情報保護學會論文誌
第12券 第3號, 2002. 6

키 복구를 지원하는 향상된 신원위탁 메커니즘*

이 용 호**, 이 임 영**, 김 주 한***, 문 기 영***

A Identity Escrow mechanism supporting key recovery

Yong-Ho Lee**, Im-Yeong Lee**, Ju-Han Kim***, Ki-Young Moon***

요 약

사용자와 서비스 제공자가 인증을 수행할 경우 사용자의 신원이 노출되는 문제가 사회의 큰 이슈로 떠오르고 있으며, 이러한 문제점을 해결하기 위해서 신원 위탁 방식이 제시되었다. 신원 위탁 방식에서는 사용자의 정확한 신원을 가지고 있는 발행자가 사용자에게 익명 인증 정보를 안전하게 전송하고, 사용자는 이것을 이용해 익명성을 유지한 채로 서비스 제공자와 인증 단계를 수행하게 된다. 본 논문에서는 신원 위탁 방식의 안전성과 신뢰성을 위한 요구사항을 제시하고 이를 만족할 수 있는 새로운 메커니즘을 제안한다. 또한 서비스 제공자가 사용자에게 컨텐츠를 안전하게 전달할 수 있는 방안과 동일 도메인 내 사용자들 간의 키 동의에 의해 생성된 키를 이용한 암호화 통신 시 키 복구를 지원하는 향상된 메커니즘을 제안한다.

ABSTRACT

In case certification between user and service provider is achieved, problem that user's identity is revealed is occurring by social issue, so it was presented identity escrow scheme to solve these problem. In identity escrow scheme, the issuer who have correct user's identity transmits securely anonymity authentication information to user, and user achieves authentication phase with service provider keeping oneself anonymity using this. In this paper, we present requirement for security and trusty of identity escrow scheme and propose new mechanism that can security this. Also, propose method that service provider can deliver securely contents to user and propose mechanism that improve that support key recovery at encryption communication that using secret key that it was generated by key agreement between users.

Keyword : *신원위탁, 키 복구, 익명성 제어, 익명성 제거 공개 검증성*

Ⅰ. 서 론

사용자들이 인터넷을 통하여 컨텐츠를 제공받기 위해서는 서비스 제공자에게 자신이 정당한 사용자임을 증명해야 하는데 이 같은 개인식별은 사용자들의 프라이버시를 침해할 수 있다. 따라서 인증 수행 시 사용자는 신원에 대해 익명성을 원하며, 서비스 제공자는 사용자의 정당성을 확인하기 원한다. 이와 같이 상이한 두 가지 조건을 충족시켜 줄 수 있는 것이 신원 위탁 방식이다.[2,3,8,10~12]

신원 위탁 방식에서는 사용자와 서비스 제공자간의 인증 수행 시 사용자는 서비스 제공자에게 자신의 신원을 제공하지 않고, 익명 인증 정보를 제공함으로써 사용자에게 익명성을 유지시킨다. 그리고 서

* 본 연구는 한국전자통신연구원 연구과제 지원으로 수행되었습니다.
** 순천향대학교 정보기술공학부(abysskey@lycos.co.kr, imylee@sch.ac.kr)
*** 한국전자통신연구원 능동보안기술연구팀({juhankim, kymoon}@etri.re.kr)

비스 제공자는 익명 인증 정보를 통해서 사용자의 신원은 알 수 없지만 정당한 사용자라는 것을 검증할 수는 있다. 그리고, 만약 사용자가 불법적인 행위를 하였을 경우에 사용자의 익명성을 제거하기 위해서 사용자로부터 제공받은 인증 정보를 법기관에게 제공하면 법기관과 발행자는 협력하여 그 인증 정보에 대응되는 사용자의 정확한 신원을 확보할 수 있다.

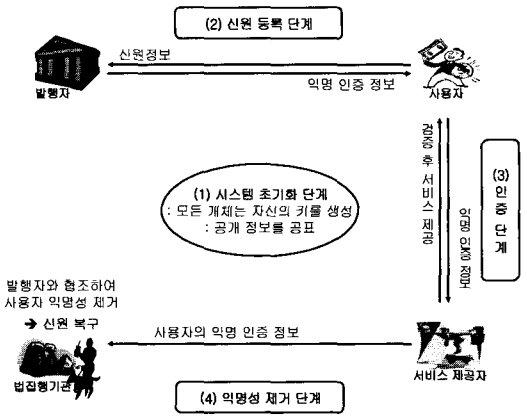
본 논문의 2장에서는 신원 위탁 방식의 구성요소와 기본단계를 알아보고, 일반적인 요구사항에 대해 알아보고, 전체 시스템의 신뢰성과 안전성을 향상시키기 위한 새로운 요구사항을 도출한다. 3장에서는 기존 방식들의 문제점에 대해 알아보고, 4장에서는 상기 요구사항을 모두 만족하는 새로운 신원 위탁 방식을 제안한다. 이와 더불어 이러한 신원 위탁 시스템을 통하여 서비스 제공자가 사용자에게 컨텐츠를 제공할 때 안전하게 키를 교환하고 이를 이용하여 안전한 통신을 수행할 수 있는 향상된 방안과 같은 시스템을 사용하는 사용자간의 키 동의에 의해 생성된 키를 이용한 암호화 통신 시 키 복구를 지원하는 향상된 메커니즘을 제안한다. 마지막으로 5장에서 결론을 맺도록 한다.

Ⅱ. 신원 위탁

2.1 신원 위탁 방식의 구성 및 단계

일반적으로 신원 위탁 방식은 다음과 같은 4개의 구성요소를 가지고 있다.[7,10,11,13]

- 사용자(A) : 일반적인 사용자로써 서비스 제공자에게 익명으로 서비스를 제공받기 위해서 발행자에게 자신의 정확한 신원을 제공하고, 서비스 제공자에게 익명으로 인증받을 수 있는 인증 정보를 제공받는다.
- 발행자(Issuer) : 익명으로 서비스 제공자에게 서비스를 제공받길 원하는 사용자의 정확한 신원을 저장하고 인증 정보를 제공한다. 유사시 법기관의 요청에 의해 사용자의 정확한 신원을 드러낸다.
- 서비스 제공자(Service Provider) : 사용자의 인증 정보를 검증하고 이상이 없으면, 서비스를 제공한다. 만약 사용자가 불법적 행동을 했을 경우에는 법기관에게 사용자의 신원에 대한 익명성 제거를 요구한다.



〔그림 1〕 일반적인 신원위탁 방식의 흐름도

- 법기관(Law Enforce Agent) : 유사시 서비스 제공자의 요구를 받아 발행자와 협력해 사용자의 정확한 신원를 드러낸다.

일반적인 신원 위탁 방식은 다음과 같이 4가지 단계로 이루어져 있다.

- 시스템 초기화 단계 : 각 참여 개체는 시스템을 초기화하기 위해 자신의 파라미터(공개키 또는 공개 파라미터)를 공표한다.
- 신원 등록 단계 : 사용자는 자신의 정확한 신원을 발행자에게 전달하고 안전하게 인증 정보를 제공받는다.
- 인증 단계 : 사용자는 익명으로 서비스를 제공받기 위해 서비스 제공자에게 자신의 인증 정보를 제공한다. 이것이 유효한 인증 정보이고 사용자가 이에 대한 비밀정보를 알고 있다면 서비스 제공자는 사용자에게 서비스를 제공한다.
- 익명성 제거 단계 : 유사시 서비스 제공자는 법기관에게 사용자가 인증 단계에서 제공한 인증 정보를 제공함으로써 사용자의 익명성을 제거하고 정확한 신원을 드러낸다.

2.2 신원 위탁 방식의 요구사항

본 절에서는 신원 위탁 방식의 요구사항에 대해 알아본다. 다음은 이러한 요구사항을 기술한 것이다.[6~11,13]

2.2.1 신원 위탁 방식의 일반적인 요구사항

- 익명성을 제공하는 인증성 : 사용자와 서비스 제

공자간의 인증 수행 시 사용자의 익명성은 제공되어야 하며, 정당한 사용자인지 검증 가능해야 한다.

- 불법 사용자의 익명성 제거 : 유사시 법기관과 발행자가 협력하면 불법 사용자에 대한 익명성을 제거할 수 있어야 한다.
- 인증 정보에 대한 비밀정보 유지 증명 : 제 3자가 사용자임을 사칭할 수 없어야 한다. 즉, 인증 정보가 해당 사용자의 것임을 증명할 수 있는 비밀값은 오직 사용자만이 가지고 있어야 한다.
- 법기관의 독립성 : 법기관과의 통신은 그 특성상 불법 사용자의 익명성 제거 요청이 있을 경우에만 수행되어야 한다.
- 불법적인 익명성 제거 방지 : 사용자의 익명성 제거는 법기관의 허가가 있어야만 가능해야 한다. 즉, 발행자나 서비스 제공자는 인증 정보와 공개된 정보만을 이용해서 사용자의 신원을 밝힐 수 없어야 한다.

2.2.2 신원 위탁 방식의 새로운 요구사항

- 익명성 제거 공개 검증성 : 법기관과 발행자가 협력하면 불법 사용자의 익명성 제거가 가능하다는 것을 참여 개체 누구라도 공개적으로 검증 가능해야 한다.

전체 시스템의 안전성과 신뢰성 향상을 위해서는 사용자의 신원이 정확히 발행자에게 위탁되었다는 것이 증명 가능해야 하고, 제 3자가 사용자의 신분을 도용할 수 없어야 한다는 것이다. 그러나 이것이 법기관이나 발행자에 의해서만 이루어지는 것은 시스템의 안전성과 신뢰성을 저하시키는 요소가 된다. 따라서 참여 개체라면 누구나 위 사실을 공개적으로 검증할 수 있어야 한다.

Ⅲ. 기본 방식 분석

본 장에서는 1998년도 CRYPTO Conference에서 소개된 2가지 방식과 2000년도 멀티미디어학회 논문지에서 소개된 2가지 방식을 적용기술에 따라 구분하여 소개한다.

3.1 방식 1-그룹 서명을 적용한 신원위탁 방식

이 방식은 1998년도 Crypto Conference에서 Joe Kilian과 Erez Petrank에 의해 제안된 방식으로 그룹 서명의 특징을 이용해 사용자의 익명성을 제공하고 있다. 발행자와 법기관이 하나의 그룹 매니저로써 그룹을 감독하는 역할을 수행한다. 그룹 매니저는 그룹에 새로운 사용자의 참여를 허락할 수 있고, 그룹의 구성자가 서명한 메시지를 증명할 수 있다는 것이 특징이다.[1,2]

이 방식은 사용자가 서비스 제공자에게 그룹 서명을 하여 익명성을 제공하면서 정당한 그룹의 소속원이라는 것을 증명할 수 있다. 또한 유사시 그룹 매니저가 서명자를 확인함으로써 익명성을 제거할 수 있다. 여기서 시스템 파라메터 z가 사용자의 정확한 신원과 연결되는 값으로 발행자가 보관하게 된다. 그러나 발행자와 법기관이 사용자의 비밀정보를 알지 못함으로 메시지를 위조할 수 없다. 하지만, 이 방식은 Camenisch의 그룹 서명에 기반을 두고 있다. Camenisch의 그룹 서명 기술을 이용하여 발행자와 법기관을 별도로 유지할 수 있으나, 초기 그룹 구성 단계 중 발행기관과 익명 철회 기관이 하나의 기관에서 두 개의 기관으로 분리되는 과정에서 법기관은 호출되게 된다. 법기관은 그 특성상 익명성 제거시에만 호출되어야 하는데 이 방식에서는 그룹 초기화시에 호출된다. 마지막으로 익명성 제거의 정당성을 공개적으로 검증할 수 없다는 문제점을 가지고 있다.

3.2 방식 2-영지식 증명을 적용한 신원위탁 방식

이 방식은 1998년도 CRYPTO Conference에서 Joe Kilian과 Erez Petrank에 의해 제안된 2번째 방식으로 그룹 서명을 적용한 방식의 문제점을 지적하고, 이를 해결하기 위해 ZKIP(Zero-Knowledge Interactive Protocol)을 적용한 방식이다. 이 방식은 영지식 증명을 적용하여 시스템 초기화시 법기관의 접촉을 제거하였다.[2,3]

이 방식은 인증 단계에서 사용자가 서비스 제공자에게 영지식 증명을 이용해 인증 정보를 가지고 있다는 것을 증명한다. 이때, 사용자의 익명성을 제거할 수 있는 추적 인자를 법기관의 공개키로 암호화하여 함께 제공한다. 유사시 서비스 제공자는 추적 인자를 법기관에게 제공함으로써 사용자의 익명성을 제거할 수 있다. 따라서 시스템 초기화시 법기관의 접촉을 제거할 수 있다. 하지만 이 프로토콜은 발행자가 사용자의 모든 정보를 가지고 있기 때문에 사용자를 사칭할 수 있는 문제점과 익명성 제거의 정

당성을 공개적으로 검증할 수 없다는 문제점을 가지고 있다.

3.3 방식 3-블라인드 기술을 적용한 신원위탁 방식

이 방식은 2000년도 멀티미디어학회 논문지에서 황보성 등에 의해 제안된 방식으로 Joe Kilian과 Erez Petrank이 제안한 2가지 방식의 문제점을 해결하기 위해 블라인드 기술을 적용하였다.[4,5,13]

이 방식은 블라인드 기술을 이용해 신원 위탁 시스템의 요구사항을 만족시키고 있다. 블라인드 서명은 사용자가 서명하는 메시지에 대한 내용을 알지 못하게 하기 위해 이용되고 블라인드 복호는 사용자가 인증 정보에 대한 비밀정보를 가지고 있는가에 대한 인증 단계에 이용된다. 또한, 신원 등록 단계에서 사용자의 정확한 신원은 발행자가 가지고 있고 이 정확한 신원과 연결되는 정보는 법기관만이 접근할 수 있다. 따라서 발행자와 법기관이 협동해야만 사용자의 신원을 알아 낼 수 있고 혼자서는 사용자의 신원을 알 수 없다. 하지만 이 방식은 신원 등록 단계에서 사용자와 법기관간의 많은 통신을 요구하고 있다. 따라서 법기관의 독립성은 제공하지 못하고 있다. 또한 익명성 제거의 정당성을 공개적으로 확인할 수 없다는 문제점을 가지고 있다.

3.4 방식 4-전자화폐 프로토콜을 적용한 신원위탁 방식

이 방식은 2000년도 멀티미디어학회 논문지에서 황보성 등에 의해 제안된 두 번째 방식으로 법기관의 독립성을 만족시키기 위해 전자화폐 프로토콜을 적용하였다.[13]

이 방식은 전자화폐 프로토콜을 응용하여 법기관의 독립성을 유지하고 사용자의 신원 사칭을 방지하고 있다. 신원 등록 단계에서 사용자는 정확한 신원과 그 신원을 알아낼 수 있는 I를 발행자에게 제공하고, 발행자는 사용자에게 인증 정보를 제공받을 수 있는 z를 사용자에게 되돌린다. 사용자는 제공받은 z를 이용해 발행자와 협력하여 인증 단계에서 사용될 인증 정보 A, B를 만든다. 인증 단계에서 사용자는 서비스 제공자에게 A, B, $sign(A, B)$, $Sign_{issuer}[E_{KP_E}(z)]$를 주고 사용자가 A, B를 구성하는 비밀정보를 가지고 있는지 확인하기 위해 challenge 값을 생성하고, 사용자는 그 값에 해당하는 비밀정보를 response 값으로 전송함으로써 사용자를 인증한다.

그러나 전자화폐 프로토콜을 적용하여 법기관의 독립성을 제공하고 있지만 이로 인하여 프로토콜 전개가 복잡해지고 계산량이 증가하는 문제점이 발행한다. 또한 익명서 제거의 정당성 증명을 공개적으로 확인할 수 없다는 문제점을 가지고 있다.

Ⅳ. 제안 방식

본 장에서는 3가지 제안 방식을 기술한다. 첫 번째로 대리 서명을 기반으로 법기관의 독립성을 제공하면서 익명성 제거의 공개 검증이 가능한 새로운 신원 위탁 방식을 제안하고, 두 번째로 이러한 신원 위탁 메커니즘에서 서비스 제공자가 사용자에게 컨텐츠를 안전하게 전달할 수 있는 향상된 방안을 제안한다. 마지막으로 위와 동일한 환경에서 동일 도메인 내 사용자들 간의 키 동의에 의해 생성된 키를 이용한 암호화 통신시 키 복구 기능을 지원하는 향상된 신원위탁 방식을 제안한다.

4.1 제안 방식 I-새로운 신원위탁 메커니즘

본 절에서 제안하는 방식은 대리 서명을 사용하여 기존 신원위탁 방식들의 문제점들을 해결하고 있으며, 새로운 요구사항인 익명성 제거 공개 검증성을 만족하고 있다.

4.1.1 시스템 계수

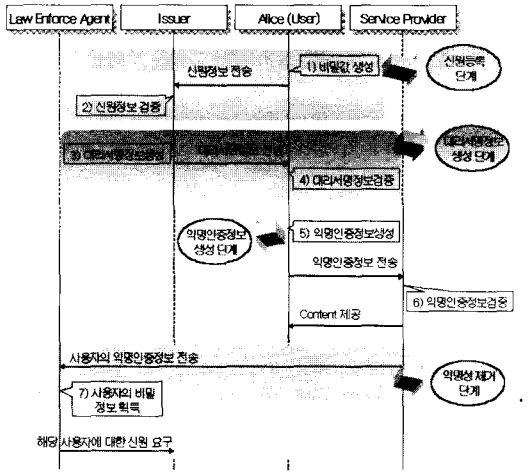
다음은 본 방식에서 사용되는 시스템 계수에 대한 설명이다.

- p, q : 큰 소수(단, $q | p-1$)
- g : Z_p^*상의 원시원소
- * : A(Alice : 사용자), ISS(Issuer : 발행자), SP(Service Provider : 서비스 제공자), LEA(Law Enforce Agent : 법기관)
- X_* : *의 비밀키
- Y_* : *의 공개키 (단, $Y\_* = g^{X\_*} \bmod p$)
- $E_*()$: *의 공개키로 암호화한 암호문
- $Sig_*()$: *의 비밀키로 서명한 서명문
- S_A : 사용자만이 가지고 있는 비밀값
- t_A, t_A : S_A를 구성하고 있는 랜덤수
- ID_A : 사용자 A의 식별자
- AID_A : 사용자 A의 가명 식별자

• *신원정보* : 사용자 정당성을 증명할 수 있는 개인 정보
• σ : 서명자의 대리 서명 정보
• $h()$: 안전한 일방향 해쉬함수

4.1.2 프로토콜

본 프로토콜은 사용자 Alice의 신원 등록 및 검증 단계, 대리 서명 정보 생성 및 검증 단계, 익명 인증 정보 생성 및 검증 단계 그리고 익명성 제거 단계로 구성되고 각각의 단계는 다음과 같다. [그림 2]는 제안 방식 I의 전체 흐름도이다.



[그림 2] 제안된 신원위탁 메커니즘 전체 흐름도

Step 1. Alice의 신원 등록 및 검증 그리고 익명성 공개 검증 단계

Phase 1. Alice에 의한 수행 단계

(a) 임의의 랜덤한 비밀정보 t_A와 t_A를 생성한 후 사용자 Alice의 비밀값 S_A를 구성한다. 그 후 t_A에 대응하는 공개정보 g^{t_A}를 공개한다.

$$S\_A = t\_A + t_A \qquad (4\text{-}1\text{-}1)$$

(b) Alice의 신원정보와 g^{S_A} 그리고 비밀 랜덤값 t_A를 발행자의 공개키로 암호화하고, t_A와 Alice의 식별자 ID_A를 법기관의 공개키로 암호화한다. 이 값에 서명을 하여 발행자에게 전송한다.

$$Sig_A(E_{ISS}(\text{신원정보}||g^{S\_A}||t_A)||E_{LEA}(t\_A||ID_A)) \qquad (4\text{-}1\text{-}2)$$

Phase 2. 발행자에 의한 수행 단계

(a) 발행자는 전송된 서명 정보를 검증한 후 자신의 비밀키를 이용해 전송된 $E_{ISS}(\text{신원정보}||g^{S_A}||t_A)$를 복호화하여 Alice의 위탁 정보가 올바른지 검증한다. 검증과정에서는 전송된 t_A에 대응하는 공개정보 g^{tA}와 Alice가 공개한 g^{t_A}를 곱한 결과가 전송된 g^{S_A}와 같은지 확인하게 된다. 만약 같다면 Alice의 비밀정보가 올바르게 위탁되었다는 것을 증명하게 된다.

$$g^{S\_A} \stackrel{?}{=} g^{tA} * g^{t\_A} \qquad (4\text{-}1\text{-}3)$$

(b) 위 검증과정이 성공하면 발행자는 Alice의 가명 식별자 AID_A를 생성한 후 AID_A와 g^{S_A} 그리고 g^{tA}를 공개한다.

Phase 3. 참여 개체들에 의한 수행 단계

(a) 신원위탁 시스템에 참여하는 개체는 누구라도 이 과정을 수행할 수 있다. 우선 Alice가 공개한 g^{t_A}와 발행기관이 공개한 Alice의 g^{tA}와 g^{S_A}를 이용하여 식 (4-1-3)과 동일하게 검증 과정을 수행한다.

(b) 만약 검증과정이 성공한다면 이것은 사용자가 부정한 행위를 할 경우 사용자의 익명성을 제거할 수 있다는 것을 증명하게 된다.

Step 2. 대리 서명 정보 생성 및 검증 단계

Phase 1. 발행자에 의한 수행 단계

(a) 임의의 랜덤값 d를 생성하고, 다음과 같이 대리 서명 정보를 생성한다.

$$D = g^d \bmod p$$
$$\sigma = (X\_ISS + d*D) \bmod p-1 \qquad (4\text{-}1\text{-}4)$$

(b) 사용자의 가명 식별자와 법기관의 공개키로 암호화된 값을 서명한 후 생성된 대리 서명 정보와 함께 Alice의 공개키로 암호화하고, 이를 Alice에게 전송한다.

$$E_A(\sigma||D||AID_A||Sig_{ISS}(AID_A||E_{LEA}(t\_A||ID_A)) \qquad (4\text{-}1\text{-}5)$$

Phase 2. Alice에 의한 수행 단계

(a) Alice는 전송된 값을 복호한 후 다음과 같이 대리 서명 정보를 검증한다. 만약 올바르다면 계속 진행하고, 그렇지 않으면 발행자에게 문의하여 다시 대리 서명 정보를 전송 받는다.

$$g^{\sigma} \stackrel{?}{=} Y\_ISS*D^{D} \bmod p \qquad (4\text{-}1\text{-}6)$$

검증과정은 다음과 같다.

$$\begin{aligned} g^{\sigma} &= Y\_ISS*D^{D} \bmod p \\ &= g^{X\_ISS}*(g^{d})^{D} \bmod p \\ &= g^{\sigma} \bmod p \end{aligned}$$

Step 3. 익명 인증 정보 생성 및 검증 단계

Phase 1. Alice에 의한 수행 단계

(a) 임의의 랜덤값 r과 서비스 요구 메시지 m을 이용하여 사용자 익명 인증 정보 $S_{\sigma}(m)$을 다음과 같이 생성한다.

$$\begin{aligned} H &= h(m) \\ R &= g^{r} \bmod p \bmod q \\ S_{\sigma}(m) &= S\_A*r - R*\sigma*H \bmod p \end{aligned} \qquad (4\text{-}1\text{-}7)$$

(b) 다음 정보를 구성하여 서비스 제공자에게 전송한다.

$$\begin{aligned} &AID_A||D||Sig_{ISS}(AID_A||E_{LEA}(t\_A||ID_A))|| \\ &R||m||S_{\sigma}(m)||Sig_A(g^{S\_A}) \end{aligned} \qquad (4\text{-}1\text{-}8)$$

Phase 2. 서비스 제공자에 의한 수행 단계

(a) 서비스 제공자는 전송된 $Sig_A(g^{S_A})$를 이용하여 공개된 g^{S_A}와 비교한다. 같으면 계속 진행하고, 같지 않으면 Alice에게 에러 메시지를 전송한다.

(b) 전송된 정보를 이용하여 H와 V를 다음과 같이 생성한다.

$$\begin{aligned} H &= h(m) \\ V &= Y\_ISS*D^{D} \bmod p \end{aligned} \qquad (4\text{-}1\text{-}9)$$

(c) 다음과 같이 사용자의 익명 인증 정보를 검증한다. 이를 통하여 사용자를 익명으로 인증하게 된다. 만약 올바르지 않으면 사용자에게 에러 메시지를 전송한다.

$$R*g^{S\_A} \stackrel{?}{=} g^{S_{\sigma}(m)}*V^{RH} \bmod p \bmod q \qquad (4\text{-}1\text{-}10)$$

검증과정은 다음과 같다.

$$\begin{aligned} R * g^{S\_A} &= g^{S_{\sigma}(m)} * V^{RH} \bmod p \bmod q \\ &= g^{S\_A*r-R*\sigma*H} *(Y\_ISS*D^{D})^{R*H} \bmod p \bmod q \\ &= g^{S\_A*r-R*\sigma*H} *(g^{X\_ISS}*g^{d*D})^{R*H} \bmod p \bmod q \\ &= g^{S\_A*r - R*\sigma*H} * g^{\sigma*R*H} \bmod p \bmod q \\ &= g^{S\_A}*R \bmod p \bmod q \end{aligned}$$

(d) 위 검증과정을 마치면 전송된 $Sig_{ISS}(AID_A||E_{LEA}(t_A||ID_A))$를 안전하게 보관하고 사용자에게 서비스를 제공한다.

Step 4. 익명성 제거 단계

Phase 1. 서비스 제공자에 의한 수행 단계

(a) 만약 Alice가 부정한 행위를 했을 경우 사용자의 익명성 제거 요청과 함께 보관하고 있는 $Sig_{ISS}(AID_A||E_{LEA}(t_A||ID_A))$를 법기관에게 전송한다.

Phase 2. 법기관에 의한 수행 단계

(a) 법기관은 전송된 $Sig_{ISS}(AID_A||E_{LEA}(t_A||ID_A))$를 이용하여 식별자 ID_A와 비밀정보 t_A를 획득한다.

(b) 법기관은 발행자에게 식별자 ID_A에 해당하는 신원을 요구한다. 이를 통해 부정한 행위를 수행한 Alice의 익명성을 제거한다.

4.2 제안 방식 II-컨텐츠 제공을 위한 향상된 신원위탁 메커니즘

본 절에서는 4.1절에서 제안한 새로운 신원위탁 메커니즘에서 서비스 제공자가 사용자에게 컨텐츠를 안전하게 전달할 수 있는 향상된 방안을 제안한다.

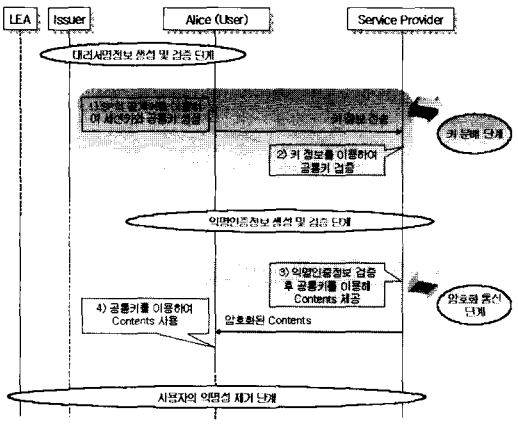
4.2.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수에 대한 설명이다. 여기서는 4.1.1절에 나와있는 시스템 계수는 명시하지 않는다.

- *Contents* : 서비스 제공자가 사용자에게 제공하는 서비스
- *Cert(SP)* : SP의 인증서
- $E_{\#}()$: 대칭키 #를 키로 이용하여 암호화한 암호문
- # : *ssk*(세션키), *PsK*(공통키)

4.2.2 프로토콜

본 절에서는 사용자 Alice와 서비스 제공자 SP (Service Provider)간의 키 분배 단계와 암호화 통신 단계로 나누어 기술한다. 여기서 Alice와 SP는 동일한 신원위탁 메커니즘을 사용한다고 가정하고, 키 분배 단계는 4.1.2-Step 2과 Step 3 사이에 이루어지며, 암호화 통신 단계는 4.1.2-Step 3과 Step 4 사이에 이루어진다. [그림 3]은 제안 방식 II에 대한 흐름도이다.



[그림 3] 제안 방식 II의 흐름도

Step 1. Alice와 SP간의 키 분배 단계

Phase 1. Alice에 의한 수행 단계

(a) Alice는 SP의 공개키 *Y_SP*를 이용하여 세션키 *ssk*를 계산한다. 그 후 랜덤수 n_1을 생성하고, 아래와 같이 공통키 *PsK*를 계산한다.

$$ssk = (g^{X\_SP})^{S\_A}$$
$$PsK = n_1 \oplus (g^{X\_SP})^{S\_A} \qquad (4\text{-}2\text{-}1)$$

(b) Alice는 다음과 같이 메시지를 암호화하여 SP에게 전송한다.

$$E_{ssk}(AID_A || n_1 || PsK) || Sig_A(g^{S\_A}) \qquad (4\text{-}2\text{-}2)$$

Phase 2. SP에 의한 수행 단계

(a) SP는 전송된 값을 이용하여 세션키 *ssk*를 계산한 후 메시지를 복호화한다. SP는 복호화된 메시지를 이용하여 사용자를 확인하고 공통키 *PsK*를 검증한다.

(b) 검증이 완료되면 Alice에게 종결 메시지를 전송한다.

Step 2. Alice와 SP간의 암호화 통신 단계

이 단계는 세션키 생성 후 *Contents*를 제공하는 단계이다. 즉, SP는 Alice의 익명 인증 정보를 검증 후에 다음과 같이 *Contents*를 제공한다.

$$E_{PsK}(Contents) || Cert(SP) \qquad (4\text{-}2\text{-}3)$$

4.3 제안 방식 III-키 복구를 지원하는 향상된 신원위탁 메커니즘

본 절에서는 4.1절에서 제안된 신원위탁 메커니즘에서 동일 도메인 내 사용자들 간의 키 동의에 의해 생성된 키를 이용한 암호화 통신시 키 복구 기능을 지원하는 향상된 메커니즘을 제안한다.

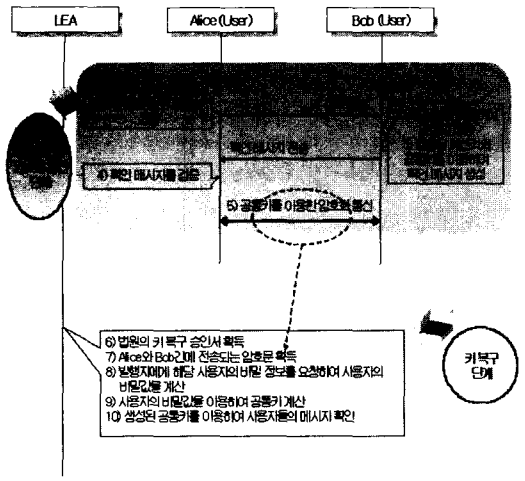
4.3.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수에 대한 설명이다. 여기서는 4.1.1절에 나와있는 시스템 계수는 명시하지 않는다.

- S_B : 사용자 Bob의 인증 정보에 해당하는 비밀값 (단, $S\_B = t\_B + t_B$)
- t_B, t_B : S_B를 구성하고 있는 랜덤수
- ID_B : 신원 등록자 Bob의 식별자
- AID_B : 신원 등록자 Bob의 가명 식별자
- $E_{@}()$: 대칭키 @를 키로 이용하여 암호화한 암호문
- @ : *seskey*(세션키), *PuK*(공통키)

4.3.2 프로토콜

본 프로토콜은 사용자 Alice와 사용자 Bob간의 키 분배 및 암호화 통신 단계와 키 복구 단계로 구성되고 각각의 단계는 아래와 같다. 여기서 Alice와 Bob은 동일한 신원위탁 메커니즘을 사용하고 있으며, 사전에 모두 수행되었다고 가정한다. [그림 4]는 제안 방식 III에 대한 흐름도이다.



〔그림 4〕 제안 방식 III의 흐름도

Step 1. Alice와 Bob간의 키 분배 및 암호화 통신 단계

Phase 1. Alice에 의한 수행 단계

(a) Alice는 Bob에 의해 공개된 g^{t_B}를 이용하여 세션키 *seskey*를 계산한다. 그 후 랜덤수 N_1을 생성하고, 아래와 같이 공통키 *PuK*를 계산한다.

$$seskey = (g^{t\_B})^{t\_A}$$
$$PuK = N_1 \oplus (g^{t\_B})^{t\_A} \quad (4\text{-}3\text{-}1)$$

(b) Alice는 다음과 같이 메시지를 암호화하여 Bob에게 전송한다.

$$E_{\_seskey}(ID_A||N_1||PuK)||g^{t\_A} \quad (4\text{-}3\text{-}2)$$

Phase 2. Bob에 의한 수행 단계

(a) Bob은 전송된 값을 이용하여 세션키 *seskey*를 계산한 후 메시지를 복호화한다. Bob은 복호화된 메시지를 이용하여 통신 상대방을 확인하고 공통키 *PuK*를 검증한 후 Alice에게 종결 메시지를 전송한다.

(b) Bob은 Alice에게 다음과 같이 암호화 데이터를 전송한다.

$$E_{\_PuK}(message)||$$
$$E_{\_seskey}(ID_A||N_1||PuK) \quad (4\text{-}3\text{-}3)$$

Step 2. Alice와 Bob간의 키 복구 단계

본 단락에서는 Alice와 Bob간에 불법적인 암호 통신이 이루어진다고 가정한다. 이러한 상황에서 법 집행권 보장을 위한 키 복구 단계를 살펴본다. 여기서는 통신 및 저장 데이터 모두가 키 복구의 대상이 된다.

Phase 1. 법기관에 의한 수행 단계

(a) 법기관은 법원의 허가를 받아 통신 시 전송되는 식 (4-3-3)을 획득한다. 그 후 발행자에게 다음 값을 요구한다.

$$E_{LEA}(t\_A||ID_A),\ E_{LEA}(t\_B||ID_B) \quad (4\text{-}3\text{-}4)$$

(b) 법기관은 자신의 비밀키를 이용하여 각 암호문을 복호화한 후 t_A와 t_B를 이용하여 세션키 *seskey*를 계산한다. 이 세션키 *seskey*를 이용하여 식(4-3-3)에서 공통키 *PuK*를 계산한다.

(c) 법기관은 *PuK*를 이용하여 불법 사용자의 암호화 통신 데이터를 복구한다.

4.4 제안 방식 비교/분석

본 절에서는 제시된 요구사항을 중심으로 제안 방식의 요구사항 만족도를 분석하고 기존 방식들과 비교/분석한다. 〔표 1〕은 신원위탁 방식별 비교 분석 표이다.

- 익명성을 제공하는 인증성 : 발행자는 정당한 사용자에게 대리 서명 인자를 전송한다. 사용자는 발행자의 대리 서명 인자와 자신의 비밀값을 이용하여 자신의 익명 인증 정보를 생성한다. 서비스 제공자는 발행기관과 사용자의 공개 정보를 이용하여 전송된 익명 인증 정보를 검증한다. 이러한 과정을 통하여 사용자는 서비스 제공자에게 익명성을 제공하는 인증을 수행하게 된다.
- 불법 사용자의 익명성 제거 : 사용자의 비밀 정보는 두 개로 구성되어 있다. 하나는 발행자가 접근할 수 있으며, 다른 하나는 법기관이 접근할 수 있도록 구성하였다. 따라서 유사시 법기관과 발행자가 협력하면 불법 사용자에 대한 익명성을 제거할 수 있다. 또한 제안 방식은 이러한 불법 사용자의 익명성 제거를 공개적으로 검증할 수 있도록 구성하여 사용자의 신뢰성을 향상시켰다.
- 인증 정보에 대한 비밀정보 유지 증명 : 사용자의

인증 정보는 사용자만이 알고있는 비밀값을 이용하여 구성하게 된다. 따라서 사용자의 비밀값을 모르는 제 3자는 정당한 사용자임을 사칭할 수 없다. 또한 제안 방식에서는 사용자가 직접 자신의 익명 인증 정보를 생성하므로 더욱 향상된 보안성을 유지하고 있다.

- 법기관의 독립성 : 제안 방식에서 법기관은 익명성 제거 시에만 참여하도록 구성하였다.
- 불법적인 익명성 제거 방지 : 사용자의 익명 인증 정보에 해당하는 비밀 정보를 두 개의 값으로 구성하여 그 중 하나는 발행자에게 안전하게 공개하고 나머지 하나는 법기관의 공개키를 이용해 암호화하였다. 또한 법기관의 공개키를 이용해 암호화한 데이터에는 사용자의 실제 신원과 관련된 정보가 포함되어 있지 않으므로 법기관이나 발행자는 사용자의 익명성을 불법적으로 제거할 수 없다.
- 익명성 제거 공개 검증성 : 사용자의 익명 인증 정보에 해당하는 비밀 정보를 두 개의 값으로 구성하여 그 중 하나는 발행자에게 안전하게 공개하고 나머지 하나는 법기관의 공개키를 이용해 암호화하고, 사용자의 비밀 정보에 해당하는 공개 정보를 공개함으로써 법기관과 발행자가 협력하면 불법 사용자의 익명성 제거가 가능하다는 것을 참여 개체 누구라도 공개적으로 검증 가능하다.

〔표 1〕 신원위탁 방식별 요구사항 비교 분석표

요구사항 \ 방식	방식 1	방식 2	방식 3	방식 4	제안 방식 I
익명성을 제공하는 인증성	O	O	O	O	O
불법 사용자의 익명성 제거	O	O	O	O	O
익명 정보에 대한 비밀정보 유지 증명	O	X	O	O	O
법기관의 독립성	X	O	X	O	O
불법적인 익명성 제거 방지	O	X	O	O	O
익명성 제거 공개 검증성	X	X	X	X	O

V. 결 론

사용자가 공개 네트워크 상에서 서비스 제공자와 인증을 수행할 경우 사용자는 자신의 신원에 대해 익명성을 가지기를 원할 것이고, 서비스 제공자는 사용자의 정확한 신원을 확인 후 서비스를 제공하기를 원한다. 이렇게 상반되는 이해관계는 신원위탁 방식을 사용함으로써 사용자와 서비스 제공자 모두의 요구사항을 만족시킬 수 있다. 본 논문에서는 기존 신원위탁 방식의 필요성과 요구사항 그리고 기존 방식들의 문제점들을 알아보았다. 이를 통하여 안전성과 신뢰성을 위한 새로운 요구사항을 제시하였고, 기존 방식들의 문제점들을 해결하면서 상기 요구사항을 모두 만족할 수 있는 새로운 신원위탁 방식을 제안하였다. 또한 이와 더불어 서비스 제공자의 컨텐츠를 안전하게 사용자에게 전송하기 위한 방안과 동일한 시스템을 사용하는 사용자들간의 암호화 통신 시 키 복구를 지원하는 향상된 메커니즘을 제안하였다. 향후 좀 더 안전하고 효율적인 신원위탁 방식의 연구가 진행되어야 할 것이다.

참 고 문 헌

〔1〕 C. Camenisch, "Efficient and generalized group signatures", Advances in Cryptology-EUROCRYPT '97, pp. 465~479, 1997.

〔2〕 J. Kilian and E. Petrank, "Identity Escrow," Advances in Cryptology-CRYPTO'98, pp. 169~184, 1998.

〔3〕 J. Kilian and E. Petrank, "Identity Escrow", Theory of Cryptography Library, ftp://theory.lcs.mit.edu/pub/ tcrypto1/97-11.ps, 1997.

〔4〕 K. Sakurai and Y. Yamane, "Key Escrow system of Protecting User's Privacy by Blind Decoding", pp. 147~157, 1998.

〔5〕 M. Stadler, "Fair blind signatures", In Proc. Eurocrypt 95, LNCS 921, pp. 209~219, 1995.

〔6〕 S. Micali, "Fair Cryptosystems", Advances in Cryptology-CRYPTO '92, pp. 113~138, 1992.

〔7〕 http://www.epic.org, "Escrowed Encryption Standard(EES)", Approval of FIPS 185, 1994.

〔8〕 http://csrc.nist.gov, "Requriements for Key Recovery Prodeucts", NIST, 1998.

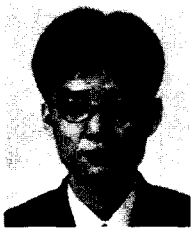
〔9〕 최용락, 소우영, 이재광, 이임영, *컴퓨터 통신 보안*, 도서출판그린, 2001.

[10] 이용호, 이임영, "익명성 제거의 공개 검증이 가능한 신원위탁 방식", CISC 2001, pp. 79~82, 2001.
[11] 황보성, 이임영, "사용자의 익명성을 제어하는 신원위탁 방식 제안", 멀티미디어학회 논문지 제3권, 제6호, pp. 617~624, 2000.
[12] 황보성, 이임영, "신원위탁 방식의 설계", WISC 2000, pp. 588~602, 2000.

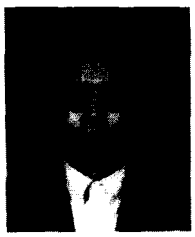
〈著者紹介〉

이 용 호(Yong-Ho Lee) 학생회원
2001년 2월 : 순천향대학교 컴퓨터공학과 졸업
2001년 3월~현재 : 순천향대학교 전산학전공 석사
〈관심분야〉 암호 프로토콜, 키 관리, 정보보호

이 임 영(Im-Yeong Lee) 종신회원
1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학전공 석사
1989년 3월 : 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재 : 순천향대학교 정보기술공학부 부교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안



김 주 한(Ju-Han Kim) 정회원
1997년 2월 : 충남대학교 컴퓨터과학과 졸업
1999년 2월 : 충남대학교 컴퓨터과학과 석사
2000년 8월~현재 : 한국전자통신연구원 능동보안기술연구팀 연구원
〈관심분야〉 XML, 정보보호, 워터마킹



문 기 영(Ki-Young Mun) 정회원
1986년 2월 : 경북대학교 전자공학과 졸업
1989년 2월 : 경북대학교 전자공학과 석사
1992년 1월~1994년 3월 : (주)대우정보시스템 기술연구소 대리
1994년 3월~현재 : 한국전자통신연구원 능동보안기술연구팀 선임연구원
〈관심분야〉 분산시스템, 정보보호, 트랜잭션