새로운 키 위탁 시스템의 설계
(Design of a New Key Escrow System)

황 보 성 † 이 임 영 ††
(Bo-sung Hwang)(Im-yeong Lee)

요 약 암호 시스템에서 가장 중요한 정보는 키 정보이다. 그러므로 공개 네트워크 상에서 비밀키의 관리는 아주 중요하다. 키가 손상되거나 유실되면 모든 정보가 유실되기 때문이다. 키 위탁 시스템이란 유사시의 상황에 대비해서 키를 특정한 위탁기관에 위탁함으로써 정보를 암호의 오용이나 키의 분실로부터 보호할 수 있는 시스템이다. 이러한 키 위탁 시스템을 이용함으로써 사용자의 키 유실이나 정부의 법 집행능력 확보를 제공할 수 있다. 일반적으로 키 위탁 시스템은 사용자와 정부사이의 요구사항들의 상충에 의해 많은 문제를 가지고 있어 기존에 발표된 키 위탁 시스템은 이러한 요구사항들을 모두 만족할 수 없었다. 따라서 본 논문에서는 Failsafe 와 Blind Decoding 방법을 기본으로한 사용자와 정부의 요구사항을 모두 만족하는 새로운 키 위탁 시스템을 제안한다.

Abstract One of the most important thing in a cryptosystem is a key information. Therefore, it is important to manage private keys on large public networks. If the private key is lost or damaged, it may lost all informations. A key escrow system can recover user's key against user's key loss and provide law-enforced access to government. Generally, in a key escrow system, there are many problems on fairness between user and government. But conventional key escrow systems can not satisfy requirements of user and government. So, this paper propose a new fair key escrow system based on Failsafe and Blind Decoding that can protect of user privacy and user can not bypass key escrow system.

1. 서 론

산업사회에서 정보화사회로 바뀌어 가면서 산업, 교육, 서비스등 모든 분야가 개방 네트워크로 바뀌어가고 있는 추세에 있다. 이러한 이유는 개방 네트워크의 가장 큰 특징인 편리성에 있기 때문이다. 하지만 개방 네트워크는 그 편리성에도 불구하고 누구나 접근할 수 있는 점에 의해 사용자의 프라이버시에 큰 피해를 입힐 수 있다는 문제점이 상존하게 된다.

이를 해결해 줄 수 있는 방법이 강력한 암호를 사용하는 것인데, 암호의 사용은 각 사용자들에게 자신의 비밀키에 해당하는 정보를 자신만이 안전하게 보관해야한다는 부담이 따른다. 만약, 시스템의 파괴나 사용자의 부주의에 의해 사용자의 비밀키가 훼손되었을 경우, 사용자는 새로운 비밀키를 만들거나 이전에 위탁한 비밀키를 복구 받아야 한다. 새로운 비밀키를 만들 경우는 이전의 키로 암호화되었거나 서명된 데이타에 대한 접근을 할 수 없다는 문제점이 있다. 이를 해결할 수 있는 방법은 두 번째 방법인 키 위탁시스템을 이용하는 것이다.[1][2][3] 또한 범법자들의 강력한 암호의 사용으로 정부가 범법자에 대한 법 집행 능력에 큰 어려움이 발생할 수도 있다. 이러한 문제-사용자들의 키 유실, 정부의 법 집행 능력 확보-를 해결하기 위해서는 키 위탁이 필요하고 실제로 미국에서는 1993년 CLIPPER 프로젝트[4][5]라는 키 위탁 정책을 발표하였고 그 후로 많은 연구가 진행 중에 있다.

CLIPPER 프로젝트 발표 이후 여러 관점에서 키 위탁 시스템에 대한 연구가 활발히 이루어져 왔다. 하지만 CLIPPER 프로젝트는 많은 반발이 일어났는데, 그 이유는 정책상의 특징으로 인해 정부측 위주의 키 복구 시스템이 설계되었고, 이로 인해 사용자와 정부사이의 공정성 및 키 복구의 일반적 요구사항이 지켜지지 않았기

† 비 회 원 : 순천향대학교 정보기술공학부
hbs@csc.sch.ac.kr
†† 종신회원 : 순천향대학교 정보기술공학부 교수
imylee@asan.sch.ac.kr
논문접수 : 2000년 1월 27일
심사완료 : 2000년 8월 21일

때문이다.[6][7][8] 이를 해결하기 위한 방법이 CRYPTO'92에서 제안된 Fair Cryptosystem이다. Fair Cryptosystem[9]은 공정성에 대한 문제를 해결하는 일반적인 키 위탁 시스템의 모델을 제시하였지만 본 논문의 2장에서 제시하는 키 위탁 시스템의 기본 요구사항들을 만족시키지 못하고 있다. 이를 해결하기 위해 RSA Cryptosystem[10], Partial Key Escrow[11], Failsafe[12], Blind Decoding[13]과 같은 여러 가지 방식들이 연구되었다. 하지만 Fair Cryptosystem과 마찬가지로 이러한 각각의 방식들은 그 특성에도 불구하고 본 논문의 2장에서 제시하는 키 위탁 시스템의 기본 요구사항을 모두 만족시키지 못하고 있다. 따라서 본 논문에서는 키 위탁의 기본 요구사항을 모두 만족시킬 수 있는 방법 제시를 위해 Failsafe와 Blind Decoding에서 제안된 기본개념을 이용해 새로운 키 위탁 시스템을 설계한다.

제 2장에서는 키 위탁 시스템의 기본적 요구사항을 설명하고, 제 3장에서는 본 논문에서 이용되는 기본 개념과 제안 방식에 대한 자세한 프로토콜을 보여준다. 제 4장에서는 제안방식이 2장에서 설명한 요구사항을 어떻게 만족하는지 설명하고 마지막으로 제 5장에서는 결론을 맺도록 한다.

2. 키 위탁 요구사항

키 위탁 시스템 구성시 정부 입장에서는 복구의 확실성과 사용자의 부정행위 방지가 보장되어야 하며, 사용자의 입장에서는 사생활 보호가 보장되어야 한다. 이를 위해서 키 위탁 시스템은 다음과 같은 일반적 요구사항들을 가진다.[10][14][15]

1) 사용자의 비밀키 생성

키 위탁 시스템의 특징상 사용자의 부정 행위를 방지하기 위해서는 정부측에서 사용자의 비밀키를 생성해 사용자에게 제공하는 것이 가장 확실한 방법이라 할 수 있다. 하지만 이러한 방법은 사용자들에게 심한 거부감을 줄 수 있다. 이를 해결하기 위해 키 위탁 시스템은 사용자의 비밀키 생성시 사용자 자신이 일부나 전체를 생성하여야 한다.

2) 암호문에 대한 안전성

키 위탁의 기본 개념은 사용자 키의 일부나 전체를 위탁 기관에게 위탁하는 것이다. 이러한 위탁은 키 위탁 요구사항과 같은 여러 가지 문제점을 보장해 주어야 한다. 문제점을 해결해 주기 위해 복잡한 프로토콜이 요구되는데 이러한 프로토콜은 가장 기본적인 송신자와 수신자 사이에 전송되는 암호문에 대한 기본적인 안전성을 보장하여야 한다.

3) 키 복구의 확실성 보장

사용자가 자신의 키의 일부나 전체를 위탁시 정부는 위탁된 키로 유사시 키 복구를 할 수 있다는 것을 보장받아야 한다. 만약 사용자가 잘못된 키를 위탁하고 정부가 이를 발견하지 못했다면, 정부는 유사시 사용자의 키를 복구할 수 없을 것이다.

4) 수사기관의 감청기한 제한

위해서 수사기관은 피감청자의 비밀키를 위탁기관으로부터 획득한다. 획득된 비밀키는 수사기관에게 감청을 할 수 있는 능력을 제공하지만, 수사기관의 감청에 대한 권한이 끝났을 경우에도 수사기관은 획득된 비밀키로 계속 피감청자를 감청할 수 있는 능력이 생긴다. 이를 방지하기 위해 키 위탁 시스템은 수사기관이 합법적인 기간 및 통신에만 감청할 수 있도록 수사기관의 감청기한을 제한하여야 한다.

5) 피감청자의 신원보호

감청을 하기 위해서 수사기관은 법기관의 도움으로 피감청자의 비밀키의 조각을 가지고 있는 위탁기관에 접촉해 피감청자의 비밀키를 획득한다. 피감청자의 신원은 법기관과 수사기관만이 알고 있어야 하며, 위탁기관은 사용자의 프라이버시를 보호한다는 차원에서 피감청자의 신원을 알지 못해야 한다. 또한 위탁기관이 사용자들의 신원을 알 수 있다면 위탁기관들이 공모해 사용자의 비밀키를 생성할 수 있다. 따라서, 키 위탁 시스템은 수사기관과 법기관을 제외하고는 피감청자의 신원을 드러낼 수 없어야 한다.

6) 사용자의 새도우 공개키(shadow public key) 생성 방지

부정한 사용자는 자신의 올바른 키를 위탁하고 실제 사용시는 위탁된 키에 대한 새도우 공개키를 사용함으로써 키 복구의 확실성과 범법자에 대한 법 집행 능력을 피해갈 수 있다. 따라서, 키 위탁 시스템은 사용자의 새도우 공개키 생성을 방지하여야 한다.

위의 2)~6)은 키 위탁 시스템에 대한 일반적 요구사항이며, 1)은 본 논문에서 추가한 요구사항이다. 사용자의 새도우 공개키 생성을 방지하기 위해 기존의 논문에서는 사용자가 아닌 키 복구에 관련된 기관이 사용자의 키를 생성하는 방법을 취한 것도 소개되었다.[13] 하지만 이러한 방법은 사용자의 반발이 있을 수 있고 사용자의 비밀키가 키 복구에 관련된 기관에 불법적으로 드러날 수 있는 가능성이 있다. 따라서 본 논문에서는 요구사항 1)을 추가함으로써 보다 안전한 키 복구 시스템을 설계할 수 있도록 하였다.

3. 제안 방식

본 장에서는 제안방식에서 이용되는 Failsafe와 Blind Decoding의 기본개념을 설명하고 이 기본개념을 바탕으로 한 새로운 방식의 프로토콜을 제안한다.

3.1 기본개념

1) 사용자와 인증기관이 협력해 사용자의 비밀키를 생성한다.

사용자와 인증기관이 협력해 키를 생성함으로써 정부는 사용자의 새도우 공개키를 막을 수 있고 사용자는 정부에 의해 자신의 비밀키가 모두 생성되는 것을 막을 수 있다. Failsafe 방식에서는 Bit Commitment 방법을 이용하여 구현함으로써 대화형이라는 단점이 있다. 본 논문에서는 인증기관이 사용자의 반쪽의 비밀키를 생성해 공개 디렉토리에 등록한다. 사용자는 자신의 키 생성 단계에서 인증기관이 생성한 반쪽의 비밀키를 선택해 이 값을 인증기관에게 블라인드 복호를 요청함으로써 사용자 반쪽의 비밀키를 얻는다. 그리고 사용자 자신이 생성한 반쪽의 비밀키를 합해 자신의 최종 비밀키를 얻는다.

2) 인증기관에 의해서 생성된 키의 반쪽은 인증기관에 의해 블라인드 복호된다.

사용자가 아닌 인증기관에 의해 생성된 키의 반쪽은 인증기관의 블라인드 복호에 의해서만 노출된다. 그러므로 사용자는 자신의 키의 반쪽을 다른 기관이 알 수 없다는 것을 보장받을 수 있다. 인증기관이 사용자의 키의 반쪽을 생성해서 공개 디렉토리에 등록했다하더라도 사용자가 랜덤하게 키쌍을 선택하고 또한 블라인드 복호를 요청함으로 인증기관은 사용자의 키를 알 수 없다. 기타 다른 기관들은 공개디렉토리에 있는 키가 인증기관의 공개키로 암호화되어있기 때문에 이 값에 접근할 수 없다.

3) 통신시 LEAF(Law Enforcement Access Field : 법 집행 접근 필드)의 사용에 의해 수사기관은 키 복구 능력을 가질 수 있다.

키 복구의 실행은 정부의 요구(사용자 감청)와 사용자 요구(유실 데이타 복구)일 때 성립된다. 사용자가 키 복구를 요구할 경우는 수신자는 복구를 수행하는 기관에서 데이타가 정확히 누구의 키로 암호화되어 있는지 밝히게 된다. 따라서 복구를 수행하는 기관은 그에 대한 비밀키(수신자 비밀키 : 복호하기 위한 키)를 쉽게 찾을 수 있다. 하지만 정부가 키 복구를 요구할 경우에는 수사기관이 암호화된 데이타를 통신로 상에서 감청하게 된다. 이러한 경우에는 수사기관이 암호화된 데이타가 정확히 누구의 키로 암호화되었는지 알 수 없다. 이를 해결하기 위해 본 논문에서는 송신자가 수신자에게 메시지를 보낼 때 수신자의 공개키를 LEAF에 삽입함으로써 수사기관은 송·수신자의 신원을 알 수 있고 키 복구 능력을 가질 수 있도록 한다.

3.2 제안방식의 구성요소

제안 방식을 구성하는 요소는 다음과 같다.

1) 사용자(U)

반쪽의 키쌍(비밀키(A_a)/공개키(P_{A_a})) 생성

2) 인증기관(CA)

사용자들에게 선택될 나머지 반쪽의 키쌍(비밀키(A_b)/공개키(P_{A_b}))들을 미리 생성해 등록기관의 공개 디렉토리상에 공개한다. 그리고 사용자의 최종 비밀키($A=A_a+A_b$)에 해당하는 공개키(P_A)에 대한 인증서를 발급한다.

3) 등록기관(RA)

인증기관의 공개키로 암호화되어 있는 반쪽의 비밀키(A_b)쌍들을 자신의 공개 디렉토리상에 가지고 있으며 사용자의 인증서 발급시 등록기관으로서의 일을 한다.

4) 수사기관(I)

LEAF로부터 수신자의 공개키를 얻는다. 법기관으로부터 수사 허가서를 발급받아 위탁기관의 도움으로 사용자의 세션키를 얻는다.

5) 법기관(J)

수사기관의 요청에 따라 수사 허가서를 발급한다.

6) 위탁기관(T)

사용자와 인증기관이 생성한 사용자의 최종 비밀키($A=A_a+A_b$)를 분산 보관한다.

3.3 세부 프로토콜

본 제안 방식은 4 단계의 과정이 있고, 각 단계별 세부 프로토콜은 아래와 같다.

1) 키 생성 단계

사용자는 자신의 비밀키(A_a)를 생성하고 인증기관이 생성한 나머지 비밀키(A_b)를 얻어 인증기관의 블라인드 복호 과정을 통해 사용자의 완전한 비밀키(A)를 생성하는 단계이다.

① 인증기관은 사용자의 비밀키의 반쪽을 생성하기 위해 랜덤한 생성자 g ($\in Z^*_p$)와 소수 p를 생성하고 이 값을 공개한다. 인증기관은 키쌍(비밀키(A_b)/공개키(P_{A_b}))들을 생성해 비밀키는 자신의 공개키(KU_{CA})로 암호화해 다음과 같이 서명하여 등록기관의 공개 디렉토리상에 공개한다.(사용자는 등록 기관의 공개 디렉토리상에 있는 서명된 키쌍

들 중 하나를 자신의 반쪽의 키로 선택한다.)

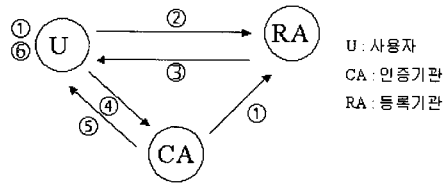

그림 1 키 생성 단계

$$Sign_{CA}[E_{KU_{CA}}(A_b), P_{A_b}]$$

또한, 사용자는 자신의 비밀키와 공개키를 다음과 같이 생성한다.

$$P_{A_a} = g^{A_a} \bmod p$$

(A_a : 사용자 A가 생성한 반쪽의 비밀키, P_{A_a} : A_a에 대응되는 공개키)

② 사용자는 자신이 생성한 공개키(P_{A_a})를 등록기관에 제공한다. 이 값은 키 위탁 과정에서 사용자의 키확인에 이용된다.

③ 등록기관은 사용자에게 인증기관에 의해 생성되고 서명된 키쌍들 중 하나를 선택할 수 있게 한다. 선택된 키쌍은 사용자에게 보내진다.

$$Sign_{CA}[E_{KU_{CA}}(A_b), P_{A_b}]$$

④ 사용자는 키의 반쪽을 획득하기 위해 인증기관의 공개키로 암호화되어 있는 $E_{KU_{CA}}(A_b)$를 인증기관에게 블라인드 복호를 요청한다. 사용자가 A_b를 알기 위해선 인증기관의 비밀키가 있어야 하지만 인증기관의 비밀키는 인증기관만이 가지고 있어야 한다. 따라서 $E_{KU_{CA}}(A_b)$를 복호화할 수 있는 개체는 인증기관뿐이다. 하지만 일반적으로 인증기관이 $E_{KU_{CA}}(A_b)$로 복호화할 경우 인증기관은 A_b를 알게 됨으로 이것은 사용자의 요구를 만족하지 못한다. 이를 해결하기 위해 블라인드 복호를 이용하는데, 블라인드 복호 프로토콜은 복호자(인증기관)는 자신이 복호하는 메시지(A_b)의 내용을 모른 체 메시지를 복호해 주는 것이고, 복호 요청자(사용자)는 복호자의 비밀키(인증기관의 비밀키)를 알지 못하고 메시지를 복호 받는 것이다.

⑤ 블라인드 복호 프로토콜에 의해 인증기관은 (A_b)를 알지 못한 채 사용자에게 복호해 준다.

⑥ 사용자는 인증기관으로부터 제공받은 A_b를 통해 다음과 같이 자신의 최종 공개키와 비밀키를 생성한다.

$$P_A = g^{A_a + A_b} \bmod p$$

($A_a + A_b = A$: 사용자 A의 최종비밀키, P_A : 사용자 A의 최종 공개키)

2) 키 위탁 단계

사용자 키 생성 단계에서 생성된 최종 비밀키를 위탁기관들에게 위탁하고 이 단계가 검증된다면 인증서를 발급하는 단계이다. 등록기관은 위탁기관에게 비밀키 조각에 대한 ID를 제공한다.(이렇게 함으로써 위탁기관들은 자신이 가지고 있는 조각키가 어떤 사용자의 키인지 알지 못한다.)

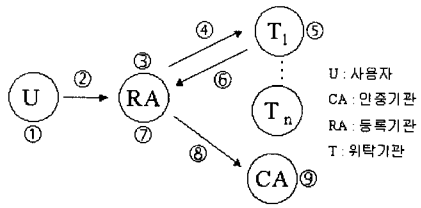

그림 2 키 위탁 단계

① 사용자는 자신이 생성한 키를 분산 위탁하기 위해서 다음과 같은 과정을 거쳐 A_i와 V_i를 생성한다.

$$A = A_1 + A_2 + \ldots + A_n \bmod p$$

$$V_i = g^{A_i} \bmod p \quad (i=1,2, \ldots, n)$$

② 사용자는 ①에서 생성된 정보를 등록기관에게 전송한다.(등록기관이 최종 비밀키의 조각정보를 알지 못하게 위탁될 기관들의 공개키로 암호화하여 전송)

$$E_{P_{Ti}}[A_i, V_i]$$

(P_{Ti} : 위탁기관들의 공개키)

③ 위탁기관들에게 ID를 제공하기 위해 다음을 계산한다.

$$U = (P_J)^{KP_{RA}} \bmod p$$

$$ID = E_U(P_A)$$

(P_J:법기관의 공개키, KP_{RA} : 등록기관의 비밀키, P_A:사용자 A의 공개키, $E_U(P_A)$:키 U와 암호화 함수를 이용해 P_A를 암호화)

④ 등록기관은 위탁기관들에게 다음을 전송한다.

$$ID,\ E_{P_{Ti}}[A_i, V_i]$$

⑤ 위탁기관들은 데이타를 복호하고 다음이 만족하는지 확인한다.

$$V_i = g^{A_i} \bmod p$$

⑥ 위의 수식이 맞다면 위탁기관들은 ID와 A_i를 저장

하고 등록기관에게 V_i와 승인 정보를 보낸다.

⑦ 등록기관은 P_A가 제대로 생성되었나를 확인하기 위해 다음 수식이 만족하는지 검사한다.

$$P_A = P_{A_a} * P_{A_b} \bmod p = g^{A_a} * g^{A_b} = g^{A_a + A_b} = g^A$$

(P_A는 사용자의 최종 공개키)

$$P_A = V_1 * V_2 * V_3 * \ldots * V_n \bmod p = g^{A_1} * g^{A_2} * \ldots * g^{A_n} = g^{(A_1 + A_2 + \ldots + A_n)} = g^A$$

⑧ 위의 과정이 모두 옳다면 등록기관은 인증기관에게 A의 인증서를 요청한다.

⑨ 인증기관은 인증서를 생성하고 공개 디렉토리에 등록한다.

3) 통신 단계

송신자(A)는 수신자(B)와 통신하기 위해 먼저 수신자의 공개키를 얻고 세션키를 생성해 다음을 수신자에게 전송한다. (실제로 메시지(M)은 세션키 K로 암호화된다.)

$$\{g_r \bmod p,\ K * P_B^r \bmod p,\ E_K[M]\}$$

(r : 랜덤값, K : 세션키, P_B : 수신자 B의 공개키, M : 메시지, $E_K[M]$: 키 K와 암호화 함수를 이용해 M을 암호화)

그리고 수신자의 공개키와 Date 정보를 포함하는 LEAF를 생성하고 이것을 수사기관의 공개키로 암호화해서 전송되는 데이타에 추가한다. 이 LEAF를 통해서 수사기관은 수신자의 신원을 파악해 키 복구 단계를 수행한다.

$$LEAF = E_{KU_I}\{P_B,\ Date,\ Sign_A[P_B,\ date]\}$$

(KU_I : 수사기관의 공개키, $Sign_A$: A의 서명)

4) 키 복구 단계

수사 기관은 사용자의 키 유실이나 감청시 전송된 데이타의 LEAF에서 수신자의 공개키를 획득한 후 법기관에게 수사 허가서를 제공받아 사용자의 세션키를 얻을 수 있는 단계이다.

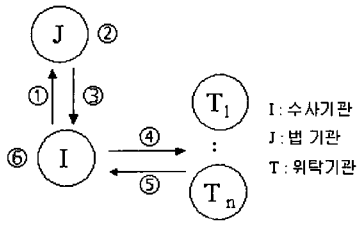

그림 3 키 복구 단계

① LEAF로부터 얻은 수신자 B의 공개키(P_B)와 수사허가서 요청을 법기관에게 보낸다.

② 법기관은 수사허가를 심사하고 다음을 계산해 피감청자(수신자)의 ID를 획득한다.

$$U = (P_{RA})^{KP_J} \bmod p$$

$$ID = E_U(P_B)$$

(P_{RA} : 등록기관의 공개키, KP_J : 법기관의 비밀키, P_B : 사용자 B의 공개키, $E_U(P_B)$: 키 U와 암호화 함수를 이용해 P_B를 암호화)

③ 법기관은 수사기관에게 다음과 같은 수사 허가서를 암호화해서 제공한다.

수사 허가서 = [ID, Date, $Sign_J$(ID, date)]

④ 수사기관은 위탁기관들에게 수사 허가서와 $g^r \bmod p$를 제공한다.

⑤ 각각의 위탁기관들은 수사 허가서의 유효성을 확인하고 수사 허가서에 나타나 있는 ID에 해당하는 자신들이 가지고 있는 키조각들을(B_1, B_2, B_3, ... ,B_n)을 다음과 같이 전송한다.

$$(g^r)^{B_i} \bmod p$$

⑥ 수사기관은 다음과 같은 수식에 의해서 세션키 K를 획득한다.

$$(g^r)^{B_1} * (g^r)^{B_2} * \ldots * (g^r)^{B_n} = g^{r(B_1 + B_2 + \ldots + B_n)} = g^{rB} = P_B^r$$

계산된 P_B^r를 통신 단계에서 수사기관이 감청한 $K * P_B^r$을 이용해 다음과 같이 계산함으로써 수사기관은 세션키 K를 얻어 암호화되어 있는 메세지를 복호할 수 있다.

$$K * P_B^r / P_B^r = K$$

$$D_K[E_K(M)] = M$$

4. 제안 방식 고찰

2장에서 키 위탁 시스템이 기본적으로 갖추어야하는 요구사항을 살펴보았다. 본 제안 방식은 2장의 요구사항들을 모두 만족하고 있는데 그 이유는 다음과 같다.

1) 사용자의 비밀키 생성

제안 방식에서는 사용자가 A_a를 생성하고 인증기관에 의해 A_b가 생성된다. 사용자의 최종 비밀키는 $A_a + A_b$가 됨으로 사용자는 자신의 비밀키의 일부 또는 전체를 생성해야하는 요구조건을 만족한다.

2) 암호문에 대한 안전성

본 제안방식에서 데이타의 암호는 일반적인 ElGamal 암호 시스템을 사용하기 때문에 사용자 키 생성 단계나

키 복구 단계가 안전하다면 암호문에 대한 안전성은 보장된다고 할 수 있다.

3) 키 복구의 확실성 보장

키 위탁 단계에서 사용자와 등록기관은 사용자가 생성한 자신의 최종 비밀키의 조각을 위탁기관에게 분산 보관하고 위탁기관들은 이를 확인한다. 그리고 위탁 기관은 확인정보를 등록기관에게 보내고 등록기관은 이들 정보를 취합하여 공개키에 해당하는지 검사함으로써 유사시 키 복구의 확실성을 보장할 수 있다.

4) 수사기관의 감청기한 제한

수사기관은 키 복구시 위탁기관들에게 $g^r \bmod p$를 제공한다. 위탁기관은 자신이 가지고 있는 정보를 $g^r \bmod p$에 승수를 해줌으로써 수사기관은 사용자의 최종 비밀키는 알 수 없고 단지 세션키만을 알 수 있다. 사용자가 통신시마다 세션키를 생성해 통신한다면 수사기관은 세션키에 해당하는 통신만을 감청할 수 있다. (자세한 수식은 제안 방식의 키 복구 단계에 설명되어 있다.)

5) 피감청자의 신원보호

위탁기관들이 가지고 있는 ID는 등록기관과 법 기관만이 알 수 있는 키(U : Diffie-Hellman의 키교환)를 사용해 피감청자의 공개키를 암호화한 것이다. 감청시 수사기관은 법기관에게 피감청자의 공개키를 제공하면 법기관은 키(U)를 계산해 피감청자의 공개키를 U로 암호화해서 제공한다. 수사기관은 ID에 해당하는 비밀키를 위탁기관들에게 요구한다. 따라서 위탁기관들은 피감청자의 신원을 알 수 없이 자신이 가지고 있는 ID에 해당하는 사용자의 조각키를 제공한다.

6) 사용자의 새도우 공개키 생성 방지

인증기관에 의해 생성된 키의 반쪽은 랜덤하다. 사용자는 자신의 생성한 비밀키에 해당하는 공개키를 미리 등록기관에 제공한 후에 인증기관에 의해 생성된 키를 선택함으로서 비밀키 $A_a + A_b$는 랜덤하다고 볼 수 있고 사용자의 새도우 공개키 생성을 방지할 수 있다.

부가적으로, 참고문헌 [4]에서 키 복구 시스템의 정부와 사용자측 요구사항을 다음과 같이 제시하였는데 정부측 요구사항은 LEAF를 통해 실현 가능하다. 사용자측 요구사항 ⑤는 실제로 데이타를 복호하면 키의 유실 여부를 알 수 있고 ⑥, ⑦은 키 복구 시스템을 이용한다면 가능할 것이다. ⑧은 일반적인 키 복구 시스템의 요구사항인 감청기한 제한과 신원보호를 통해 만족시킬 수 있다.

① 정부기관이 정보에 접근하는 것은 사용자의 동의 없이도 가능해야 한다. (정부)

② 정보의 소유자(사용자)는 정부기관의 접근 사실을 인지하지 못해야 한다. (정부)

③ 어떠한 (시간적, 공간적)상황 속에서도 평문 정보에 가능한 신속하게 접근 가능해야 한다. (정부)

④ 정보의 형태에 관계 없이 정보를 얻을 수 있어야 한다. (정부)

⑤ 키가 유실/손상되었음을 신속하게 감지할 수 있어야 한다. (사용자)

⑥ 유실된 키를 신속하게 복구할 수 있어야 한다. (사용자)

⑦ 키의 손상위협에서부터 정보를 보호할 수 있어야 한다. (사용자)

⑧ 시행되는 동안은 사생의 보호와 정보 누출 방지가 되어야 한다. (사용자)

본 시스템은 위와 같은 요구사항 만족을 통해서 다음과 같은 사용자와 정부사이의 요구사항을 만족할 수 있다. 사용자와 인증기관이 사용자의 최종 비밀키를 만들기 때문에 사용자는 키에 대한 불법적인 조작이나 키 복구 시스템을 회피할 수 없다는 것을 정부에게 보장해 줄 수 있다. 또한 사용자에게는 정당한 경우에만 정부가 키 복구에 참여하고 복구에 따른 신원보호와 감청 기한을 제한할 수 있다는 것을 보장할 수 있다.

표 1은 키 위탁 방식의 대표적인 Fair Cryptosystem와 본 논문의 기초가 된 Failsafe, Blind Decoding 방식을 제안방식과 비교해 본 것이다.

표 1 키 위탁 시스템 비교

	Fair Crypto system	FailSafe Key Escrow	Blind Decoding	제안 방식
사용자의 비밀키 생성	O	O	X	O
암호문의 안전성	O	O	O	O
키 복구의 확실성	O	O	O	O
감청기한 제한	X	X	O	O
피감청자의 신원보호	X	X	O	O
새도우 공개키 방지	X	O	O	O

Fair Cryptosystem은 사용자가 자신의 비밀키를 생성함으로써 비밀키의 랜덤성을 보장할 수 없고 비밀키의 랜덤성을 보장하지 못한다면 새도우 공개키를 방지할 수 없다. 또한 감청기한 제한 및 피감청자의 신원보호의 요구사항에 대해선 확실한 방법을 제시하지 못하였다. 그리고 FailSafe Key Escrow는 감청기한 제한 및 피감청자의 신원보호를 언급하고 있지 않고 다만, 사

용자와 키 복구에 관련된 기관이 협력해 사용자의 비밀키를 생성하는 방법만 제시하였다. 마지막으로 Blind Decoding은 사용자의 비밀키를 키 복구에 관련된 기관 단이 생성함으로 본 논문에서 제시한 요구사항 1)을 만족하지 못한다.

5. 결 론

지금까지 제안방식의 프로토콜을 설명하고 제안방식이 키 복구 요구사항(사용자, 정부기관 측면)들을 어떻게 만족시키고 있는지 살펴보았다. 그리고 본 논문에서는 언급하지 않았지만 제안방식을 이용해 사용자가 위탁기관에게 키 위탁시 (k, n) threshold의 확장도 가능할 것이다.

키 복구 시스템이 글로벌 네트워크 상에서 실행되기 위해서는 국가 공개키 기반 구조상에서 연동되어야 한다. 그러기 위해서는 공개키 기반 구조에 키 복구를 위한 별도의 기관인 위탁기관과 법기관, 수사기관이 필요할 것이다. 또한, 공개키 기반 구조에서 키 복구를 위해서는 새로운 추가된 기관과 기존의 공개키 기반 구조를 구성하는 기관들 사이의 연동을 위해 새로이 모듈의 정립이 필요하다. 즉, 공개키 기반 구조의 구성요소들에게 기존의 기능에 부가적으로 키 복구를 수행하기 위한 모듈들의 추가가 필요할 것이다. 이를 해결하기 위한 첫 번째 방법은 기존의 공개키 기반 구조의 기관들에 키 복구 모듈을 추가하는 것이고 또 다른 방법은 다른 임의의 키 복구 기관을 두어 공개키 기반 구조에서의 키 복구를 연동시키는 방법이 있다. 하지만 두 번째 방법을 선택했을 때도 키 정보와 사용자 정보의 교환을 위해서는 키 복구 센타가 다른 공개키 기반구조의 기관들과의 통신은 불가피하다. 따라서 본 논문에서는 등록기관과 인증기관에 별도의 키 복구 모듈(본 논문에서 제안한 프로토콜의 4 단계)을 추가함으로써 공개키 기반구조에서 키 복구를 수행하게 하였다.

마지막으로 본 본문에서는 새도우 공개키를 방지하기 위해 사용자와 인증기관이 협력해 사용자의 비밀키를 생성하는 방법을 취하였다. 하지만 궁극적으로는 오직 사용자만이 자신의 비밀키를 생성하고, 이 키의 랜덤성을 키 복구에 관련된 기관이 증명가능해야 할 것이다. 또한 키 복구 모듈을 공개키 기반 구조에 연동시키기 위해선 키 복구 시스템의 새로운 요구사항에 대한 정립이 필요할 것이다. 앞으로 이러한 사항들에 대한 지속적인 연구를 통해 보다 안전한 키 복구 시스템을 구성할 수 있을 것이다.

참 고 문 헌

[1] David Paul Maher, Crypto Backup and Key Escrow, Communications of the ACM, Vol.39, No.3, pp. 48-53, 1996.

[2] Ravi Ganesan, The Yaksha Seurity System, Communications of the ACM, Vol.39, No.3, pp.55-60, 1996.

[3] Stephen T. Walker, Steven B. Lipner, Carl M. Ellison and David M. Balenson. Commercial Key Recovery, Communications of the ACM, Vol.39, No.3, pp.41-47, 1996.

[4] 이임영, 채승철, Key recovery 시스템에 관한 고찰, 한국통신정보보호 학회지, 제7권 제4호, pp.45-58, 1997.

[5] 채승철, 이임영, Key recovery 시스템에 관한 고찰 II, 한국통신정보보호 학회지, 제8권 제4호, pp.97-112, 1998.

[6] Dorothy E. Denning, The U.S. Key Escrow Encryption Technology, Building in Big Brother: The Cryptographic Policy Debate(Edited by Lance J.Hoffman), Springer-Verlag, pp.111-118, 1997.

[7] Dorothy E. Denning, A Taxonomy for Key Recovery Encryption System, Communications of the ACM, Vol.39, No.3, pp.34-40, 1996.

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

[9] Silvio Micali, Fair Cryptosystems, Advances in Cryptology-CRYPTO '92, pp.113-138, 1992.

[10] Yoshiki Sameshima, A Key Escrow System of the RSA Cryptosystem, SCIS'98, pp.75-85, 1998.

[11] Shaoquan Jiang and Yufeng Zhang, Partial Key Escrow Monitoring Scheme, CrypTEC'99, pp.86-91, 1999.

[12] Joe Kilian and Tom Leighton, Fair Cryptosystems, Revisited, CRYPTO 95, pp.208-221, 1995.

[13] Kouichi Sakurai and Yoshinori Yamane, Key Escrow System of Protecting User's Privacy by Blind Decoding, ISW'97, Springer-Verlag, pp.147-157, 1998.

[14] Lenstra A, Winkler P and Yacobi Y, A Key Escrow System with Warrant Bounds, Advances in Cryptology: Proceedings of CRYPTO'95, Springer-Verlag, pp.197-207, 1995.

[15] Yamane.Y and Sakurai.K, How to restrict investigators' tapping in Key Escrow Systems, The 1996 Symposium on Cryptography and Information Security 7C, 1996.

황 보 성

1999년 2월 순천향대학교 전산학과 졸업. 1999년 3월 ~ 현재 순천향대학교 전산학과 대학원 석사과정. 관심분야는 암호이론, 컴퓨터 보안.

이 임 영

1981년 8월 홍익대학교 전자공학과 졸업. 1986년 3월 오사카대학 통신공학과 석사. 1989년 3월 오사카대학 통신공학과 박사. 1989년 1월 ~ 1999년 2월 한국전자통신연구원 선임연구원. 1994년 3월 ~ 현재 순천향대학교 정보기술공학부 부교수. 관심분야는 암호이론, 정보이론, 컴퓨터 보안.