論文
3-8-14

전자 거래를 위한 키복구 기술
(Key Recovery Technology for E-Transaction)

이 병 수* 조 시 용**
(Byung-Soo Lee) (Shee-Yong Cho)

요 약

이전에 군사상의 목적 등 국가적 차원에서 주로 이용되었던 암호의 사용이 전자 거래가 일반화되면서 민간 부분으로 급속히 확대되고 있다. 이는 인터넷을 통한 정보의 유통 시에 발생 가능한 도청, 변조, 위조 등의 여러 가지 취약점을 방지하기 위한 암호의 사용이 일반화하게 하였다. 그러나 키의 분실로 인한 암호문의 복구 불가능, 암호의 불법 단체 및 개인에 의한 불법적인 사용 등의 역기능이 존재한다. 본 논문에서는 암호문에 대응되는 개인키 소유자가 아니더라도 약속된 조건을 만족시킬 경우 암호문을 해독할 수 있는 키 복구 기술에서 요구되는 기본 요소 기술을 분석하고, 선진국의 기술 개발 동향과 정책을 분석하고 각 정책과 기술을 비교 분석한다.

ABSTRACT

This paper has presented three types of key recovery methods, which are known as key escrow, key encapsulation, and trusted third party scheme. we have analyzed the existing key recovery products, which have been developed by the advanced nations for electronic commerce and electronic government. we have also analyzed the key recovery policies proposed by the advanced nations, such as The United States of America, Great Britain, and Japan.

In this paper, several key recovery policies are proposed for the e-commerce and e-government system. And we have proposed key recovery scheme for the e-commerce system utilizing the on-line secret sharing scheme based on the Internet and public bulletin board.

1. 서론

세계는 지금 산업사회에서 정보사회로의 전환기를 맞이하고 있다. 정보의 보고라는 인터넷의 확대 보급을 통하여 가정에서 손쉽게 필요한 정보에 접근할 수 있게 되었고, 전자 상거래의 실용화 등을 통해 사회 생활의 편리성이 향상되고 있으나, 그에 따른 정보의 위·변조 등에 의한 범죄나 부정행위도 급증하고 있다.

따라서 기존의 군사 및 외교용으로 국한되어 사용되었던 암호 기술의 민간 사용에 대한 요구가 급증하였고, 현재 암호기술에 대한 많은 연구 및 개발이 진행되고 있다. 그러나 테러 및 안보에 큰 위협 요소로 악용될 수 있어, OECD 등 선진 각국은 암호 사용의 역기능 방지를 위해 노력하고 있다.

* 정회원 : 순천향대학교 정보기술공학부 교수
** 정회원 : 순천향대학교 정보통신공학박사

논문접수 : 2002. 7. 25.
심사완료 : 2002. 8. 14.

정보를 보호하기 위해 이전에, 정치적 군사상의 목적 등 국가적 차원에서 주로 이용되었던 암호의 사용이 민간부분으로 급속히 확대 되었다. 그러나 수많은 일반 사용자들이 다량의 정보에 접근이 가능해짐으로써 정보가 무방비로 노출됨으로써 변조, 도용 등 정보가 침해될 가능성 또한 많아 졌다. 현재 컴퓨터 기술의 발달과 함께 개인용 컴퓨터의 일반 사용자도 쉽게 고도의 계산 능력을 갖는 개인용 컴퓨터를 이용하는 것이 가능하게 되어 암호를 이용해서 정보를 은닉하는 것이 어렵지 않게 되었다. 그러나 장점에 반하여 다음과 같은 문제가 발생하게 되었다.

국가가 범죄 수사 등의 합법적인 이유로 암호문에 접근해야 할 필요성이 있을 경우, 암호는 키를 아는 사람만이 암호문을 복호할 수 있는 기밀성 때문에 범죄자들은 암호를 사용함으로써 합법적인 수사를 방해할 수 있다. 또한 개인 사용자가 자신의 키의 분실이나 손상으로 인하여 자신의 정보에 접근할 수 없는 경우이다. 이와 같은 키의 도난이나 손상 등의 위협이 항상 존재하게 된다.

이러한 암호의 부당한 사용은 개인에게는 데이터의 손실을 가져올 뿐만 아니라, 크게는 국가의 기본 질서를 위협할 수 있다. 이에 암호의 부당한 사용으로 발생하는 역기능을 방지하기 위한 연구가 필요하며, 세계 각국에서는 암호키에 대한, 사회적이고 국가적인 접근을 위한 대책으로, 암호문의 소유자가 아니더라도 약속된 조건을 만족시킬 경우 암호문을 풀 수 있도록 하는 암호키관리 기반구조에 대한 필요성이 대두됨에 따라 연구가 진행 되고 있다.

본 논문에서는 각국의 암호 사용의 역기능을 방지하기 위한 키복구 기술에 대한 정책 동향을 분석하여 이를 분석함으로써, 우리나라에서 암호 사용 부정 방지 대책을 마련하기 위한 기초 자료를 제공하는데 본 연구의 목적이 있다.

2. 키복구 시스템을 위한 암호 알고리듬

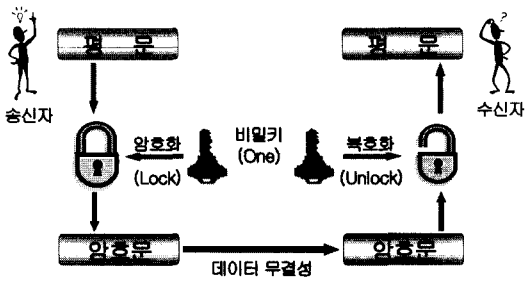
본 장에서는 키복구 시스템에서 사용되는 암호 알고리듬에 관하여 정의 하고, 각각 이를 간단히 설명해 보고자 한다. 이때 사용되는 암호 시스템은 키 관리 형태에 따라 크게 대칭키 암호시스템과 공개키 암호시스템으로 나뉘어 질 수 있다. 또한 여러 가지 비밀 분산 방식에 관하여 각각 설명하고 이를 비교 분석한다.

2.1 대칭키 암호방식

대칭키 암호방식[2]은 비밀키 암호방식, 관용암호방식 또는 단일키 암호시스템으로도 불리며, 암호화와 복호화에 같은(동일한)키를 사용하는 방식을 말한다. 예를 들면, 송신자는 전송하고자 하는 평문과 비밀키를 암호 알고리듬을 통해 암호문으로 변환하여 수신자에게 전송한다. 수신자는 송신자와 동일한 비밀키를 복호 알고리듬에 사용해서 원래의 평문을 만들어 내게 된다. 이때 송신자와 수신자는 암호화 통신을 하기 전에 안전하게 미리 비밀키를 교환하여야 하며, 암호 통신을 도청하려는 제 3 자는 송신자와 수신자가 암복호에 사용한 비밀키가 없으면 원래의 평문을 해독할 수 없게 된다.

대칭키 암호시스템의 보안성은 여러 가지 요소에 의해 좌우되나, 그 중에서도 가장 중요한 점은 안전하게 키를 보관하는 것이다. 즉, 암호화 통신을 하는 송수신자는 자신들이 가지고 있는 키가 노출이 되지 않도록 비밀로 간직해야 하는데, 이것은 암·복호화 알고리듬이 공개가 되더라도 키를 알지 못하면 암호문을 해독할 수가 없도록 설계되었기 때문이다.

이와 같은 특징으로 인하여 암호화 통신을 하고자 하는 상대방이 많으면 그에 따라 관리해야 하는 키의 수도 증가하게 되며 키 관리상의 문제가 생기게 된다. 그러나 대칭키 암호시스템은 많은 다양한 알고리듬(DES, RC5, SKIPJACK, IDEA, SEAL, RC4 등)이 나와 있으며 암·복호화 속도가 공개키 암호방식보다 빠르기 때문에 현재에도 평문을 암호화하기 위해 가장 많이 사용하고 있다. 다음 그림 1. 은 일반적인 대칭키 암호 방식을 이용한 통신 시나리오를 설명한다.



[그림 1] 대칭키 암호 방식을 이용한 통신 시나리오

[Fig 1] Communication scenario using symmetric-key cryptosystem

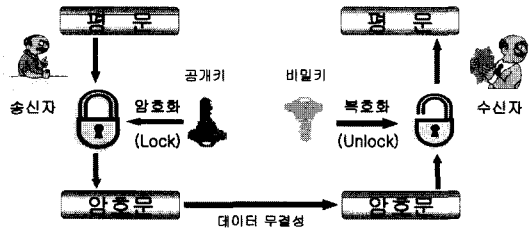
2.2 공개키 암호방식

공개키 암호 시스템은 비대칭키 암호시스템이라고도 하며 수학적 함수를 기반으로 하여 대칭키 암호시스템과 달리 키 쌍이 존재하여 하나의 키는 누구든지 사용할 수 있도록 공개하며 다른 하나는 자신만이 비밀스럽게 보관하는 방식을 말한다. 이때 공개하는 키를 공개키라고 하며 비밀스럽게 보관하는 키를 개인키라고 한다.

공개키 암호시스템은 대칭키 암호시스템의 키 관리와 분배의 문제점을 해결해 주고 있다. 즉, n명의 사람들과 암호화 통신을 하기 위해서 대칭키 암호시스템에서는 $n(n-1)/2$ 개의 키가 필요하지만, 공개키 암호시스템에서는 각 사용자당 2개씩의 키만 필요하게 되므로 전체적으로 $2n$ 개의 키들만이 필요하게 된다. 그러나 이러한 장점이외에 키 사이즈가 크다는 점과 2진수를 10진수로 변환하는 연산시간이 길다는 단점이 있으며 선택적 평문 공격에 대한 취약성을 가지고 있다.

공개키 암호를 이용해서 송신자와 수신자가 암호통신을 하기 위해서는 다음과 같은 과정을 거친다. 먼저 송신자는 수신자의 공개키로 메시지를 암호화하여 전송한다. 그러면 수신자는 자신의 개인키로 암호문을 복호화하여 평문을 얻는다. 네트워크 상에서 누군가 암호문을 얻더라도 개인키 없이는 암호문을 복호화할 수 없으므로 안전하게 데이터를 전송할 수가 있다. 개인키는 언제나 소유자만이 보관하고 있으며 전송되거나 다른 사람에게 알려질 필요가 없기 때문이다.

그러나 이러한 공개키 암호시스템은 그 역사도 짧으며, 현재 나와 있는 알고리듬(RSA, ElGamal, ECC 등)도 그리 많은 편이 아니다. 또한 대칭키 암호시스템보다도 데이터 암호화 속도가 매우 느리기 때문에 일반적으로 데이터 암호화에는 사용하지 않으며 키 분배나 디지털 서명 등에 많이 사용되고 있다. 다음 [그림 2]는 일반적인 공개키 암호 방식을 이용한 통신 시나리오를 설명하며, 이러한 사실로부터 대칭키와 공개키를 비교하면 <표 1>과 같다[2].



[그림 2] 공개키 암호 방식을 이용한 통신 시나리오

[Fig. 2] Communication scenario using public-key cryptosystem

2.3 비밀 분산 방식

비밀 분산에 대한 개념은 Shamir와 Blakley가 각각 소개한 이후로 많은 방식에 대한 연구가 진행되었다. 비밀 분산이란 어떠한 비밀 정보가 있을 때, 이것을 여러 개의 정보로 분할한 후, 각각의 참여자에게 분배하고 모든 사용자에게 분할된 정보를 모으면 다시 비밀 정보를 복원할 수 있는 방식을 말한다. 이때 각각의 분할된 정보를 shadow 라고 한다.[3][4]

이는 안전성과 효율성을 위해 n 개의 shadow가 있을 때 k ($\leq n$)개 의 shadow만을 모으면 비밀 정보가 복구 가능하도록 구성될 수 있어 (k, n) -threshold 방식이라고 한다.

2.3.1 Shamir의 비밀 분산방식

<표 1> 대칭키와 공개키 비교

<Table 1> Comparison of symmetric-key and public-key cryptosystem

키의 종류	특 징	기 밀	인공지능
대칭키 암호방식	· 수신자마다 다른 키가 필요 · 수신자에 대한 암호키의 배신(配信)risk가 수반됨 · 암호화속도가 빠름	· 송신자와 수신자만이 사용하는 암호키에 의해 암호화됨	· 송신자 및 수신자만이 사용하는 암호키에 의해 정보의 암호화 및 복합화 됨
공개키 암호방식	· 1개의 암호키에 의해 여러 사람간의 통신이 가능 · 암호키의 배신(配信)risk가 없음 · 암호화속도가 느림	· 수신자 공개키에 의해 암호화 됨	· 송신자의 비밀 서명(디지털 서명)을하고, 송신자가 공개키에 대해 검증함에 의함

■ 시스템 설정

- $p : p \geq n+1$ 인 큰 소수
  (단, n은 비밀 분산에 참여하는 전체 참가자의 수)
- K : 분산하고자 하는 비밀 $K \in GF(p)$
- D : 각 참가자에게 부분정보를 분배하는 분배자
- P : 전체 참가자의 집합 $P=(P_1, P_2, \cdots, P_n)$
- S_i : 참가자 P_i 에게 분배하는 부분 정보

■ 비밀 분산 과정

① 분배자는 $GF(p)$상에서 0이 아닌 n 개의 원소 $x_1, x_2, \cdots, x_n$을 랜덤하게 선택한다.

② 분배자는 $GF(p)$상에서 $a_1, a_2, \cdots, a_n$을 랜덤하게 선택하고 다음과 같이 $(k-1)$차 다항식을 생성한다.

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

③ 분배자는 각 참가자 $P_1, P_2, \cdots, P_n$에게 분배할 부분 정보 S_i $(1 \leq i \leq n)$를 다음과 같이 계산하여 P_i $(1 \leq i \leq n)$ 에게 비밀리에 전송한다.

$$S_i = f(x_i) \quad (1 \leq i \leq n)$$

④ $x_1, x_2, \cdots, x_n$는 공개하고 $a_1, a_2, \cdots, a_n$와 부분 정보 S_i $(1 \leq i \leq n)$는 비밀리에 보관한다.

■ 비밀 복원 과정

비밀 복원에 참여하는 참가자의 집합을 $\{P_1, P_2, \cdots, P_t\}$라 하자.

① t 명의 참가자들은 Lagrange의 다항식 보간법에 이해 $f(x)$상의 t 개의 서로 다른 점 (x_i, s_i) $(1 \leq i \leq t)$를 이용하여 다음과 같이 $f(x)$를 계산한다.

$$f(x) = \sum_{i=1}^{t} y_i \prod_{1 \leq j \leq t,\, j \neq i} \frac{x - x_j}{x_i - x_j}$$

② 복원하고자 하는 비밀 $K = f(0)$일 경우, 다음과 같이 계산될 수 있다.

$$K = \sum_{i=1}^{t} c_i y_i \quad (\text{단}, c_j = \prod_{1 \leq j \leq t,\, j \neq i} \frac{x_j}{x_j - x_i})$$

다항식 보간법을 이용하는 Shamir의 비밀분산 방식은 $t(t \leq n)$ 명 이상의 참가자들의 협조에 의해서만 본래의 비밀 K를 복원할 수 있고 $(t-1)$명 이하의 참가자들은 비밀 K에 대해 아무런 정보도 얻을 수 없다. 이와 같은 비밀 분산을 (t, n)-threshold 방식이라 한다.

2.3.2 온라인 비밀 분산 방식

비밀 분산 방식에서 본래의 비밀 K를 복원할 수 있는 허가된 참가자들의 집합인 액세스 구조(access structure)가 동적으로 변하는 경우 즉, 임의의 참가자가 제거되거나 새로운 참가자가 참여하는 경우에 남아있는 참가자들에게 새로운 부분 정보를 비밀리에 재분배하지 않고 기존의 부분 정보를 그대로 사용할 수 있는 비밀 분산 방식을 온라인 비밀 분산 방식이라 한다.[4]

Shamir가 제안한 비밀 분산 방식은 각 참가자들이 보관해야 하는 부분 정보의 크기가 본래의 비밀 K의 크기와 거의 같고 허가되지 않은 참가자들이 비밀 K에 대해 아무런 정보도 얻을 수 없는 무조건적으로 안전한 비밀 분산 방식이라는 장점이 있지만, 비밀이 한번 복원된 이후에는 참가자들의 부분 정보를 재사용 할 수 없다는 단점이 있다. 또한 비밀을 복원할 수 있는 참가자의 집합인 액세스 구조가 변하는 경우에 분배자는 새로운 다항식을 생성하고 기존의 참가자들에게도 새로운 부분 정보를 분배해야 하는 문제점이 있다.

이러한 문제점을 해결하기 위해 C. Cachin은 온라인 비밀 분산 방식을 처음으로 제안하였다.[5]

■ 시스템 설정

- P : 비밀 분산에 참여하는 참가자의 집합 $P=(P_1, P_2, \cdots, P_n)$
- D : 각 참가자에게 부분 정보를 분배하는 분배자 (단, $D \notin P$)
- Γ : 액세스 구조(access structure) $\Gamma \subset 2^{|P|}$ X 가 Γ의 원소인 경우, X에 속하는 참가자들의 부분 정보들로부터 본래의 비밀 K를 복원할 수 있고 X가 Γ의 원소가 아닐 경우에는 비밀을 복원하는 것이 불가능함
- Γ^* : 최소 허가 집합(minimal authorized set), Γ 의 원소 중 비밀을 복원하는 데 필요한 참가자의 수가 가장 적은 것들의 집합
- K : 분산하고자 하는 본래의 비밀 정보
- S_i : 참가자 P_i에게 분배하는 부분 정보
- p : 512비트 이상의 큰 소수
- q : $q|p-1$인 큰 소수
- g : 위수가 q인 Z_p상의 원소
- $f()/h()$: 충돌 회피성 일방향 함수
- S_{p_i} : 참가자 P_i의 디지털 서명

C. Cachin은 액세스 구조가 동적으로 변하는 경우에도 기존에 분배된 부분 정보를 그대로 이용할 수 있고 본래의 비밀 K와 같은 크기를 갖는 하나의 부분 정보만을 이용하여 다수의 비밀을 복원할 수 있는 온라인 비밀 분산 방식을 제안하였다. Cachin이 제안한 방식은 모든 참가자들이 접근할 수 있는 공개 보드에 인증된 정보를 공개하고 액세스 구조가 변하는 경우에 공개 정보들의 값만을 변경하여 기존의 참가자들의 부분 정보는 그대로 유지할 수 있도록 하였다.

■ 비밀 분산 과정

① 분배자 D는 각 참가자에게 분배할 부분 정보 $S_i (1 \le i \le n)$를 랜덤하게 선택한다.

② 분배자 D는 $S_i (1 \le i \le n)$값을 비밀리에 각 참가자 P_i에게 전송한다.

③ 분배자 D는 $X \in \Gamma^*$인 X에 대해 다음과 같이 T_X값을 계산한다.

$$T_X = K - f\left(\sum_{X : P_x \in X} S_X\right)$$

④ 분배자 D는 Γ^*에 속하는 원소 X에 대해 T_X값을 공개 보드에 공개한다.

■ 비밀 복원 과정

비밀 K를 복원하기 위한 참가자 집합을 $X=\{P_1, P_2, \cdots, P_t\}$라 하자.

① 집합 X에 속하는 참가자 P_i $(1 \le i \le t)$의 부분 정보를 이용하여 다음과 같이 V_X를 계산한다.

$$V_X = \sum_{X : P_x \in X} S_X$$

② 계산한 값 V_X값에 일방향 함수 $f(x)$를 적용한다.

③ 공개 보드로부터 T_X 값을 읽어 와서 다음과 같이 비밀 K를 복원한다.

$K = T_X + f(V_X)$

Cachin이 제안한 방식은 각 참가자가 보관해야 하는 부분 정보의 크기가 본래 비밀 K의 크기와 거의 같고 계산적으로 안전한 온라인 비밀 분산 방식이다. 그리고 새로운 참가자가 참여하는 경우, 해당 참여자에게만 부분 정보를 비밀리에 안전하게 전송하고 공개 보드에 공개된 정보만 변경하면 기존의 참가자들의 부분 정보는 그대로 유지할 수 있다. 그러므로 이 방식은 참가자나 액세스 구조 또는 비밀이 자주 변경되는 키 관리, 키복구 시스템 등에 적용될 수 있다.

이 방식에서 공개 보드에 공개되는 정보는 제 3자에 의해 불법적으로 변경되지 않도록 분배자의 디지털 서명을 생성하여 공개하여야 하며, 공개되는 정보의 크기는 액세스 구조 Γ 의 크기에 비례하여 증가한다. 그러나 공개 보드의 크기는 제한되어 있으므로 전체 정보를 모두 공개하는 방식보다 비밀을 복원하는 경우에 각 참가자의 요구에 의해 해당하는 공개 정보의 값을 디지털 서명과 함께 전송해 주는 방식으로 구현하는 것이 더 효율적이라고 할 수 있다.

이 방식의 안전성은 해쉬 함수에 의존하므로 소모적 공격을 막기 위해 분산하는 비밀 K의 크기가 너무 작아서는 안 된다.

3. 키복구 기술 및 제품 분석 및 비교

3.1 키복구 시스템의 정의

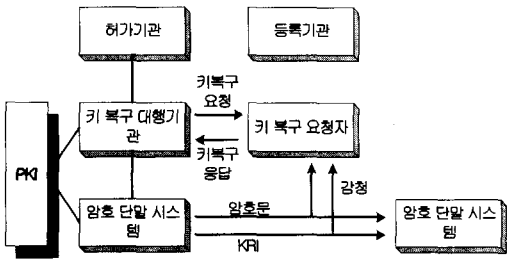
암호는 키를 소유한 사용자만이 암호화된 정보로부터 평문을 얻을 수 있다는 특성으로 인해 부작용이 발생할 수 있으며, 이러한 문제는 암호 사용자에게 큰 손실을 입히거나 사회·국가적인 위협이 될 수 있다. 이러한 문제를 인식한 세계 각 국에서는 90년대 초반부터 암호사용 시에 발생할 수 있는 부작용에 대한 해결책으로써 키복구에 대한 연구를 활발히 진행하고 있다.[1]

초기에는 키위탁이나 키 캡슐화 등과 같이 특정 방식을 나타내는 용어가 각각 사용되었으나 최근 들어서는 이러한 기술들을 모두 포함하는 의미로 키복구라는 용어가 포괄적으로 사용되고 있다.

키복구 시스템(key recovery system)은 암호문의 소유자(일반적인 암호 시스템에서 키를 소유한 사람)가 아닐지라도 사전에 약속된 어떤 특정한 조건하에서 허가된 사람에게 복호가 가능한 능력을 제공하는 암호 시스템이라고 정의할 수 있다. 여기서 미리 약속된 조건이란 암호가 나쁜 목적으로 사용되었을 경우의 법 집행 권한 확보를 위한 허가일 수도 있고, 데이터 암호용 키를 잊어 버렸을 경우가 될 수도 있다. 일반적인 암호 시스템에서는 올바른 키 없이는 해당 암호문을 복호할 수 없다. 키복구 시스템은 이러한 상황에 대비해서 제 3자가 키를 안전하게 보관하고, 일정한 조건이 갖추어졌을 때 키를 복원해주는 시스템이라고 할 수 있다.

3.2 키복구 시스템의 구성

키복구 시스템은 키복구를 수행하는 데 참여하는 여러 가지 구성요소로 이루어지며 사용되는 기술에 따라 키복구에 참여하는 구성 요소는 조금씩 달라진다. 그림 3. 은 전형적인 키복구 시스템의 구성요소와 그들의 상호작용을 보여준다.



[그림 3] 키복구 시스템의 일반적인 구성요소

[Fig. 3] General component of key-recovery system

3.3 키복구 방식

현재까지 제시된 키복구 기술은 데이터를 암호화하고 복호화하는 사용자 보안 구성요소와 키복구 기관에 의해 관리되는 복구 기관 요소, 그리고 암호문에 부가된 데이터 복구 영역에서 얻어지는 정보와 복구 기관 요소에서 획득 가능한 정보로부터 암호화된 데이터를 복구할 수 있는 데이터 복구 구성요소의 특징에 따라 크게 위탁 방식과 캡슐화 방식, 그리고 TTP 기반의 방식으로 구분된다.[6]

3.3.1 키위탁 방식

키위탁 방식은 복구될 사용자의 비밀키, 비밀키의 부분 또는 키 관련정보를 하나 이상의 신뢰기관에 위탁하는 방식으로 위탁되는 키는 사용자가 오랫동안 사용하게 되는 키(long-term key)이다. 이 방식에서는 사용자의 비밀키가 위탁 기관에 직접 맡겨져야 하므로 개인의 프라이버시가 전적으로 위탁 기관에 의존한다. 그러므로 위탁 기관의 신뢰성이 매우 중요한 문제이며 이를 보장하기 위한 방법으로 두개 이상의 위탁기관을 이용하는 비밀 분산 개념이 주로 사용되고 있다. 또한 법 집행기관에 의해 복구되는 키가 사용자의 긴 주기를 갖는 키가 아닌, 일정기간 동안만 사용하는 세션키가 되게 한다면 사용자들의 프라이버시 침해에 대한 거부감 문제도 어느 정도 해결이 가능하다. 그러나 위탁되는 키의 유효성에 대한 문제도 해결이 되어야 하는 문제점도 있다. 반면에 이러한 키위탁 방식은 유사시에 키복구를 확실하게 할 수 있는 장점이 있으며 위탁 기관의 신뢰성만 보장된다면 편리하고 안전한 키복구 방식이다.

3.3.2 키 캡슐화 방식

캡슐화(encapsulation) 방식은 키위탁 방식과는 달리 암호문을 생성하는 각 세션마다 키를 복구해 낼 수 있는 정보를 포함하는 필드를 생성해서 해당 암호 메시지에 부가시키는 방식으로 실제적인 키위탁이 일어나지는 않는다. 법 집행기관의 키복구는 복구 기관이 가진 복구키를 이용하여 암호화된 데이터에 부가된 복구 필드를 복구한 후 목적키를 얻을 수 있다. 그러므로 복구되는 키가 사용자의 긴 주기를 갖는 키(long-term key)가 아니라 세션키가 되도록 할 수 있기 때문에 도청기관의 복구 능력을 제한할 수 있게 되어 사용자의 입장에서는 키위탁 방식보다는 안전에 대한 확신을 가질 수 있다. 또한 기존의 프로토콜에서 확장 필드가 존재한다면 이를 이용하여 복구 필드를 부가시킴으로써 구현 비용의 절감과 높은 호환성이 가능하다는 장점이 있다. 그러나 복구 필드의 생성이 사용자 측에서 일어나므로 이 필드에 대한 사용자의 부정이 충분히 가능하다. 그러므로 복구 필드의 유효성 확인 과정이 반드시 필요하며 복구 기관의 신뢰성도 키위탁 방식에서와 마찬가지로 보장되어야 한다.

3.3.3 TTP(Trusted Third Party) 방식

TTP 키복구 방식은 신뢰할 수 있는 제 삼자 즉, TTP(Trusted Third party)를 가정하여 복구될 사용자의 비밀키를 그 사용자의 TTP로 지정된 기관에서 모두 생성하고 사용자에게 분배하는 방식으로 실제적인 키의 위탁은 일어나지 않으나 사용자의 긴 주기를 갖는 키(long-term 키)를 TTP가 직접 가지고 있으므로 위탁된다고 말할 수도 있다. 사용자들의 비밀키를 TTP로 지정기관에서 생성·분배하므로 각 기관들의 신뢰성 보장이 절대적이어야 한다.

키 생성시 각 사용자들의 TTP들은 비밀키를 사용하여 사용자들의 긴 수명을 갖는 키(long-term key)를 생성한다. 사용자들은 이 키를 받아 세션키를 생성하여 비밀 통신을 하게 된다.

TTP들이 사용자들의 비밀키를 모두 가지고 있으므로 유사시에 TTP에 의한 키복구가 확실히 보장되며 TTP 사이의 키 생성 방식이 연동된다면 국가간 호환성이 뛰어나다는 장점이 있다. 그러나 개인의 프라이버시가 전적으로 TTP에 의존하며 TTP의 수가 너무 많이 요구되고 이에 따르는 TTP와 사용자 사이의 병목현상과 TTP 자체 사이의 병목현상이 심하다는 단점이 있다.

3.3.4 세 방식의 특징 비교

키위탁방식은 long-term 키를 복구하는 데 적합하고 유사시 키복구를 확실하게 할 수 있으며 위탁기관의 신뢰성이 보장된다면 편리하고 안전한 방식이

다. 그러나 사용자의 비밀키가 위탁기관에 직접 맡겨져야 하기 때문에 개인의 프라이버시 문제가 발생한다.

키 캡슐화 방식은 세션키를 복구하므로 복구 기관의 능력을 제한할 수 있어 사용자 입장에서 키위탁 방식보다 개인의 프라이버시를 안전하게 지킬 수 있다는 확신을 갖게 한다. 기존 프로토콜의 확장 필드를 이용하여 복구 필드를 부가시키는 방식을 이용하면 높은 호환성과 구현 비용의 절감 효과를 얻을 수 있으나 복구 필드를 사용자가 생성하기 때문에 이 필드에 대한 사용자의 수정이 가능하므로 복구 필드의 유효성 확인 과정이 반드시 필요하다며 복구 기관의 신뢰성도 요구된다.

TTP 기반은 사용자들의 비밀키를 TTP로 지정된 기관에서 생성하고 분배하므로 각 기관들의 신뢰성 보장이 절대적으로 요구된다. TTP가 사용자의 비밀키를 모두 가지고 있으므로, 유사시에 TTP에 의한 키복구가 확실히 보장되며 TTP 사이의 키 생성 방식이 통일된다면 국가간 호환성이 뛰어나다는 장점이 있지만 개인 프라이버시 문제와 많은 수의 TTP가 필요하고 TTP와 사용자간의 병목현상과 TTP 자체의 부하가 심하다는 단점이 있다.

4. 키복구 정책동향 분석 및 비교

최근 인터넷의 급격한 보급이나, 전자상거래의 발전은 인터넷의 활용을 급속하게 증가하고 있다. 인터넷 상에서 안전한 전자상거래의 실현에 암호기술은 불가결하고, 최근의 정보 시스템의 성능 향상에 동반하여, 암호의 강도에 대한 요구수준은 나날이 높아지고 있다.

키위탁/키복구는 이용자가 비밀키 또는 그것을 복원하기위한 정보를 제삼자 기관에 위탁하여, 필요가 생긴 경우에 그의 비밀키를 제공 또는 복원하는 것이고, 암호문을 해설할 수 있게 하는 장치이다. 1993년 미국 정부에 의해 키 복구 시스템의 구상을 제안한데서 시작하였고, 그 후 몇 번의 궤도수정을 거쳐, 그 개념은 「범죄수사」로부터 「키분실 시의 대응」으로 초점이 이동하여 그의 명칭도 「recovery」가 주류가 되었다. 그러나 정책상의 초점이 법률 집행기관에 의해 암호문의 해독의 합법화로 변화하지는 않고, 법제화를 목표로 하는 정부기관과 privacy보호단체등과의 논쟁이 이어지고 있다.

4.1 미국

미국은 1993년에 발표한 Clipper Chip과 Skipjack을 기본으로 하는 Key escrow 구상 이후, 법제화를 목표로 하는 정부기관과 그것에 반전하는 privacy보호단체나 암호제품 maker와의 진통이 이어지고 있다.

<표 2> 키 복구 방식의 비교

<Table 2> Comparison of key-recovery systems

비 교	키 위 탁	키 캡슐화	TTP
키위탁 여부	위탁함	위탁하지 않음	위탁함
복구 되는키	장기간 개인키	세션키	세션키
특 징	· 확실한 키복구 보장 · 기존 프로토콜 과의 호환성 · 위탁기관의 신뢰성이 중요 · 사용자의 비밀키 노출에 대한 거부감 · 비밀정보의 집중 · 위탁된 키의 관리부담	· 사용자의 비밀정보보호 · 세션키 접근 · 사용자의 키관리 부담 없음 · 복구기관의 능력제어 · 복구 필드에 대한 사용자 부정개입 가능 · 기존 프로토콜과 호환가능	· TTP의 신뢰성이 중요 · TTP로의 병목 현상 · 확장성 및 호환성 우수

미국정부는, 1995년 12월에 키위탁 기관을 채용한 암호제품의 수출규제를 완화하는 방침을 발표하고, 키위탁 제도를 추진하는 방책으로서 암호제품의 수출규제를 이용한 approach를 하였다. 더욱이 동년 10월에는 지금까지의 시책의 궤도수정을 근거로 한 고어부통령의 공식 성명에서, 「Key escrow」에서 「recovery」로의 방향전환과, 2년 이내의 키복구 기능의 등재를 전제로서, 키길이 56bit이하의 암호제품의 수출을 허가하는 방침이 확실하게 되었다.

1996년 5월에 「키관리 기반구조(KMI: Key Management Infrastructure)」로서, 공개키 기반구조에 키위탁기관의 개념을 합친 형태이고, 수사당국의 비밀키로의 합법적인 접근을 가능하게 하는 구상을 제안했다. 더욱이 미국정부는, OECD 등을 통해서 여러 외국에 대해서도 lobby활동을 전개함으로써, 해외정부에서 키복구 제도의 채용을 추가하고, 국제협력의 관점에서 KMI를 실현에 기여하는 포석을 두고 있다.

1997년 3월에는 KMI구상을 포함한 Electronic Data Security of Act 1997로 불려지는 법안이 발표되었다. 이 법안은 키복구 기능을 포함한 PKI를 추진하는 것이었다. 실시까지는 몇 가지의 장해도 있고, 수정을 거친 법안은 어떠한 암호의 사용도 법률로 제시된 경우를 제외하면 합법적으로, 키복구 제도의 의무화를 추구하지 않고, 산업과 법집행 간의 대화에 따른다.

4.2 프랑스

프랑스에서는, 국가가 지정한 암호 시스템 이외는 이용을 인정하지 않는 등, 종래부터 통제가 강한 시책을 실시하고 있다. 그러나 90년대 후반부터는 암호시책의 규제완화를 추진하고 있다. 그 한편, 키위탁제도의 도입에서는 의욕적이고, 1996년 7월에 공표된 전기통신법의 일부개정에 있어서는

- 정보은닉을 목적으로 하는 암호장치를 이용하는 경우에, 그의 암호키를 정부에서 승인한 조직에 위탁하는 것
- 암호통신 서비스를 제공하는 사업자는, 법률집행의 틀에 기초해서, 관리하는 비밀키를 법률집행기관에 제공하는 것이 의무화되고 있다. 그 후 1998년 2월의 법령에서도 키위탁 기관에 요구되는 요건을 나타내고, 다음 3월에는
- 키위탁 기관 및 키위탁 법안이 승인된 경우, 키위탁 기관에 암호키를 위탁한 사용자는 그들의 키로 암호시스템을 자유로이 사용하는 것이 가능하게 됨.
- 키위탁기관은 어떤 특정의 상황 하에서 법률 집행기관에 키를 건네주도록 요구되는 것 등을 나타낸 법령을 시행했다. 이때 키위탁 기관으로서 유일하게 승인된 것은 SCSSI(service central de la securite des systemes d'information)이였다.

4.3 독일

독일에서는 1996년 12월에 전자서명법이 정해지고, 그 중에 「법률 집행 기관은 필요에 의하여 인증기관이 관리하는 개인정보를 얻을 수 있다」(제12조)로 하는 합법적 접근항목이 명기되었다.

다만 정부는 암호규제에 대해서는 3가지 선택을 고려하고 있다.

① 암호서비스 공급자는 위탁키를 소유하고, 필요가 있으면 그 키를 법률 집행 기관에 제공해야 한다.
② (①에 첨가하여) 암호제품의 거래에 대해서는 허가증을 필요로 한다.
③ (① 및 ②에 첨가하여) 비인가 또는 비위탁 암호를 금지한다.

1996년 12월에는 연방과 주장관이, 암호규정에 대해서 논의하고, 인가를 받는 암호만 사용할 수 있으며, 암호제작자와 분배자는 법률 집행기관에 암호의 source code와 개인 위탁키를 맡기는 것 등의 제안을 하고 있다.

4.4 영국

영국에서는 1997년 3월 무역산업성(DTI : Department of Trade and Industry)이, 암호 service의 규정을 위한 TTP의 인가에 관한 보고서를 발표했다. 이 보고서는 1996년 6월의 조사서에 따르고, 규제의 대상을 공공 네트워크에서의 암호의 사용에서 일반

적인 암호의 사용에까지 확대할 것이다. 그 주요한 목적은 TTP가 행하는 서비스에 대한의 신뢰성을 야기 시키는 것이다. 그 결과를 근거로 한 정책이 1998년 4월에 발표되었다.

제안된 법률은 암호 서비스를 제공하는 CA(Certification Authorities), KEA(Key Escrow Agencies) 등의 TTP에의 DPT에 의한 인가를 규정한 것이다. 이것에 의해 개인에게는 없는 조직에 의해서 공공이나 사업에 공급된 모든 암호 서비스(기업 내 TTP나 유료 TV에의 암호 서비스는 제외)는 정부의 지배를 받고, 인가를 받지 않은 서비스의 제공은 금지되었다.

4.5 선진국의 키복구 정책비교

고도의 정보화 사회에서 정보 보호를 위해 일반적으로 사용하는 암호의 특성 중 하나는 키를 아는 사람만이 암호화된 정보를 복호할 수 있어 기밀성을 유지할 수 있다는 것이다. 그러나 이러한 암호의 특성은 범죄자나 국의 암호정책을 이유로 자신의 관할권을 통과하는 암호화된 정보의 자유로운 흐름을 방

<표 3> 주요선진국에 있어서 키위탁/ 키복구의 개요

<Table 3> Outline of key-escrow / key-recovery system in the advanced countries

*1: Cyberspace Electronic Security Act 1999

*2 : 무기수출을 규제하는 우세나조약을 위배하게 된다(1999년 9월 1일)

국명	recovery system	키복구 기관	인증기관	암호제품의 수출입규제	기타
미국	수출암호제품에 키 위탁기능 탑재(계획가능)을 의무화. 1999년 12월에 철폐예정	· 키위탁기관의 틀을 만드는 중. · 비위탁키의 이용은 자유. · 경찰은 제3자가 보유하고 있는 암호문을 해독하기위한 키의 사용허가를 법정에 요구가능.	· 연방정부수준에서 법안 단계. · 유타주, 워싱턴주에서는 인증기관에 대한 임의의 자격제도를 도입. · 캘리포니아주에서는 면허를 의무화.	수출 · 64bit이하 사전제품제출 · 64bit초과 사전심사필요 terror의 위험이 있는 7개국에는 수출금지	· 범죄정보의 비밀화 목적의 암호이용을 처벌하는 법안*1 제출 · FBI내에 암호해독 기술을 연구하는 센터 설립
프랑스	위탁키 이용자는 그의 키로 자유롭게 암호이용	· KEA는 필요에 따라 위탁키를 법집행기관에 인도가 필요. · 인가KEA의 후보는 SCSSL	· 인증기관에 대한 면허제도의 의무화는 하지 않는 방향. · EU국 및 기타의 국제기관의 방향을 모방할 방침	· 중명 목적제품 vender의 신청으로 무제한 · 40 bit이하 : vender의 신청으로 무제한 · 40bit초과 : 공급, 수출입 : 수상의 허가필요 이용 : 서전의 허가, SCCI검사	· 종래는 암호의 사용에 수상의 허가가 필요했지만, 1996년, 1998년의 법개정으로 완화
독일	키 위탁기술을 이용한 제품에 보증을 부여. 마음대로 사용	—	· 인증기관에 대한 임의의 자격제도를 도입	· 수출: 자유화 고도의 암호기술을 가진 software 제품*2	· 기본적으로는, 암호를 이용하는 자유를 보장. · 법률 집행 기관은 필요에 의해 인정기관의 개인정보를 입수가능
영국	키위탁/키복구제도 장려. 의무화하지 않음	· TTP는 필요에 따라 위탁키를 정부에 제공이 필요	· 인증기관과 KEA를 구별. · 어느 쪽이든 임의의 자격 인증 제도를 도입하는 방향	· 수출: 인가필요	· 평문 · 해독키 · pass word의 요구권이 있음

해할 수 없다.

선진 각국의 암호 정책은 자국 내에서의 암호사용 규제, 암호 관련 기술 및 제품의 수출입 제한, 암호의 불법 사용에 대한 법집행력 확보로 귀결된다고 볼 수 있다. 대부분의 선진국에서는 자국 내에서의 암호 사용을 자유롭게 허용하고 있으나 일부 국가에서는 강력한 규제를 하고 있다. 그리고 많은 국가들은 암호 기술 규제의 필요성에 대해서는 합법적인 접근권과 관련하여 유동적인 양상을 보이고 있다. 한편 암호기술 및 제품의 수입은 대다수의 국가에서 제한을 하지 않고 있으나 수출에 대해서는 까다로운 규정을 두고 있어 자국의 암호기술이 외국으로 유출되는 것을 방지하고 있다.

키복구 정책에 있어서 암호사용 규제와 연관성이 있어 각국에서는 조심스런 접근을 하고 있으며 암호 정책은 법집행 기관의 접근보다는 전자상거래 활성화와 프라이버시 보호 등을 위해서 필요하다는 인식을 하고 있다. 그러나 일부 국가에서는 법집행력 확보와 사용 규제를 연계하려는 정책이 논점이 되고 있고 그들은 이러한 정책을 통하여 자국의 불법적인 암호사용을 규제하는 한편 원활한 법집행을 확보하고자 하는 것이다. 키복구 정책에서는 프라이버시 보호라는 기본권과 상충되는 면을 지니고 있어 정부와 개인의 이익을 최대한 보장할 수 있는 균형점을 찾는 것이 관건일 것이다.

향후 선진국의 암호 정책은 전자상거래 등의 진흥을 위해 활발하게 논의될 것이고 자국 내에서의 암호 사용 규제는 최대한 보장하나 정부의 접근권을 어떠한 형태로든 고려할 것이다. 그것은 접근권 확보를 위한 암호사용 규제의 필요성에는 공감하기 때문이다. 그러나 실현 방법에서는 시각차이가 있으며 법제화되기에는 상당한 시일이 요구될 것으로 보인다. 그리고 선진국에서는 자국의 기술 보호를 위해 수출에 대해서는 더욱더 규제가 강화될 것으로 보이고 암호 정책 수립 과정이나 수출 허가 과정에서 정보기관의 직·간접적인 개입이 더욱더 증가할 것으로 예상된다. 따라서 이러한 선진국의 정책적 입장과 흐름을 고려하여 우리의 키복구 정책 관련의 법제도를 보안하는 접근이 필요할 것이다.

5. 결론

정보 시장의 창출로 인한 정보의 접근가능성이라는 긍정적 측면이 있음과 동시에 정보의 노출로 인한 정보의 침해가능성이라는 부정적 측면을 동시에 초래하였다는 점이다. 이것은 특히 인터넷상의 모든 정보가 디지털화된 것이라는 점에서 더욱 그러하다. 디지털화된 정보는 복제가 쉬울 뿐 아니라 그 복제의 사실을 인식하기 어렵고 위조나 변조의 경우도 이를 쉽게 포착하기 어려우며 비록 원거리에 위치하더라도 통신망을 이용하여 자료원에 쉽게 접근할 수 있기 때문이다. 또한 인터넷을 기반으로 하는 인터넷 전자상거래의 성장은 해를 더해 갈수록 가히 폭발적이어서 안전한 전자상거래의 확보를 위한 정보보호의 필요성은 불가결한 요소가 되었다.

이러한 정보를 보호하기 위해 많은 방법들이 제시되고 있다. 물리적인 접근을 통제하는 것으로부터 비밀번호의 다단계 이용, 컴퓨터 운영체제의 강화 등 많은 수단이 있다. 그러나 컴퓨터 시스템과 각종 통신에서 저장과 교환의 대상이 되는 정보의 직접적인 보호가 가장 기본적이고 안전한 수단이며 또한 최후의 방법으로 논의된다. 그리고 정보의 직접적인 보호는 평이한 정보를 암호화된 정보로 만드는 것이다.

암호는 여러 가지 이점을 주는 도구로서 자료의 무결성과 기밀성을 보장하는 것은 물론 개인의 프라이버시를 보호하고, 더 나아가 국가의 이익을 지키는 수단을 제공한다. 그러나 암호가 정당하지 못하게 사용된다면 그로 인한 역효과는 대단히 클 것이다. 범죄자는 자신의 범죄행위를 감추기 위해 암호를 사용할 것이고, 마약거래, 국제 테러 등 여러 가지의 범죄 행위에 이용할 것이다. 따라서 정부의 법집행력은 약화되고 공공의 안녕과 국가 안보를 유지하는데 위협이 아닐 수 없다.

선진 각국의 암호 정책은 대체적으로 국내에서의 암호사용규제, 암호 관련 기술 및 제품의 수출입규제, 정부의 합법적인 접근권을 보장하기 위한 수단 등에 따라 특성을 갖는다. 대부분의 국가에서 암호 사용의 자유를 보장하고 있으나 접근권을 확보하기 위한 방안을 모색하고 있고, 암호제품 및 기술의 수출에 대해서는 대부분의 국가에서 규제를 하고 있다. 정부의 적법한 접근을 보장하기 위해서 미국 등 선진국에서는 키복구 시스템의 도입을 놓고 논의가 활

발히 전개되고 있다. 키복구 시스템은 사용자의 비밀키를 보관함으로써 개인의 프라이버시를 침해할 우려와 비용, 시스템의 복잡성, 키 보관상의 문제점 등으로 인한 비판을 받고 있으나 뚜렷한 대안은 없는 실정이다. 따라서 키복구 시스템은 접근권 확보라는 명제를 해결할 방안으로 지속적인 연구가 진행될 것이고, 아울러 암호 분야의 연구개발을 촉진하고 관련 산업을 지원할 수 있는 법제도 또한 뒷받침되어야 할 것이다. 본 논문의 결과는 우리나라 전자거래를 위한 키 복구 정책을 설정하는데 유용하게 활용될 수 있을 것이다.

※ 참고문헌

[1] 한국정보보호센터, "키복구 정책 동향 보고서", 연구보고서, 1998

[2] 일본경찰청,"情報セキュリティビジョン策定委員會"보고서, http://www.npa.go.jp, 1998.3

[3] A. Shamir, "How to share a secret", Communication of the ACM, 21, pp.120-126, 1979

[4] G.R.Blakely,"Safeguarding cryptographic key", In Proceeding of AFIPS National Computer Conference, pp.313-317, 1979

[5] C.Cachin, "On-line secret sharing", In C.Boyd, editor, Proceeding of the 5th IMA conference in Cryptography and Coding, pp.190-198, Springer-Verlag, 1995

[6] 전자통신연구원, 정보기술연구본부"CMS 프로토콜검증기술", http://technomart.etri.re.kr/, 1999.11

[7] 한국정보보호진흥원, 공개키 기반구조, http://www.kisa.or.kr/technology/sub1/PKI.htm, 2001.2.

이 병 수

1975. 2 한양대학교 전자공학과 졸업
1982. 2 건국대학교 대학원
1985. 2 건국대학교 대학원 신호처리 전공 공학박사
1988. 3 순천향대학교 정보기술공학과 교수 (현재 재직중)

조 시 용

1973. 2 서울대학교 학사
1991. 8 연세대학교 산업대학원 공학석사
1993. 6 미국 오하이오대 이학석사
2002.6 순천향대학교 전기전자공학(정보통신전공) 박사