通信情報保護學會論文誌
第 10 券 第 1 號, 2000. 3

키 위탁 시스템 설계 모델에 관한 연구

채 승 철*, 황 보 성**, 이 임 영**

A Study on the Design Model of the Key Escrow System

Seung-Chul Chae*, Bo-Sung Hwang**, Im-Yeong Lee**

요 약

암호 시스템에서 가장 중요한 정보는 키 정보이다. 키가 손상되거나 유실되면 모든정보가 유실되기 때문이다. 키 위탁 시스템이란 유사시의 상황에 대비해서 키를 특정한 위탁기관에 위탁함으로써 정보를 암호의 오용이나 키의 분실로부터 보호 할 수 있는 시스템이다. 키 위탁 시스템은 유사시에 확실하게 키를 복원할 수 있어야 하며, 동시에 복구 정보의 안전한 보관이 이루어져야 한다. 그리고 위탁 시스템으로 인해 사생활이 침해되지 않는 것 또한 중요하다. 이러한 요구사항들은 서로 상충되는 점이 있기 때문에 모든 요구사항을 만족시키는 키 위탁 시스템을 설계하기는 매우 어렵다. 본 논문에서는 키 위탁 시스템 설계시에 고려해야할 요소를 도출하고, 키 위탁 시스템 설계 및 분석을 위한 모델을 제안한다. 이 모델은 정의된 요구사항을 만족시키는 키 복구 시스템을 설계할 때 유용하게 사용될 수 있으며, 이미 제안된 키 복구 시스템을 분석하는 도구로 활용될 수 있다.

ABSTRACT

One of the most important thing in a cryptosystem is a key information. If the encryption key is lost or damaged, it may lost all information. A technique known as key escrow, which recovers the encryption key(or message) from encrypted data, can provide solutions for the situations. A key escrow system protects valuable encrypted information in emergency situations(e.g. lost keys). Key escrow system must recover keys using stored escrow information when emergency situation is occurred.

Additionally, the escrow system should not threaten user's privacy. The design of key escrow system is very difficult because these requirements are collided with each other. In this paper, we propose a new key escrow model which can be used for better analysis and designing of a system. The newly developed model can effectively describe relations and operations of all participating objects of the key escrow system, so that it can be used for detecting possible system flaws and attacks.

keyword : *key escrow, key recovery*

Ⅰ. 서 론

정보의 중요성이 부각되면서 암호 기술이 매우 빠른 속도로 보급되고 있다. 암호는 인증, 무결성과 기밀성 등의 기능을 제공하여 안전한 환경을 만들어준다. 하지만 암호의 기밀성은 범죄 목적에 사용되었을 때 정부의 수사 능력을 약화시키며, 키를 분실하였을 경우에는 정보가 유실될 수도 있다. 근래에 이러한

* 이니텍(주)
** 순천향대학교 정보기술공학부

암호의 양면성으로 인한 부작용을 방지하기 위한 대안이 연구되기 시작했는데 유력한 대안은 키 복구(key recovery) 방식이다. 키 복구 방식이란 유사시 키를 복구함으로써 사전에 적법하게 허가된 사람에 한해서 암호의 기밀성을 제거해줄 수 있는 방법을 말한다.

키 복구 방식에는 여러 가지 종류가 있지만 그 중에서 가장 개념적으로 간단하고 현실적인 방법이 키 위탁(key escrow) 방식이다. 키 위탁은 말 그대로 사용자가 암호화에 사용하는 키를 위탁함으로써 나중에 키 복구를 할 수 있도록 한다는 것이다. 하지만 키 위탁은 사용자가 자신의 비밀키를 제 3자에게 노출시킨다는 것에 거부감을 갖게 될 수 있고, 사생활 침해 등의 소지가 높다. 현재까지 이러한 점을 보완할 수 있는 연구가 꾸준히 진행되었지만 사용자의 사생활 침해 가능성을 없애면서 유사시 확실한 키 복구를 할 수 있도록 하는 방식은 제안되지 않았다. 키 위탁 시스템은 그 속성상 설계 단계에서 한 가지 점만 취약하게 설계되면 전체 시스템에 치명적인 영향을 미치기 때문이다.

본 논문에서는 이러한 점을 방지하기 위해서 키 위탁 시스템의 동작을 분석하고, 시스템이 올바르게 동작하기 위한 새로운 모델을 제안한다. 새로운 모델은 위탁 시스템이 수행하는 연산의 정의와 그 수행 주체의 관계를 도시함으로써 취약점을 쉽게 발견하고, 보완할 수 있다. II장에서는 먼저 키 위탁 시스템이 가져야될 요구사항을 정의하고, III장에서는 일반적인 키 위탁 시스템을 구성하는 주체와 연산의 정의를 기술하고 이들의 일반적인 구성 모델을 제시하였으며, VI장에서는 여러 가지 사항을 고려한 확장 모델을 정의하였다.

II. 키 위탁의 정의 및 요구 사항

키 위탁은 여러 가지로 정의되지만 일반적으로 "하나 또는 그 이상의 기관이 비밀키(또는 키의 일부나 키를 복구할 수 있는 정보)를 보관하는 키 복구의 한가지 방법"이라고 할 수 있다. 암호는 수학적인 계산상의 어려움에 근거해서 읽을 수 있는 평문을 해독하기 어려운 암호문으로 바꾸어주며, 이러한 암호문은 키 없이는 해독이 계산적으로 불가능하다. 키 위탁 시스템은 이러한 암호문을 유사시에 복구할 수 있도록 한다는 점에서 이러한 암호의 개념에 위배되는 측면이 있다. 따라서 충분한 안전장치를 확보하지 못한다면 본래 암호의 안전성을 깨뜨릴 수 있다. 따라서 키 위탁 시스템은 여러 가지 측면에서 안전성을 확보해야 한다. 기본적으로 키 위탁 시스템은 다음과 같은 요구 사항을 만족해야 한다.

요구사항 1. 유사시 키(또는 메시지)의 복구가 가능해야 한다.

이것은 키 위탁 시스템의 기본적인 목적이다. 키 위탁 시스템은 이 요구 사항을 만족시키기 위해서 사용자의 키 정보를 저장해야 한다. 기본적인 키 위탁 시스템은 단지 사용자들이 암호화에 사용하는 비밀키(또는 개인키)를 미리 저장함으로써 이러한 목적을 달성할 수 있다. 하지만 이 방법은 키 저장의 위험성, 개인 정보의 침해 가능성 때문에 일반적으로 사용되기가 어렵다. 또한 키 위탁 시스템은 그 속성상 여러 가지 위협요소가 산재해 있기 때문에 단순히 키를 저장하는 것만으로는 유사시 키 복구라는 목적을 만족시키기 어렵다. 따라서 다음과 같은 사항을 고려해서 설계해야만 키 위탁 시스템의 기본적인 목적을 성취할 수 있다.

- 사용자가 올바른 키를 위탁했음을 확인할 수 있어야 한다.[3]
- 사용자가 시스템을 우회하거나 교묘하게 회피할 수 있는 방법이 존재하지 않아야 한다.[4]

요구사항 2. 사용자의 키 정보는 안전하게 보관되어야 한다.

암호 시스템을 사용하는 이유는 정보를 안전하게 저장하고, 전송하기 위함이다. 따라서 키 위탁 시스템이 이러한 목적에 위배되어서는 안된다. 따라서 키 위탁 시스템이 보관하게 되는 키의 복구와 관련된 정보(저장된 키, 키의 일부분, 복구키 등)에 대한 외부/내부로부터의 접근을 통제할 수 있어야 한다. 또한 외부/내부로부터의 여러 가지 공격에 대해서 안전성을 확보해야 하며, 위탁된 정보의 손실에 대한 대비책도 마련되어야 한다.

따라서 추가적으로 다음과 같은 사항이 요구된다.

- 보관된 정보는 손상 위협으로부터 안전해야 한다.[3]
- 허가되지 않은 접근을 방지할 수 있어야 한다.[6]
- 허가된 접근에 대해서도 접근 시간을 제한 할 수 있어야 한다.[5]

요구사항 3. 사용자의 사생활이 보장되어야 한다.

키 위탁 시스템을 통해 불법적으로 키가 복원되어서 사용자의 사생활을 침해하면 안된다. 만약 이러한

위협이 있다면 사용자는 키 위탁 시스템에 참여하지 않을 것이다. 또한 합법적으로 사용자의 키를 복원하더라도 사용자의 신원은 복구를 요청한 주체만 알 수 있는 것이 바람직하다.

- 사용자의 키를 복구하기 위해서는 반드시 적법한 절차에 따라야 한다.[1]
- 사용자의 신원은 복구 요청자만이 알 수 있어야 한다.[6]

키 위탁 시스템이 이와 같은 요구사항을 만족시키는지 검증하기 위해서 본 논문에서는 다음과 같은 과정을 수행하였다..

- 시스템에 참여하는 개체의 구분
- 시스템에서 실행 단계의 구분
- 시스템에서 실행되는 연산의 명확한 정의
- 연산 수행 주체의 명시

각 연산과 주체를 명확하게 구분함으로써 다음과 같은 잇점을 얻을 수 있다.

- 정의된 연산의 오류 유무 검증
- 연산의 수행 주체에 따른 구조적 문제점 도출

Ⅲ. 키 위탁 시스템 설계 모델 구성

키 위탁 시스템은 대칭키 암호 방식과 공개키 암호 방식에 모두 적용될 수 있지만, 본 논문에서는 현재 널리 사용되고 있는 공개키 방식에 기반한 키 위탁 시스템에 관한 모델만을 다룬다. 본 논문에서 키 위탁 시스템은 시스템에 참여하는 참여 개체와 이들 사이에 일어나는 연산으로 정의한다. 본 장에서는 이러한 키 위탁 시스템의 개체와 연산을 정의해서 키 위탁 시스템의 구성요소를 도출한다.

1. 참여 개체

키 위탁 시스템은 기본적으로 시스템에 참여하는 사용자, 사후의 키 또는 메시지 복구에 필요한 여러 가지 정보의 보관을 담당하는 보관 개체, 그리고 실제 키 복구 과정에 참여하는 복구 개체, 그리고 이러한 복구를 필요로 하는 복구 요청 개체 등으로 구성된다. 본 논문에서는 이와 같이 일반적인 키 위탁 시스템에서 반드시 필요한 참여 개체를 기본 개체라고 정의한다. 기본 개체들은 키 위탁 시스템을 구성하는 기본 요소이며 각각의 표기와 역할은 표 1과 같다. 이러한 기본 개체들 이외에 추가적으로 다음과 같은 개체들이 사용될 수 있다. 이러한 개체를 확장 개체라고 정의한다. 확장 개체는 필요에 따라 추가적으로 정의될 수 있으며, 키 복구 자체보다는 키 복구와 통합된 별도의 서비스를 수행하기 위한 개체이다.

- 보안 정책 감시 개체 : 시스템에 정의된 정책을 정의하고, 정책을 위배할 수 없도록 하는 방지 기능 수행
- 참여 인증 개체 : 시스템에 참여한 사용자를 공개적으로 인증할 수 있는 기능 수행(예 : CA)

2. 키 위탁 시스템의 동작 단계

키 위탁 방식은 크게 위탁 단계, 통신 단계, 복구 단계의 세 단계로 구분될 수 있다. 각 단계의 정의는 다음과 같다.

- 위탁 단계 : 사후에 키(또는 메시지)를 복구할 수 있는 정보를 사전에 위탁하는 단계
- 통신 단계 : 위탁된 키를 이용해서 암호문을 송/수신하는 단계
- 복구 단계 : 통신단계에서 생성된 암호문의 키(또는 메시지)를 복구하는 단계

3. 키 위탁 시스템의 연산

키 위탁 시스템은 각 단계별로 표 2와 같은 연산을 갖는다. 각 연산은 시스템 구성에 반드시 필요한 기본 연산과 특정한 목적을 수행하기 위한 확장 연

〔표 1〕 기본 개체의 표기와 역할

기본 개체	표기	역 할
사용자	P	자신의 키를 유사시 복구를 위해 위탁하는 것에 동의하며, 키를 위탁하고, 위탁된 키를 이용하여 암호화 통신을 수행
보관 개체	T	사용자가 위탁한 정보의 안전한 저장을 수행
복구 개체	R	키 위탁시 신원 확인 및 키 복구시 복구요청 확인과 위탁 정보 수집을 수행
복구 요청 개체	I	유사시 적법한 절차에 따라 키(메시지)의 복구를 위한 복구 요청을 수행

〔표 2〕 키 위탁 시스템 기본 연산

	명 칭	표기	동 작
위 탁	공개키 생성 및 위탁 연산	PGen	사용자의 공개키, 개인키 생성, 위탁 정보 생성
	복구 정보 보관 연산	SV	복구에 필요한 정보를 저장하기 위한 연산
	위탁 정보 확인 연산	VP	위탁 정보 유효성 확인
통 신	세션 정보 생성 연산	SGen	세션키 생성 / 세션별 복구 정보 생성
	세션키 암호/복호 연산	E / D	세션키 암/복호화
	복구 정보 유효성 확인 연산	VS	복구 정책 유효성 확인
복 구	식별 연산	ID	암호문의 소유자 판별
	키 복구 요청 연산	RR	키 복구 요청
	복구 정보 수집 연산	RC	복구에 필요한 정보 수집
	복구 연산	DR	복구정보를 이용한 세션키 복구

산으로 분류할 수 있다. 본 절에서는 각 단계에서 반드시 필요한 기본 연산만을 정의한다.

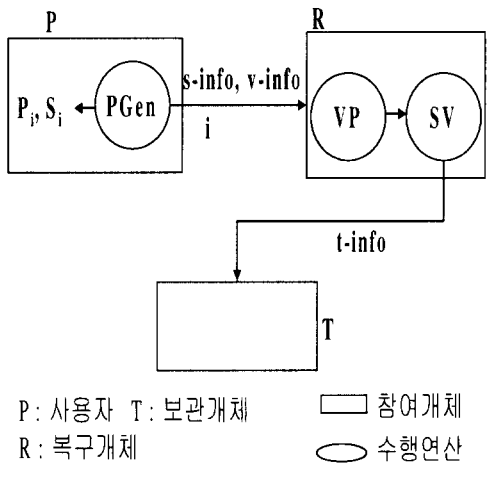
1) 위탁 단계

가) 공개키 생성 및 위탁 연산(Public Key Generation and Escrow Operation) : PGen

$$PGen(uid)=(i,\ pi,\ si,\ s\text{-}info,\ v\text{-}info) \quad (1)$$

(uid : 사용자의 신원 정보, i : 사용자 식별정보, p_i : 사용자의 공개키, s_i : 사용자의 비밀키, s-info : 위탁 정보, v-info : 위탁 확인 정보)

시스템의 사용자 P는 자신의 신원 정보를 제공하고, PGen 연산을 통해서 자신의 유일한 식별정보 I와 공개키/개인키 쌍(p_i, s_i)을 얻는다. 또한 사용자의 개인키와 관련된 위탁 정보 s-info가 생성된다. s-info는 개인키 자체가 되거나 개인키에서 유도된 어떤 값이 될 수 있다. 이 연산의 주체는 기본적으로는 사용자 P가 된다.



〔그림 1〕 위탁 단계의 연산 모델

나) 위탁 정보 확인 연산(Private Key Information Verify Operation): VP

$$VP(s\text{-}info, v\text{-}info) = (ACCEPT/REJECT) \quad (2)$$

(s-info : 위탁 정보, v-info : s-info의 유효성 증명 정보)

다) 복구 정보 저장 연산(Recovery Information Saving Operation) : SV

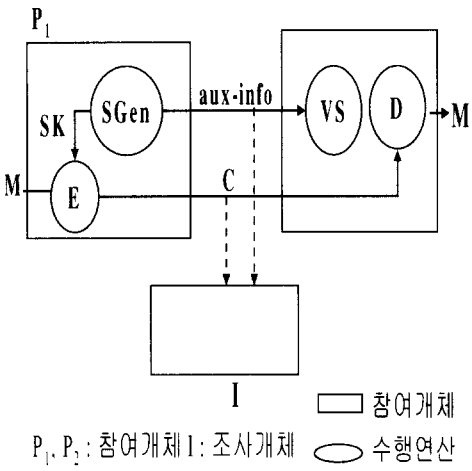
$$SV(i, s-info) = (t-info) \quad (3)$$

(i : 사용자 식별정보, s-info : 위탁 정보, t-info : 저장된 위탁정보)

PGen에서 생성된 위탁 정보를 보관개체 T에게 위탁하는 동작을 수행한다. 연산 수행의 주체는 사용자 또는 복구개체 R이 될 수 있다. 만약 저장기관이 다수이면 이 연산을 통해 다수의 t-info를 생성해서 저장한다.

2) 통신 단계

가) 세션 정보 생성 연산(Session Key Generate Operation) : SGen



〔그림 2〕 통신 단계의 연산 모델

$$SGen(SS) = (SK, aux-info) \quad (4)$$

(SS : 세션에 사용되는 정보(예 : 랜덤수), SK : 세션키, aux-info : 세션별 복구 정보)

각 세션에 필요한 세션키 SK와 세션별 복구 정보 aux-info를 생성한다.

나) 암호화 연산(Encrypt Operation) : E

$$E(SK, M) = C \quad (5)$$

(SK : 세션키, M : 평문, C : 암호문)

세션키 SK와 메시지를 입력으로 받고, 암호문를 출력한다. 암호문안에는 키 교환 필드가 포함된다. 키 교환 필드는 수신자만이 사용할 수 있도록 구성된다.

다) 복호화 연산(Decrypt Operation) : D

$$D(C) = M \quad (6)$$

(C : 암호문, M : 평문)

키 교환 필드가 포함된 암호화 메시지를 입력으로 받고, 메시지를 출력한다. 복호화 연산은 수신자만이 수행할 수 있다.

라) 복구 정보 확인 연산(Session Key Information Verify Operation): VS

$$VS(C, aux-info) = (ACCEPT/ERJECT) \quad (7)$$

(C : 암호문, aux-info : 세션별 복구 정보)

각 세션에서 생성된 aux-info의 유효성 여부를 확인한다. 복구정보 확인 연산의 수행 시점은 통신 시점, 복호 시점, 복구 시점 등이 될 수 있다.

3) 복구 단계

가) 식별 연산(Identify Operation) : ID

$$ID(C, aux-info) = i \quad (8)$$

(C : 암호문, aux-info : 세션별 복구 정보, i : 사용자 식별정보)

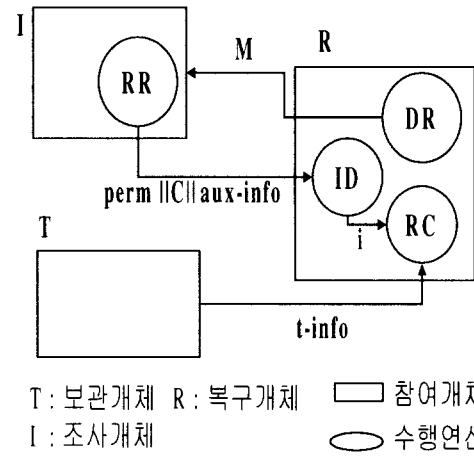
암호문과 공개정보, aux-info를 입력으로 받아서 $i \in 1, 2, \ldots, n$을 출력하는 연산. i는 암호문을 복호할 수 있는 사람의 식별정보가 된다.

나) 복구 요청 연산(Recovery Request Operation) : RR

$$RR(C, perm) = (ACCEPT/REJECT) \quad (9)$$

(C : 암호문, perm : 승인 정보)

이 연산은 복구요청 개체 I가 복구 개체 R에게 데이터의 복구를 요청하기 위해 수행된다. 연산을 수행하기 위해 복구 요청 개체 I는 적절한 승인 perm을 얻어야 한다. perm을 얻는 과정은 RR연산 내에 포함된다.



〔그림 3〕 복구 단계의 연산 모델

다) 복구 정보 수집 연산(Recovery Information Collect Operation) : RC

$$RC(i) = t\text{-}info \quad (10)$$

(t-info : 보관개체 T가 저장하는 위탁 정보)

보관 개체 T가 보관하고 있는 복구 정보를 수집해서 위탁정보 t-info를 재구성한다.

라) 복구연산(Recovery Operation): DR

$$DR(C, i, t-info) = SK \quad (11)$$

(C : 암호문, i : 암호문의 식별정보, t-info : 저장된 위탁 정보)

암호문과 인덱스 i, 저장된 위탁정보 t-info을 입력으로 받아서 세션키 SK를 출력한다. 키 위탁 시스템이 올바른 결과를 출력하기 위해서는 다음과 같이 동작해야 한다.

$$ID(E(SK, p_i), (p_1, , p_n), aux-info) = i \quad (12)$$

$$DR(E(SK, p_i), i, t-info) = SK \quad (13)$$

$(\forall i \in \{1, , n\}, SK \in \alpha$ (α : 세션키 생성 공간))

4. 기본 모델 구성

앞에서 살펴본 그림 1, 2, 3은 기본적인 참여 개체와 수행 연산들을 이용한 위탁, 통신, 복구단계의 기본 모델이다. 본 모델은 위에서 정의된 각 단계에서의 수행 연산을 수행 주체와 더불어 표기할 수 있다.

그림 1의 위탁단계 기본 모델에서 각 송신자(P_1)/수신자(P_2)가 키를 생성하여 복구개체 R에게 위탁하는 단계를 거친다. 복구개체 R은 위탁정보 s-info를 v-info를 이용해 확인한 후에 위탁 정보를 보관기관에게 보내서 저장한다. 그림 2의 통신단계는 일반적인 암호 통신 방법과 동일하지만 복구 정보 필드인 aux-info가 추가된다. aux-info는 암호문의 소유자 식별, 세션키 정보 등을 가지고 있다. 그림 3의 복구 과정 모델에서 복구 요청 개체 I는 암호문 C와 aux-info를 얻어서 적절한 승인(perm)과 함께 복구 개체로 전송함으로써 암호문을 복구할 수 있다. 복구개체 R은 복구 정보 aux-info와 암호문 C로 암호문의 소유자를 식별하고, 보관 개체에 보관된 s-info를 이용하여 복구 연산인 DR 연산을 수행해서 메시지를 복구한다.

VI. 기본 모델 문제점 분석 및 키 위탁 연산 확장 모델

그림 1에 정의된 키 위탁 모델이 정의된 연산처럼 동작한다면 2장에서 정의된 요구사항을 만족할 수 있지만 실제로는 여러 가지 위협 및 오용의 위험성이 상존한다. 본 절에서는 키 위탁 시스템 설계시에 시스템이 올바르게 동작할 수 있도록 고려되어야 할 점을 위에서 제시한 설계모델에 적용하여 시스템이 보다 안전하게 동작할 수 있도록 확장시킨다.

1. PGen 연산 확장

1) 참여 주체

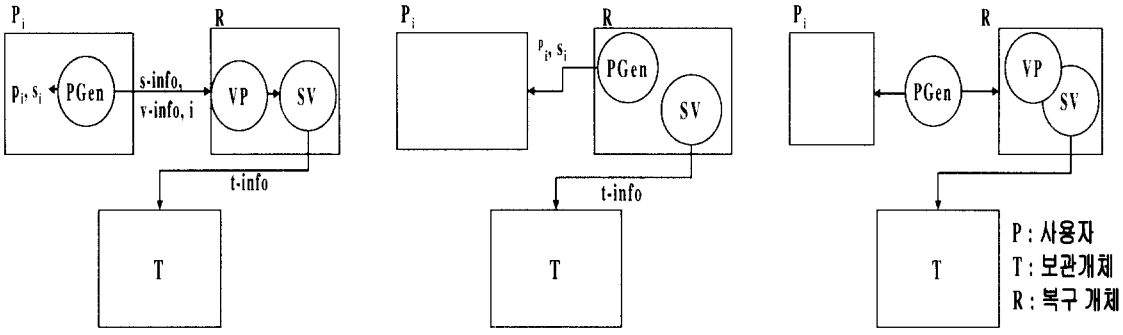
일반적인 공개키 암호 시스템에서 사용자의 공개키는 사용자가 랜덤하게 생성한다. 하지만 키 위탁 시스템에서는 사용자가 전적으로 키를 생성할 때 다음과 같은 문제점이 발생할 수 있음을 Killian[4]등이 지적하였다.

- 사용자는 키에 특별한 조작을 가해서 위탁 시스템을 우회하면서 암호를 사용할 수 있다.

공개키 기반구조의 참여 조건으로 키 위탁이 이루어질 경우, 사용자는 shadow 공개키를 이용한 은닉 채널(subliminal channel)을 구성함으로써 실제로는 키 위탁을 하지 않은 것과 마찬가지의 효과를 노릴 수 있다. 이것은 2장에서 제시한 모델에서 공개키 생성 및 위탁을 수행하는 PGen 연산을 사용자 P가 혼자서 수행하도록 구성되는 경우 s-info의 내용을 복구 연산 DR의 입력으로 사용하면 올바른 키를 얻을 수 없는 가능성이 높아진다는 것을 의미한다. 이러한 문제점을 해결하기 위해서는 다음과 같은 방법이 가능하다.

가) 신뢰받는 제 3자에 의한 키 생성

이 방법은 신뢰받는 제 3자(Trusted Third Party, 이하 TTP라고 한다)가 사용자의 공개키, 비밀키 쌍을 생성해 주는 것이다.[6] 하지만 키 생성을 TTP가 할 경우 사용자 입장에서는 키가 랜덤하게 선택되었다는 것을 확신할 수 없다. 사용자 입장에서는 자신의 키가 랜덤하게 선택되었다는 것을 확신할 수 없다면, 시스템 전체를 신뢰할 수 없을 것이다. 이러한 점을 방지하기 위해서 TTP는 미리 여러 개의 키 쌍을 생성하고, 사용자가 이러한 키 쌍중에서 하나를 자



(a) 사용자 (b) 복구개체 (c) 사용자-복구개체

〔그림 4〕 PGen 연산 확장 모델 - 수행 주체 (위탁 단계)

신의 공개키, 비밀키 쌍으로 선택하는 방법이 있다.

나) 규칙 기반(Rule Based)의 키 생성

사용자가 키를 생성하되, 미리 정해진 규칙에 따라 키를 생성하고 생성된 키가 규칙에 따랐는지 여부를 검사한다.[7] 이러한 방법으로 사용자가 키를 생성하더라도 은닉 채널 구성을 막을 수 있다. 하지만 이 방식에서는 마스터 키가 존재하게 되므로 마스터 키의 분산 보관 및 복원시 정보 누출 가능성에 대한 대책이 필요하다.

다) 사용자-TTP의 상호작용에 의한 키 선택

키 선택을 공평하게 하기 위해서 bit-commitment 등의 기법이나 cut and choose 방식이 많이 이용된다.[4] 이렇게 선택된 키는 사용자와 보관개체 모두 랜덤하다는 것을 확신할 수 있다.

하지만 기존의 공개키 기반구조의 키 발급 과정과 절차가 매우 달라진다는 단점이 있다. 이 방식은 그림 4의 (a)에서 처럼 사용자가 키를 생성할 때 부정을 방지하기 위해 사용된다.

그림 4에서는 PGen 연산의 수행 주체에 따른 모습을 기술하고 있다. (a)는 일반적으로 사용자가 키를 생성하고, 위탁하는 형태이며, (b)는 복구 개체가 키의 생성과 위탁을 수행한다. (c)의 경우는 사용자와 복구개체가 키 생성의 일부를 담당한다.

표 3에서는 PGen 연산의 수행 주체에 따른 장단점을 정리하였다. 수행주체는 각각의 상황에 따라 장단점을 고려해서 정해질 수 있다.

2) 키 위탁 확인 연산 VP 확장

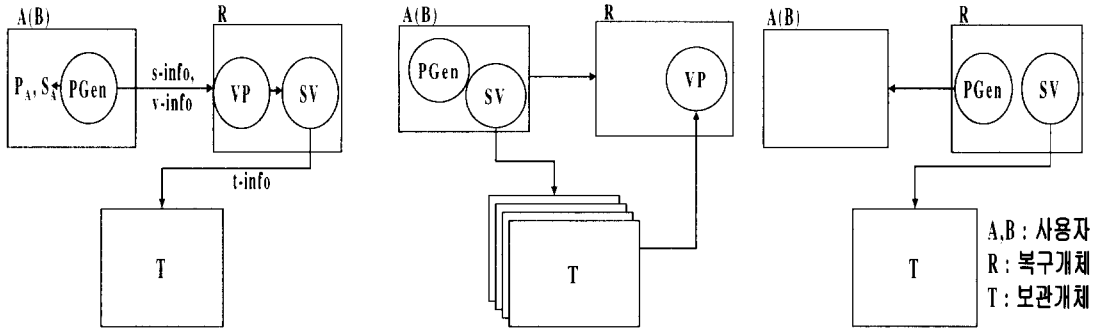
키를 위탁할 때에는 키가 올바르게 위탁되었다는 것을 증명할 수 있어야 한다.

이 문제는 PGen 연산에서 키 생성을 서버 측에서 담당할 경우에는 발생하지 않는다. 또한 사용자가 키를 생성하더라도, 하나의 보관개체에 위탁할 경우는 이러한 증명이 간단해 지지만 여러 개의 보관개체에 분산 위탁할 경우는 과연 사용자가 위탁하는 키가 실제 사용자의 개인키인지 확인하기는 어렵다. 하지만 키 보관의 안전성을 고려한다면 보관 개체 T를 다수로 구성하는 것이 좋다.

또한 PGen 연산은 사용자의 통신량과 보관개체의 부하 문제를 줄일 수 있도록 설계되어야 한다. PGen 연산을 설계할 때는 다음과 같은 기법이 많이 적용된다.

〔표 3〕 PGen 연산의 수행 주체에 따른 장단점

주 체	장 점	단 점
사용자	· 사용자가 자신의 키의 안전성에 대해 확신. · 공개키 기반구조와의 연계 가능	· 위탁된 사용자 키의 유효성 여부 판정 · 사용자의 은닉 채널 구성 가능
복구개체	· 사용자는 별도의 위탁 및 확인 과정이 필요 없음(복구개체가 위탁)	· 사용자가 자신의 키가 랜덤한지 확신할 수 없음 · 복구개체의 불법적 복구가능
사용자-복구개체	· 은닉채널 구성이 불가능 · 양쪽이 키의 안전성에 대해 확신	· 키 생성 과정시 통신량의 증대



(a) 복구개체를 통한 키 위탁 (b) 사용자 직접 위탁 (c) 복구기관의 생성 및 위탁

〔그림 5〕 복구 정보 보관 연산 SV와 및 확인 연산 VP (위탁 단계)단계)

가) 사용자의 VSS(Verifiable Secret Sharing, 증명 가능한 비밀 분산) 수행

자신의 개인키를 비밀 분산에 따라 여러 개로 분할하고 확인 정보를 만든다. 이것은 VSS 방식의 개념에 따라 위탁되는 시점에서 키 정보의 유효성 여부가 확인 가능하다. 가능한 상호작용하지 않도록(non-interactive) 구성하는 것이 바람직하다. 또한 이 개념이 도입되면 (k, n) threshold 등의 기법으로 키 보관의 안전성을 높일 수 있다.

나) 보관 개체의 영지식 증명(Zero-knowledge Proof) 수행

보관정보의 확인을 위해 영지식 증명만을 사용한다. 영지식 증명의 주체는 사용자가 아니라 보관개체가 된다. 보관개체는 복구개체 R 또는 다른 주체에게 올바른 키 정보를 위탁받았음을 확신 시켜 줄 수 있다.

3) 세션별 복구 정보 생성 연산 SGen

SGen 연산의 주체는 사용자 P가 된다. 그러나 출력값의 유효성 확인이 필요한 경우, 수신자, 보관개체 또는 제 3자가 유효성을 확인하기 위해 이 연산에 참여할 수 있다. SGen 연산은 각 세션별로 달라지는 데이터 암호화 키(data encryption key)와 관련된 복구 정보 aux-info를 생성한다. 또한 aux-info안에는 이 정보의 소유자의 신원을 알 수 있는 정보가 포함될 수 있다. 출처 인증이 다른 방법으로 이루어질 수 있는 경우에는 신원 정보가 포함되지 않아도 된다. aux-info는 해당 세션에 관련된 정보만을 포함해야 하며, 그렇지 않을 경우에는 복구 기한의 제한이 어려워진다.

SGen 연산의 출력은 직접 복구개체에게 전송할 수도 있지만, 효율적인 측면에서 일반적으로 암호문과 함께 연접해서 전송된다.

aux-info의 유효성확인 주체는 그림 5에서와 같이 수신자, 보관개체 또는 제 3자가 될 수 있다. 수신자는 세션키 SK 정보를 수신하므로 쉽게 복구 정보의 유효성 여부를 판별할 수 있지만, 송/수신자가 공모한 경우의 부정은 방지할 수 없다. T의 경우 저장된 위탁정보 비밀 정보인 t-info를 알고 있기 때문에 비교적 쉽게 유효성을 검사할 수 있지만, 이 때 비밀키가 노출되지 않도록 주의해야하며, 제 3자의 경우는 아무런 정보가 없기 때문에 aux-info 자체에서 유효성 여부를 판별할 수 있는 매커니즘을 별도로 설계해야 한다.

표 4에서는 SGen 연산이 출력 가능한 정보를 기술하였다. SGen 연산은 필요에 따라 표에 기술된 정보들의 조합을 생성할 수 있다.

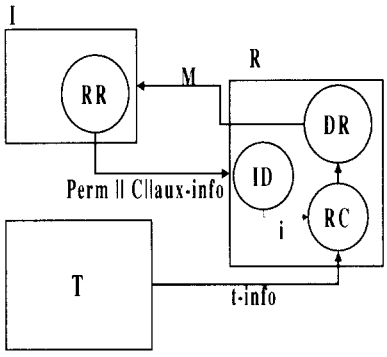
〔표 4〕 SGen 연산의 출력 정보

출력 정보	용 도	비 고
세션키 SK	데이터 암호화 키	복구 기한의 제한
세션키 복원 정보	키 복구 정보	직접 정보(키 캡슐화) 간접 정보(키 관련 정보)
사용자 식별 정보	해당 사용자의 비밀키 검색	별도의 출처 인증이 가능하면 생략 가능
aux-info 확인 정보	전체 aux-info의 유효성 확인	확인 주체의 고려 : 수신자, 복구개체, 제 3자

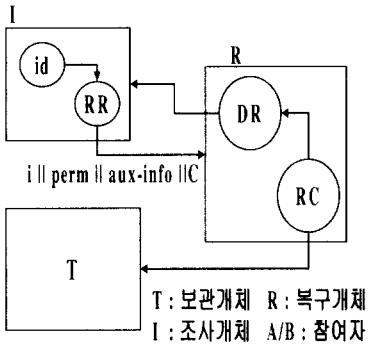
4) 암호문의 소유자 식별을 위한 ID 연산의 고려사항 : 사용자 신원의 보호

사용자 신원을 보호하기 위해서는 참여 개체들 중 최소의 개체만이 사용자의 신원을 알 수 있도록 하는 것이 바람직하다. 따라서 ID 연산을 수행할 수 있는 주체를 제한할 수 있도록 설계하는 것이 바람직하다. ID 연산의 수행 제한은 입력인 세션별 복구 정보 aux-info 등의 정보를 암호화하는 것으로 가능하다. 또한 여기서 얻어진 i와 사용자의 신원 정보를 분리함으로써 사용자의 신원을 보호할 수 있다.

그림 6은 사용자의 신원 보호를 위해 복구 요청 객체가 복구 요청 연산만을 담당하는 수동적인 역할에서 능동적인 역할을 담당하도록 구성된 모델이다. 기본 모델에서는 ID 연산의 수행 주체가 복구 개체이다. 복구 요청 개체 I는 수동적인 역할로써 복구 요청 RR을 통해 세션키 SK를 수신한다. 이러한 경우 사용자의 신원은 복구 요청 개체 I 뿐아니라 ID 연산 수행 개체인 R에게도 노출된다. 하지만 그림 6의 (b)에서처럼 복구 요청 개체 I가 사용자의 신원을 식별하는 ID 연산을 수행한다면 사용자의 신원은 I에게만 노출되며 R, T는 사용자의 신원을 알 수 없다.[8]



(a) 복구단계



(b) 신원보호를 위한 확장

[그림 6] 사용자의 신원 보호(복구 단계)

5) DR(복구 연산) 확장

복구 연산 설계시에 고려되어야 할 사항은 적절한 상황이 되었을 때만 수행될 수 있도록 하여야 한다는 것이다. 이러한 상황의 제한은 복구 연산 자체에서 고려될 수도 있고 이전 단계인 ID 연산에서 고려될 수도 있다. 또 한가지 고려되어야 할 사항은 복구 기한의 제한 문제이다. 이러한 시간 제한은 세션키 SK가 시간(또는 메시지) 단위로 변화하도록 설계하거나 DR 연산의 입력 정보인 보관 개체에 저장된 위탁 정보 t-info 자체를 변화하도록 설계할 수 있다. 그러므로 복구 개체가 보관 개체로부터 받은 t-info를 계속 이용하는 것을 막을 수 있고, 이 경우 s-info와 t-info가 달라지게 된다.

복구 연산은 저장된 위탁 정보인 t-info 정보를 입력으로 하기 때문에 별도의 t-info 정보를 획득할 수 있는 방법이 있어야 한다. 또한 ID 연산의 결과인 i를 입력으로 한다.

$$DR(C, i, t-info) = M \quad (14)$$

(C : 암호문, i : 사용자 식별정보, t-info : 저장된 위탁정보)

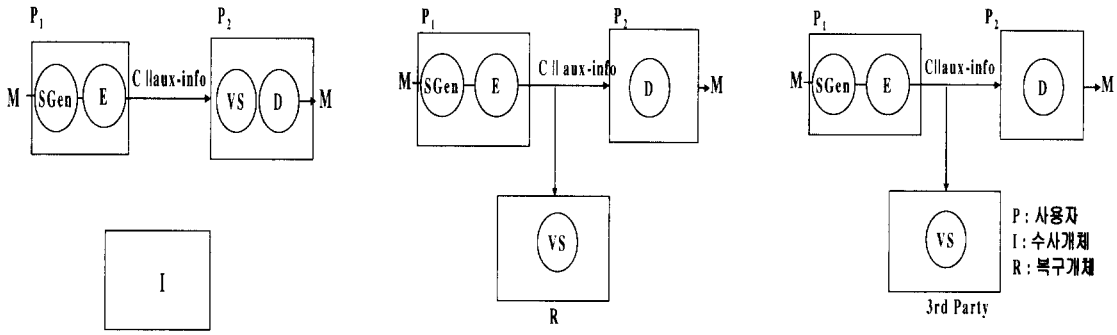
6) TTP들의 공모 방지

키 위탁에서 고려되어야할 또 한가지 중요한 점은 보관개체 T, 복구개체 R, 복구 요청개체 I 등의 부정 방지 기능이다. 위탁 시스템은 설계 단계에서부터 이러한 부정을 방지할 수 있어야 사용자의 사생활을 보호할 수 있다. 이러한 개체들은 서로 독립적인 역할을 수행하도록 설계되어야 한다. 예를 들면 복구 요청개체 I는 암호문 C의 획득과 ID 연산 수행, 보관개체 T는 s-info의 분산 보관, 복구개체 R은 DR 연산의 수행 등으로 분리하면, R이 DR 연산을 수행하기 위해서는 I와 T의 협조가 필요하며, I 또한 R과 T의 협조없이는 조사가 불가능하다.

7) VS 연산의 수행 주체

VS 연산은 통신단계에서 각 세션 정보가 올바른지 확인하는 역할을 수행한다. 그림 7은 VS 연산의 수행이 가능한 주체를 나타내고 있다.

그림 7의 (a)에서 수신자가 복구 정보 aux-info의 유효성을 확인하는 경우에는 송수신자가 공모하면 부정을 저지를 소지가 있다. 따라서 tamper-proof 하드웨어를 사용해야 이러한 문제를 방지할 수 있다. 그림 5의 (b)와 (c)에서는 이러한 부정을 방지하기



(a) 수신자에 의한 수행 (b) 복구개체에 의한 수행 (c) 제 3자에 의한 수행

[그림 7] 세션 복구 정보의 확인

위해서 각각 복구 개체와 제 3의 개체가 이러한 확인 역할을 수행한다. 그러나 복구 개체 R이 확인을 수행하는 경우에는 R의 부하가 높아지며 제 3자가 이것을 확인하기 위해서는 SGen에서 별도의 확인 정보를 생성해 주어야 한다.

본 장에서는 3장에서 정의된 시스템 구성 개체와 연산을 이용해서 키 위탁 시스템 동작시에 일어날 수 있는 위협 요소를 분석하고 이를 해결하기 위해 기본 모델에서 변화되어야할 시스템 구조를 기술하였다. 키 위탁 시스템은 크게 두가지 위협 요소를 지 니고 있는데 첫 번째 위협 요소는 사용자 정보의 침해 가능성이며, 두 번째 요소는 키(또는 메시지)가 복구될 수 없도록 하는 위협이다. 이러한 공격 위협에 대한 취약점을 보완하기 위해서는 시스템의 설계 단계에서 발생할 수 있는 취약점을 고려해야 하며, 그렇지 않으면 설계 후에는 전체 시스템의 안전도가 크게 떨어지고, 취약점을 보완하기가 매우 어렵다. 또한 한 가지 취약점을 보완하기 위한 방법이 새로운 취약점을 발생시키지 않는지도 항상 고려되어야 한다.

따라서 키 위탁 시스템은 적용될 분야의 적절한 요구사항과 위협요소에 대한 대비책을 고려해서 시스템을 설계해야 한다. 본 모델은 시스템에 필요한 모든 개체와 연산 그리고 고려요소를 명확하게 분리하고 정의함으로써 이러한 설계에 유용하게 사용될 수 있도록 하였다.

V. 결 론

본 논문에서는 암호화된 메시지에 접근이 불가능한 경우에 대비해서 키 위탁 방식을 보다 안전하고 효율적으로 설계하기 위한 모델을 제시하고 설계시 요구사항과 공격 위협을 분석하고, 키 위탁에 필요한 주체와 연산을 분류하였다.

또한 이러한 요구사항과 위협에 대처하기 위해서 필요한 구성 방법을 고찰함으로써 키 위탁 시스템의 설계와 분석의 도구로 사용될 수 있는 모델을 제시하였다.

현재까지 키 위탁 시스템에 관한 모델에 대한 정의는 Denning[2]과 NIST(National Institute of Standards and Technology)의 KRS(Key Recovery Standard)에서 제시된 모델이 존재한다. 하지만 Denning 모델의 경우 이해를 돕기 위한 개념적 모델로 매우 단순한 구조만을 기술하고 있으며, KRS에서 제시한 모델은 제품 평가를 위해 복구 시스템에 포함되어야 할 각 기능들의 포괄적인 정의만을 표시할 수 있다. 이러한 두 가지 모델은 수많은 키 복구 방식을 전부 포괄하도록 구성되었기 때문에 매우 추상적이고, 따라서 기존 시스템의 안전도와 효율성을 분석하거나 새로운 시스템을 설계하기 위해서는 보다 세부적인 모델이 필요하다.

본 논문에서 제시한 모델은 그 범위를 키 위탁 방식을 사용하는 시스템으로 한정하고, 각각의 세부적인 연산에 대한 정의와 동작을 정의하였다. 또한 위탁 시스템의 구성 형태에 따른 문제점과 해결책을 제시하였다. 본 모델은 기존의 모델과 다음과 같은 점에서 구별된다.

- 각 연산의 수행 주체의 표기
- 시스템의 안전도를 구조적 관점에서 분석
- 각 연산의 구체적 고려사항 제시

따라서 이러한 모델을 사용하면 시스템 설계시 요구사항에 따른 구성 형태의 도출이 용이해지고, 만들어진

시스템의 검증 및 분석시에는 세부적인 분석 지침을 만드는데 이용될 수 있을 것이다.

참 고 문 헌

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

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

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

[4] Joe Kilian and Tom Leighton, "Fair Cryptosystems, Revisited", Advances in Cryptology-CRYPTO '95, pp. 208-221, 1995.

[5] Arjen K. Lenstra, Peter Winkler and Yacov Yacobi, "A Key Escrow System with Warrant Bound", Advances in Cryptology-CRYPTO '95, pp. 197-207, 1995.

[6] Kouichi Sakurai, Yoshinori Yamane, Shingo Miyazaki and Tohru Inoue, "A Key Escrow System with Protecting User's Privacy by Blind Decoding", 1998.

[7] Adam Young and Moti Yung, "Auto-Recoverable Auto-Certifiable Cryptosystems", Eurocrypto '98, pp. 17-31, 1998.

[8] Patrick Hoster, Markus Michels and Holger Petersen, "A new key escrow system with active investigator", University of Technology Chemnitz-Zwickau, Technical Report TR-95-4-F, 1995.

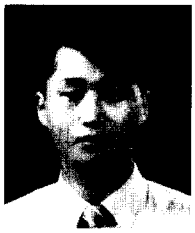
[9] 이임영, 채승철, "Key recovery 시스템에 관한 고찰", 한국통신정보보호 학회지, 제 7권 4호, pp. 45-58, 1997.

[10] 채승철, 이임영, "키 복구 시스템에 관한 고찰 II", 한국 통신정보보호 학회지, 제8권 제4호, pp. 46-61, 1998.

[11] 채승철, 이임영, "키 복구 시스템의 공격 방식에 관한 연구", '98 통신 정보보호학회 충청지부 학술발표논문집 제2권 제1호, pp. 223-233, 1998.

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

〈著者紹介〉



채 승 철 (Seung-Chul Chae) 학생회원
1997년 8월 : 순천향대학교 전산학과 졸업
1999년 8월 : 순천향대학교 전산학과 대학원 졸업
1999년 8월 - 현재 : 이니텍(주) 근무
〈관심분야〉 암호 이론, 컴퓨터 보안

황 보 성 (Bo-Sung Hwang) 학생회원
1999년 2월 : 순천향대학교 전산학과 졸업
1999년 3월 - 현재 : 순천향대학교 전산학과 대학원 석사과정
〈관심분야〉 암호 이론, 컴퓨터 보안

이 임 영 (Im-Yeong Lee) 정회원
1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학과 석사
1989년 3월 : 오사카대학 통신공학과 박사
89년 1월 - 94년 2월 : 한국전자통신연구원 선임연구원
94년 3월 - 현재 : 순천향대학교 정보기술공학부 부교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안