通信情報保護學會論文誌
第 2 卷 第 1 號, 1992. 6

ID기반의 영지식 대화형 프로토콜을 이용한 개인 식별 및 키 분배 프로토콜에 관한 연구

이윤호* · 양형규* · 권창영* · 원동호*

A Study on the Identification and Key Distribution Protocol Using ID-Based Zero-Knowledge Interactive Protocol

Yun-Ho Lee and Hyung-Kyu Yang and Chang-Young Kwon and Dong-Ho Won

요 약

본 논문에서는 ZKIP의 랜덤 정보를 이용한 영지식 키 분배 프로토콜을 제안하였다. 제안한 방식은 이미 안전하다고 입증된 ZKIP을 이용한 개인 식별을 행하고 더 이상의 정보 교환 없이 키 생성을 할 수 있다. 또한 키 분배 프로토콜을 행할 때, 센터에 대한 의존도를 줄이기 위해 확장 Fiat-Shamir 방식과 Schnorr 방식을 결합하여 인증을 행하도록 하였다. 결합된 프로토콜은 제 3 자의 일반적인 위장을 방지할 수 있으며, 센터와 가입자의 결탁도 방지할 수 있다.

Abstract

In this paper, we proposed a zero-knowledge key distribution protocol which utilizes randomness of ZKIPs. The protocol performs user-identification using ZKIPs known to be secure and shows two end users can generate a session key without additional information transfer. And to reduce the degree of dependency on center, we use Fiat-Shamir-like scheme and Schnorr scheme. The proposed protocol can protect the general forgery of an adversary and the conspiracy of the center and the special users.

* 성균관대학교 정보공학과

1. 서 론

현대 사회는 정보화 사회로 변화하는 과정에서 고도의 통신 처리 및 정보 처리 기술을 필요로 하고 있다. 특히, 현재의 업무 형태를 정보화 사회에 걸맞는 새로운 형태 즉, '전자적인 형태'로 변환시키기 위해서는 신분 확인, 서명, 동시성 등의 문제가 해결되어야 한다. 또한, 정보 시스템 내에서 축적, 처리, 전송되는 정보는 전기적 현상을 이용하여 디지탈화 대용량화되고 있어 정보에 대한 적절한 보호 대책이 없으면 전송, 처리 혹은 기억 장치에 보관된 상태에서 불법 유출, 삭제 및 수정 등의 위험에 노출되기 쉽다. 이러한 불법적인 사고는 개인 정보의 침해 뿐만 아니라 막대한 경제적 손실을 당할 우려가 있어 정보 보호 대책에 대한 관심이 고조되고 있다.

정보 보호 방법으로는 암호 방식이 많이 이용되고 있다. 대개의 경우 암호라고 하면 비밀 통신을 연상하게 되는데 일상 업무 중에서는 비밀 문서의 취급보다는 일반 문서에 대한 서명이 훨씬 많이 취급되고 있는 바 정보화 사회의 도래로, EDI 시스템의 확산에서도 볼 수 있듯이 모든 문서가 '전자화'될 것은 자명하다.[1, 2] 그러므로 일상 생활의 거의 모든 분야가 '전자화'되어 부가가치가 높은 각종 통신 서비스를 제공하기 위해서는 메시지 인증(message authentication), 사용자 인증(entity authentication), 개인식별(identification), 디지탈 서명(digital signature)등이 비밀 통신 이상으로 아주 중요한 기능이다.

일반적으로 인증, 서명 등은 안전할 것으로 생각되는 암호 방식을 사용하여 해결하고 있으나, 암호 방식은 정보의 비밀성을 키에 의존하여 정보 보호 서비스를 실현하는 방식으로 개인 식별 및 안전한 키 분배 방식이 전제되어야 한다.[3]

본 논문에서는 ID 정보를 기반으로 하여 암호화 프로토콜의 안전성 문제를 해결하기 위하여 제시된 모델인 영지식 대화형 증명 방식(ZKIPs: Zero Knowledge Interactive Proof Systems)을 결합하여 카드 발급 센터 의존도를 줄이고 센터와 특정 가입자간의 결탁시 야기되는 문제점을 해결할 수 있도록 두 가지의 개인 식별 프로토콜을 결합하였다. 그리고 이 결합된 프로토콜을 이용하여 각종 서비스를 제공하는데 필수불가결한 키 분배 문제를 해결하기 위한 방안을 제시하였다. 이 방안은 키 분배시의 사전 통신량을 감소시키고 키 분배의 안전성을 향상시킬 수 있으리라 사료된다.

2. 영지식 대화형 증명 방식

1985년 Goldwasser, Micali, Rackoff가 ZKIP 개념을 발표하면서 시작된 ZKIP 이론은 증명자 P가 검증자 V에게 자신을 증명함에 있어서 증명자 P와 검증자 V가 대화형(interactive)으로 증명을 하는 방식으로 어떤 사실의 정당성에 관한 정보만을 전송하므로 그 이외의 어떤 정보도 노출시키지 않는다는 의미를 갖고 있다.[4-6] 즉, 증명자가 자신만이 아는 비밀 정보를 검증자에게 직접 전송하지 않고, 자신의 비밀 정보가 아닌 어떤 다른 정보를 전송하여 검증자에게 자신만이 비밀 정보를 알고 있다는 것을 증명할 수 있는 방식이다. 따라서 인증 방식에 있어서는 가히 혁신적인 방법이라 말할 수 있다. 즉, 자신의 신분을 증명하면서 상대방에게 확신 이외에는 전달되는 정보가 없기 때문에 지금까지 알려진 증명 방법 중 가장 안전한 증명 방법이라고 할 수 있다.

1986년 Fiat, Shamir에 의해 구체적인 방식이 제시된 이후 여러 가지 ZKIP 방식이 발표되었고 현재 활발히 연구가 진행되고 있다.[6] 다만 통신량이 많다는 것이 ZKIP의 단점인데 이 문제를 해결하기 위한 연구가 활발히 진행되고 있다.

그림 1과 같이 패스워드를 이용한 단순한 사용자 인증을 생각하여 보자. 즉, 컴퓨터 시스템의 사용자(P)가 컴퓨터 시스템(V)으로 패스워드를 전송하면, 컴퓨터 시스템은 이 패스워드가 컴퓨터 시스템 사용자의 패스워드인지 검증하여 사용자를 인증하는 방식은 NP 증명 방식의 전형적인 예이다.

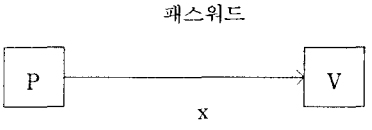


그림 1. 패스워드를 이용한 사용자 인증

위와 같은 NP 증명 방식은 증명자가 검증자에게 전송하는 정보 x가 너무나 중요하여 암호학의 입장에서 보면 그 적용 분야가 극히 한정될 수 밖에 없다. 그러므로, NP 증명방식의 약점을 배제하기 위한 새로운 증명 방식이 필요하다.

영지식 증명 방식은 NP 증명 방식을 두가지 면에서 일반화시킨 증명 방식으로 NP 증명 방식은 deterministic Turing machine 상에서 정의되었으나, 대화형 증명 방식은 probabilistic Turing machine 상에서 정의되며, NP 증명 방식은 증명자가 검증자에게 자신의 정보를 전송하는 일방향 방식이나, 대화형 증명 방식은 검증자도 자신의 정보를 증명자에게 전송하는 양방향 방식이다. 대화형 증명 방식을 구체적으로 정의하면 다음과 같다.

[정의] 대화형 증명 방식(interactive proof system)

대화형 증명 방식은 대화형 통신이 가능한 무한 계산 능력을 갖는 interactive Turing machine P와 다항식 계산 능력을 갖는 interactive Turing machine V로 구성된 그림 2와 같은 대화형 프로토콜 (P, V)가 아래 조건을 만족하면 대화형 증명방식이라고 한다.

조건 1) 완전성(completeness)

(P, V)는 NP 문제인 X를 공통 입력 정보로 받아들이며, x가 문제 X의 해일 경우, 증명자 P는 검증자 V에게 x가 문제 X의 해인지 $1 - |x|^{-c}$ 이상의 확률로 증명할 수 있어야 한다.

$$x \in L\text{이면, } \forall c, \exists N, \forall |x| > N$$
$$\text{Prob}(V \text{ accept}) \geq 1 - |x|^{-c} \quad (1)$$

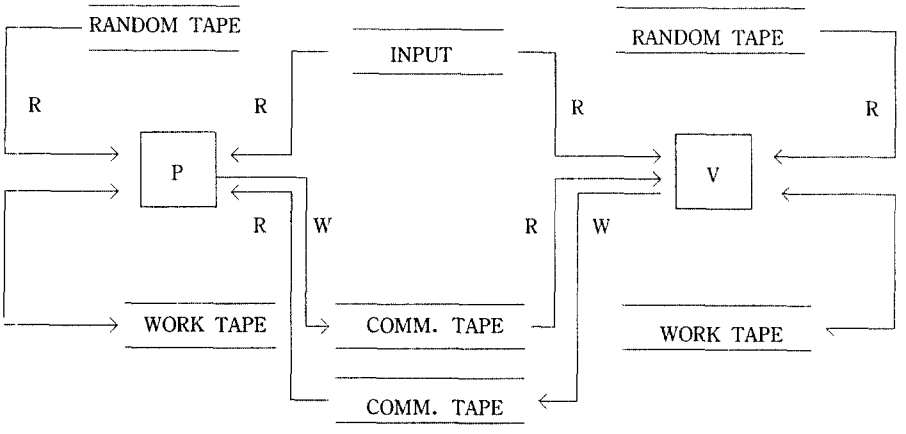
(단, 확률은 P와 V의 동전 던지기와 관련)

조건 2) 건전성(soundness)

(P*, V)는 NP 문제인 X를 공통 입력 정보로 받아들이며, x가 문제 X의 해가 아닐 경우, 임의의 증명자 P*는 검증자 V에게 x가 문제 X의 해임을 증명할 수 있는 확률은 $|x|^{-c}$ 이하이어야 한다.

$$x \notin L\text{이면, } \forall c, \exists N, \forall |x| > N \ \forall P^*$$
$$\text{Prob}(V \text{ accept}) \leq |x|^{-c} \quad (2)$$

(단, 확률은 P*와 V의 동전 던지기와 관련)



R: read-only, W: write-only

그림 2. 대화형 프로토콜

이러한 정의는 증명 방식(proof system)이 가져야 할 직관적인 특성을 가지고 있다. 즉, 조건 1)은 x가 문제 X의 해일 경우, V는 압도적인 확률로 수락되어야 한다는 것을 의미하며, 조건 2)는 x가 문제 X의 해가 아닐 경우, V가 수락할 확률이 무시할 정도로 적은 확률이어야 한다는 의미이다.

또한, 영지식(zero-knowledge)이란 시뮬레이터와 view의 개념을 도입해서 정의할 수 있는데, view는

검증자 V가 증명자 P와의 프로토콜을 종료한 후 볼 수 있는 모든 것으로 P와 상호 통신하는 동안 전송받은 정보 및 자신이 발생한 난수 등이 이에 속한다. 여기서 만약 프로토콜을 시작하기 전과 프로토콜 종료 후의 view를 비교하였을 때, indistinguishable하다면, 프로토콜 진행 중에 받은 정보는 새로운 지식을 전혀 포함하고 있지 않았다는 것을 의미하게 되고 따라서 프로토콜을 종료시 V의 지식의 증가는 없다고 볼 수 있다. 위와 같이 프로토콜 시작전에 view를 생성하는 알고리즘을 시뮬레이터라고 하며, 지식의 증가가 없을 때, 영지식성을 만족시킨다고 할 수 있다. 영지식 대화형 증명 방식을 좀 더 체계적으로 정의하면, 다음과 같다.

[정의] 영지식 대화형 증명 방식

대화형 증명 방식 (P, V)가 다음의 조건을 만족하면, 영지식 증명 방식이라고 한다.

조건 1) 임의의 다항식 계산 능력을 갖는 검증자 V^*에 대하여, 다항식 계산 능력을 갖는 probabilistic Turing machine Mv^*가 존재하고 $\{Mv^*[X]\}$와 $\{(P, V^*)[X]\}$는 indistinguishable 하여야 한다.

3. 기존의 개인 식별 방식 및 문제점

개인 식별(identification)은 가입자 A가 가입자 B와 협조하여 A는 B에게 자신이 A임을 증명할 수 있으나, 제3자인 C는 A로 위장하여 B에게 자신이 A라고 속일 수 없는 사용자 인증(entity authentication) 기능에 가입자 B도 제3자 D에게 자신이 A라고 증명할 수 없다는 조건이 추가된 기능이다. 일반적으로 개인 식별 방식은 유용하고 안전하기 위해서 아래의 3가지 조건을 만족하여야 한다.

① 합법적인 검증자는 합법적인 증명자의 identity 증명을 높은 확률로 accept 하여야 한다.

② 합법적인 검증자는 불법적인 증명자의 identity 증명을 낮은 확률로 accept 하여야 한다.

③ 불법적인 검증자는 합법적인 증명자와 다항식 횟수 만큼 상호 통신하여도 어떤 사람에게도 자신이 합법적인 증명자라고 흉내낼 수 있는 아무런 정보도 획득할 수 없어야 한다.

즉, 효율적인 개인 식별은 영지식 대화형 증명의 개념과 상통한다. 그러므로 본 논문에서는 영지식 대화형 증명을 이용한 기존의 대표적인 개인 식별 프로토콜들을 언급하고 그 문제점들을 지적하고 해결책을 제시하였다. 기술 내용을 간결하 하기 위하여 아래와 같은 수학 기호를 사용하였다.

$$Z_n = \{x | 0 \le x < n\} \quad (3)$$

$$Z_n^* = \{x | 0 \le x < n,\ (x, n) = 1\} \quad (4)$$

$$r \in_R Z_n^* \quad (5)$$

즉, Z_n은 mod n에 관한 완전 잉여계(complete residue system modulo n)이며 Z_n^*는 mod n에 관한 기약 잉여계(reduced residue system modulo n)이다. 또한 식 (5)의 의미는 Z_n^*에 속하는 임의의 원소 r을 랜덤하게 선택한다는 의미이다.

3.1 Fiat-Shamir 개인 식별 방식

Fiat-Shamir 개인 식별 방식(이하 FS 방식)은 ZKIP의 개념에 Shamir 자신이 제안한 ID 개념[7]을 첨가한 방식이다.[8] 개인 식별 정보 ID_i의 평방잉여 s_i를 계산하여 가입자의 비밀키로 사용하였다. 이 방식의 안전성은 충분히 큰 두 소수 p, q의 곱인 n의 소인수분해를 모를 때, 제곱근(square root)을 구하는 문제는 어려운 문제(NP 문제)라는 것에 근거한다.

사전 준비 과정에서 신뢰할 수 있는 센터(center)는 소수 p, q를 비밀리에 선택하고, 그 곱인 n을 공개한다. 카드발급 과정에서 센터는 합법적인 사용자에게 카드를 발급할때 그 사용자에 관한 정보(이름, id 번호, 주소, 주민등록번호 등)와 카드에 관한 정보(유효기간 등)를 담고 있는 ID_i를 준비하고, mod n상에서 ID_i의 평방근을 계산하여 그 역수 s_i를 각 가입자의 비밀키로 한다.

즉, 이 방식에서는 모든 ID_i가 mod n 상에서 평방근을 갖지는 않으므로, 이 문제의 회피책으로 임의의 스트링이 입력되면 [0, n)이 출력되는 pseudo random function h를 선택하여 아래와 같이 비밀키를 생성한다.

① $v_j = h(ID_i, j)$ $(j = 1, \cdots, m)$을 구한다.

② 이 중에서 k개의 평방잉여 선택, 각 v_j^{-1}의 가장 작은 제곱근 s_j를 k개 계산.

③ ID_i와 k개의 s_j, 그리고 각각의 j값을 카드에 담아 사용자에게 발급.

가입자 A와 가입자 B가 개인 식별을 행하는 프로토콜은 아래와 같다.

프로토콜 1.

순서 1-1. 가입자 A는 ID_A를 가입자 B에게 전송한다.

순서 2-1. 가입자는 B는 $v_j = h(ID_A, j)$ (j = 1, …, k)를 계산한다.

순서 3-1. 가입자 A는 $r \in_R Z_n^*$ 를 선택한다.

순서 3-2. 가입자 A는 $x = r^2 \pmod n$를 계산한다.

순서 3-3. 가입자 A는 x를 가입자 B에게 전송한다.

순서 4-1. 가입자 B는 $(d_1, \cdots, d_k) \in_R \{0, 1\}$를 선택한다.

순서 4-2. 가입자 B는 가입자 A에게 $(d_1, \cdots, d_k)$를 전송한다.

순서 5-1. 가입자 A는 $y = r \prod_{d_j=1} s_j \pmod n$를 계산한다.

순서 5-2. 가입자 A는 y를 가입자 B에게 전송한다.

순서 6-1. 가입자 B는 $x = y^2 \prod_{d_j=1} v_j \pmod n$이 성립하는지 검증한다.

순서 7-1. 순서 3-1에서 순서 6-1을 t회 반복한다.

FS 방식은 영지식이며 안전성은 매개 변수(security parameter) k, t에 의존한다(2^{-kt}). FS방식에서 t회 동안 보낼 모든 x 및 d를 1회에 전송하는 병렬 방식은 영지식이 아니다.[8]

FS방식은 스마트 카드의 마이크로 프로세서(smart card microprocessor)와 인터페이스되는 산업 표준 퍼스널 컴퓨터간의 대화형 개인 식별 방식(interactive identification scheme)으로 구현하려고 시도되었으며,[9] 1988년 Micali와 Shamir는 증명자의 계산 복잡도에는 변화가 없으나, 검증자의 계산 복잡도를 2회 이하의 modular 곱셈으로 감소시킨 중앙 집중식 컴퓨터 네트워크에서 효율적인 방식을 제안 하였다.[10]

FS 방식의 문제점은 현재 스마트 카드 프로세서의 제약 조건들은 사용 알고리즘의 선택시 엄격한 제한을 수반하게 되는데 비해 반복(iteration) 횟수와 증명자가 많은 메모리를 필요로 한다는 것이다. 또한, 만약 센터의 비밀 정보가 노출되는 경우 전혀 안전성이 보장되지 않으며, 센터와 특정 가입자간의 결탁으로 임의의 가입자의 비밀 정보를 이용하여 부정한 행위를 행할 수 있는 가능성이 있다.

3.2 확장 Fiat-Shamir 개인 식별 방식

확장 Fiat-Shamir 개인 식별 방식(이하 확장 FS 방식)은 FS 방식의 효율성을 개선한 방식으로 FS 방식의 멱승 지수부를 기소수 L로 확장한 방식이다.[11-13] FS 방식의 문제점인 증명자와 검증자 사이의 반복 통신 횟수(round)를 1회로 개선하였으며, 적은 메모리로 개인 식별이 가능한 방식이다. 계산량에 있어서는 FS 방식에 비하여 약 2~3배 정도 증가한다.

확장 FS 방식은 사전 준비 과정에서 신뢰할 수 있는 센터가 소수 p, q를 비밀리에 선택하고, 그 곱인 n을 공개한다. 또한, $\Phi(n)$과 서로소인 L를 선택하여 공개한다.

카드발급 과정에서 센터는 합법적인 사용자 i에게 카드를 발급할 때 그 사용자에 관한 정보(이름, id 번호, 주소, 주민등록번호 등)와 카드에 관한 정보(유효기간 등)를 담고 있는 ID_i를 준비하고, GQ 방식에서는 mod n 상에서 ID_i의 L승근을 계산하여 그 역수로 각 가입자의 비밀키 s_i로 하며, OhO 방식에서는 mod n 상에서 ID_i의 L승근을 각 가입자의 비밀키 s_i로 한다.

GQ 방식에서는 shadowed identity J의 v승근을 이용하여 반복 횟수를 1회로 줄였으며, shadowed identity J에 대한 내용은 ISO-DP 9796("digital signature scheme with shadow" 표준화)에 자세히 언급되어 있다.

프로토콜 2.

순서 1-1 가입자 A는 $r \in_R Z_n^*$ 를 선택한다.

순서 1-2 가입자 A는 $x = r^L \pmod n$을 계산한다.

순서 1-3 가입자 A는 x를 가입자 B에게 전송한다.

순서 2-1 가입자 B는 $d \in_R Z_L$를 선택한다.

순서 2-2 가입자 B는 가입자 A에게 d를 전송한다.

순서 3-1 가입자 A는 $y = r \cdot s_A^d \pmod n$을 계산한다.

순서 3-2 가입자 A는 y를 가입자 B에게 전송한다.

순서 4-1 가입자 B는 $y^L = x \cdot ID_A^d \pmod n$이 성립하는지 검증한다.

FS 방식에서는 순서 3-1에서 순서 6-1을 t회 반복하는데 반하여 확장 FS 방식에서는 순서 1-1에서 순서 4-1을 1회 행하므로 통신 효율을 개선하였다. 그러나, 이 방식의 안전성 역시 센터의 비밀 정보에 의존적이며, 센터와 특정 가입사간의 결탁 문제는 상존한다.

3.3 Schnorr 개인 식별 방식

1988년 Chaum, Evertse 그리고 Graaf는 이산 대수를 이용하여 영지식 대화형 프로토콜(프로토콜 1)을 제안하였으며,[14] 또한 1989년 Schnorr는 이산 대수 문제를 이용한 개인 식별 방식(이하 S 방식)을 제안했다.[15] 이 방식을 살펴보면 아래와 같다.

사전 준비 단계에서 센터는 p-1이 140비트 정도의 소수 q를 인수로 가지는 512 비트의 소수 p를 정하고, Z_p 상에서 위수(order)가 q인 원소 a를 정한다.

$$q \mid p-1,\ q \geq 2^{140},\ p \geq 2^{512} \qquad (6)$$
$$a^q \equiv 1 \pmod p,\ a \neq 1$$

센터 자신의 비밀키와 공개키를 정하는데 이러한 과정을 거친 후 p, q, a, 센터의 공개키 등을 공개한다.

카드발급 과정에서 새로운 사용자 i가 가입 신청을 할 때, 먼저 자신만이 비밀키 s_i를 정하고 센터가 공개한 공개 정보를 이용해서 아래 식에 의해 공개키 v_i를 생성한다.

$$s_i \in_R \{1, 2, \cdots, q-1\}$$
$$v_i = a^{-s_i} \pmod p \qquad (7)$$

센터는 가입 신청자의 신원을 확인한 후, 그 사용자에 관한 개인 정보(이름, ID 번호, 주소, 주민등록번호 등) I_i와 신청자의 공개키 v_i의 쌍(I_i, v_i)에 센터 자신의 비밀키를 이용하여 서명 S를 생성한다.

프로토콜 3.

순서 1-1 가입자 A는 난수 $r \in_R \{1, 2, \cdots, q-1\}$를 선택한다.

순서 1-2 가입자 A는 $x = a^r \pmod p$를 계산한다.

순서 1-3 가입자 A는 I_A, v_A, S, x를 가입자 B에게 전송한다.

순서 2-1 가입자 B는 signature S를 검증하여 가입자 A의 identification을 확인.

순서 2-2 가입자 B는 난수 $e \in_R \{0, \cdots, 2^t - 1\}$를 선택한다.

순서 2-3 가입자 B는 난수 e를 가입자 A에게 전송한다.

순서 3-1 가입자 A는 $y = r + s_A \cdot e \pmod q$를 계산한다.

순서 3-2 가입자 A는 y를 가입자 B에게 전송한다.

순서 4-1 가입자 B는 $x = a^y \cdot v_A^e \pmod p$이 성립하는지 검증한다.

제 3 자인 C가 e를 추측하여 아래 식 (8)을 만족하는 x, y를 전송하여 인증에 성공할 확률은 2^{-t}이다.

$$x = a^y \cdot v^e \pmod p,\ y = r \qquad (8)$$

검증자 B는 A로부터 유효한 정보를 획득하기 위해서 순서 2에서 비트 스트링 e를 자유롭게 선택할 수 있다. 엄밀하지는 않지만 약식으로 생각하면, x와 y는 난수이기 때문에 A는 아무런 정보도 노출시키지 않으며, y는 x의 이산대수를 포함하므로 유효한 정보를 노출시키지 않는다. 즉, 제 3 자가 x로부터 $r = \log_a x$를 유추할 수 없다.

$$y = \log_a x + e \cdot s \pmod q \qquad (9)$$

그러나, S 방식에서 (x, y, e)는 방정식 $x = a^y \cdot v^e \pmod p$의 부분해이기 때문에 엄밀한 의미에서 영

지식은 아니다.

S 방식은 안전성이 FS 방식이나 FS 확장 방식이 가지고 있는 문제점처럼 센터의 비밀 정보에 의존적인 방식은 아니다. 그러나, S 방식은 가입자의 비밀 정보에 절대적으로 의존적인 방식이다.

4. 확장 FS 방식과 S 방식의 결합 프로토콜

앞에서 살펴본 바와 같이 FS 방식, 확장 FS 방식, S 방식 등은 안전성이 센터의 비밀 정보에 절대적으로 의존적이거나, 가입자의 비밀 정보에 절대적으로 의존적이다. 이러한 문제점을 해결하기 위해 확장 FS 방식과 S 방식을 결합하여 안전성이 센터나 각 가입자에 의존적이지 않는 개인 식별 프로토콜을 만들 수 있다.

4.1 결합된 개인 식별 프로토콜

센터는 가입 신청을 받기 전에 아래의 사전 동작으로 충분히 큰 두 소수 p, q를 정하고 아래의 식에 의해 N을 구한다.

$$N = p \times q \tag{10}$$

이와 함께 P - 1이 140비트 정도의 소수인 Q를 인수로 갖는 512비트의 소수 P를 정하고, Z_P 상에서 위수(order)가 Q인 원소 a를 정한다.

$$Q|P-1,\ Q \geq 2^{140},\ P \geq 2^{512} \tag{11}$$
$$a^Q \equiv 1 \pmod P,\ a \neq 1$$

이와 함께 일방향 해쉬 함수 $h(\cdot)$와 트랩도어 함수 $f(\cdot)$을 정한다. 센터는 이중에서 N, P, Q, a, $h(\cdot)$, $f(\cdot)$를 공개하고, p, q, $f^{-1}(\cdot)$는 비밀 정보로 보관하며, 가입 신청을 하는 사용자는 공개된 정보를 이용할 수 있다.

이 후 가입자 i가 새로 통신망에 등록하는 경우, 센터가 공개한 a와 자신이 임의로 비밀 정보 SK_i를 선택하여 $PK_i = a^{-SKi}$를 구해서 자신의 이름, 주소, 전화번호, 주민등록번호 등으로 구성한 identity ID_i와 함께 센터에게 제시한다.

센터는 ID_i의 타당성을 확인한 후에 가입자 i의 공개 정보 V_i, 비밀 정보 S_i 및 CA_i를 아래의 식에 의해 구한다.

$$V_i = h(ID_i) \tag{12}$$
$$S_i = V_i^{1/L} \tag{13}$$
$$CA_i = f^{-1}\ (PK_i \| V_i) \tag{14}$$

센터는 이것과 함께 N, P, Q, S_i, $h(\cdot)$, $f(\cdot)$, a, L을 스마트 카드에 가입자 i에게 전달한다. 이상의 과정을 정리하면 다음과 같다.

가입자 A가 가입자 B에게 자신이 A임을 증명하기 위한 개인 식별 프로토콜은 아래와 같다.

프로토콜 4.

순서 1-1 가입자 A는 $r_1 \in_R Z_n^*$를 선택한다.

순서 1-2 가입자 A는 $x = r_1^L \pmod N$를 계산한다.

순서 1-3 가입자 A는 자신의 CA_A와 x를 가입자 B에게 전송한다.

순서 2-1 가입자 B는 공개함수 f를 이용하여 CA_A로 부터 A의 PK_A와 V_A를 구한다.

순서 2-2 가입자 B는 $d \in_R Z_L$를 선택한다.

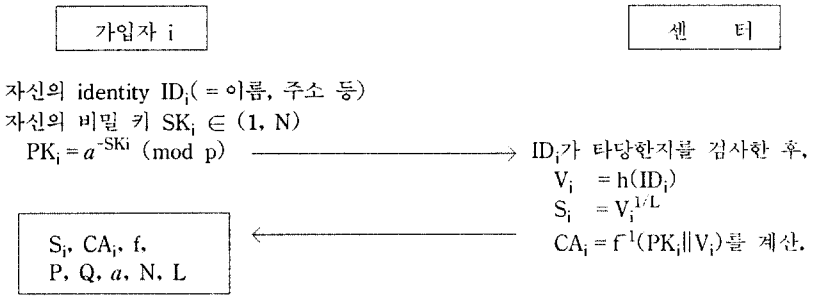


그림 3. 카드 발급 과정

순서 2-3 가입자 B는 가입자 A에게 d를 전송한다.

순서 3-1 가입자 A는 $y = r_1 \cdot S_A^d \pmod N$을 계산한다.

순서 3-2 가입자 A는 y를 가입자 B에게 전송한다.

순서 4-1 가입자 B는 $y^L = x \cdot V_A^d \pmod N$이 성립하는지 검증한다.

순서 5-1 가입자 A는 난수 $r_2 \in_R \{1, 2, \cdots, q-1\}$를 선택한다.

순서 5-2 가입자 A는 $z = a^{r2} \pmod P$를 계산한다.

순서 5-3 가입자 A는 z를 가입자 B에게 전송한다.

순서 6-1 가입자 B는 난수 $e \in_R \{0, \cdots, 2^t - 1\}$를 선택한다.

순서 6-2 가입자 B는 난수 e를 가입자 A에게 전송한다.

순서 7-1 가입자 A는 $T = r_2 + e \cdot SK_A \pmod Q$를 계산한다.

순서 7-2 가입자 A는 T를 가입자 B에게 전송한다.

순서 8-1 가입자 B는 $z = a^T \cdot PK_A^e \pmod P$가 성립하는지 검증한다.

4.2 결합된 개인 식별 프로토콜의 검토

위 프로토콜 4의 순서 4에서 검증이 성립하지 않으면, 이 프로토콜은 즉시 중지되며, 순서 8에서의 검증이 성립되지 않으면, 역시 이 프로토콜은 중지된다. 즉, 순서 4 및 순서 8의 검증과정이 모두 성립하여야만 가입자 B는 가입자 A의 증명을 수락(accept)하고 프로토콜을 정상적으로 종료한다.

프로토콜의 순서 1에서 순서 4까지는 증명자가 어떤 수의 L승 근을 아는지 확인하는 과정으로 공격자의 일반적인 부정행위 즉, 정당한 가입자인 것처럼 위장하는 행위(forgery)를 방지하는 것이나, 센터와 특정 가입자간의 결탁(conspiracy)으로 획득할 수 있는 불특정다수 가입자의 비밀키를 이용하여 행하는 불법적 행위는 방지하지 못한다. 그러므로 각 가입자가 스스로 선택한 비밀 정보에 의한 순서 5에서 순서 8을 추가하여 인증을 행하기 때문에 센터라 하더라도 가입자의 비밀 정보 SK_i를 모르면 인증을 성공시킬 수 없도록 하여 3장에서 언급한 문제점을 해결하였다.

5. 결합된 개인 식별 방식을 이용한 키 분배 프로토콜의 제안

5.1 키 분배 방식

관용 암호 방식의 키 분배 문제를 해결하기 위해서 1976년 Diffie와 Hellman은 이산대수의 어려움에 근거한 키 분배 방식을 제안했다.[16] 이 방식은 공개 디렉토리에 각 가입자가 자신의 공개 정보를 등록하고 키 분배 과정에서 상대방의 공개 정보를 이용하여 양자가 공통키를 생성하는 방식이다. 이 방식은 공개 디렉토리 관리의 어려움, 키의 동일성 등의 단점이 있지만, 대부분의 키 분배 방식은 이 방식을 기초로 하고 있다.

Shamir는 1984년 ID 정보를 기반으로 하는 암호 시스템을 제안했는데,[7] 한 개인의 ID란 다른 사람과 구별이 가능한 이름, 주소, 주민등록번호 등으로 구성할 수 있으며, 이 ID 개념을 키 분배에 이용한 것이 ID 정보를 기반으로 하는 키 분배 방식이다. 이 방식의 장점으로는 공개 디렉토리 대신 각 가입자를 구별할 수 있는 ID를 이용함으로써 공개 디렉토리가 필요없다는 점이다. 이 ID 개념은 ZKIP과 결합되어 많은 암호화 프로토콜의 기반이 되고 있다.

인증 방식과 키 분배 방식을 결합하는 방법은 크게 키 분배에 의한 인증과 인증에 의한 키 분배로 나눌 수 있다.[17] 먼저 키 분배에 의한 인증이란 통신망의 각 가입자가 자신만의 비밀 정보를 소유하고 있을 때, 임의의 양 가입자는 공통키를 생성할 수 있으며, 양자가 정확한 키를 소유하였을 때 상대방을 인증하는 방법이다. 키 분배 방식으로는 DH 방식, ID 기반의 키 분배 방식 등을 이용할 수 있으며 이러한 인증 방식법은 키 분배 방식의 안전성에 의존한다.

인증에 의한 키 분배란 먼저 인증을 행한 후, 인증 과정에서 사용된 데이타를 이용해서 공통키를 생성하는 방법을 말한다. 이 방법의 장점은 이미 안전하다고 입증된 영지식 대화형 증명 방식을 인증 방식에 이용하여 안전한 키 분배를 할 수 있다는 점인데 이미 제안된 방식으로는 1989년 Bauspieβ가 Beth의

ZKIP[18]을 이용하여 키 분배를 행한 것과 FS 방식을 이용한 것이 있다.[17, 19]

5.2 결합된 개인 식별 프로토콜을 이용한 키 분배 프로토콜의 제안

영지식 대화형 증명에서는 증명자와 검증자 사이에 랜덤 정보(randomized information)가 전송되며 증명자의 랜덤성(randomness)은 영지식(zero knowledge) 조건을 만족시키기 위해서 사용된다. 이 랜덤 정보는 영지식 대화형 증명에만 국한되어 사용되고 있는데, 만약 이 랜덤 정보를 좀 더 효과적으로 사용하면 많은 통신정보보호 분야에 적용 가능할 것으로 사료된다. 그러므로 영지식 증명에서 증명자의 랜덤 정보를 이용하여 암호화 키 분배(key distribution)에 이용 가능하다.

즉, 난수 R에 대신에 f(r, a)를 사용하는 것이다. 단, g(f(r, a))와 g(R)의 분포는 indistinguishable 하다. a는 고정 파라메터이고, g(R)은 영지식 증명을 이용하여 증명자로 부터 검증자에게 전송되는 하나의 메시지이다. 만약 g(f(r, a))와 g(R)의 분포가 indistinguishable하다면, 영지식 증명은 가능하다. 즉, f(r, a)의 예인 a^r mod n같은 함수는 ID 기반의 키 분배 방식을 구성하는데 사용할 수 있다.

이와 같은 생각에서 제안한 개인 식별의 첫번째 인증 과정을 이용하여 키분배도 해결하기 위해 센터의 사전 준비 동작 단계에서 센터는 GF(p) 및 GF(q) 상에서 동시에 원시원소가 되는 g를 선택하여 다른 공개 정보와 함께 각 가입자의 스마트 카드에 저장하여 공개한다. 그리고, 위의 프로토콜 4를 이용하여 양방향으로 인증을 수행한다. 아래의 프로토콜 5는 양방향 인증 중 A가 B에게 증명을 하는 과정이다.

프로토콜 5.

순서 1-1. 가입자 A는 r_{A1}을 선택한다.

순서 1-2. A는 $x_A = (g^{r_{A1}})^L \pmod N$을 계산한다.

순서 1-3. 프로토콜 4와 동일

순서 2-1. 프로토콜 4와 동일

순서 2-2. 프로토콜 4와 동일

순서 2-3. 프로토콜 4와 동일

순서 3-1. 가입자 A는 $y_A = (g^{r_{A1}}) \cdot S_A^d \pmod N$을 계산한다.

순서 3-2. 프로토콜 4와 동일

순서 4-1. 가입자 B는 $y_A^L = x_A \cdot V_A^d \pmod N$이 성립하는지 검증한다.

순서 5-1 부터 순서 8-1은 프로토콜 4와 동일.

양 가입자가 공통키를 생성하기 위한 선행 동작으로 프로토콜 5를 이용하여 양 가입자간의 인증이 성공적으로 끝났을 경우, 순서 1-1 부터 순서 4-1을 이용해서 공통키를 생성할 수 있다.

가입자 A는 순서 1-3에서 가입자 B로부터 x_B를 받게 되며, 인증이 양자간에 성공적으로 끝났을 경우, 아래 식을 이용해서 공통키 K_{AB}를 생성할 수 있고, 마찬가지로 가입자 B도 X_A를 이용해서 K_{AB}와 같은 K_{BA}를 생성할 수 있다.

$$\begin{aligned} K_{BA} &= K_{AB} \\ &= (x_B)^{r_{A1}} \\ &= (g)^{L \cdot r_{A1} \cdot r_{B1}} \pmod N \end{aligned} \tag{15}$$

5.3 제안한 키 분배 프로토콜의 검토

두번째 인증 과정(순서 5-1 부터 8-1까지)은 이미 영지식이 아니라고 밝혀졌다.[15] 따라서 두번째 인증에서 사용된 데아타로 키 분배를 행한다면 그 과정 역시 영지식이 아니므로 영지식 증명임이 입증된 첫번째 인증 과정을 이용해서 키 분배를 행했다.

인증 과정이 영지식이라는 의미는 양자간 전송되는 즉 x_A, x_B, d_A, d_B, y_A, y_B로부터 $g^{r_{A1}}$, $g^{r_{B1}}$, S_A, S_B등에 대한 정보가 노출되지 않는다는 것을 의미하며, 따라서 이들 전송 데이타와 자신이 선택한, 노출되지 않은 난수(r_{A1}, r_{B1})를 이용해서 공통키를 생성한다면, 인증 과정 이외에 다른 전송이 없기 때문에 키 분배 과정 역시 영지식이라 할 수 있다.

6. 다른 키 분배 방식과의 비교

CDH(composite DH방식) 방식이란 원래의 DH 방식이 mod p(p는 소수)상에서 연산하는데 반해 두

소수 p, q의 곱인 m을 이용하여 mod m상에서 연산하는 DH 방식을 말한다. Shmuely, McCurley는 CDH 방식에서 m과 원시 원소 g를 적절히 선택한다면 그것을 깨는 문제는 어렵다는 것을 증명했다.[20-22]

[illegible] A, B가 통신을 하고자 할 때, CDH 방식과 제안한 키 분배 프로토콜을 비교해 보면 표 1과 같다.

표 1. CDH 방식과 제안한 프로토콜의 비교

	CDH	본 방식
비 밀 키	s_i	r_{A1}
공 개 키	g^{s_i}	$g^{L_i \cdot r_{A1}}$
원 시 원 소	g	g
공 통 키	$g^{s_i s_j}$	$g^{L_i \cdot r_{A1} \cdot r_{B1}}$

기존의 영지식 증명을 이용한 키 분배 방식인 Bauspieβ 방식과 제안한 프로토콜을 계산 복잡도, 전송 횟수 및 센터에 대한 의존도 측면에서 비교해 보면 표 2와 같다.

표 2. Bauspieβ 방식과 제안한 프로토콜의 비교

대상 \ 방식		Bauspieβ 방식	제안한 프로토콜
계산 복잡도	인 증	4 EXP + 5 MUL + ADD	5 EXP + MUL 3 EXP + 2 MUL + 1 ADD
	키생성	3 EXP	1 EXP
	키인증	임의의 문장에 대한 암호화 및 복호화 필요	필 요 없 음
	전 체	7 EXP + 5 MUL + 1 ADD + 암호화 및 복호화 시간	9 EXP + 4 MUL + 1 ADD
인증 이외의 전송		양자가 1번씩	필 요 없 음
센터에 대한 의존도		매 우 높 음	없 음

표 2에서 볼 수 있듯이 Bauspieβ 방식이 계산 복잡도 면에서는 약간 유리하지만, Bauspieβ 방식은 키생성 과정을 마친 이후에 양 가입자가 키의 인증을 위한 암호화와 복호화 및 양자가 한번씩의 전송을 필요로 하며, 센터에 전적으로 의존해야 하는 단점이 있는 반면, 제안한 키 분배 방식은 두번의 인증과정을 통해 센터에 대한 의존도를 줄였으며, 키의 검증을 위한 통신 및 암호화와 복호화 과정이 필요없는 장점이 있다.

7. 결 론

현대 사회는 정보화 사회로 변환하는 과정에서 고도의 통신 처리 및 정보 처리 기술이 필요하다. 특히, 고도의 부가가치가 있는 각종 서비스를 제공하기 위하여 안전하고 효율적인 암호화 프로토콜들이 필요하다. 본고에서는 암호화 프로토콜의 안전성을 제시하기 위한 모델인 영지식 대화형 증명에 대하여 간략히 논하고 그 구체적인 프로토콜들의 문제점을 지적하였으며, 기존의 개인 식별 프로토콜인 확장 FS 방식과 S 방식을 결합하여 각각의 단점을 해결할 수 있음을 보였다. 이렇게 결합함으로서 센터가 계산한 가입자의 비밀 정보와 사용자 자신이 직접 선택한 비밀 정보를 이용하여 두번의 인증을 행하여 센터에 대한 의존도를 줄였고, 영지식 증명 방식을 인증에 이용함으로써 키 분배 과정 또한 영지식이 되도록 만들었으며 사용자의 비밀키에 대한 어떠한 정보도 노출시키지 않기 때문에 기존의 다른 어떤 키 분배 방식 보다 안전하다고 할 수 있다. 또한 인증 과정의 반복 통신 t회를 1회로 줄였으므로 적은 횟수의 통신으로도 개인 식별과 함께 이 프로토콜을 직접 키 분배시 활용할 수 있도록 키 분배 프로토콜을

제안하였다.

앞으로의 연구 과제로는 일반적으로 영지식 대화형 증명을 이용한 암호화 프로토콜들은 영지식 대화형 방식을 구성하는데 소요되는 통신 횟수 및 통신량이 많다는 약점을 갖고 있으므로 최근 이러한 약점을 극복하기 위하여 영지식 대화형 증명 방식과 관련한 이론적이고, 실제적인 관점에서의 의문점인 "round complexity의 최적 bound는 얼마인가?"하는 문제에 관한 연구가 활발히 진행되어야 할 것으로 사료된다.

국내 정보 보호 관련 분야 연구에서도 영지식 대화형 증명 방식이 활발히 연구되어 고도 정보화 사회에서 요구되는 전자 송금 등의 서비스 구현시 필요한 기반을 확고히 하여야 하겠다.

참 고 문 헌

1. 현대암호학, 한국전자통신연구소편저, 1991. 8.

2. M.A. Emmelhainz, Electronic Data Inter change, VAN Nostrand Reinhold, 1990.

3. 원동호, "암호방식과 키 분배", 한국통신정보보호학회지, 1권, 1호, 1991.

4. S. Goldwasser, S. Micali, C. Rackoff, "Knowledge Complexity of Interactive Proofs", Proc. 17th STOC, 1985, pp.291-304.

5. O. Goldreich, S. Micali, A. Wigderson, "Proofs that Yield Nothing But their Validity", Proc. Crypto'86, pp.171-185, 1986.

6. 원동호, 양형규, 권창영 외, "ZKIP 이론에 관한 연구", 한국전자통신연구소 최종보고서, 성균관대, 1991. 11.

7. A. Shamir, "Identity-based Cryptosystems and Signature Schemes", Crypto 84. pp.47-53, 1984.

8. U.Fiat, A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems", Proc. Crypto'86, pp.186-194, 1986.

9. H.J. Knobloch, "A Smart Card Implementation of the Fiat-Shamir Identification Scheme", Eurocrypt'88, pp.87-95, 1988.

10. S. Micali, A.Shamir, "An Improvement of the Fiat-Shamir Identification and Signature Scheme", Crypto'88, pp.244-247, 1988.

11. L.C. Guillou, J.J.Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing both Transmission and Memory", Eurocrypt'88, pp.123-128, 1988.

12. L.C. Guillou, J.J.Quisquater, "A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge" Crypto'88, pp.216-231, 1988.

13. K. Ohta, T. Okamoto, "A Modification of the Fiat-Shamir scheme", Crypto'88, pp.233-243, 1988.

14. D. Chaum, J.H. Evertse, J. van de Graaf, "An Improved Protocol for Demonstration Possession of Discrete Logarithms and Some Generalization", Eurocrypt'87, pp.127-141, 1987.

15. Schnorr, "Efficient Identification and Signatures for Smart Cards", Crypto'89, 1989.

16. Diffie, Hellman, "New Directions in Cryptography", IEEE Trans. on Information Theory, IT-22, 1976.

17. Bauspieβ, "How to Keep Authenticity Alive in A Computer Network", Eurocrypt'89, 1989.

18. T. Beth "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Proc. Eurocrypt'88, pp.77-84, 1984.

19. 이윤호, 양형규, 장청룡, 원동호, "영지식 증명을 이용한 키 분배 방식에 관한 연구", 한국통신정보보호학회 '91 정보보호학술발표 논문집, 1991.

20. Shmuely, "Composite Diffie-Hellman Public-Key Generating Systems Are Hard to Break", TR. No. 356, Computer Science Dept. Technion, IIT, 1985.

21. McCurley, "A Key Distribution System Equivalent to Factoring", J. of Cryptology, Vol. 1, No. 2, 1988.

22. 이필중, 임채훈, 문희철, "ID-based Cryptosystem에 관한 연구", 과학기술처 특정과제 위

탁연구 최종보고서 모음집 Vol. 1, pp.557-634, 1991. 12.

13. 박춘식, "고신뢰 센터를 고려하지 않는 강력한 개인 식별 방식", JCCI'91, 논문집 제 1 권, pp.43-46, 1991.

24. 박춘식, 이임영, "A Fiat-Shamir-like Identification Protocol without a Highly Reliable Trusted Center", private letter.

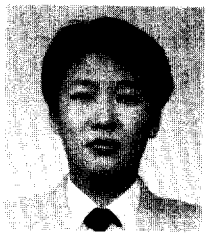
□ 著者紹介

원 동 호(정회원)

1949년생
1976년 성균관대학교 전자공학과 졸업(공학사)
1978년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1988년 성균관대학교 대학원 전자공학과 졸업(공학박사)
1978년~1980년 한국전자통신연구소 전임연구원
1985년~1986년 일본 동경공대 객원연구원
1982년~현재 성균관대학교 정보공학과 조교수, 부교수, 교수

권 창 영(정회원)

1957년생
1983년 성균관대학교 수학교육과 졸업(이학사)
1991년 성균관대학교 대학원 정보공학과 졸업(공학석사)
1991년~현재 성균관대학교 대학원 정보공학과 박사과정 재학중
1982년~1988년 (주)KOLON 정보 SYSTEM실 팀장



양 형 규(정회원)

1959년생
1983년 성균관대학교 전자공학과 졸업(공학사)
1985년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1991~현재 성균관대학교 대학원 정보공학과 박사과정 재학중
1985년~1991년 삼성전자 컴퓨터부문 선임연구원

이 윤 호(학생회원)

1969년생
1991년 성균관대학교 정보공학과 졸업(공학사)
1991년~현재 성균관대학교 대학원 정보공학과 석사과정 재학중