Short Group Signature를 이용한 가명 기반 PKI

이석준* · 한승완* · 이윤경* · 정병호*

*한국전자통신연구원 지식정보보호연구팀

Pseudonym-based Anonymous PKI with Short Group Signature

Sokjoon Lee* · Seung-Wan Han* · Yun-Kyung Lee* · Byung-Ho Chung*

*Knowledge-based Security Research Team, ETRI

E-mail : {junny, hansw, neohappy, cbh}@etri.re.kr

요 약

최근 들어, 인터넷은 우리의 삶의 필수 요소가 되고 있다. 즉, 우리는 정보 검색, 온라인 쇼핑, 이메일 서비스와 같은 다양한 인터넷 서비스를 활용할 수 있다. 그러나, 인터넷 서비스를 이용하는 이면에는 개인의 프라이버시 침해에 대한 위협이 존재하고 있다. 온라인 서비스 제공 업체는 과도한, 그리고 필수적이지 않은 정보까지 개인에게 요구하려는 경향이 있으며, 개인 정보에 대하여 책임의식을 동반한 관리가 이루어지지 않아 여러 피해 사례가 보고되고 있다.

이를 해결하기 위해, 익명 인증에 관한 연구가 이루어지고 있다. 익명 인증은 사용자가 자기 자신의 신분을 증명하면서, 자신의 주민등록번호와 같은 ID 값 혹은 개인 정보를 노출하지 않는 것을 의미한다. 이들 연구는 다소 현재 인터넷 환경에서의 인증 구조에 적용하기 어려운 단점이 있다.

본 논문에서는 이러한 단점을 해결하기 위하여, Short Group Signature를 이용한 가명 기반 PKI 구조를 제안한다. 제안하는 방식을 통하여, 조건부 추적성을 지원하는 익명성을 가지는 PKI 구조 및 익명 인증 서비스를 제공할 수 있다.

ABSTRACT

Nowadays, Internet becomes an essential element in our life. We can make use of numerous on-line services through Internet such as information search, on-line shopping, e-mail service, etc. But, while getting the benefits of Internet service, invasion of our privacy frequently occurs because on-line service providers tend to request excessive or unnecessary personal information. So, there have been some researches on anonymous authentication, which means that user can authenticate herself, not revealing her identity or personal information. But, most of the researches are not somewhat applicable to current authentication infrastructure. In this paper, we propose a pseudonym-based anonymous PKI with short group signature. Using our proposed scheme, we can provide anonymity with conditional traceability to current PKI.

키워드

Short Group Signaure, 그룹 서명, Pseudonym, PKI

1. 서 론

최근 들어, 인터넷은 우리의 삶의 필수 요소가 되고 있다. 즉, 우리는 정보를 검색하거나 공유하고, 상품을 구매하며, 이메일을 주고 받는 등 다양한 종류의 온라인 서비스를 인터넷을 통하여 받고 있다. 그러나, 인터넷 서비스를 이용하는 이면에는 개인의 프라이버시 침해에 대한 위협이 함께 존재한다. 온라인 서비스 제공 업체는 과도한, 그리고 필수적이지 않은 정보까지 개인에게 요구하려는 경향이 있다. 업체들이 과도하게 요구하는 정보의 예로, 주민등록번호, 휴대폰 번호, 생년월일, 취미 등이 있으며, 이러한 개인 정보에 대해 업체는 책임의식을 동반한 관리가 필수적임에도 부주의하게 관리하여 개인 정보 침해 사고가 꾸준하게 발생하고 있다.

이러한 개인 프라이버시 문제를 풀기 위하여 여러 가지 방법들이 제안되고 있는데, 여기에는

각 개인이 믿을 수 있는 제 3의 기관에 개인 정보를 위탁하여 온라인 서비스 업체들이 정책에 따라 이 기관에게 부분적인 개인 정보를 요청하는 방법이 있다. 그러나, 이러한 방법은 기본적으로 개인의 프라이버시를 신뢰 기관에게 전적으로 맡겨야 하는 한계점을 가진다. 사실상 온라인 서비스 제공 업체가 알아야 하는 것은 서비스 이용자의 개인 정보라기 보다는 그 이용자가 과연 그 서비스를 이용할 권한이 있는가이다.

이러한 문제를 해결하기 위해, 서비스 이용자는 주민등록번호와 같은 신분 정보나 개인 정보를 드러내지 않으면서도 인증을 받을 수 있는 익명 인증에 대한 연구들이 이루어지고 있다. 이러한 연구는 '가명(Pseudonym)', '익명 신용장(Anonymous Credential)'에 기반한 연구[4,6,7]들과, 그룹 서명(Group Signature)[1,5], 링 서명(Ring Signature)[10], 추적 가능 서명(Traceable Signature)[11]과 같은 익명 서명 기반 연구들로 나뉜다. 이러한 연구들 대부분은 익명 인증을 이론적인 면으로 다르고 있으며, 따라서 실제 인터넷 사용 환경에 적용하는 것이 다소 적합하지 않다. 예를 들어, 현재 널리 사용되고 있는 인증 구조인 PKI에 이러한 연구들을 그대로 적용하는 것은 쉽지 않다.

본 논문은 이러한 문제점들을 해결하기 위하여, Short Group Signature를 이용한 가명 기반 PKI 구조를 제안한다. 본 논문에서 제안하는 방식은 조건부 추적성을 지원하는 익명 PKI 구조 및 익명 인증 서비스를 제공할 수 있다.

II. 논문의 배경

익명 인증은 서비스 이용자가 어느 수준의 익명성을 만족하는 형태로 인증 및 서비스에 대한 사용 승인을 받을 수 있는 기술을 의미한다. 이는 일반적으로 '가명'을 사용한 기법 및 익명 서명 기법 등을 통하여 이루어질 수 있다. 가명 시스템으로 알려진 방법은 사용자가 다양한 업체 혹은 기관과 익명으로 통신할 수 있는 수단을 제공한다. 여기서 각 기관에서 사용하는 가명들은 각각 서로 연관이 있음을 추측할 수 없어야 한다.

가명 시스템에 대한 연구의 시초는 D. Chaum[4]으로부터 시작되었으며, 여기에서 사용자는 다양한 기관과 익명으로 자신의 신분을 증명할 수 있다. 이 연구를 발전시킨 많은 연구[6,7]들이 있으나, 오늘날 실용적으로 널리 사용되고 있지는 않다. 몇몇 연구들은 매우 복잡한 영지식 상호 증명 프로토콜(Zero-knowledge interactive protocol)을 사용하며, 이러한 점으로 인하여 실용적인 프로토콜을 구성하는 것이 쉽지 않다. 또한 사회적으로 혹은 법과 제도상으로 추적 및 연결이 불가능한 익명성을 받아들이기 힘든 점도 가명 시스템을 받아들이기 힘들게 한다.

2.1 그룹 서명

익명 서명 기법[1,5,10,11]은 익명 인증을 제공하는 또 다른 기술이다. 이 중 그룹 서명은 D. Chaum 등[5]에 의해 처음 제안된 기법으로, 그룹에 속한 멤버는 누구라도 서명할 수 있으며 검증자는 서명의 옳고 그름을 검증할 수는 있으나 서명자에 대해 어떤 정보를 알아낼 수 없다.

그룹 관리자는 그룹 서명 기법에서 가장 중요한 존재이다. 그룹 관리자는 서명을 추적하여 서명자의 신원을 알아낼 수 있다. 그룹 서명에 대한 많은 연구들이 있었으나, 대부분의 그룹 서명 기법은 다음과 같은 절차를 가진다.

- ***키 생성 혹은 초기화(Key Generation or Setup)*** : 몇몇 보안 매개 변수를 이용한 그룹 공개키 및 그룹 비밀키의 생성 과정
- ***참여(Join)*** : 그룹 관리자와 사용자 간의 프로토콜로, 여기에서 사용자는 그룹 멤버가 될 수 있다. 그룹 멤버는 이 프로토콜을 통하여 각각의 그룹 멤버용 비밀키를 받는다.
- ***서명(Sign)*** : 각 멤버는 자신의 멤버용 비밀키를 이용하여 그룹 서명을 할 수 있다.
- ***검증(Verify)*** : 그룹 서명의 유효성을 검증하는 알고리즘으로 이 알고리즘을 통하여 검증자가 서명자의 정보를 알 수는 없다.
- ***신원 공개(Open)*** : 문제 발생시, 그룹 관리자가 특정 서명에 대한 서명자의 신원을 공개하는 알고리즘

2.2 Short Group Signature

그룹 서명은 서명자의 프라이버시를 보호하기 위한 것으로 이러한 그룹 서명의 특징들을 필요로 하는 응용들이 있다. 이러한 응용들은 서명자의 프라이버시 뿐만 아니라, 대체로 짧은 서명 길이를 요구 사항으로 가진다.

이러한 요구 사항 때문에, D. Boneh 등은 Short Group Signature[1]를 제안하였다. 이 방식에서는, 그룹 서명의 생성을 위해 강한 Diffie-Hellman(SDH; Strong Diffie-Hellman) 문제에 대한 영지식 증명 프로토콜을 이용하고 있다. 그룹 관리자의 서명자에 대한 신원 공개(Open) 과정을 위하여, 서명자의 가명(멤버용 비밀키의 일부)이 결정적 선형 가정(Decisional Linear Assumption)에 기반한 선형 암호화(Linear Encryption) 기법에 의해 숨겨지며, 이 선형 암호화를 풀 수 있는 비밀키는 그룹 관리자만 알 수 있도록 하고 있다. Short Group Signature에서는 4 종류의 참여자가 있다.

- ***그룹 관리자*** : 상황에 따라 서명자의 신원을 공개 및 취소할 수 있으며, 그룹의 공개키 $gpk=(g_1,g_2,h,v,h,w)$를 공개한다. 그룹 관리자의 비밀키는 $gmsk=(\xi_1,\xi_2)$이다.
- ***멤버 비밀키 발급자*** : 각 사용자의 비밀키 쌍

을 발급하며, 발급할 때 사용하는 비밀키 γ를 가진다.

- ***사용자*** : 그룹의 멤버가 되기 위해 그룹에 참여하는 사람으로, 자신의 비밀키 쌍 $gsk[i]=(A_i,x_i)$을 이용하여 익명으로 서명할 수 있다.
- ***검증자*** : 서명을 검증하고 서명자가 그룹의 멤버인지만을 확인할 수 있다.

Short Group Signature는 2.1에서의 일반적인 그룹 서명 절차와 같은 5 단계를 가진다.

- ***키 생성*** : 그룹 관리자는 키 쌍을 생성하여 그룹 공개키를 공개한다. 그룹 관리자와 멤버 비밀키 발급자는 각각 자신의 비밀키가 $u^{\xi_1}=v^{\xi_2}=h, w=g_2^{\gamma}$를 만족하도록 선택한다.
- ***참여*** : 멤버 비밀키 발급자 혹은 사용자가 무작위로 $x_i \in_R \mathbf{Z}_p^*$를 선택하고, 비밀키 발급자는 사용자에게 멤버 비밀키로 $gsk[i]=(A_i,x_i)$를 준다. 여기에서 비밀키 쌍에 있는 두 값은 $A_i=g_1^{1/(\gamma+x_i)} \in \mathbf{G}_1$의 관계를 만족하도록 한다.
- ***서명*** : 사용자는 메시지 M에 대한 서명으로 $\sigma=(T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\delta_1},s_{\delta_2})$를 계산한다. 여기에서, T_1,T_2,T_3는 A_i를 감추기 위한 선형 암호화 결과이며, $s_\alpha,s_\beta,s_x,s_{\delta_1},s_{\delta_2}$는 (A_i,x_i)에 대한 영지식 증명을 위한 값이고, c는 M과 다른 값의 해쉬값이다.
- ***검증*** : 메시지 M과 서명 $\tilde{\sigma}=(\tilde{T}_1,\tilde{T}_2,\tilde{T}_3,\tilde{c},\tilde{s}_\alpha,\tilde{s}_\beta,\tilde{s}_x,\tilde{s}_{\delta_1},\tilde{s}_{\delta_2})$에 대해, 검증자는 $\tilde{R}_1,\tilde{R}_2,\tilde{R}_3,\tilde{R}_4,\tilde{R}_5$를 다음과 같이 계산한다. $\tilde{R}_1 \leftarrow u^{\tilde{s}_\alpha}\cdot\tilde{T}_1^{-\tilde{c}}$, $\tilde{R}_2 \leftarrow v^{\tilde{s}_\beta}\cdot\tilde{T}_2^{-\tilde{c}}$, $\tilde{R}_3 \leftarrow e(\tilde{T}_3,g_2)^{\tilde{s}_x}$, $\tilde{R}_4 \leftarrow \tilde{T}_1^{-\tilde{s}_x}\cdot u^{-\tilde{s}_{\delta_1}}$, $\tilde{R}_5 \leftarrow \tilde{T}_2^{\tilde{s}_x}\cdot v^{-\tilde{s}_{\delta_2}}$. 검증자는 $\tilde{c}$가 $H(M,\tilde{T}_1,\tilde{T}_2,\tilde{T}_3,\tilde{R}_1,\tilde{R}_2,\tilde{R}_3,\tilde{R}_4,\tilde{R}_5)$와 같은지를 확인하여 같을 경우 서명의 정확성을 받아들인다.
- ***신원 공개*** : 그룹 관리자는 서명자의 신원을 확인할 수 있는 정보인 A_i를 $A_i=T_3/(T_1^{\xi_1}\cdot T_2^{\xi_2})$로 계산하여 공개한다.

이 논문에 따르면, 이 방식의 전체 서명의 길이는 1533 bits (192 bytes)이며, 보안성은 1024 bit RSA 서명과 유사한 수준이므로, 실제 응용에 적용할 수 있는 수준으로 보고 있다.

2.3 익명성과 PKI

X.509 공개키 및 속성 인증서[9]는 인터넷에서 사용자를 인증하기 위하여 널리 사용된다. X.509 공개키 인증서는 특정한 공개키와 그 공개키에 대응하는 비밀키를 가진 사용자가 연결되어 있음을 설정해주는 역할을 한다. 따라서 이 인증서에는 그 사용자의 신원 정보를 담고 있게 되며, 이는 인증서가 익명성을 제공하지 않음을 뜻한다.

X.509 기반 PKI에 익명성을 제공하려는 연구 결과는 크게 2가지 접근 방향이 있다. 첫번째 접근 방법은 익명 서명 방법을 지원하기 위해 X.509 인증서의 의미를 확장하는 것이다[2]. 이 논문에서는 공개키가 특정 사용자에게만 연결되는 것이 아니라, 특정한 개념(concept)으로 연결시키는 X.509 인증서를 제안하였다. 여기에서 개념은 전통적인 공개키 인증서에서는 하나의 사용자가 될 수 있으며, 그룹 서명 기법에서는 모든 그룹의 멤버 집합이 될 수도 있다. 이러한 접근 방법은 그룹의 개별 멤버들이 각기 다른 속성(attribute)을 가지고, 그에 따라 서비스 인가를 받아야 하는 환경에서는 적합하지 않을 수 있다.

두번째 접근 방법은 사용자의 실제 신원 대신 사용자의 가명(Pseudonym)을 사용하는 것이다[3,8]. 이러한 방법에서 중요한 포인트는 가명의 발급 단계에서 제 3자에 의해 가명과 실제 신원의 대응 관계가 공개되지 말아야 하며, 특정한 발급 기관이 이러한 관계 정보를 모두 알고 있지 않도록 해야 한다는 것이다. 만약, 특정한 발급 기관이 이를 모두 알 수 있도록 시스템이 구성된다면, 이 기관은 모든 사용자의 신원을 확인할 수 있는 빅브라더(Big Brother)가 될 수 있으며, 이는 바람직하지 않다. 또한, 두번째 접근 방법은 2.1의 연결 불가능성(Unlinkability)를 해치는데, 이는 특정한 사용자의 통신이 그 인증서에 있는 가명으로 모두 연결되기 때문이다.

III. 실제 환경에서의 요구 사항

3.1 연결성(Linkability) 및 추적성(Traceability)

사용자의 프라이버시를 제공하기 위한 익명 인증 기법에 대한 많은 연구들이 있지만, 이들은 대체로 이론적인 접근 방법만을 다루고 있어 실생활에서의 서비스에 적용하기 어려운 부분이 있다.

실생활에서의 요구 사항은 그룹 서명 혹은 가명 시스템의 요구 사항과 다소 다르다. 대부분의 익명 인증 기법은 연결 불가능성을 지원하지만, 서비스 제공자들은 '한정된 연결성(Local Linkability)'를 필요로 한다. '한정된 연결성(Local Linkability)'이란 특정 서비스에서 한 사용자가 여러 개의 서명을 한 경우 이 서비스를 제공하는 서비스 제공자는 이 서명들이 동일한 사용자의 서명임을 확인할 수 있지만, 다른 서비스 제공자는 이를 구분하지 못하는 것을 의미한다. 서비스 제공자는 일반적으로 통계 및 서비스 전략을 위하여 이러한 한정된 연결성을 필요로 한다. 물론, 이러한 요구 사항은 사용자의 프라이버시를 일부 희생시키지만, 이 정도 수준의 희생이 없다면 서

비스 제공자는 사용자(서비스 소비자)에 대한 정보를 전혀 얻을 수 없어 사업 계획과 전략을 수립하기 어려울 것이다.

링 서명[10]과 같은 익명 인증 기법들은 추적 불가능성(Untraceability)을 지원한다. 그러나, 법적인 이유 혹은 응급 상황 등 때문에 이는 바람직하지 않다. 인터넷에서는 사이버 폭력, 명예 훼손과 같은 불법 상황이 자주 발생한다. 추적 불가능한 익명성은 일부 사용자들이 이러한 범죄에 더 빠져들게 할 수 있으며, 피해자를 구제하기 어렵게 할 수도 있다. 따라서, 조건부 추적성은 실세계에서 반드시 필요로 한다고 볼 수 있다.

3.2 서비스 인가(Service Authorization)

그룹 서명은 실생활의 익명 인증을 위한 좋은 후보 기법이 될 수 있다. 그러나, 이 기법은 서비스 인가를 위해 사용자에 대한 어떠한 정보도 제공하지 않는다. 때때로 인터넷 서비스는 나이, 직업과 같은 사용자의 속성을 필요로 한다. 성인 서비스라든지 인재 스카우팅 서비스와 같은 예에서, 익명성과 함께 그 사람의 실제 속성을 증명할 수 있다면 더 원활한 서비스가 가능할 것이다.

익명성만 지원 가능하다면 PKI 속성 인증서는 좋은 수단이 될 수 있다. PKI는 사용자를 인증하기 위해 널리 사용되고 있지만, 익명 인증 기법을 PKI에 적용하는 것은 쉽지 않다.

Ⅳ. 제안 기법

3장에서 언급한 실세계의 요구 사항을 만족시키기 위해서는 한정된 연결성 및 조건부 추적성을 가지는 익명 PKI 기법을 생각해볼 수 있다. 본 논문에서는 여기에서 Short Group Signature를 이용한 가명 기반 PKI 기법을 제안한다.

앞서 익명 PKI의 2가지 접근 방법을 언급한 바 있다. 가면 기반 PKI는 연결 불가능성을 제공하지는 않지만, 실세계에서는 한정된 연결성 및 추적성을 필요로 하므로 이러한 접근 방법을 택할 수 있다. 인증서를 안전하게 발급받는 문제를 풀기 위해, 본 논문에서는 Short Group Signature를 사용한다.

4.1 제안하는 익명 PKI 구조

기존의 PKI에서, CA는 사용자의 실제 신원이 연결된 공개키 인증서를 발급하였다. 하지만 익명 PKI 환경에서는, CA가 사용자에 대한 신원 확인 후 실제 신원 대신 가명을 포함한 공개키 인증서를 발급한다고 하더라도, CA는 항상 가명과 실제 신원을 연결시킬 수 있게 되며 CA는 완전한 추적성을 가질 수 있게 되는데, 이는 CA가 빅브라더(Big Brother)의 힘을 가질 수 있게 되어 위험하다 할 수 있다.

따라서, 이러한 경우에 빅브라더의 역할을 할 수 있는 Entity의 권한을 분산(Separation of Authority)하는 것이 필요하며, 본 논문에서도 마찬가지로 CA를 두 기관으로 나누고자 한다. 이 중 한 기관은 사용자의 실제 신원을 검증할 수 있는 기관이며, 다른 하나는 사용자의 가명 인증서를 발급하는 기관이다. 따라서 본 논문이 제안하는 익명 PKI의 구조는 그림 1과 같다.

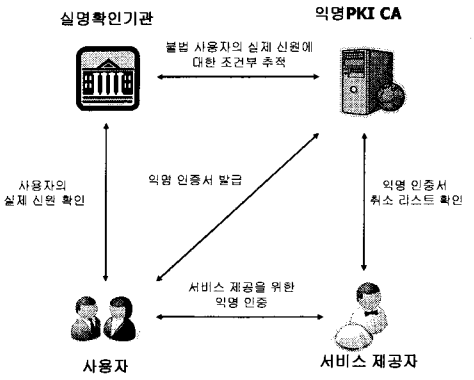

그림 1. 본 논문의 익명 PKI 구조

- ***실명확인기관*** : 사용자의 실제 신원을 확인하여 이 정보를 유지하는 기관이다. 이 기관은 그룹 서명에 대한 개인키를 만들고, 가명 인증서를 발급할 수 있는 일회성 신용장을 사용자에게 전달한다.
- ***익명PKI CA*** : 사용자의 가명 PKI 인증서를 발급하는 기관이다. 실명확인기관의 신용장을 이용하여 사용자에게 가명 공개키 인증서와 속성 인증서를 발급해준다.
- ***사용자*** : 서비스 제공자로부터 서비스를 이용하는 사람으로, 가명 인증서를 바탕으로 익명으로 서비스를 제공받는다.
- ***서비스 제공자*** : 사용자를 익명으로 인증하고 속성 인증서를 바탕으로 사용자의 권한에 맞는 적절한 서비스를 제공하는 기관이다.

본 논문에서는 실명확인기관과 익명PKI CA가 상호독립적인 기관이며, 합법적인 절차에 의한 승인이 있는 특별한 조건을 제외하고는 공모하지 않는다고 가정한다.

4.2 인증서 발급 프로토콜

사용자는 가명 기반 인증서를 발급받기 위해 다음의 절차를 거친다.

① 사용자 ↔ 실명확인기관

사용자는 실명 인증서 혹은 오프라인 방문을 통하여 자신의 실제 신원과 속성(나이, 성별 등)을 확인받는다. 실명확인기관은 Short Group Signature에서의 멤버 비밀키 발급자 및 그룹 관리자로서의 역할을 담당하며, 멤버 비밀키에 해당

하는 (A_i, x_i)를 발급한다. 또한, 이 기관은 일련번호, 사용자의 속성 정보 및 이에 대한 전자 서명을 포함하는 일회성 신용장을 발급한다. 실명확인기관은 사용자의 신원 정보와 멤버 비밀키에 대한 정보를 데이터베이스에 유지하여야 한다.

② 사용자 ↔ 익명 PKI CA

사용자는 가명 인증서 발급 요청 및 실명확인기관의 일회성 신용장을 포함하는 메시지를 만들어 그룹 서명을 한 후, 이를 CA에게 보낸다. 인증서 발급 요청 메시지에는 메시지 헤더, 타임스탬프와 사용자의 서명이 들어 있는데, 이 서명은 실명 PKI상의 공개키에 의한 서명으로 이 서명을 그대로 담으면 실명이 노출될 수 있기 때문에 실명확인기관의 공개키를 이용한 암호화 과정을 거치도록 한다. CA는 발급 요청 정보 및 일회성 신용장을 실명확인기관에 보내서 이 메시지의 정상 여부를 확인한다. 실명확인기관은 사용자의 서명을 복호화하여 검증한 후, 서명 검증 성공 여부 및 일회성 신용장 검증 여부만을 전달한다.

이렇게 실명확인기관으로부터 확인을 받은 후, CA는 Short Group Signature의 검증자로서 역할을 담당한다. 즉, CA는 그룹 서명와 일회성 신용장을 검증하고, 정상적일 경우 CA는 가명 공개키 인증서 및 이에 대한 속성 인증서를 발급한다. CA는 사용자의 발급 요청 메시지 및 그룹 서명, 그리고 가명 정보를 DB에 유지하여야 한다. 이 단계에서 실명확인기관은 특정 사용자의 가명 정보를 알아낼 수 없다.

4.3 사용자의 신원 추적

가명 인증서 사용 시나리오는 사용자의 신원 추적을 제외하고는 실명 인증서의 시나리오와 동일하다. 사용자의 신원을 추적하여야 할 경우, 서비스 제공자는 CA에게 사용자의 가명 및 서명이 포함된 메시지를 보고한다. CA는 사용자의 서명을 검증한 후, 사용자의 신원 추적을 실명확인기관에 요청하기 위해 그룹 서명이 포함된 인증서 발급 요청 메시지를 전송한다. 실명확인기관은 사용자의 신원을 추적하기 위해 멤버 비밀키를 찾아 낸 후에(Short Group Signature의 신원 공개 단계), 데이터베이스를 이용하여 사용자의 실제 신원 정보를 알 수 있게 된다.

V. 결 론

본 논문에서는 Short Group Signature를 이용한 가명 기반 PKI에 대해 제안하였다. 이 방법에서, 사용자의 프라이버시 보호 및 익명성 제공을 위해 가명 인증서가 사용되었다. 사용자의 익명성을 보장하기 위하여 가명 인증서를 발급받을 때 그룹 서명 기법을 활용하고 있다.

본 논문은 가명 인증서를 사용함으로써 여러 트랜잭션이 같은 사용자들 것인지를 알 수 있는 연결성(Linkability)을 가지지만 한정된 연결성(Local Linkability)을 제공하는 방법에 대해서도 연구하고 있다. 이 외에도 보다 효율적이며 실용적인 익명 인증 기법을 만들기 위한 연구가 필요하며, 이런 기법이 구현될 경우 보다 프라이버시가 강화된 인터넷 서비스가 가능해질 것이다.

참고문헌

[1] D. Boneh, X. Boyen, H. Shacham, "Short group signatures," CRYPTO '04, volume 3152 of LNCS, pp. 41-55, 2004.

[2] V. Benjumea, S. G. Choi, J. Lopez and M. Yung, "Anonymity 2.0 - X.509 extensions supporting privacy-friendly authentication," CANS '07, pp. 265-281.

[3] V. Benjumea, J. Lopez, J. A. Montenegro, and J. M. Troya, "A First Approach to Provide Anonymity in Attribute Certificates," PKC 2004, volume 2947 of LNCS, pp. 402-415.

[4] D. Chaum, "Security without identification transaction systems to make Big Brother obsolete," Communications of the ACM, Vol. 28, No. 10, 1985.

[5] D. Chaum and E. van Heyst, "Group signatures," EUROCRYPT 1991, volume 547 of LNSC, pp. 257-265.

[6] A. Lysyanskaya, R. L. Rivest, A. Sahai, and Stefan Wolf, "Pseudonym systems," SAC '99, pp. 184-199.

[7] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," EUROCRYPT 2001, volume 2045 of LNCS, pp. 93-118.

[8] T. Kwon, J. H. Cheon, Y. Kim, and J. Lee, "Privacy Protection in PKIs: A Separation-of-Authority Approach," WISA 2006, volume 4298 of LNCS, pp.297-311.

[9] X.509, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks," ITU-T Recommendation X.509, March 2000. Also available at ISO/IEC 9594-8, 2001.

[10] R. Rivest, A. Shamir, Y. Tauman, "How to leak a secret," ASIACRYPT 2001, volume 2248 of LNCS, pp. 552 - 565, 2001

[11] A. Kiayias, Y. Tsiounis, M. Yung, "Traceable signatures," EUROCRYPT 2004. volume 3027 of LNCS, pp. 571 - 589, 2004