通信情報保護學會誌
第2卷, 第2號, 1992. 6

영지식 대화형 증명방식 및 응용에 관한 연구

권창영* · 양형규* · 원동호*

1. 서 론

현대 사회는 정보화 사회로 변화하는 과정에서 고도의 통신처리 및 정보처리 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. 일반적으로 신분 확인, 전자 서명 등은 안전할 것으로 믿어지는 공개키 암호방식을 사용하여 해결하고 있으나, 동시성에 관한 문제 등은 신분 확인, 전자서명과는 다른 방법인 암호화 프로토콜들을 이용하고 있다[1].

암호화 프로토콜은 기존의 암호화/복호화 알고리즘과는 달리 불특정 다수의 송/수신자가 통신망을 이용하여 정보를 교환함으로써 어떤 목적을 달성하고자 하는 통신 알고리즘으로, 그 과정에 암호 알고리즘이 포함되는 특성을 갖는다. 즉, 암호화 알고리즘은 암호 알고리즘이 포함된 통신 알고리즘(communication algorithm)을 의미하며, 그 예로는 동전 던지기(coin flipping), Oblivious Transfer, 전자 계약 프로토콜 등이 있다.

암호화 프로토콜의 대두로 암호화 프로토콜의 안전성 문제 및 효율성 문제를 고려하여야 하는 바, 본고에서는 암호화 프로토콜이 '정말 안전한가?' 하는 안전성 문제를 해결하기 위하여 제시된 모델인 영지식 증명방식(ZKIPs : Zero Knowledge Interactive Proof Systems)을 소개한다. 현재 영지식 대화형 증명방식은 선진 각국에서 활발히 연구되고 있으며, 영지식 증명방식으로 간주되는 암호화 프로토콜들이 많은 응용 분야에서 제안되고 있는 실정이다.

2. 영지식 증명방식

1985년 Goldwasser, Micali, Rackoff가 ZKIP 개념을 발표하면서 시작된 ZKIP 이론은 증명자가 검증자에게 자신을 증명함에 있어서 증명의 타당성 이외의 어떠한 정보도 유출시키지 않는다는 것으로, 상대방 인증방식에 있어서 가히 혁신적인 것이었다[2]. 이후 많은 ZKIP 방식들이 발표되었으며 이러한 방식들은 $P \neq NP$라는 가정하에 NP에 속하는 언어(language)들을 이용하여 상대방 인증을 행하는데, NP에 속하는 모든 언어는 ZKIP에 이용할 수 있음을 Goldreich, Micali, Wigderson이 확인하였다[3]. 이러한 NP에 속하는 언어들로는 평방 잉여 문제(quadratic residue), 그래프 동형 문제(graph isomorphism), 그래프 비동형 문제(graph non-isomorphism), 만족도 문제(satisfiability) 등이 있다.

직관적으로 영지식 증명방식을 설명하면, 증명자

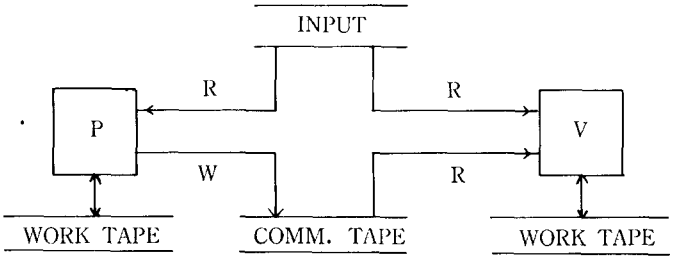
* 成均館大學校 情報工學科

P와 검증자 V가 대화(interactive)를 통하여 증명을 하는 방식으로 어떤 사실의 정당성에 관한 정보만을 전송하므로 그 이외의 어떤 정보도 노출시키지 않는다는 의미를 갖고 있다. 즉, 증명자가 자신만이 아는 비밀정보를 검증자에게 직접 전송하지 않고, 자신의 비밀정보가 아닌 어떤 다른 정보를 전송하여 검증자에게 자신만이 비밀정보를 알고 있다는 것을 증명할 수 있는 방식이다.

영지식 증명방식은 NP 증명방식을 일반화시킨 방식으로 암호화 프로토콜의 안전성 문제를 해결하기 위하여 제시된 모델이므로 NP 증명방식, 대화형 증명방식, 영지식 대화형 증명방식 순으로 설명하여 보겠다.

[정의] NP 증명방식

NP 증명방식은 대화형 통신이 가능한 무한한 계산 능력을 갖는 deterministic Turing machine P(증명자)와 다항식 계산 능력을 갖는 deterministic Turing machine V(검증자)로 구성되며, P, V는 NP 문제인 X를 공통 정보로 입력받아 들인다. 이때, 무한한 계산 능력을 갖는 증명자 P는 문제 X의 해 x를 구하여 검증자 V에게 전송하면, 다항식 계산 능력을 갖는 검증자 V는 x가 X의 해인지 판단하는 방식을 NP 증명방식이라고 한다.



R : read-only W : wirte-only

그림 1. NP 증명방식

NP 증명방식의 예로는 패스워드를 이용한 단순한 사용자 인증을 들 수 있다. 컴퓨터 시스템의 사용자 P가 컴퓨터 시스템 V에게 패스워드를 전송하면, 컴퓨터 시스템은 이 패스워드가 컴퓨터 시스템 사용자의 패스워드인지 검증하여 인증하는 방식이다.

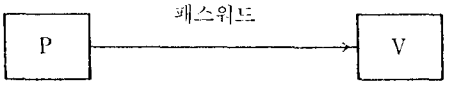


그림 2. 단순한 사용자 인증

위와 같은 NP 증명방식은 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 증명방식이 필요하다.

NP 증명방식을 두가지 면에서 일반화시킨 증명방식이 영지식 증명방식이다. 즉, NP 증명방식은 deterministic Turing machine상에서 정의되었으나, 대화형 증명방식은 probabilistic Truing machine 상에서 정의된다. 또한, NP 증명방식은 증명자가 검증자에게 자신의 정보를 전송하는 일방향 방식이나, 대화형 증명방식은 검증자도 자신의 정보를 증명자에게 전송하는 양방향 방식이다.

대화형 Truing machine에 대한 정의를 내려보면 아래와 같다.

[정의] 대화형 Truring machine(ITM)

한 개씩의 read-only tape, work tape, random tape, read-only communication tape, write-only communication tape를 갖는 Truing machine을 대화형 Turing machine이라 한다.

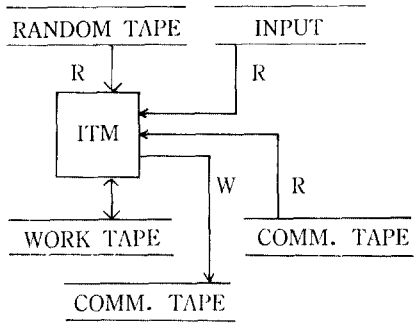


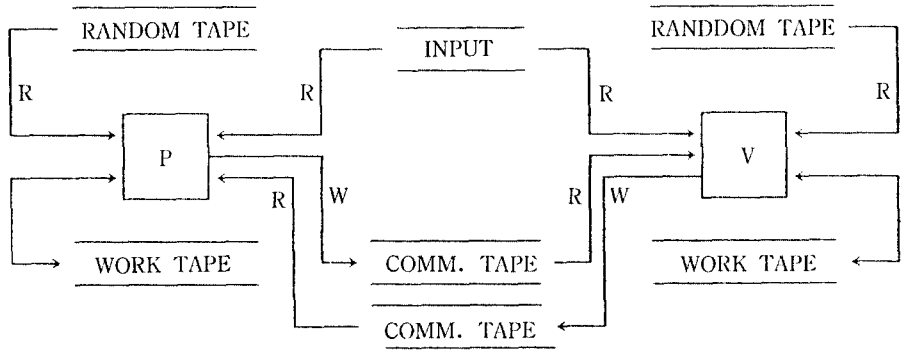
그림 3. 대화형 Turing machine

random tape는 무한한 random bit들로 구성되어 있으며, 왼쪽에서 오른쪽으로만 scan이 가능하다. ITM이 '동전을 던진다(flips a coin)'는 의미는 ITM이 자신의 random tape에서 다음 비트를 읽는다는 것이다.

[정의] 대화형 프로토콜(interactive protocol)

input tape를 공유하는 ITM P와 V의 순서쌍을 대화형 프로토콜이라 하며 (P, V)로 표시한다.

V의 write-only communication tape는 P의 read-only communication tape이며 P의 write-only communication tape는 V의 read-only communication tape이다.



R : read-only W : wirte-only

그림 4. 대화형 프로토콜

machine V의 계산 시간은 공통 입력 X의 길이로 표현되는 다항식으로 제한되지만(bounded), machine P의 계산 시간은 계산적으로 제한되지 않는다.

두 개의 machine는 V가 최초로 active되고, 서로 번갈아 가면서 active된다. P(V)가 active stage인 동안 input tape, work tape, communication tape, random tape를 이용하여 내부적인 계산(internal computation)을 처음으로 행하고, 자신의 write-only communication tape에 계산 결과(string)를 기록한다. P(V)의 i번째 메세지는 자신의 i번째 active stage동안 자신의 communication tape에 기록된 모든 string이다.

machine P(V)는 자신의 메세지를 기록하자마자 deactive되고, machine V(P)가 active된다. 각 machine는 active stage에서 아무런 메세지도 전송하지 않으면, 프로토콜을 끝낼 수 있다.

machine V는 accept(또는 reject)를 출력하여 입력 x를 accept(또는 reject)하고, 프로토콜을 중지한다.

machine V의 계산 시간은 V의 active stage 동안 V의 계산 시간의 합이며, machine V의 계산 시간은 입력 X의 길이(|X|)로 표시되는 다항식으로 제한된다.

[정의] 대화형 증명방식

대화형 증명방식은 대화형 통신이 가능한 무한 계산 능력을 갖는 interactive Turing machine P와 다항식 계산 능력을 갖는 interactive Truing machine V로 구성된 (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 $1-1/n^k$ 이상의 확률로 증명할 수 있어야 한다.

조건 2) 건전성(completeness)

(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 확률이 $1/n^k$ 이하이어야 한다.

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

mod N상에서 평방근을 갖지 않는 집합은 아래와 같이 표시되며, 평방 비잉여 문제를 이용하여 대화형 증명방식의 구체적인 예를 구성하면 아래와 같다.

$$QNR=\{(N, Z) \mid Z \neq S^2 \bmod N \text{ for } \forall S\} \quad (1)$$

순서 1. V는 랜덤 bit $\{b_i\}$와 임의의 난수 $\{r_i\}$ (단, $i=1, 2, \cdots, |N|$)를 선택한 후

$$x_i = Z^{b_i} \cdot r_i^2 \bmod N \quad (2)$$

x_i을 계산하여 $\{x_i\}$ (단, $i=1, 2, \cdots, |N|$)를 P에게 전송한다.

순서 2. P는 x_i가 평방잉여인지 아닌지를 $\{c_i\}$를 계산하여 V에게 전송한다.

$$c_i = \begin{cases} 0 \ (\text{for } \exists w_i,\ x_i = w_i^2 \ (\text{mon } N)) \\ 1 \ (\text{for } \forall w_i,\ x_i \neq w_i^2 \ (\text{mon } N)) \end{cases} \quad (3)$$

순서 3. V는 모든 i에 대하여 $b_i=c_i$가 성립하면, $(N, Z) \in QNR$임을 accept한다.

이 경우 $(N, Z) \in L$이면, 완전성은 1이며, $(N, Z) \notin L$이면, 건전성은 $1/2^n$이다.

M을 probabilistic Truing machine이라 할 때, 임의의 입력 정보 X에 대해 자신이 가지고 있는 랜덤 테이프에 의해 확률 공간 M[X]를 생성하게 된다. 이 때 확률 공간 M[X]를 random variable로 간주할 수 있으며, 입력 정보 X를 변화시켜 random variable들의 집합을 구성할 수 있다.

대화형 증명방식 (P, V)는 임의의 입력 정보 X에 대하여 자신들이 가지고 있는 랜덤 테이프에 따라서 (P, V)[X]로 표시되는 확률 공간을 생성한다. 이 확률 공간 (P, V)[X]의 특성에 의해 영지식 증명방식 (P, V)가 정의된다.

이때 확률 공간 (P, V)[X]를 랜덤 변수로 간주할 수 있으며, 입력 정보 X를 변화시켜 random variable들의 집합 $\{(P, V)[X] : X \in \{0, 1\}^*\}$을 생성할 수 있다.

[정의] indistinguishable

랜덤 변수들의 집합 {A[X]}, {B[X]}가 다음의 조건을 만족하면, indistinguishable이라 한다.

조건 1) indistinguishable

모든 다항식 시간 ($|X|$에 대한) 알고리즘 M, 모든 $c>0$, 그리고 충분히 큰 수 N에 대해 다음식이 성립한다.

$$|P_M^A - P_M^B| \leq |X|^{-c}, \quad |X|>N \quad (4)$$

단, P_M^A; 임의의 알고리즘 M에 대해 확률 공간 A[X]에 따라 변하는 원소를 입력으로 선택할 때 M이 1을 출력할 확률

$|X|$; X의 길이

[정의] 영지식 대화형 증명방식

대화형 증명방식 (P, V)가 다음의 조건을 만족하면, 영지식 증명방식이라고 한다.

조건 1) 임의의 다항식 계산 능력을 갖는 검증자 V*에 대하여, 다항식 계산 능력을 갖는 probabilistic Turing machine M_{v*}가 존재하여 $\{M_{v*}[X]\}$와 $\{(P, V^*)[X]\}$는 indistinguishable하다.

3. 영지식 대화형 증명의 구체적인 예

영지식 대화형 증명의 의미를 분명히 하기 위해서 이산대수 문제를 이용한 구체적인 예를 들어 보기로 하겠다.

증명자 P는 소수 p, $p-1$이하의 정수 a, $p-2$이하의 비밀 난수 x를 선택하여 $b=a^x \pmod p$를 계산한다.

증명자 P는 x를 비밀리에 보관하고 {a, b, p}를 검증자 V에게 전송한다. 이러한 준비하에서 아래와 같이 영지식 대화형 증명을 행한다.

프로토콜 1. 이산 대수 문제를 이용한 영지식 대화형 증명 : $b=a^x \pmod p$

순서 1. 증명자 P는 임의의 난수 r을 선택, $R=a^r \pmod p$를 계산하여 검증자 V에게 전송한다.

순서 2. 검증자 V는 2진수 e=0 또는 1을 랜덤하게 선택하여 증명자 p에게 전송한다.

순서 3. 증명자 P는 e를 수신한 후 e=0이면, 난수 r을 검증자 V에게 전송한다. e=1이면, $t=x+r \pmod{p-1}$을 검증자에게 전송한다.

순서 4. 검증자 V는 e=0인 경우에는 $a^t=R \pmod p$을 검사하고, e=1인 경우에는 $a^t=bR \pmod p$을 검사한다.

순서 5. 검사식이 성립하지 않는 경우, 증명자가 P가 아니라고 확인되므로 종료한다. 검사식이 성립하는 경우, 증명자가 P임을 신뢰할 수 있도록 순서 1에서 순서 4를 반복 수행한다.

위의 예에서 e=0인 경우에는 증명자 P가 x를 소유(possession) 하고 있는 것이 확실하지 않지만, e=1인 경우에는 증명자 P가 x를 소유하고 있지 않으면 검증이 성립되지 않는다. 검증자 V가 e의 선택을 완전하게 랜덤으로 선택하면, e=1일 확률은 1/2이므로 순서 1에서 순서 4를 n회 반복 수행하는 경우 e=1이 선택될 확률은

$$1/2+(1/2)^2+\cdots+(1/2)^n=1-(1/2)^n \quad (5)$$

이므로 n이 충분히 큰 경우에는 거의 확률 1로 $a^t=bR \pmod p$을 검사하게 된다.

또한, 순서 2에서 검증자 V가 항상 e=1을 전송한다고 가정하면, 문제가 발생한다. 만약 검증자 V가 항상 e=1을 전송한다는 것을 제 3 자 P*가 안다면, P*는 P로 위장할 가능성이 있다. 즉, 순서 1에서 제 3 자 P*는 난수 r을 선택, $R=a^r/b \pmod p$를 계산하여 검증자 V에게 전송하고, 순서 3에서 제 3 자 P*는 t 대신에 자신이 선택한 난수 r을 검증자 V에게 전송한다. 검증자 V는 순서 4에서 다음식을 검증하게 되므로 항상 제 3 자 P*를 증명자 P라고 확신하게 된다.

$$a^t=bR \pmod p \Leftrightarrow a^r=b(a^r/b) \pmod p \quad (6)$$

4. 영지식 대화형 증명의 종류 및 개념

영지식 증명의 종류로는 언어의 영지식 증명, 지식의 영지식, 계산 능력의 영지식이 있으며, 각각에서 완전 영지식, 통계적 영지식, 계산적 영지식을 정의할 수 있으나, 본고에서는 언어, 지식, 계산 능력의 영지식에 대한 개념을 간략히 소개하기로 한다[4].

어떤 집합 L과 그 원소 x에 대하여 다음의 조건을 만족하는 (P, V)를 언어의 영지식증명이라고 한다.

완전성 : $x \in L$이면, (P, V) (x)는 증명을 수락한다.

건전성 : $x \notin L$이면, 어떤 P*에 대해서도 (P*, V) (x)는 증명을 수락하지 않는다.

영지식성 : 어떤 V*에 대해서도 (P, V*)는 $x \in L$ 이외의 정보는 노출 시키지 않는다.

Goldwasser의 정의에 의하면, 증명자 P는 무한의 능력을 갖고 있는 것으로 정의하지만 실제 방식의 응용을 고려하면 이와같은 정의는 비현실적이다. 그러므로 Feige와 Tompa에 의하여 어떤 정보를 소유하는 영지식 대화형 증명이 제안되었다. Tompa의 정의에 따르면, 공개정보 I와 비밀 정보 S에 대하여 증명자 P는 'I에 대응하는 S를 갖는' 확률적 다항식 시간 Turing machine이 되고 다음 3가지 조건을 만족하는 것이 된다. 이것을 지식의 영지식 증명이라고 한다.

완전성 : P가 S를 소유하면, (P, V)(I)는 증명을 수락한다.

건전성 : P*가 S를 소유하지 않으면, 어떤 P*에 대해서도 (P*, V)(I)는 증명을 수락하지 않는다.

영지식성 : 어떤 V*에 대해서도 (P, V*)(I)는 S의 정보를 노출시키지 않는다.

Kurosawa는 지식에 의해 표현하지 못하는 범위로 확장하기 위하여 능력의 영지식 증명을 제안했다. 어떤 함수 f에 대하여 'f(x)로 부터 x를 구할 수 있다'는

것을 증명하는 것으로 다음의 조건을 만족하는 것이다.

완전성 : p가 f^{-1}을 계산할 수 있다면, (P, V)(f)는 증명을 수락한다.

건전성 : P*가 f^{-1}을 계산할 수 없으면, 어떤 P*에 대해서도 (P*, V)(f)는 증명을 수락하지 않는다.

영지식성 : 어떤 V*에 대해서도 (P, V*)(f)는 P가 계산 능력을 갖는다는 것 이외의 정보를 노출시키지 않는다.

5. 영지식 대화형 증명방식의 응용

가. 개인 식별 방식

개인 식별(identification) 문제는 암호학의 여러 분야에서 발생하는 매우 중요한 문제중의 하나이다. 본 절에서는 개인 식별 문제를 영지식 증명 시스템을 이용하여 어떻게 해결할 수 있는 지를 설명하겠다. Fiat, Shamir의 개인 식별 방식을 비롯한 전형적인 ID 정보 및 영지식 대화형 증명을 이용한 개인 식별 프로토콜을 소개하면 아래와 같다.

(1) Fiat-Shamir 방식[5,6]

(2) 확장 Fiat-Shamir 방식 ((1)의 고차 버전)[7,8,9]

(3) Beth 방식 ((1)의 이산 대수 버전)[10]

위의 각 방식은 각기 3가지 변형이 있다.

(a) sequential 버젼

(b) parallel 버젼 (1 round 또는, 3 moves 버젼)

(c) non-interactive 버젼

이러한 변형들 중 sequential 버젼 (a) 방식 (1)-(3)는 zero-knowledge identification이다. scheme (1)의 parallel 버젼 (b)는 no-transferable information를 이용하여 안전하다는 것이 증명되었다[6]. scheme (2)의 parallel 버젼 (b)는 no-transferable information를 이용하여 안전하다는 것이 부분적으로 증명되었다. non-interactive 버젼 (c)는 parallel 버젼 (b)와 일방향 함수 h에 근거하여 구성된다. non-constructive 버젼에서는 증명자는 E=h(X)를 자기 자신이 생성하고 Y를 생성한다. 즉, X, E, Y를 생성한 후 그것들을 검증자에게 전송한다. 검증자에 의한 검증은 perallel 버젼과 같다. non-interactive 버젼의 안전성은 일방향 함수의 성질과 parallel 버젼의 안전성에 근거한다.

1) 구체적인 예

Fiat-Shamir 개인 식별 방식은 ZKIP의 개념에 Shamir 자신이 제안한 ID 개념[11]을 결합한 방식이다. 개인 식별 정보 ID_i의 평방 잉여 s_i를 계산하여 가입자의 비밀키로 사용하였다. 이 방식의 안전성은 충분히 큰 두 소수 p, q의 곱인 n의 소인수 분해를 모를 때, 제곱근(square root)을 구하는 문제는 어려운 문제(NP 문제)라는 것에 근거한다.

사전 준비 과정에서 신뢰 센터(center)는 소수 p, q를 선택(비밀)하고, 그 곱인 n을 공개한다. 카드 발급 과정에서 센터는 합법적인 사용자에게 카드를 발급할 때 그 사용자에 관한 정보(이름, id번호, 주소, 주민등록번호 등)와 카드에 관한 정보(유효기간 등)를 담고 있는 ID_i를 준비하고, mod n 상에서 ID_i의 평방근을 계산하여 그 역수 s_i를 각 가입자의 비밀키로 한다.

가입자 A와 가입자 B가 개인 식별을 행하는 프로토콜은 아래와 같다.

프로토콜 2. 순서 1에서 순서 4를 t회 반복한다.

순서 1. 가입자 A는 $r \in_R Z_n^*$를 선택하고 $x=r^2 \pmod n$를 계산하여 가입자 B에게 전송한다.

순서 2. 가입자 B는 $(d_1, \cdots, d_k) \in_R \{0, 1\}$를 선택하여 가입자 A에게 $(d_1, \cdots d_k)$를 전송한다.

순서 3. 가입자 A는 $y=r\prod_{d_j=1} s_j \pmod n$을 계산하여 가입자 B에게 전송한다.

순서 4. 가입자 B는 $x=y^2\prod_{d_j=1} v_j \pmod n$이 성립하는지 검증한다.

나. 키 분배 방식

영지식 대화형 증명에서는 증명자와 검증자 사이에 랜덤 정보(randomized information)가 전송되며 증명자의 랜덤성(randomness)은 영지식(zero knowledge) 조건을 만족시키기 위해서 사용된다[2]. 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 랜덤성을 이용하여 암호화 키 분배(key distribution)에 이용 가능하다.

즉, 난수 R 대신에 f(r, a)를 사용하는 것이다. 단, g(f(r, a))와 g(R)의 분포는 indistinguishable이다. a는 고정 파라메터이고, g(R)은 영지식 증명을 이용하여 증명자로 부터 검증자에게 전송되는 하나의 메세지이다. 만약 g(f(r, a))와 g(R)의 분포가 indistinguishable 한다면, 영지식 증명은 가능하다. f(r, a)의 예인 $a^r \bmod n$ 같은 함수는 identity-based key distribution 방식을 구성하는데 사용할 수 있다. 또 다른 함수 bit-commitment functions들은 디지탈 서명방식에 적당하다.

1) 구체적인 예

신뢰 센터는 가입자 A와 가입자 B를 위하여 Fiat-Shamir 방식의 비밀키 $s_{1,j}$와 $s_{2,j}$(j=1, 2, …, k)를 각각 생성한다. 센터의 비밀키는 (p, q)이고, 공개키는 (n, g) 및 $1/s_{i,j}=(f(I_j, j))^{1/2} \bmod n$ (i=1, 2, j=1, 2, …, k)이다. 단, p, q는 소수이며, p'=(p−1)/2, q'=(q−1)/2 역시 소수이고 n=pq이다. $g \in Z_n^*$인 g의 order는 p'q'이며, $|p|=c_1|n|$, $|q|=c_2|n|$ (단, c_1, c_2는 상수)이다. I_i는 가입자 i의 identity이다.

가입자 A와 가입자 B가 개인 식별 및 키 분배를 행하는 프로토콜은 아래와 같다.

프로토콜 3. 순서 1에서 순서 5를 t회 반복한다.

순서 1 ; 가입자 A는 난수 $r_1 \in Z_n$을 선택한다.

가입자 B에게 $x_1=g^{2r_1} \bmod n$을 전송한다.

순서 2 ; 가입자 B는 랜덤 2진 벡터 $(e_{1,1}, \cdots, e_{1,k})$를 가입자 A에게 전송한다.

가입자 B는 마찬가지로 난수 $r_2 \in Z_n$을 선택한다.

가입자 A에게 $x_2=g^{2r_2} \bmod n$을 전송한다.

순서 3 ; 가입자 A은 가입자 B에게 y_1를 전송한다.

$$y_1=g^{r_1}\prod_j s_{1,j}^{e_{1,j}} \bmod n \qquad (7)$$

가입자 A은 랜덤 2진 벡터 $(e_{2,1}, \cdots, e_{2,k})$를 가입자 B에게 전송한다.

순서 4 ; 가입자 B는 $x_1=y_1^2 \prod_j f(I_1, j)^{e_{1,j}} \bmod n$를 검증한다.

검증이 성립되면, K_i을 생성한다.

$$K_1=x_1^{r2} \bmod n \qquad (8)$$

가입자 B는 가입자 A에게 y_2를 전송한다.

$$y_2=g^{r2}\prod_j s_{2,j}^{e_{2,j}} \bmod n \qquad (9)$$

순서 5 ; 가입자 A는 $x_2=y_2^2 \prod_j f(I_2, j)^{e_{2,j}} \bmod n$를 검증한다.

검증이 성립되면, K_1을 생성한다.

$$K_1=x_2^{r1} \bmod n \qquad (10)$$

t회 procedure cycles가 통과된 후에는 가입자 A와 가입자 B는 공통키(common key) K를 계산한다.

$$K=K_1+K_2+\cdots+K_t \bmod n \qquad (11)$$

다. 디지탈 서명 방식

Fiat-Shamir 디지탈 서명방식은 가. 절에서 언급한 개인 식별 방식과 동일한 준비과정을 행하며 증명자가 메세지 M에 대하여 서명을 만들어 확인자에게 전송해야 하므로 개인 식별 방식처럼 대화형 방식은 이용할 수 없다. 그러므로 증명자는 해쉬함수를 이용하여 서명하려는 메세지와 자신이 선택한 랜덤수에 의존하는 2진 벡터 $\{e_{ij}\}$를 생성하여 이용한다.

프로토콜 4.

순서 1. [디지탈 서명의 생성]

① 가입자 A는 $r_1, \cdots, r_t \in_R Z_n^*$를 선택하여 $x_i=r_i^2 \pmod n$를 계산한다.

② 가입자 A는 $f(M, x_1, \cdots, x_t)$를 계산하여 처음의 kt 비트 e_{ij}($1 \le i \le t$, $1 \le j \le k$)를 메세지 M에 대한 서명으로 한다.

③ 가입자 A는 $y_i=r_i \prod_{e_{ij}=1} s_j \pmod n$을 계산하여 가입자 B에게 ID_A, M, $\{e_{ij}\}$ 및 y_i를 전송한다.

순서 2. [디지탈 서명의 검증]

① 가입자 B는 $V_j=f(ID_A, j)$ ($i \le j \le k$)를 계산한다.

② 가입자 B는 $z_i=y_i^2 \prod_{e_{ij}=1} v_j \pmod n$을 계산한다.

③ 가입자 B는 $f(M, z_1, \cdots, z_t)$를 계산하여 처음의

kt 비트가 e_{ij}와 동일한가 검증한다.

가입자 A와 가입자 B는 이 프로토콜을 사용하여 가입자 B는 가입자 A의 서명이 정당한가 항상 확인할 수 있다. 이와같은 서명 방식은 영지식 증명은 아니나, Feige와 Shamir가 전용 가능한 정보(transferable information) 개념을 제안하여 안전하다는 것을 증명하였다.

6. 결 론

현대 사회는 정보화 사회로 변화하는 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 논하고 그 구체적인 예를 들어 설명하였다. 또한, 영지식 대화형 방식을 이용한 개인 식별, 키 분배, 디지탈 서명에 대하여 기술하였다.

영지식 대화형 증명을 이용한 암호화 프로토콜들은 영지식 대화형 방식을 구성하는데 소요되는 통신 횟수 및 통신량이 많다는 약점을 갖고 있다. 그러므로 최근 이러한 약점을 극복하기 위하여 영지식 대화형 증명 방식과 관련한 이론적이고, 실제적인 관점에서의 의문점인 "round complexity의 최적 bound는 얼마인가?"하는 문제에 관한 연구가 활발히 진행되고 있다. 또한, Kurosawa는 일방향성 함수를 이용하여 두개 이상의 영지식 대화형 방식을 결합할 때 유용한 다중 영지식 대화형 방식(multi zero knowledge interactive proof systems)을 제안하였다[12]. 즉, 영지식 대화형 증명을 이용하면, 안전한 암호화 프로토콜의 구성이 가능하므로 그 효율성을 극대화하려는 노력이다.

국내 정보 보호 관련 분야 연구에서도 영지식 대화형 증명방식이 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. S. Goldwasser, S. Micali, C. Rackoff, "Knowledge Complexity of Interactive Proofs", Proc. 17th STOC, pp. 291-304, 1985.

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

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

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

6. U. Fiat, A. Fiat, A. Shamir, "Zero Knowledge Proofs of Identity", STOC, pp. 210-217, 1987.

7. 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.

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

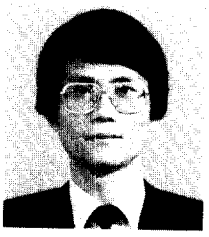
9. K. Ohta, T. Okamoto, "A Modification of the Fiat-Shamir scheme", Crypto'88, pp. 233-243, 1988.

10. T. Beth "Efficient Zero-Knowledge Indentification Scheme for Smart Cards", Proc. Eurocrypt'88, pp. 77-84, 1988.

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

12. K. Kurosawa, S. Tsujii, "one way function & multi zero knowlege interactive proof systems", ISEC90-6, 1991.

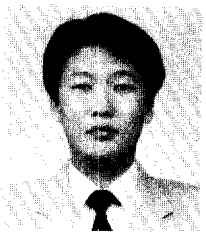
□ 著者紹介



권 창 영(正會員)

1957년 4월 22일생
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

□ 著者紹介



양 형 규(正會員)

1959년 2월 1일생
1983년 성균관대학교 전자공학과 졸업(공학사)
1985년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1991년~현재 성균관대학교 대학원 정보공학과 박사과정 재학중
1985년~1991년 삼성전자 컴퓨터부문 선임연구원

□ 著者紹介

원 동 호(正會員)

1949년 9월 23일생
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