密히 交信코자 할때 다음과 같은 共用 키 K_{ij}를 利用해야 한다. 即,

$$K_{ij} \equiv \alpha^{X_iX_j} \pmod q \qquad (4)$$

使用者 i는 公開綴(public file)에서 Y_j를 얻어냄으로써 共用 키 K_{ij}를 다음과 같이 計算한다. 即,

$$\begin{aligned} K_{ij} &\equiv Y_j^{X_i} \pmod q \\ &\equiv \alpha^{X_jX_i} \pmod q \\ &\equiv \alpha^{X_iX_j} \pmod q \end{aligned} \qquad (5)$$

使用者 j도 같은 方法으로 共用 키 K_{ij}를 다음과 같이 計算한다.

$$K_{ij} \equiv Y_i^{X_j} \pmod q \qquad (6)$$

따라서, 使用者 i는 Y_i와 Y_j로부터 다음과 같이 共用 키 K_{ij}를 計算하면 된다.

$$K_{ij} \equiv Y_i^{(\log_\alpha Y_j)} \pmod q \qquad (7)$$

따라서 GF(q)上의 對數(logarithm)를 쉽게 計算할 수 만 있다면 그 暗號 시스템은 쉽게 깨질 수 있음을 알 수 있다. 反面에 GF(q)上의 對數計算이 難解하다면 그 暗號 시스템은 安全할 것이다. 結論的으로 祕密 키 X_i와 X_j를 알아내지 않고 公開 키 Y_i와 Y_j로부터 共用 키 K_{ij}를 計算한다는 것은 무모한 試圖이다. 事實 素數 q가 1000비트 以上의 큰 값을 가질때 暗號解讀者(cryptanalysis)가 式(7)을 計算한다는 것은 거의 不可能하다. 다음 例題는 共用 키 K_{ij}를 求하는 過程을 提示한 매우 簡單한 例이다.

[例題 1] 有限體 $GF(2^3)$, m=3, 의 體元素를 생각해 보자. 2元體 GF(2)上의 3차 原始多項式은 $p(x)=1+x+x^3$이다. α를 p(x)의 한 根이라 하면 $p(\alpha)=0$, 즉 $\alpha^3=1+\alpha$로부터 生成되는 $GF(2^3)$의 元素들은 다음 表 1과 같다.

表 1. q=7에 對한 $GF(2^3)$의 元素

冪	多項式	벡타
1	1	1 0 0
α	α	0 1 0
α^2	α^2	0 0 1
α^3	$1+\alpha$	1 1 0
α^4	$\alpha+\alpha^2$	0 1 1
α^5	$1+\alpha+\alpha^2$	1 1 1
α^6	$1+\alpha^2$	1 0 1

使用者 i와 j가 各其 $X_i=2$와 $X_j=5$를 擇했다고 假定하자. 勿論 X_i와 X_j는 祕密 키이므로 公開 키는 各各

$$Y_i \equiv \alpha^{X_i} \pmod 7 \equiv \alpha^2 \pmod 7 = 0\ 0\ 1$$
$$Y_j \equiv \alpha^{X_j} \pmod 7 \equiv \alpha^5 \pmod 7 = 1\ 1\ 1$$

이며, 이 값들은 公開綴에 保管한다. 使用者 i가 公開綴로부터 $Y_j=111$를 利用하여 使用者 j와 交信코자 한다면 兩者間의 共用 키 K_{ij}는 다음과 같이 求해질 것이다.

$$\begin{aligned} K_{ij} &\equiv (Y_j)^{X_i} \pmod 7 \equiv (\alpha^5)^2 \pmod 7 \\ &\equiv \alpha^{10} \pmod 7 = \alpha^3 = 1\ 1\ 0 \end{aligned}$$

使用者 j도 같은 方法으로 共用 키 K_{ij}를 얻을 수 있다. 即

$$\begin{aligned} K_{ij} &\equiv (Y_i)^{X_j} \pmod 7 \equiv (\alpha^2)^5 \pmod 7 \\ &\equiv \alpha^{10} \pmod 7 = \alpha^3 = 1\ 1\ 0 \end{aligned}$$

이며, 이와같이 해서 兩者 i와 j는 共用 키를 求할 수 있다.

3. Merkle-Hellman Knapsack 暗號시스템

暗號硏究에 있어 knapsack 問題는 數學的으로 魅力을 느끼게 한다. trapdoor knapsack 問題를 基礎로 考察한 公開 키 非對稱 暗號 시스템이 Merkle-Hellman 方式이다.

3.1 Additive knapsack 方法

公開 키의 集合을 $K_p=\{k_1, k_2, \cdots, k_n\}$ 여기서 正數 $k_i \in Z_q=\{1, 2, \cdots, q-1\}$, $1 \leq i \leq n$이라 하고 平文을 $X=\{x_1, x_2, \cdots, x_n\}$ 여기서 $x_i \in GF(2)$, $1 \leq i \leq n$라 하자. knapsack 暗號 시스템은 n비트 平文을 n비트 暗號文으로 다음과 같이 暗號化 한다.

$$Y=K_p \cdot X=k_1x_1+k_2x_2+\cdots+k_nx_n = \sum_{i=1}^{n} k_ix_i \quad (8)$$

暗號文 Y는 式(8)에서 보는 바와 같이 簡單히 計算되나 暗號文 Y와 公開 키 K_p로부터 平文 X를 復元하는 일은 knapsack 問題를 푸는 것이라서 n가 大端히 큰 수 일때는 一般的으로 難題라 하겠다. 그러나 公開 키 K_p의 各 要素 k_i를 그 以前 모든 要素의 合보다 크도록 選定한다면 knapsack 問題 풀이는 簡單해 진다.

$$k_i > k_1+k_2+\cdots+k_{i-1}=\sum_{j=1}^{i-1} k_j, \quad 1 \leq i \leq n \quad (9)$$

그런데, 暗號文 Y의 各 要素 y_i, $1<i<n$를 다음과 같이 놓으면

$$y_1=k_1x_1$$
$$y_2=k_1x_1+k_2x_2$$
$$\vdots$$
$$y_n=k_1x_1+k_2x_2+\cdots+k_nx_n$$

y_i와 k_i, $1 \leq i \leq n$, 로부터 平文 X를 復元하는 節次는 다음과 같다. 萬一 $y_n<k_n$일 경우에는 $x_n=0$ 그리고 $y_{n-1}=y_n$라 놓지만, $y_n>k_n$일 때에는 $x_n=1$ 그리고 $y_{n-1}=y_n-k_n$으로 놓아야 한다. 計算해서 얻은 y_{n-1}의 값을 利用하여 같은 方法으로 x_{n-1}과 y_{n-1}을 求해야 한다. 따라서 復元作業은 $X=(x_1, x_2, \cdots, x_n)$가 完全히 求해질 때까지 繼續해야 한다. knapsack 問題를 다음의 簡單한 例로 說明코자 한다.

[例題 2] 平文을 X=(1 1 0 0 1) 그리고 公開 키를 $K_p=(151, 187, 426, 1091, 2412)$라 할때 暗號文 Y는

$$Y=K_p \cdot X=151+187+2412=2750$$

이 된다. $Y=y_5=2750$이 暗號文인 故로 y_5와 k_5로부터 x_5의 復元은 $x_5=1$이 되는데 그 理由로는 $y_5=2750>k_5=2412$이기 때문이다. 따라서 平文의 各 要素 x_i, $1<i<5$, 는 다음과 같이 해서 求하게 된다.

$y_5=2750>k_5=2412$, $x_5=1$
$y_4=y_5-k_5=338<k_4=1019$, $x_4=0$
$y_3=338<k_3=426$, $x_3=0$
$y_2=338>k_2=187$, $x_2=1$
$y_1=y_2-k_2=151=k_1=2412$, $x_1=1$

이와같이 해서 復元된 平文은 X=(1 1 0 0 1)이 됨을 알 수 있다. 그런데 이 例題에서 보듯이 Y로부터 X를 너무 簡單히 求할 수 있으므로 knapsack 벡터 K_p를 公開 暗號 키로 使用하는 것은 賢明치 않다.

公開 키의 生成은 數 100個의 要素를 갖는 knapsack 벡터 K_p를 選定하는 問題에 歸着한다. 平文 X를 受信者(receiver)에게 傳送코자 하는 者는 暗號文 $Y=K_pX$를 滿足할 수 있도록 公開 키 K_p를 使用하여 于先 平文 X를 暗號化 해야 한다. 送信者(sender)는 먼저 m>w가 되도록 大端히 큰 數 m과 w를 選擇한다. 이때, 이 두 數는 서로 素(relatively prime) 即 gcd(w, m)=1이어야 한다. 더우기 m은 $m>\Sigma k'_i$, $1 \leq i \leq n$, 가 되도록 選擇된 大端히 큰 正數이다. 平文 X를 暗號文 Y로부터 復元하기 위해서 때로는 正數 v를 媒介로 하여 Y를 Y'로 變換하는 境遇가 必要하다.

$$Y'_1 \equiv vY \pmod{m} \quad (10)$$

여기서 v는 w의 逆乘算(multiplicative inverse), 即 $v=w^{-1} \pmod{m}$의 關係인 祕密 數이다.

$$wv \equiv 1 \pmod{m}$$

또는

$$ww^{-1} \equiv 1 \pmod{m} \quad (11)$$

따라서 式(11)을 利用하면 式(10)은 다음과 같다.

$$Y \equiv wY' \pmod{m} \quad (12)$$

勿論 受信者(user)는 trapdoor knapsack 벡터 K_p를 公開 키로 選擇하고 $v=w^{-1}$와 m을 祕密 키로 祕藏할 수도 있다. 公開 knapsack 벡터(public knapsack vecter) K_p는 다른 knapsack 벡터 K'_p의 各 要素 k'_i, $1 \leq i \leq n$와 w와의 곱으로 生成될 수 있으므로

$$k_i \equiv w\ k'_i \pmod m,\quad 1 \leq i \leq n \qquad (13)$$

가 된다. 式(10)을 利用하여 送信者는 變換된 暗號文 Y′를 다음과 같이 計算할 수 있다.

$$\begin{aligned} Y' &\equiv w^{-1}\ Y \pmod m \\ &\equiv w^{-1} \sum_{i=1}^{n} k_i x_i \pmod m \end{aligned}$$

式(13)을 이 式에 代入하면 아래와 같이 된다.

$$\begin{aligned} Y' &\equiv w^{-1} \sum_{i=1}^{n} w\ k'_i\ x_i \pmod m \\ &\equiv w\ w^{-1} \sum_{i=1}^{n} k'_i\ x_i \pmod m \\ &\equiv K'_p X \end{aligned} \qquad (14)$$

한편 $Y = K_p X = \sum_{i=1}^{n} k_i x_i$인 故로

$$Y \equiv \sum_{i=1}^{n} [w\ k'_i \pmod m] x_i$$

여기서 $k'_i \equiv w^{-1} k_i \pmod m$이므로

$$\begin{aligned} Y &\equiv \sum_{i=1}^{n} (w\ w^{-1}) k_i x_i \pmod m \\ &\equiv \sum_{i=1}^{n} k_i\ x_i \pmod m = K_p X \end{aligned} \qquad (15)$$

임을 알 수 있다. 따라서 式(14)의 knapsack 問題를 X의 값을 푸는데 있어 보기에는 어렵게 생각되지만 쉽게 求할 수 있으며 그것은 또한 式(15)의 trapdoor knapsack 問題의 解答이기도 하다. 讀者에게 knapsack 問題의 背景을 仔細히 理解시키기 위해 다음에 簡單한 例題를 들어 說明하고자 한다.

[例題 3] Knapsack 벡터 K'_p를 正數의 增加數列

$$K'_p = (151,\ 187,\ 426,\ 1091,\ 2412)$$

로 選定하면

$$\sum_{i=1}^{5} k'_p = 151 + 187 + 426 + 1091 + 2412 = 4267$$

이다. 祕密 키 (w, m)가 m>w 그리고 gcd(w, m)=1이 되도록 m=4617과 w=1175를 定하자. 于先, Euclid 알고리즘을 利用하여 gcd(1175, 4617)=1 即, w와 m가 서로 素가 되는가를 알아보기로 하자.

$$\begin{aligned} 4617 &= (1175)3 + 1092 \\ 1175 &= (1092)1 + 83 \\ 1092 &= (83)13 + 13 \\ 83 &= (13)6 + 5 \\ 13 &= (5)2 + 3 \\ 5 &= (3)1 + 2 \\ 3 &= (2)1 + 1 \\ 2 &= (1)2 \end{aligned}$$

剩餘가 零일때 이 過程은 完了되나 最後의 零이 아닌 剩餘가 바로 最大公約數(greatest common divisor)가 됨으로 이 경우에는 1이므로 gcd(1175, 4617)=1이다. 따라서, 두 數 w=1175와 m=4617은 서로 素임이 證明된다.

式(13)에서 $k_i \equiv 1175k'_i \pmod{4617}$, $1 \leq i \leq 5$, 의 關係를 利用하면

$$\begin{aligned} k_1 &= (151)(1175) - (38)(4617) = 1979 \\ k_2 &= (187)(1175) - (47)(4617) = 2726 \\ k_3 &= (426)(1175) - (108)(4617) = 1914 \\ k_4 &= (1091)(1175) - (277)(4617) = 3016 \\ k_5 &= (2412)(1175) - (613)(4617) = 3879 \end{aligned}$$

와 같이 되어 knapsack 벡터 K_p는

$$K_p = (1979,\ 2726,\ 1914,\ 3016,\ 3879)$$

와 같이 計算이 된다.

다음 예제를 통하여 knapsack 벡터 K'_p를 잘못 選擇하였을때 올바른 平文 X를 復元할 수 없다는 것을 보이고자 한다.

[例題 4] $v = w^{-1}$의 값을 구하기 위하여 Euclid 알고리즘 gcd(w, m)=vw+um을 利用해 보자. gcd(w, m)=gcd(1175, 4617)=1으로부터 1=1175v+4617u이 成立된다. 따라서, $1 \equiv 1175\ v \pmod{4617}$의 線形 congruence로 表現할 수 있고 앞에서 求한 gcd를 얻기 위해 행해진 Euclid 나눗셈 알고리즘은,

$$\begin{aligned} 1 &= 3 - (2)1 \\ 1 &= (3)2 - 5 \\ 1 &= (13)2 - (5)5 \\ 1 &= (13)32 - (83)5 \\ 1 &= (1092)32 - (83)421 \\ 1 &= (1092)453 - (1175)421 \\ 1 &= (4617)453 - (1175)1780 \end{aligned}$$

와 같이 展開된다. 여기서 最後의 方程式을 살펴보면 $1 \equiv -(1175)(1780) \pmod{4617}$으로 表示됨으로 m=4617를 法으로 하는 v의 값 v=1780은 w의 값 w=1175의 逆乘算같이 보이나 實際로는 그렇지 않다.

다음에는 變換된 暗號文 $Y' \equiv Yv \pmod{m}$와 $Y' \equiv K'_p X \pmod{m}$를 利用해서 平文 X를 復元하기 위해 trapdoor knapsack 公開 키 알고리즘을 생각해 보자. knapsack 벡터 K=(1979, 2726, 1914, 3016, 3879)를 公開 키로 選定하자. 그리고 祕密正數 v=1780은 앞에서 주어진 K'_p=(151, 187, 426, 1091, 2412)로부터 求해지며 두개의 祕密正數는 w=1175와 m=4617로 決定되었다. 따라서 暗號文 $Y=K_p X=1979+2726+3879=8584$와 變換 暗號文 $Y' \equiv Yv \pmod{m} \equiv (8584)(1780) \pmod{4617} \equiv 15279520 \pmod{4617} = 1867$ 등이 計算된다. 이와같이 해서 X를 復元하면 아래와 같다.

i	Y'_i K'_i	X_i
5	1867<2412	0
4	1867<1091	1
3	776> 426	1
2	776> 187	1
1	589> 151	1

따라서 平文 X의 값은 (1 1 1 1 0)으로 計算되나 實際는 X=(1 1 0 0 1)이므로 그 結果가 判異함을 알 수 있다. 그런 故로 단한번의 施行結果로 正確한 平文 X를 알아낸다는 것은 至極히 無理이다. 全 32個의 平文 X중 徹底한 施行錯誤調査를 거쳐 正確한 平文 X를 알아내야 하는데 이러한 knapsack 問題는 n의 값이 크면 클 수록 K'_p의 選定과 아울러 大端히 어려운 問題로 남아 있다. 따라서 正確히 knapsack K'_p를 選擇함으로서 주어진 平文 X를 正確하게 復元하는 問題는 다음 號에서 다루기로 하자. (다음 號에 계속)

參 考 文 獻

1. Diffie, W. and M.E. Hellman : "New Direction in Cryptography," IEEE Trans. Inform. Theory, vol. IT-22, pp.644-654, 1976.

2. Merkle, R.C. and N.E. Hellman : "Hiding Information and Signatures in Trap Door Knapsacks," IEEE Trans. Inform. Theory, vol. IT-24, no. 5, pp.525-530, 1978.

3. Shamir, A. : "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem," IEEE Trans. Inform. Theory, vol. IT-30, no. 5, 1984.

4. Pohlig, S.C. and M.E. Hellman : "An Improved Algorithm for Computing Logarithms Over GF(p) and its Cryptographic Significance," IEEE Trans. Inform. Theory, vol. IT-24, no. 1, 1978.

5. Desmedt, Y., J. Vandewalle, and R. Govaerts : "How Iterative Transformations can help to crack the Merkle-Hellman Cryptographic Schemes," Electron. Letter, vol. 18, pp.910-911, 1982.

6. Desmedt, Y., J. Vandewalle, and R. Govaerts : "A Critical Analysis of the Security of Knapsack Public-Key Algorithm," IEEE Trans. Inform. Theory, vol. IT-30, no. 4, 1984.

7. Shamir, A. and R.E. Zippel : "On the Security of the Merkle-Hellman Cryptographic Scheme," IEEE Trans. Inform. Theory, vol. IT-26, no. 3, 1980.

8. Adleman, L.M. : "On Breaking the Iterated Merkle-Hellman Public Key Cryptosystem," in Advances in Cryptology : Proc. of Crypto'82, New York : Plenum Press, 1983.

9. Brickell, E.F., J.C. Lagarias, and A.M. Odlyzko : "Evaluation of the Adleman Attack on Multiply Iterated Knapsack Cryptosystems," in Proc. of Crypto'83, New York : Plenum Press, 1984.

10. Lagarais, J.C. : "Knapsack Public Key Cryptosystems and Diophantine Approximation," in Advances in Cryptology, Proc. of Crypto'83, New York : Plenum Press, 1984.

(著者紹介는 p.23 참조)