情報保護學會論文誌
第12券 第1號, 2002. 2

PKI 연동 키복구 암호 시스템 설계에 관한 연구

최 희 봉*, 오 수 현**, 홍 순 좌*, 원 동 호**

On Design of the Recoverable Cryptosystem in Public Key Infrastructure

Hee-bong Choi*, Soo-hyun Oh**, Soon-jwa Hong*, Dong-ho Won**

요 약

1998년 A. Young 등은 공개키 기반구조(PKI)를 이용한 자동 키복구 및 자동 인증 암호시스템을 제안하였다. 우리는 소프트웨어 키위탁 체계를 수행할 수 있는 자동 키복구 및 자동 인증 암호시스템의 설계 개념을 적용하여 새로운 공개키 연동 키복구 암호시스템을 제안한다. 새로운 공개키 연동 키복구 암호시스템은 사용자의 비밀키와 공개키가 키위탁 기관의 마스터 비밀키와 마스터 공개키가 서로 연관되어 있다. 제안한 키복구 암호시스템은 RSA 암호시스템에 기반을 두고 있으며 매우 효율적이고 안전성을 갖고 있다.

ABSTRACT

In 1998, A. Young and M. Yung proposed the auto-recovery auto-certificate cryptosystem in public key infrastructure. We propose the new recoverable cryptosystem in public key infrastructure which is designed with the concept of A. Young et al's auto-recovery auto-certificate cryptosystem. It has the private/public key pairs of the user and the master private/public key pairs of the escrow authority. It is based on RSA cryptosystem and has efficiency and security.

keyword : *auto-recovery auto-certificate cryptosystem, RSA, software key escrow*

Ⅰ. 서 론

암호 학자들은 최근 키복구를 효율적이고 안전하게 수행시킬 수 있는 시스템에 대하여 많은 연구를 하여 왔다. 인터넷과 IMT-2000과 같은 통신 네트워크의 광범위한 사용으로 대규모 키복구 시스템을 개발해야 하는 필요성이 대두되고 있지만, 이러한 시스템 개발 기술이 매우 어려우므로 만족할 만한 시스템이 개발되지 않고 있다.

일반적으로 키복구란 암호문의 소유자(일반적으로 암호 시스템에서 키를 소유한 사람)만이 평문으로 복호할 수 있는 암호화된 데이터에 대해 특정한 조건(암호가 나쁜 목적으로 사용되었을 경우 법집행권을 확보하기 위한 합법적 허가, 데이터 암호용 키를 분실 및 손상하였을 경우)이 만족될 경우에 한해서 허가된 사람 또는 기관에게 복호가 가능한 능력을 제공하는 기술 및 체계를 말한다.

키복구는 각 특성에 따라 키위탁 방식, 캡슐화 방식, TTP 기반의 방식으로 나눌 수 있다. 키복구 방식을 현재의 암호 사용자 환경에 무조건 도입하는 것은 시간과 비용, 구현 기술 등에서 어려움이 많다.

현재 각 나라에서는 전자상거래와 같은 암호 응용 분야에서 유용하게 사용될 수 있는 공개키 기반 구조 구축이 진행되고 있으며 여러 선진국에서는 이미

* 국가보안기술 연구소(hbchoi@etri.re.kr)
** 성균관대학교 전기전자및컴퓨터공학과 정보통신보호연구실(shoh@dosan.skku.ac.kr, dhwon@simsan.skku.ac.kr)

구축이 되어 서비스가 진행중이다. 따라서 이러한 공개키 기반구조에 키복구 방식을 도입하는 것은 효율적인 방법이라 할 수 있으며 또한 현재까지 이러한 연구가 상당히 이루어진 상태이다.

1998년 A. Young과 M. Yung은 공개키 기반 구조를 이용하여 다수의 위탁 기관이 참가 가능한 자동 키복구 자동 인증 암호 시스템(ARC, auto-recoverable auto-certifiable cryptosys tem)을 제안하였다.[1] 사용자는 위탁 기관의 공개키를 이용하여 자신의 비밀키를 생성하고 이를 인증 기관에 증명함으로써 공개키에 대한 인증서를 발급 받는다. 그러나 이 방식은 사용자의 비밀키가 위탁기관의 공개키를 사용하여 생성되었음을 증명하는 증명서를 공개키 인증서와 함께 저장할 수 있는 저장공간이 필요하다. 이것은 사용자의 비밀키를 복구할 때 이 증명서가 필요하기 때문이다. 따라서 위탁기관과 인증기관 사이의 통신이 필요하다는 단점도 있다.

1999년 P. Paillier와 M. Yung은 마스터 키를 갖는 SE-PKI 시스템을 제안하였다.[2] SE-PKI는 마스터 키를 사용하였기 때문에 사용자의 비밀키를 복구할 때 키복구 가능 확인 증명서가 필요하지 않기 때문에 증명서 저장공간이 필요하지 않다.

ARC와 SE-PKI 암호 시스템은 사용자의 암호 방식이 ElGamal 암호 방식에 대한 것이고, ARC의 키위탁 기관의 암호 방식은 이산대수 문제에 기반한 암호 방식이고 SE-PKI의 키위탁 기관의 암호 방식은 Paillier 암호 방식이다.

본 논문에서는 PKI 연동 키복구 암호 시스템의 설계 개념을 적용한 새로운 키복구 암호 시스템을 제안한다. 우리가 제안한 암호 시스템은 널리 사용되고 있는 RSA 암호 방식에 기반한 키복구 암호 시스템으로서 SE-PKI 암호 시스템과 같이 ARC 암호 시스템에서 필요한 증명서 저장 공간을 없애고, 이에 따라 위탁기관과 인증기관 사이의 통신도 필요없게 되었다. 제안한 암호 시스템은 사용자와 키위탁 기관의 암호 방식이 동일한 RSA 암호 방식이기 때문에 구현할 때 또는 운용할 때 편리하다. 그리고 위탁기관도 비밀 분산 개념을 적용하여 다수의 위탁 기관으로 설계될 수 있다.[3,4]

본 논문의 구성은 다음과 같다. 2장에서는 PKI와 연동하는 소프트웨어 키위탁 암호 시스템의 설계 개념에 대하여 알아보고 3장에서는 A. Young과 M. Yung이 제안한 자동 키복구 자동 인증 암호시스템에 대하여 설명하고 4장에서는 RSA 암호 시스템에 기반한 소프트웨어 키위탁 암호 시스템의 스킴을 제안하고 5장에서는 제안한 스킴의 효율성과 안전성을 분석하고 6장에서는 결론을 내린다.

II. PKI 키위탁 설계 개념

이 절에서는 소프트웨어 키위탁 PKI 설계 내용에 대하여 설명한다. 이것은 기술문서나 암호학자 간에 협의된 내용 그리고 시스템 개발로부터 얻은 사항들에 대한 것이다.

2.1 PKI 키위탁 필요조건

일반적으로 소프트웨어 키위탁 PKI의 설계 규격은 아래와 같은 조건을 만족해야 한다.

[조건 1]
소프트웨어로 구현할 수 있어야 한다. 전체 시스템에 대해서나 혹은 시스템 구성요소에 대하여 탬퍼 보호 하드웨어가 필요 없다.

[조건 2]
소프트웨어로 배포될 수 있어야 한다. 사용자에게 필요한 소프트웨어는 공개된다. 즉 배포하기가 용이하다.

[조건 3]
키를 사용자가 생성할 수 있어야 한다. 사용자는 자신의 비밀키를 독자적이고 효율적으로 생성할 수 있어야 한다. 비밀키는 키위탁 기관만이 복구할 수 있다. 통신상의 데이터는 이 사용자의 키로 암호화된다.

[조건 4]
키위탁 기관이 참여하는 범위는 최소가 되어야 한다. 키위탁 기관은 시스템 설정할 때와 키 복구할 때만 참여한다.

[조건 5]
키위탁 PKI의 인증서 발급과정은 PKI의 인증서 발급과정과 호환할 수 있어야 한다. 키를 인증받기 위하여 사용자는 일반적인 PKI에서와 같이 인증기관(CA)에 인증서 요청 메시지를 보낸다. 사용자는 이 메시지를 독자적이고 효율적으로 생성할 수 있어야 한다.

〔조건 6〕
인증키는 키복구가 가능해야 한다. 비밀키가 인증기관에 의해 복구될 수 있음이 증명되면 인증기관은 사용자의 공개키를 인증한다. 이 증명 작업은 인증서 요청 메시지에 있는 데이터를 이용하여 수행한다. 이 증명작업에서 키가 아주 높은 확률로 복구될 수 있다고 증명되면 그 증명은 성공하였다고 결정한다.

〔조건 7〕
키위탁 PKI 인증서는 PKI 인증서와 호환할 수 있어야 한다. 키위탁 PKI 인증서에 포함된 키는 일반 PKI 공개키에 포함된 키와 같은 정보를 갖는다.

〔조건 8〕
키복구는 종합적으로 증명될 수 있어야 한다. 사용자가 공개키 인증을 요청할 때 인증서 요청서를 보내게 되는데 이 때 사용자는 키복구를 증명할 수 있는 증명서를 메시지에 포함한다. 그러면 인증기관은 비밀키가 키위탁 기관에 의해 복구될 수 있음을 증명할 수 있다.

〔조건 9〕
키복구는 효율적으로 수행될 수 있어야 한다.

〔조건 10〕
키위탁 PKI의 사용자 시스템은 일반 PKI의 사용자 시스템과 호환성을 가져야 한다. 소프트웨어 키위탁 PKI의 시스템은 공개키 암호 시스템으로서 사용자에게 쉬워야 하고 소프트웨어로 구현될 수 있어야 한다. 그러므로 키위탁 PKI의 시스템은 일반 PKI의 구성과 같아야 한다. 이것의 솔루션은 소프트웨어로 안전하게 구현될 수 있기 때문에 소스 코드 양식으로 구현될 수 있고 배포될 수 있다.

〔조건 11〕
키위탁 PKI의 소프트웨어 및 아키텍처 영역에서 일반 PKI와 호환성을 가져야 한다. 기반구조와 시스템 종합적인 측면에서 동작영역은 여러가지로 나누어 질 수 있다. 첫 번째 영역은 키위탁 기관으로 구성되어 있으며 이 기관은 시스템을 설정할 때와 비밀키를 복구할 때만 동작한다. 키위탁 기관의 동작은 사용자와 독립적으로 이루어진다. 두 번째 영역은 공개키 기반 구조이며 여기서 사용자와 인증기관는 사용자의 비밀키와 쌍을 이루는 인증키를 생성한다. 세 번째 영역은 통신과 공개키 디렉토리에서 인증 공개키를 사용한다.

〔조건 12〕
키위탁 PKI의 통신 프로토콜은 일반 PKI의 통신 프로토콜과 호환성을 가져야 한다. 키위탁 PKI 솔루션은 일반 PKI 프로토콜의 외부에 있는 헤더와 데이터를 변경해서는 안된다. 데이터 송신자는 현재 PKI에서 운용되고 있는 통신 프로토콜을 그대로 사용해야 한다.

〔조건 13〕
키위탁 암호 스킴은 하드웨어나 소프트웨어적으로 필요할 때 언제든지 무시될 수 있도록 설계되어야 한다.

〔조건 14〕
공개키는 PKI를 운용하는 모든 기관에서 안전해야 한다.

〔조건 15〕
시스템은 shadow 공개키 배포를 가능하게 하는 subliminal 채널을 포함해서는 안된다. 이러한 성질은 입증하기는 어렵지만 키위탁 시스템에서 공개해야 하는 정보는 일반 공개키 시스템에서 공개해야 하는 정보와 같다는 것을 의미한다.

PKI 연동 소프트웨어 키위탁 시스템을 설계할 때 필요조건을 설명하였다. 그러나 위와 같은 필요조건 외에도 특정한 키복구 시스템의 안전성을 요구할 경우 구현 환경에 따라 추가해야 할 필요조건이 있을 수 있다.

2.2 일반 필요조건

PKI 키위탁 시스템의 사용성을 높이기 위해 설치 비용이 다른 키위탁 시스템보다 적게 들어야 한다. 즉 사용자가 PKI 사용자와 비교하여 비용을 추가하지 않는 것이 바람직하다. 그러나 CA는 일반 PKI와 비교하여 약간의 비용이 추가로 들어갈 수 있다. 실제적인 비용은 키위탁 기관을 관리하고 운영하는데 추가된다. 특히 키위탁 기관의 안전성이 중요하므로 탬퍼보호 기능을 갖는 하드웨어로 설계되어야 할 필요가 있다.

Ⅲ. 자동 키복구 자동 인증 암호 시스템

이 장에서는 A. Young과 M. Yung이 제안한 ARC(auto-recoverable auto-certifiable cryptosystem)에 대한 구조를 설명한다.[1] ARC는 사용자가 공개키 기반 구조와 연계하여 효율적인 자동 인증키를 생성할 수 있도록 설계된 시스템이다. 일반 PKI는 일반적으로 많이 사용하고 있는 PKI를 인용하였다. 이들을 비교할 수 있도록 아래와 같이 설명하였다.

3.1 공개키 기반 구조(PKI)

다음은 일반적인 공개키 기반 구조에 대한 설명이다. 여기서 인증기관의 주소와 파라메터는 미리 공개되어 있다고 가정한다.

① 각 사용자는 공개/비밀키 쌍을 생성하고 인증기관에게 ID와 함께 공개키를 승인받기 위하여 송부한다.
② 인증기관은 ID를 검증하고 서명함으로써 공개키를 인증하고 공개키 데이터 베이스에 인증서를 보낸다.
③ 메시지를 비밀 통신하기 위하여 사용자는 공개키 데이터 베이스로부터 수신자의 공개키와 인증서를 받아서 인증기관의 서명을 검증한다.
④ 사용자는 수신자의 공개키로 암호화하여 암호문을 수신자에게 보낸다.
⑤ 수신자는 자신의 비밀키로 암호문을 복호화한다.

3.2 자동 키복구 자동 인증 암호 시스템

A. Young과 M. Yung이 제안한 ARC를 설명한다. 여기서 시스템 파라메터 설정이 완성되어 있다고 가정한다. 또 키위탁 기관은 위탁 공개/비밀키 쌍을 생성하고 있고 키위탁 기관의 공개 파라메터와 인증기관의 파라메터는 배포되어 있다고 가정한다.

① 각 사용자는 공개/비밀키 쌍을 생성한다. ID와 함께 공개키와 키복구를 확인할 수 있는 증명서를 인증기관에게 보낸다.
② 위탁 공개키를 사용하여 인증기관은 키복구 인증서을 검증한다. 이 검증이 성공하고 ID가 확인되면 인증기관은 공개키를 서명함으로써 공개키를 인증하고 공개키 데이터 베이스에 인증서를 보낸다.
③ 메시지를 비밀 통신하기 위하여 사용자는 공개키 데이터 베이스로부터 수신자의 공개키와 인증서를 받아서 인증기관의 서명을 검증한다.
④ 사용자는 수신자의 공개키로 메시지를 암호화하고 이 암호문을 수신자에게 보낸다.
⑤ 수신자는 자신의 비밀키로 복호화한다.
⑥ 특정 사용자에 대하여 키복구 권한이 주어지면 키위탁 기관은 사용자의 공개키 그리고 인증기관으로부터 그 사용자의 키복구 증명서을 얻어 개인키를 복구한다.

ARC에서 수행하는 세가지 작업 즉 GEN, VER, REC은 아래와 같이 설명될 수 있다.

① GEN은 공개적으로 알려진 다항식-시간 확률적 튜링 기계이다. 이 기계는 입력은 없고 출력으로서 탭을 갖는 (K_1,K_2,P)를 생성한다. 여기서 K_2는 랜덤하게 생성된 비밀키이고 K_1은 대응되는 공개키이다. P는 K_2가 P를 사용한 키위탁 기관에 의해 키복구될 수 있음을 증명하는 증명서이다.
② VER은 공개적으로 알려진 다항식-시간 결정적 튜링 기계이다. 이 기계는 입력으로 (K_1,P)를 취하고 부울값을 출력한다. 매우 높은 확률로 VER이 참을 출력할 필요충분조건은 P가 비밀키 K_2를 복구하는데 사용될 수 있는 것이다.
③ REC는 개인 ID를 입력으로 하는 결정적 튜링 기계이다. 분산 구현 환경에서 REC_i $(1<i<m)$는 입력으로서 P를 취하고 출력으로서 K_2 중 i를 공유시키는 다항식 시간 결정적 튜링기계이다. 여기서 K_2는 위탁된다고 가정한다. 튜링기계 REC_i $(1<i<m)$는 공동으로 K_2를 복구하는데 사용될 수 있다.
④ REC $(REC_1,\ldots,REC_m)$없이 주어진 K_1과 P로 K_2를 복구하는 것은 어렵다.

A. Young 등은 ElGamal/Diffie-Hellman 암호 시스템에 기반한 ARC 스킴을 설계하였다.

Ⅳ. 제안하는 PKI 키위탁 시스템

이 장에서는 A. Young 등이 제안한 PKI 연동 키복구 시스템 설계 개념을 적용하여 새로운 PKI

연동 키복구 시스템을 제안한다. 제안하는 PKI 연동 키복구 시스템은 RSA 암호시스템에 기반을 두고 있으며 마스터의 공개/비밀키 쌍을 도입한다.

4.1 PKI 키위탁 스킴

키위탁 기관은 마스터 공개/비밀키 쌍을 생성하고 키위탁 기관의 공개 파라메터와 인증기관의 파라메터는 배포되어 있다고 가정한다.

① 각 사용자는 위탁기관의 공개키를 사용하여 공개/비밀키 쌍을 생성한다. ID와 함께 공개키와 키복구를 확인할 수 있는 증명 요청을 인증기관에게 보낸다.
② 마스터 공개키와 사용자 공개키를 사용하여 영지식 증명 방식으로 인증기관은 키복구 가능성을 검증한다. 이 검증이 성공하고 ID가 확인되면 인증기관은 공개키를 서명함으로써 공개키를 인증하고 공개키 데이터 베이스에 인증서를 보낸다.
③ 메시지를 비밀 통신하기 위하여 사용자는 공개키 데이터 베이스로부터 수신자의 공개키와 인증서를 받아서 인증기관의 서명을 검증한다.
④ 사용자는 수신자의 공개키로 메시지를 암호화하고 이 암호문을 수신자에게 보낸다.
⑤ 수신자는 자신의 비밀키로 복호화한다.
⑥ 특정 사용자에 대하여 키복구 권한이 주어지면 키위탁 기관은 공개키 데이터 베이스로부터 사용자의 공개키를 얻어 마스터 비밀키로 사용자의 비밀키를 복구한다.

여기서 마스터 비밀키의 비밀 분산에 의하여 키위탁 기관을 다수로 둘 수 있다.[3,4]

이 논문에서 제안하는 PKI 키위탁 스킴은 ARC와 비슷하나 6번 항의 키복구 과정에서 키위탁 기관은 사용자의 공개키 만을 사용한다. 그러나 ARC인 경우 키복구 과정에서 위탁기관은 사용자의 공개키와 인증기관에서 저장하고 있는 증명서 P가 필요하다.

4.2 PKI 키위탁 암호 시스템 구조

본 논문에서는 RSA 암호방식을 사용한 키위탁 시스템을 제안한다. 구체적인 시스템의 구조는 다음과 같다. 4.2.1에서는 시스템 설정과 암호화/복호화 프로토콜를 설명하고 4.2.2에서는 사용자가 키복구 가능한 공개키를 생성하였는지를 검증하는 프로토콜을 설명하고, 4.2.3에서는 키복구 과정을 설명한다.

4.2.1 시스템 설정과 암호화/복호화 프로토콜

RSA 암호방식은 소인수 분해 문제의 어려움에 기반한 암호방식으로 실제로 많이 사용하고 있는 시스템이다. 키복구 시스템을 설정하기 위한 동작과정과 사용자간의 암호화/복호화 과정은 다음과 같다.

키위탁 기관은 RSA 암호방식과 같은 방식으로 마스터 공개/비밀키 쌍을 생성하여 마스터 공개키를 인증기관의 서명을 받아 공개한다. 이것을 [그림 1]에 나타내었다.

```
P, Q : 소수
N=PQ
Φ=(P-1)(Q-1)
마스터 공개키 E : gcd(Φ,E)=1
마스터 비밀키 D : ED=1 mod Φ

공개정보 : N, E
비밀정보 : P, Q, D
```

[그림 1] 마스터 공개/비밀키 쌍

사용자는 마스터 공개키를 사용하여 RSA 암호방식과 같은 방법으로 공개/비밀키 쌍을 생성한다. 이것은 [그림 2]에 나타내었다.

암호 통신을 하고자 하는 사용자는 공개키 데이터 베이스로부터 수신 사용자의 공개키를 받아 이 공개키로 암호화하고 암호문 $c=m^e \bmod n$을 송신한다. 수신 사용자는 자신의 비밀키를 사용하여 암호문을 복호하고 메시지 $m=c^d=m^{ed} \bmod n$을 얻는다.

```
p, q : 소수
n=pq
φ=(p-1)(q-1)
사용자 공개키 e
        - gcd(φ,e)=1
        - e=p^E mod N (키복구 조건)
사용자 비밀키 d
        - ed=1 mod φ

공개정보 : n, e
비밀정보 : p, q, d
```

[그림 2] 사용자의 공개/비밀키 쌍

4.2.2 키복구 가능성 검증

이 과정은 사용자의 공개/비밀키 쌍이 위탁 기관의 마스터 공개키를 사용하여 생성되었기 때문에, 위탁

기관의 비밀키를 사용하여 사용자의 공개키로부터 사용자의 비밀키를 복구할 수 있음을 인증기관이 검증해야 한다. 여기서 인증기관은 마스터 및 사용자의 비밀키를 알지 못한 조건에서 검증해야 하기 때문에 영지식 증명 방식을 사용한다. 이 영지식 증명 방식에서 증명해야 하는 사항은 $e=p^E \bmod N$과 $n=pq$에 대한 것이다. 만약 $e=p^E \bmod N$만 증명하면 사용자는 가짜 p를 생성하여 키복구를 공격할 수 있다.

영지식 증명 방식에 의한 증명은 [그림 3]과 같이 나타내었다.

① 인증기관은 nN^2보다 큰 임의의 소수 H_1, H_2를 생성하고 원시근 $g_1 \in Z^*_{H_1}$, $g_2 \in Z^*_{H_2}$를 얻어 사용자에게 보낸다.

② 사용자는 소수 P와 원시근 g_1, g_2를 확인하고 $r \in_R Z_N$을 선택한다. 사용자는 인증기관에게 $X_1 = r^E \bmod N$ 및 $X_2 = g_1^r \bmod H_1$ 및 $X_3 = g_2^r \bmod H_2$를 보낸다.

③ 인증기관은 $k \in_R \{0,1\}$를 선택하여 사용자에게 보낸다.

④ 사용자는 $k=0$ 일때 $Y=r$를 $k=1$일때 $Y=rp$ 및 $S=r+q$를 인증기관에게 보낸다.

⑤ 인증기관은 $k=0$일때 $X_1 = Y^E \bmod N$ 및 $X_2 = g_1^Y \bmod H_1$, $X_3 = g_2^Y \bmod H_2$를 검증하고 $k=1$일때 $YS < H_1$ 및 $YS < H_2$ 인가를 확인하고

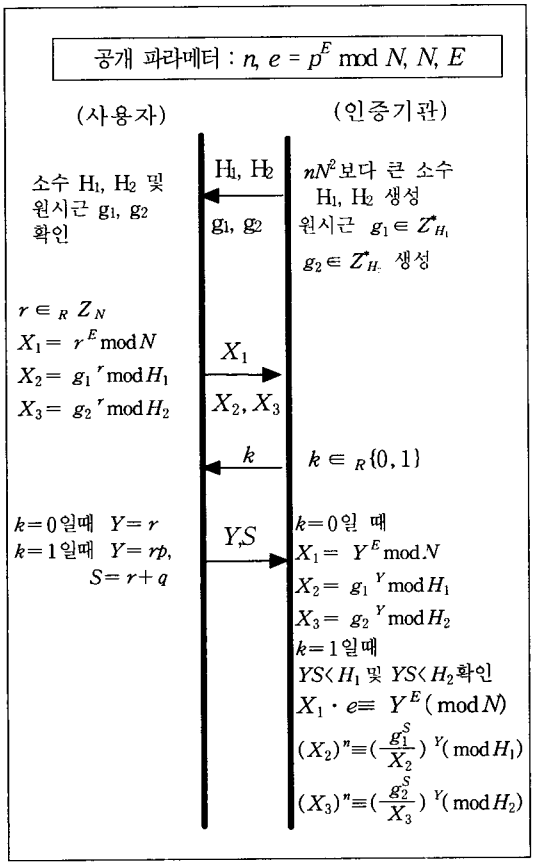
$X_1 \cdot e \equiv Y^E \pmod N$,

$(X_2)^n \equiv (\frac{g_1^S}{X_2})^Y \pmod{H_1}$,

$(X_3)^n \equiv (\frac{g_2^S}{X_3})^Y \pmod{H_2}$를 검증한다.

⑥ 인증기관은 $k=1$일 때 H_1-1/Y, H_2-1/Y 인 소수 H_1, H_2를 생성하고 ①단계의 두 원시근을 얻어 사용자에게 보낸 후 ②단계로 가고, $k=0$일 때 그대로 ②단계로 간다.

4단계로 되어 있는 4-pass 프로토콜을 n라운드 반복하여 높은 확률로 증명을 성공하면 검증자가 승인한다. 검증자 즉 인증기관이 증명을 승인하면 사용자의 공개키 e를 서명하여 공개키 데이터 베이스에 공개하게 된다. 여기서 ⑥ 단계는 $k=1$일 때 한 번 수행하고 다시 되돌아 올 때는 수행하지 않아도 된다.



[그림 3] 키복구 검증을 위한 영지식 증명 방식

4.2.3 키복구

합법적인 키복구를 법집행하기 위해서 키위탁 기관이 해당 사용자의 비밀키를 복구하는 과정을 설명한다. 키위탁 기관은 공개키 데이터 베이스에서 법집행된 사용자의 공개키를 가져 와서 마스터 비밀키로 사용자의 비밀 정보을 계산해 낼 수 있음을 [그림 4]에서 설명한다.

사용자의 공개키 $e = p^E \bmod N$

1. 마스터 비밀키로 사용자의 비밀 정보를 계산한다.
   $e^D = p^{DR} \bmod N = p$
2. 공개 파라메터를 사용하여 q를 계산한다.
   $q=n/p$, $\varphi=(p-1)(q-1)$
3. 유클리드 알고리즘을 사용하여 사용자의 비밀키 d를 계산한다.
   $ed = 1 \bmod \varphi$

[그림 4] 사용자의 비밀키 복구과정

PKI를 설정할 때 시스템의 신뢰성은 인증기관의 시스템에 따르고 키를 복구할 때 시스템의 신뢰성은 키위탁 기관의 시스템에만 좌우됨을 알 수 있다.

V. 안전성 및 효율성

제안하는 키복구 시스템은 시스템 설정 과정과 시스템 운영과정, 비밀키 복구과정으로 나누어 안전성을 설명한다. 그리고 효율성에 대하여 설명하고 제안한 PKI 연동 키복구 시스템과 A. Young의 ARC에 대하여 비교한다.

5.1 안전성

시스템 설정 과정에서 키복구 조건을 만족하는 사용자의 공개/비밀키 생성과 키복구의 안전성을 위한 키복구 가능한 공개키 인증이 필요하다. 사용자의 공개키는 생성할 때 키복구 조건을 만족하여야 하기 때문에 안전성이 낮아질 가능성이 있다. 소인수 분해의 어려움에 기반하고 있지만 랜덤하게 생성되어야 할 사용자의 공개키가 제약조건으로 그렇게 되지 못하기 때문이다. 또한 $e=p^E \bmod N$에서 사용자의 비밀 정보인 소수 p의 LSB가 노출된다. 그러나 이러한 것은 키복구 암호 시스템에 심각하게 안전성을 해치는 것은 아니다. 사용자가 생성한 공개키를 키복구 가능한가를 검증하는 인증기관은 키위탁 기관의 마스터 비밀키를 알지 않고 검증해야 하기 때문에 ZKIP를 사용하여 안전성을 확보하였다.

시스템을 운영할 때 일반 PKI와 같은 프로토콜을 사용함으로써 연동할 수 있는 PKI의 안전성에 의존하게 된다.

사용자의 비밀키를 복구할 때는 키위탁 기관만이 참여한다. 키위탁 기관의 비밀키 즉 마스터 비밀키의 안전성은 소인수 분해의 어려움에 기반하는 RSA 문제와 같다. 사용자의 공개키만 알면 키위탁 기관은 자신의 마스터 비밀키로 사용자의 비밀키를 복구해 낼 수 있다. 따라서 키위탁 기관에 템퍼 보호 기능을 갖춘 비밀키 저장소가 필요하다.

5.2 효율성

본 논문에서 제안된 키위탁 암호 시스템은 ARC 암호 시스템과 같이 PKI 연동 키위탁 암호 시스템의 설계 개념을 적용하고 있다. 그러므로 제안된 시스템이 이미 구축된 PKI에서 사용된다면 매우 효율적이다. 그리고 사용자와 키위탁 기관이 동일한 암호 방식인 RSA 암호 방식을 사용하고 있기 때문에 구현할 때나 운용할 때 편리하다. 또한 제안한 키위탁 암호 시스템은 P. Paillier의 SE-PKI 암호 방식과 같이 마스터 키 개념을 적용하고 있기 때문에 키복구 가능함을 증명하는 증명서를 저장할 필요가 없다. 따라서 A. Young의 ARC 보다 인증기관의 메모리 관리 측면에서 보다 효율적이다.

5.3 제안한 시스템과 ARC의 비교

본 논문에서 제안한 PKI 연동 키복구 시스템과 A. Young이 제안한 ARC에 대한 비교는 아래 [표 1]에서 설명한다.

표에서 알 수 있는 바와 같이 현재 보안 응용분야에서 많이 사용되고 있는 RSA 암호 시스템을 이용하여 키복구 암호 시스템을 구현할 수 있으므로 사용성이 우수할 것이다. 키복구 확인 증명서도 인증기관이 저장하여 관리할 필요가 없으므로 편리하다. 그러나 사용자의 프라이버시를 침해할 수 있는 키위탁 기관이 한 개로 설계되어 있으므로 사용자의 프라이버시를 침해할 수 있다. 이것은 키위탁 기관의 비밀키를 비밀분산 방법에 의해 키위탁 기관을 다수로 구성함으로써 해결할 수 있다.

[표 1] 제안 시스템과 ARC의 비교

	ARC	제안한 시스템
사용자 암호 시스템	ElGamal 암호 방식	RSA 암호 방식
키위탁 암호 시스템	이산대수 문제에 기반한 암호 방식	RSA 암호 방식
PKI 연동성	가능함 .	가능함.
키복구 확인 증명서	인증기관에 저장해야 함.	인증기관에 저장할 필요 없음.
소프트웨어 키복구 시스템	가능함.	가능함.
키위탁 기관	다수.	한 개 (비밀 분산 방법에 의해 다수로 가능)

VI. 결 론

본 논문에서는 공개키 기반 구조와 연동 가능한 효율적인 PKI 연동 키복구 시스템을 제안하였다. 공개키 기반 구조와 연동 가능한 키복구 시스템은 이미 구축된 PKI 시스템을 기반으로 하여 키복구 방식을 구현할 수 있으므로 사용자들에게 요구되는

비용이 적기 때문에 매우 효과적인 방법이다. RSA 암호 시스템에 기반을 둔 PKI 연동 키복구 시스템은 키위탁 기관의 마스터 공개/비밀키와 사용자의 공개/비밀키가 서로 연관되어 있다. 이 키복구 시스템은 키복구 과정에서 증명서를 사용하지 않기 때문에 A. Young의 ARC 보다 효율적이다.

PKI 연동 키복구 시스템에서의 안전성 연구가 더욱 필요하며 사용자 공개키 생성 시 Shadow 공개키 생성을 방지할 수 있는 암호 시스템 연구가 많이 필요하다.

참 고 문 헌

[1] A. Young, M. Yung, "Auto-Recoverable and Auto-Certifiable Cryptosystems", *Advanced in Cryptology-Eurocrypt '98*, Springer-Velag, Lecture Notes in Computer Science, Springer-Verlag, 1998, pp. 17~31.

[2] P. Paillier, Moti Yung, "Self-Escrowed Public Key Infrastructures", *Proceedings of ICISC '99, The 2nd International Conference on Information Security and Cryptology*, Springer-Verlag, Lecture Notes in Computer Science, LNCS, Dec. 9 10, 1999, Seoul, Korea.

[3] D. Boneh, M. Franklin, "Efficient generation of shared RSA keys", *In Proceedings Crypto '97*, Lecture Notes on Computer Science, Vol. 1223, Springer-Verlag. pp. 425~439, 1997.

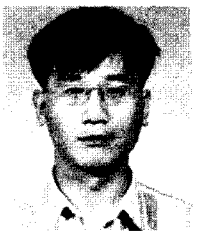
[4] G. Poupard, J. Stern, "Generation of Shared RSA Keys by Two Parties", *Advanced in Cryptology-Asiacrypt '98*, Springer-Velag, Lecture Notes in Computer Science, Springer-Verlag. LNCS 1514, 1998, pp. 11~24.

[5] P. Paillier, "Public-Key Cryptosystem Eased on Composite Degree Residuosity Classes", *Advanced in Cryptology-Eurocrypt '99*, Springer-Velag, Lecture Notes in Computer Science, Springer-Verlag, 1999, pp. 223~238.

〈著者紹介〉

최 희 봉 (Hee-bong Choi) 정회원
1984년 2월 : 부산대학교 전기공학과 학사
1987년 2월 : 부산대학교 전기공학과 석사
1997년 3월~현재 : 성균관대학교 전전컴공학부 박사과정
1987년 2월~2000년 1월 : 국방과학연구소 선임연구원
2000년 2월~현재 : 국가보안기술연구소 선임연구원
관심분야 : 암호이론, 네트워크보안, 보안시스템 설계

오 수 현 (Soo-hyun Oh) 정회원
1998년 2월 : 성균관대학교 정보공학과 학사
2000년 2월 : 성균관대학교 전전컴공학부 석사
2000년 3월~현재 : 성균관대학교 전전컴공학부 박사과정
관심분야 : 암호이론, 정보이론



홍 순 좌 (Soon-jwa Hong)
1989년 2월 : 숭실대학교 전산학과 학사
1991년 2월 : 숭실대학교 전산학과 석사
1991년 3월~ 2000년 1월 : 국방과학연구소 선임연구원
2000년~현재 : 국가보안기술연구소 선임연구원
관심분야 : 암호이론, 네트워크 및 인터넷 보안

원 동 호(Dongho Won) 종신회원
1976년 2월 : 성균관대학교 전자공학과 학사
1978년 2월 : 성균관대학교 전자공학과 석사
1988년 2월 : 성균관대학교 전자공학과 박사
1978년 4월~1980년 3월 : 한국전자통신연구원 연구원
1985년 9월~1986년 8월 : 일본 동경공업대 개원연구원
1982년~현재 : 성균관대학교 전전컴공학부 정교수
관심분야 : 암호이론, 정보이론