증명가능한 비밀 분산 방식을 이용한 키 복구 시스템에 관한 연구

채승철*0, 김해만*, 이인수**, 박성준**, 이임영*
*순천향대학교 컴퓨터학부 **한국정보보호센터

A Study on the Key Recovery System using Verifiable Secret Sharing Scheme

Seung-chul Chae*0, Hae-man Kim, In-soo Lee**, Sung-jun Park**, Im-yeong Lee*
* Dept. of Computer Science, Soonchunhyang Univ.
** Korea Information Security Agency

요 약

암호의 사용은 사용자에게 많은 이점을 주지만, 키와 분실이나 범죄 집단의 암호의 악용과 오용 등의 가능성이 있다. 이러한 것을 해결하기 위해 나온 방식이 키 복구(key recovery)방식이다. 본 논문에서는 비밀 분산 방식을 이용한 새로운 키 복구 방식을 제안한다. 또한 키 복구 시스템에서는 유사시에 키를 얻을 수 있는 확실한 보장이 있어야 하는데, 본 제안 방식에서는 사용자의 부정조작을 검사할 수 있게 함으로써 키 획득에 대한 보장을 할 수 있도록 하였다.

1. 서론

현대 사회에서 모든 정보들은 점차적으로 종이 문서의 형태에서 전자적 형태로 변환되어 전달되어지고 있다. 이미 개인간의 전화, 팩스, E-mail 등의 이용은 보편화되었으며, 개개인의 건강/인사 기록과 같은 사적인 정보에서부터 은행간의 거래, 중요한 사업상의 정보 등의 기밀성을 요하는 자료 및 비행관제 시스템, 교통 정보 시스템 등과 같은 국가 기간망에 이르는 많은 정보들이 전자적 형태로 이동되고 있다. 이처럼 전자적인 정보의 유통량이 증가하고 정보의 가치가 높아질수록 정보 보호의 문제가 부각된다. 정보 보호란 보다 안전하고 신뢰성 있게 정보를 전달할 수 있도록 하는 것으로 암호학에 그 기반을 두고 있다. 암호란 키와 수학적인 알고리즘을 이용하여 평문을 알아보기 힘든 암호문의 형태로 변환시키는 것으로, 안전하게 구현된 암호 시스템에서는 키를 알지 못하는 사람은 암호화된 데이터를 복호할 수 없다는 것을 전제로 한다.

암호의 사용은 정보의 누출 및 오용을 방지하고 상대의 신원 확인을 가능하게 함으로써, 온라인상에서의 전자상거래나 전자 계약을 가능하게 하는 등 많은 장점을 가지고 있다. 그러나 암호는 본래 가지고 있는 키 관리의 어려움 때문에 다음과 같은 문제가 발생할 수 있다.

첫째, 키의 분실이나 손실로 인해 사용자가 자신의 키(또는 암호문)에 접근할 수 없을 경우이다. 이 경우에는 자신이 적법한 소유자임에도 불구하고 자신의 정보에 대하여 접근을 할 수 없음으로 해서 많은 손실을 가져올 수 있다.

둘째, 국가가 범죄 수사 등의 적법한 이유로 키(또는 암호문)에 접근해야 할 필요성이 있을 경우에 발생되는 문제점이다. 범죄자는 암호문을 사용함으로써 합법적인 수사를 방해할 수 있다.

셋째, 암호가 오용됨으로써 발생할 수 있는 잠재적인 위협이다. 사업장에서 피고용인이 중요한 정보를 암호화하고 키를 담보로 금품을 요구할 수도 있으며, 키의 도난이나 손상 등의 위협이 항상 존재한다.

본 논문에서는 이와 같은 위협에 대응하기 위하여 비밀 분산에 기반한 안전한 키 복구 방식(Key Recovery System)을 제안한다. 먼저 2장에서 키 복구 방식과 비밀 분산에 대한 개념과 구성 방식을 소개한다. 3장에서는 안전한 키 복구 방식에 대한 요구사항 및 새로운 방식을 제안하며, 4장에서 결론을 맺기로 한다.

2. 기본 개념

2.1 비밀 분산(Secret Sharing) 방식

비밀 분산에 대한 개념은 Shamir[1]와 Blakley[2]가 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. 각각의 분할된 정보를 shadow라고 한다.

이것은 안전성과 효율성을 위해 n개의 shadow가 있을 때 k(≤n)개의 shadow만을 모으면 비밀 정보가 복구 가능하도록 구성될 수 있다. 이것을 (k, n) threshold 방식이라고 하며 다음과 같은 성질을 갖는다.

- 비밀정보 S는 n개의 shadow로 분할된다.
- k개 이상의 shadow를 모으면 S는 쉽게 계산된다.
- k-1 이하의 shadow는 S에 대한 아무런 정보도 주지 않는다.

2.1.1 Shamir가 제안한 비밀 분산 방식[1]

비밀을 알고 있는 분배자는 다음과 같은 형태의 다항식 $f(x)$를 만든다.

$$f(x)=a_{k-1}x^{k-1}+\ldots+a_1x+S \pmod p$$

여기서 $a_1 \ldots a_{k-1}$ 은 [0, p-1]에서 랜덤하게 선택하고, S(≥0)는 비밀정보, p는 큰 소수로 한다.

분배자는 다음을 계산해서 참여자 P_i에게 안전하게 전송한다.

$$S_i=f(i) \bmod p \ , \ 1\le i\le n$$

k개 이상의 비밀 조각이 모이면 k개의 서로 다른 점 $(x,y)=(i,S_i)$ 을 알 수 있고, 이 정보를 기반으로 Lagrange의 보간법에 의해 $f(x)$의 지수 $a_j(1\le j\le k-1)$ 를 계산할 수 있다. 비밀정보는 다음에 의해서 계산된다.

$$f(0)=S$$

k차의 다항식 $f(x)$의 지수를 모를 때, 점 (x_i,y_i) $(1\le i\le k)$이 주어지면 다음의 Lagrange 보간법의 공식에 의해 다항식이 구해진다.

$$f(x)=\sum_{i=1}^{k} y_i \prod_{1\le j\le k,\ j\ne i} \frac{x-x_i}{x_i-x_j}$$

$f(0)=S$ 이기 때문에 분산된 비밀은 다음과 같이 표현된다.

$$S=\sum_{i=1}^{k} C_iY_i \quad \left(C_j=\prod_{1\le j\le k,\ j\ne i} \frac{x_j}{x_i-x_i}\right)$$

이와 같은 방식은 분배자를 신뢰한다는 가정하에 이루어진다. 하지만 일반적인 경우에 있어서는 분배자가 올바른 shadow를 보내는지 확인해야 할 필요성이 있다. 이러한 문제를 해결하기 위해서 확인 가능한 비밀 분산(Verifiable Secret Sharing) 방식이 제안되었다. 본 논문에서는 이러한 확인 가능한 비밀 분산 방식 중에서 비대화형 증명 가능한 비밀 분산(non-interactive verifiable secret sharing) 방식[3]을 이용한다.

이 방법은 Shamir[1]의 방법을 위탁(Commitment) 방식과 조합하여 확장한 방식으로 다음과 같이 구성된다.[3]

2.1.2 위탁 방식(Commitment Scheme)

어느 누구도 $\log_g(h)$를 계산할 수 없는 G_q의 원소 g와 h를 선택한다(G_q는 위수가 q인 Z^*_p의 부분집합, p, q는 큰 소수, g와 h는 신뢰기관에 의해 선택된다). 위탁자는 $t\in Z_q$를 랜덤하게 선택해서 $s\in Z_q$에 대해 다음을 계산한다.

$$E(s,t)=g^sh^t$$

이와 같은 위탁은 이후에 s와 t를 밝힘으로써 공개된다. E(s, t)는 s에 대한 아무런 정보도 포함하고 있지 않으며, 위탁자는 $\log_g(h)$를 풀지 않는 한 s를 $s'\ne s$로 공개할 수 없다.

2.1.3 비대화형 증명 가능한 비밀 분산 (Non-Interactive Verifiable Secret Sharing) 방식

이 방법은 shadow의 수신자가 분배자나 다른 수신자와 상호 작용하지 않고 자신의 shadow가 올바른 것인지 확인 할 수 있다.

위의 위탁 방법과 같은 $g, h \in Z_q$를 선택한 후, $s \in Z_q$를 다음과 같이 분배한다.

1) 분배자는 다음과 같은 s를 위탁하기 위한 E_0를 계산한다.

$$E_0 = E(s,t) = g^s h^t (t \in Z_q \text{는 랜덤})$$

2) 분배자는 $F(0)=s$ 를 만족하는 k-1차의 다항식 $F \in Z_q[x]$를 선택하고 다음의 shadow 정보 s_i를 계산한다.

$$s_i = F(i) \quad (i=1, ..., n)$$

3) 위에서 선택된 임의의 다항식을 $F(x) = s + a_1 x + ... + a_{k-1} x^{k-1}$ 이라 하자. 분배자는 $b_1,...,b_{k-1} \in Z_q$ 를 랜덤하게 선택하고 b_i를 이용해서 다항식의 지수 a_i (i=1,...,k-1)를 위탁하기 위한 E_i를 다음과 같이 계산한다.

$$E_i = E(a_i, b_i) \quad (i=1,...,k-1)$$

4) $G(x) = t + b_1 x + ... + b_{k-1} x^{k-1}$ 이라고 할 때 다음과 같은 shadow 확인 정보 t_i를 계산한다.

$$t_i = G(i) \ (i=1,...,n)$$

5) 분배자는 (s_i, t_i)와 E_i(i=0, ..., k-1)를 수신자 P_i(i=1, 2, ... , n)에게 안전하게 전송한다. P_i가 자신의 shadow와 확인정보 (s_i, t_i)를 받으면 다음을 양변의 결과가 일치하는지 확인한다.

$$E(s_i, t_i) = \prod_{j=0}^{k-1} E_j^{i^j}$$

6) 이후에 비밀 정보는 다음과 같이 계산된다.

$$s = \sum_{i \in s} a_i s_i \quad (a_i = \prod \frac{i}{i-j} \quad)$$

2.2 키 복구 시스템(Key Recovery System)

키 복구 방식의 정의는 사전에 약속된 어떤 특정한 조건하에서 허가된 개체에게 암호문의 키나 평문의 복구가 가능한 능력을 제공하는 기법이라고 할 수 있다.

이러한 키 복구 시스템은 크게 두가지로 분류할 수 있다. 첫 번째는 비밀키 위탁 방식(Key Escrow)으로 자신의 비밀키의 일부 또는 전부를 특정한 방법으로 복구 기관이나 기타 신뢰 기관(Trusted Third Party)에 위탁하는 것이다. 이 방법은 복구가 필요할 때 비밀키를 얻게 되므로 유사시에 키(또는 평문)을 얻을 수 있는 확실한 보장이 되며, 해당 사용자의 모든 암호화에 관련된 행동에 대한 확인이 가능하다. 이러한 속성은 범죄 수사나 범죄 방지 등에는 매우 유용하게 사용될 수 있으나, 일반 사용자의 입장에서는 프라이버시의 침해에 대한 우려와 같은 이유로 인해 거부감을 느낄 수 있다. 또한 키가 유출되면 해당 사용자가 키를 바꾸기 전까지는 복호화 뿐만 아니라, 키를 사용한 인증이나 서명과 같은 다른 기능에 대한 위/변조가 가능하기 때문에 위탁된 키를 보관하는 보관 기관의 신뢰성과 보관 방법의 안전 등이 보장되어야 한다. 이러한 방식으로는 Clipper라고 불리우는 미국의 EES(Escrow Encryption Standard)[5], 영국의 GCHQ 프로토콜[6] 등이 있으며, 이에 대한 여러 가지 문제점과 개선 방향에 대한 연구가 진행되었다.[7][8]

두 번째로 키 복구 필드(Key Recovery Field)를 생성해서 암호문에 부가한 후, 복구가 필요한 경우 이 영역에 포함된 정보를 바탕으로 암호화에 사용된 키나 평문을 복구하는 캡슐화(Encapsulation) 방식이 있다.

이 방식은 키 위탁 방식과는 달리 비밀키 정보의 위탁이 일어나지 않고, 해당 암호문을 복구 할 수 있는 세션키(session key)만을 이용하기 때문에 키 복구시에 발생할 수 있는 문제점을 줄일 수 있다. 하지만 이 방식의 경우 사용자가 생성하여 암호문에 부가하기 때문에, 복구 필드에 대한 수정이나 조작이 가능해서 유사시에 키를 얻을 수 없는 경우가 발생할 가능성을 내포하고 있다. 일반적으로는 TIS사의 RecoveryKey[9], IBM사의 SecureWay[10] 등과 같은 상용 시스템에서 이런 방식을 적용하였다.

2.3 기존 키 복구 방식의 안전성

키 복구 시스템에 대한 많은 방식이 제안되어 왔으며[4], 또한 많은 공격 방법이 존재한다. 본 절에서는 키 복구 시스템이 갖추어야할 요구 사항을 정의하고, 공개키에 근거한 방식 중에서 인증필드의 조작 문제에 대하여 고찰한다.

일반적으로 키 복구 시스템이 갖춰야 하는 요구조건은 다음과 같다.

1) 무결성과 기밀성을 만족해야 한다.
2) 널리 사용될수 있도록 유연한(flexible) 방식을 가져야 한다.(정책 등에 상관없이 국제적으로 통용

될 수 있어야 한다.)

3) 사용자가 안전도를 확신할 수 있도록 복구 방식의 상세한 부분들은 공개되는 것이 바람직 하다.
4) 법 집행을 방해해서는 안된다. 범죄자 등의 수사를 위한 도청이 가능해야 한다.
5) 오용이 어려워야 하고 오용의 감지는 쉽게 할수 있어야 한다.
6) 마스터 키로 도청이 시작되면 그 이후의 통신은 모두 노출되므로 도청 시간의 제한에 대한 보장이 필요하다.
7) 새롭게 개발된 알고리즘의 적용이 용이해야 한다.
8) 누구나 쉽게 사용할 수 있어야 하고, 비싸지 않아야 한다.

일반적으로 공개키를 이용하면 사용자의 암호화된 메시지는 다음과 같은 요소로 구성되어 간단하게 키 복구를 구현할 수 있다.

1) 랜덤한 세션키를 선택 한 후 그 키를 이용해서 암호화된 메시지
2) 수신자의 공개키로 암호화된 세션키
3) 복구기관의 공개키로 암호화된 세션키

위와 같이 구성된 복구정보를 메시지에 부가하면, 복구기관이 메시지를 복원할 필요성이 있을 경우에 자신의 공개키로 세 번째 영역을 복구해서 세션키를 얻을 수 있다. 이 방법에서는 사용자의 키를 위탁할 필요가 없다. 단지 통신에 사용되는 임시적인 세션키에 대한 접근 능력을 부여해 주면 된다. 이와 같은 개념은 몇가지 복구 방식의 기반을 이루고 있다.(AT&T CryptoBackup, TIS commercial key escrow)

그러나 이 개념의 중요한 약점은 세번째 영역이 정말로 올바른 세션키를 포함하고 있는지를 검사할 수 없다는 것이다. 이것은 복구 기관이 복호를 시도해 볼 때까지는 알 수 없다. 제안 방식에서는 이러한 검사 시점을 암호문을 평문으로 바꾸는 복호 시점에서 좀더 앞당길 수 있도록 한다.

3. 제안 방식

3.1 개념

앞서 살펴본 바와 같이 인증필드를 이용할 경우 해당 인증 필드에 대한 조작이 가능하다는 단점이 있다. 이것을 방지하기 위해서는 다음과 같은 조건을 만족시켜야 한다.

조건 i) 사용자가 키 복구 시스템을 사용하면 적법한 절차에 따라 키를 복구할 수 있어야 한다.

조건 ii) 사용자가 키 복구 시스템을 사용할 때 인증필드에 대한 조작을 수행하면, 감지(detect)가 가능하거나 암호시스템을 사용할 수 없어야 한다.

이러한 두 조건을 만족하는 시스템은 사용자가 수신자에게는 메시지를 보내면서 복구기관은 복구를 할 수 없도록 하는 부정조작을 막을 수 있다.

본 방식에서는 이와 같은 조건을 만족시키기 위해 확인 가능한 비밀 분산(Verifiable secret sharing)를 이용하여 인증필드를 다음과 같은 세 영역으로 구분한다.

영역 1) 송신자가 수신자에게 보내는 데이터 암호화 키에 대한 shadow 정보(수신자의 공개키로 암호화)

영역 2) 송신자가 복구 기관에게 보내는 데이터 암호화 키에 대한 shadow 정보(복구기관의 공개키로 암호화)

영역 3) 복구 기관을 포함한 제 3자의 확인이 가능한 키에 대한 shadow 정보(평문 정보)

수신자는 첫 번째와 세 번째 영역을, 복구 기관은 두 번째와 세 번째 영역을 이용해서 키를 얻게 된다. 세 번째 영역에 들어가는 shadow 정보는 평문으로 공개되어 수신자와 키 복구 기관을 비롯한 모든 사용자가 볼 수 있다. 이중에서 세 번째 영역은 다음과 같은 조건을 만족한다.

영역 3 조건 i) 제 3자는 해당 필드로부터 키와 관련된 아무런 정보도 얻을 수 없어야 한다.

영역 3 조건 ii) 제 3자는 해당 필드가 올바른지 여부를 알 수 있어야 한다.

3.2 구성 방식

본 절에서는 제안된 방식에서 키 복구 필드를 구성하는 방법을 소개한다.

• 사전 계산 단계

1) 송신자는 자신이 전송하고자 하는 평문을 랜덤한 세션키를 가지고 암호화한다.

$C = E_s(M)$ (s : 세션키)

2) 송신자는 암호화에 사용된 키 s를 이용해서 다음과 같은 위탁 방식에 근거해서 키를 위탁하기 위한 정보 E_0를 계산한다.

$$E_0 = E(s,t) = g^s h^t$$

($g, h \in G_q$, $s \in Z_q$ $t \in Z_q$는 랜덤)

여기서 g, h는 사전에 복구기관에 의해 선택되어 모두가 알고 있는 공개 파라미터이다.

3) 송신자는 $F(0)=s$를 만족하는 1차 함수 $F \in Z_q[x]$를 선택한 후 다음을 계산한다.

$$s_i = F(i) \quad (i=1, 2, 3)$$

4) $F(x)=s+ax$ 이라 하자. 송신자는 $b \in Z_q$을 랜덤하게 선택하고 b을 이용해서 a를 위탁하기 위한 정보 E_1을 계산한다.

$$E_1 = E(a,b) = g^a h^b \quad (i=1,...,k-1)$$

5) $G(x)=t+bx$ 라고 할 때 다음의 확인 정보 t_i를 계산한다.

$$t_i = G(i) \ (i=1, 2, 3)$$

• 복구필드 생성 단계

1) (s_1,t_1)을 수신자의 공개키로 암호화한다.

2) (s_2,t_2)를 복구기관의 공개키로 암호화한다.

3) (s_3,t_3)와 계산된 s와 a의 위탁 정보 E_0,E_1를 연접(concatenation)한다.

4) 1, 2, 3 항목을 연접하고, 송/수신자의 식별자, 복구기관의 식별자, 사용된 암호 알고리즘 등과 같은 부가 정보를 붙인 후 자신의 공개키로 서명한다.

5) 위와 같이 구성된 복구 필드를 1단계에서 암호화한 암호문 C와 연접한다.

• 복구 필드의 조작유무 확인

1) 수신자는 복구 필드중 첫 번째 영역을 자신의 비밀키로 복호한 후, shadow (s_1,t_1)를 가지고 다음을 확인한다.

$$g^{s_1} h^{t_1} = E_0 \ E_1^{\ 1}$$

2) 복구기관은 복구필드 중 두 번째 영역을 자신의 비밀키로 복호한 후, shadow (s_2,t_2)를 가지고 다음을 확인한 후 안전하게 저장한다.

$$g^{s_2} h^{t_2} = E_0 \ E_1^{\ 2}$$

3) 세번째 영역은 복구 기관을 포함한 제 3자의 확인이 가능하다.

$$g^{s_3} h^{t_3} = E_0 \ E_1^{\ 3}$$

• 세션키 정보 확인

다음과 같은 연립 방정식의 해를 구함으로써 수신자나 복구기관은 세션키 s을 얻을 수 있다.

1) 수신자 : 영역 1과 3의 정보를 이용해서 세션키를 재조합한다.

$$s = s_1 - a*1 \ , \ s = s_3 - a*3$$

2) 복구 기관 : 영역 2와 3의 정보를 이용해서 세션키를 재조합한다.

$$s = s_2 - a*2 \ , \ s = s_3 - a*3$$

3.3 고찰

1) 안전성 고찰

제안된 방식은 다음과 같은 안전도를 갖는다. 첫 번째 영역은 수신자만이 자신의 비밀키로 복구할 수 있다. 두 번째 영역은 복구 기관만이 자신의 비밀키로 복구할 수 있다.

비밀 분산(secret sharing)의 개념에 의해서 세 번째 영역에 공개된 shadow는 키에 대한 어떠한 정보도 포함하지 않는다.(정보량의 측면에서 안전하다.) 즉, 복구 필드는 전체 시스템의 비도에 영향을 미치지 않는다.

2) 송신자의 부정 조작에 대한 고찰

송신자가 위와 같은 복구 프로토콜에 따른다면 복구기관은 두 번째와 세 번째 영역의 shadow를 조합하여 키를 재구성할 수 있다. 세 번째 영역에 대한 shadow를 조작한다면 수신자조차도 암호화에 사용된 키를 얻을 수 없다.

송신자가 복구 기관에게 전송되는 정보를 조작하면 확인 단계에서 shadow를 확인 가능한 성질에 따라 암호문을 해독하지 않고도 조작 여부를 알 수 있다. 이러한 성질은 위에 기술한 조건 i)를 만족한다. 복구 기관은 자신의 공개키로 암호화된 정보를 비밀키로 복호한 후에 올바른 shadow인지를 확인하고, 저장해 두거나 랜덤하게 추출된 임의의 통신문에서 이와 같은 작업을 수행함으로써 사용자의 부정 조작을 검출하거나 방지할 수 있다.

3) 요구조건에 대한 만족도

제안된 방법은 다음과 같이 요구조건에 부합된다. 제안된 복구 시스템 자체가 비도에 영향을 미치지 않기 때문에 무결성과 기밀성을 만족해야 한다는 요구조건 1)을 만족시킨다. 제안된 방식에서는 유사시의 키 복구를 할 수 있는 기능을 제공하며(요구조건 4), 함수의 선택을 n차로 확장함으로써 복구기관의 수를 늘릴 수 있으며(요구조건 2), 모든 암호 알고리즘에 대한 적용이 가능하다(요구조건 7).

또한 이 방식은 모든 알고리즘이 공개되어도 안전도에 영향을 미치지 않으며(요구조건 3), 소프트웨어로 구현 가능하기 때문에 구현물의 가격을 저렴하게 할 수 있다(요구조건 8). 도청 시간의 제한 문제와 같은 것들은 세션키를 사용하거나 기존에 제안된 여러 방법을 도입함으로써 해결이 가능하다(요구조건 6).

4. 결론

본 논문에서는 암호 사용시에 발생할 수 있는 키의 분실 및 암호의 오용이나 악용을 방지하기 위한 새로운 키 복구 방식을 제안하였다. 키에 대한 적법한 접근이 필요할 때 올바른 키를 얻을 수 있도록 키 복구 필드의 구성 방법 및 복구 필드의 조작에 대한 방지와 검출이 가능하도록 한 방식을 제안하였다. 이 방식은 앞서 살펴본 바와 같이 암호문을 복호하지 않고서도 복구키의 조작 여부를 알 수 있다. 또한 키를 사용하는 모든 암호화 알고리즘에 적용 가능하며, 다양한 암호 정책과 모델에 적용할 수 있다. 구현은 소프트웨어나 하드웨어 모두 가능하며, 프로토콜의 확장과 가상의 수신자를 지정함으로써 복구 기관을 쉽게 추가하거나 바꿀 수 있다. 그리고 복구 기관의 신뢰도를 높이기 위해서는 복구기관의 비밀키를 비밀 분산을 사용하여 분배하거나 암호문의 성격에 따라 복구 기관 선택을 사용자가 하는 등 기존에 제안되었던 방식의 적용이 가능하다.

* 본 연구는 '98년 정보통신 산학연 공동 기술 개발 과제인 "키 복구 기능을 갖는 안전한 전자 우편 시스템 개발" 과제로서 수행중입니다.

[참고 문헌]

[1] A. Shamir, "How to share a secret", Communications of the ACM, Vol. 22, pp 612-613, 1979

[2] G.R. Blakley, "Safeguarding cryptographic keys", In Proceedings AFIPS 1979 Nat. Computer Conf., pp 313-319, 1979

[3] Torben Pryds Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing", Advances in Cryptology-CRYPTO '91 Proceedings, pp 129-140, 1991

[4] Dorothy E.Denning, "A Taxonomy for Key Recovery Encryption System", Communications of the ACM, Vol. 39, pp 34-40, 1996

[5] Dorothy E. Denning and Miles Smid, "Key Escrowing Today", IEEE Communications, Vol. 32, pp. 58-68, 1994

[6] "Securing electronic mail within HMG part I. Infrastructure and protocol", draft c. http://www.rdg.opengroup.org/public/tech/security/pki/casm/casm.htm, 1996.

[7] Silvio Micali, "Fair Cryptosystems", Advances in Cryptology-CRYPTO '92, 113-138, 1992

[8] Ross Anderson, "The GCHQ protocol and it's problems", EURO-CRYPTO '97, pp. 134-148, 1997

[9] Stephen T. Walker, Stephen B. Lipner, Carl M.Ellison, and David M. Balenson, "Commercial Key Recovery", Communications of the ACM, Vol. 39, pp. 41-47, 1996

[10] Rosario Gennaro, Don Johnson, Paul Karger, Mike Matyas, Mohammad Peyravian, Allen Roginsky, David Safford, Michael Willet, Moti Yung and Nev Zunic, "Secure Key Recovery", IBM Technical document, 1997

[11] 이임영, 채승철, "Key recovery 시스템에 관한 고찰", 한국통신정보보호 학회지, 제 7권 4호, pp. 45-58, 1997

[12] 최용락, 소우영, 이재광, 이임영, "통신망 정보보호", 도서출판 그린, 1996