特輯

영지식 대화형 증명 방식 및 응용 프로토콜

權 蒼 英*, 李 仁 淑**, 元 東 豪*
成均館大學校 情報工學科*, 韓國通信 通信網 硏究所**

Ⅰ. 서 론

정보화 사회의 도래로 정보 통신의 수요가 증가되어 컴퓨터 단말기간에 데이타 통신이 활발히 이루어지고 있으며 일반 공중통신망을 이용한 PC 통신 역시 각광을 받고 있다. 이와 같이 서로 다른 컴퓨터망 사이의 상호접속이 빈번해진 상황에서 정보 보호 문제를 포함한 현재의 업무 형태를 '전자적인 형태'로 발전시키기 위한 방안으로 국내에서도 암호학에 대한 연구가 활발히 진행되고 있다. 단순히 정보보호라 하면, 암호화/복호화를 의미하는 현대 암호학의 함수적인 면이 강조되나, 현재의 업무 형태를 고도 정보화 사회에서 필요한 전자송금, 전자우편, 전자거래, 홈쇼핑, 홈 뱅킹, 전자현금 등의 '전자적인 형태'로 실현하려면, 현대 암호학의 프로토콜적인 면이 강조되어야 한다. 80년도 중반부터 대두된 암호화 프로토콜은 그 범위가 매우 넓으며 역할이 매우 중요하게 인식되고 있다.

암호화 프로토콜의 의미는 단편적인 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 프로토콜은 암호 알고리즘이 포함된 통신 알고리즘(communication algorithm)을 의미하며, 그 예로는 동전 던지기(coin flipping), oblivious transfer, bit commitment, 전자 선거, 전자 포커, 전자 계약, 전자 우편, 전자 현금, 다자간 프로토콜 등이 있다[1].

현재까지 연구되어 온 많은 암호화 프로토콜들의 안전성 문제는 학문적으로 엄밀하게 증명되었다기 보다는 "안전할 것이다"라는 가설로 남아 있는 상태라고 보는 것이 합당할 것이다.

영지식 대화형 증명 방식을 이용한 암호화 프로토콜은 그 안전성을 학문적으로 엄격하게 증명할 수 있는 방법이므로 본고에서는 암호화 프로토콜이 "정말 안전한가?"라는 안전성 문제를 해결하기 위하여 제시된 모델로 현재 선진 각국에서 활발히 연구되고 있는 영지식 대화형 증명 방식(ZKIPs : zero knowledge interactive proof systems)을 소개하고 그 예를 들어 자세히 설명하였으며, 응용 프로토콜을 예를 들어 설명하였다.

Ⅱ. 영지식 대화형 증명 방식

1985년 Goldwasser, Micali, Rackoff가 ZKIP 개념을 발표하면서 시작된 ZKIP 이론은 증명자가 검증자에게 자신을 증명함에 있어서 증명의 타당성 이외의 어떠한 정보도 유출시키지 않는다는 것으로, 상대방 인증 방식에 있어서 가히 혁신적인 것이었다.[2] 이후 많은 ZKIP 방식들이 발표되었으며 이러한 방식들은 P≠NP라는 가정하에 NP에 속하는 언어(language)들을 이용하여 상대방 인증을 행하는데, NP에 속하는 모든 언어는 ZKIP에 이용될 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

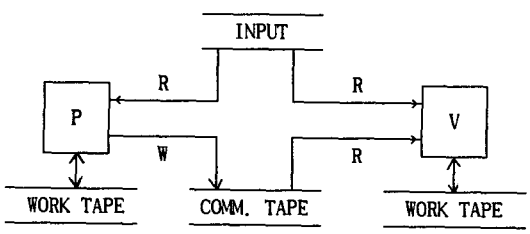
있다.

직관적으로 영지식 대화형 증명 방식을 설명하면, 증명자 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 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.

영지식 대화형 증명 방식은 NP 증명 방식을 일반화시킨 방식으로 암호화 프로토콜의 안전성 문제를 해결하기 위하여 제시된 모델이므로 NP 증명 방식, 대화형 증명 방식, 영지식 대화형 증명 방식 순으로 설명하여 보겠다.

[정의] NP 증명 방식

NP 증명 방식은 대화형 통신이 가능한 무한 계산 능력을 갖는 deterministic Turing machine P(증명자)와 다항식 계산 능력을 갖는 deterministic Turing machine V(검증자)로 구성되며 P, V는 NP 문제 X를 공통 입력 정보로 받아 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 증명 방식이라고 한다.



R:read-only W:write-only

그림 1. NP 증명 방식

NP 증명 방식의 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.

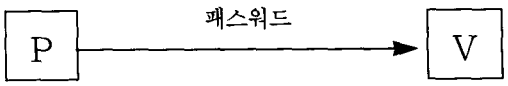


그림 2. 단순한 사용자 인증

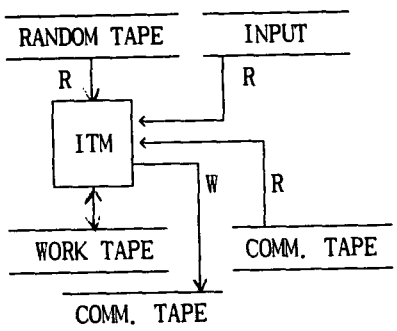
위와 같은 NP 증명 방식은 증명자가 검증자에게 전송하는 정보 x가 너무나 중요하여 암호학의 입장에서 보면 그 적용 분야가 극히 한정될 수 밖에 없다. 그러므로, NP 증명 방식의 약점을 배제하기 위한 새로운 증명 방식이 필요하다.

NP 증명 방식을 두 가지 면에서 일반화시킨 증명 방식이 영지식 대화형 증명 방식이다. 즉, NP 증명 방식은 detetminiстic turing machine상에서 정의되었으나, 대화형 증명 방식은 probabilistic turing machine 상에서 정의된다. 또한, NP 증명 방식은 증명자가 검증자에게 자신의 정보를 전송하는 일방향 방식이나, 대화형 증명 방식은 검증자도 자신의 정보를 증명자에게 전송하는 양방향 방식이다.

대화형 turing machine에 대한 정의를 내려보면 아래와 같다.

[정의] 대화형 Turing machine(ITM)

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



R:read-only W:write-only

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.

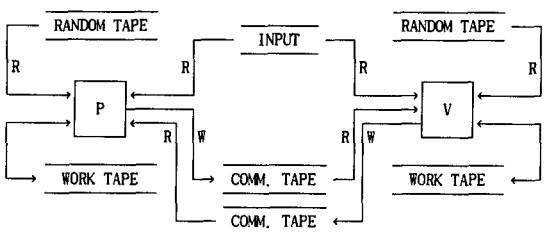


그림 4. 대화형 프로토콜

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

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

두 개의 machine은 V가 최초로 active되고, 서로 번갈아 가면서 active된다. P(V)가 active stage인 동안 input tape, work tapes, 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 메시지는 자신의 i번째 active stage동안 자신의 communication tape에 기록된 모든 string이다.

Machine P(V)는 자신의 메시지를 기록하자마자 deactive되고, machine V(P)가 active된다. 각 machine은 active stage에서 아무런 메시지도 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 증명 방식

대화형 증명 방식은 대화형 통신이 가능한 무한 계산 능력을 갖는 interactive turing machine P와 다항식 계산 능력을 갖는 interactive turing machine V로 구성된 (P,V)가 아래 조건을 만족하면 대화형 증명 방식이라고 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 해임을 $1-1/n^k$ 이상의 확률로 증명할 수 있어야 한다. (단, $n = \log_2 X$)

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 확률이 $1/n^k$ 이하이어야 한다. (단, $n = \log_2 X$)

이러한 정의는 효과적인 증명 방식(proof system)이 가져야 할 직관적인 성격을 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.

mod N상에서 평방근을 갖지 않는 집합은 아래와 같이 표시되며, 평방비잉여 문제를 이용하여 대화형 증명 방식의 구체적인 예를 구성하면 아래와 같다.

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

프로토콜 1. 평방비잉여 문제에 대한 대화형 증명방식

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

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

순서 3. V는 모든 i에 대하여 $b_i = c_i$가 성립하면, (N,Z) QNR임을 accept한다.

이 경우 (N,Z) ∈ L이면, 완전성은 1이며, (N,Z) ∉ L 이면, 건전성은 $1/2^{|N|}$이다.

M을 probabilistic Turing 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 증명 방식 (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 증명 방식 (P,V)가 정의 된다.

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) 알고리듬 M, 모든 c > 0, 그리고 충분히 큰 수 N에 대해 다음 식이 성립한다.

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

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

P_M^B ; 임의의 알고리듬 M에 대해 확률 공간 B[X]에 따라 변하는 원소를 입력으로 선택할 때 M이 1을 출력할 확률

|X| ; X의 길이

[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 M_{V^*}가 존재하고 $\{M_{V^*}[X]\}$ 와 $\{(P,V^*)[X]\}$는 indistinguish able 해야 한다.

Ⅲ. 영지식 대화형 증명의 구체적인 예

영지식 대화형 증명의 의미를 분명히 하기 위해서 몇 가지 구체적인 예를 들어 보기로 하겠다.

1. 평방잉여 문제에 대한 영지식 대화형 증명

평방잉여 문제(quadratic residuosity problem)에 관한 완전 영지식 대화형 증명의 예를 들어 보자.

$$QR = \{(N, Z) \mid Z = S^2 \bmod N\}$$

프로토콜 2. 평방잉여 문제에 대한 영지식 대화형 증명 : P, V의 공통 입력 (N,Z)

순서 1. 증명자 P는 임의의 난수 r을 선택, $x = r^2 \pmod N$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, y = r을 검증자 V에게 전송하고, e = 1이면, $t = r \cdot S \pmod N$을 검증자에게 전송한다.

순서 4. 검증자 V는 e = 0인 경우에는 $y^2 = x \pmod N$을 검사하고, e = 1인 경우에는 $y^2 = x \cdot Z \pmod N$을 검사한다.

순서 5. 검사식이 성립하지 않는 경우, 증명자가 P가 부정행위를 하고 있는 것이 확인되므로 종료하고, 검사식이 성립하는 경우, (N,Z)∈QR임을 신뢰할 수 있도록 순서 1에서 순서4를 |N|회 반복한다. (단, |N| : N의 bit 수)

위의 예에서 e = 0인 경우에는 증명자 P가 S를 소유(possession)하고 있는 것이 확실하지 않지만, e =

1인 경우에는 증명자 P가 S를 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 $y^2 = x \cdot Z \pmod N$을 검사하게 된다.

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

$$y^2 = x \times Z \pmod N \Leftrightarrow r^2 = (r^2/Z) \times Z \pmod N \quad (6)$$

2. 이산 대수 문제를 이용한 영지식 대화형 증명

증명자 P는 소수 p, p-1이하의 정수 a, p-2이하의 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 3. 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, t = 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 순서4를 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

$$1/2 + (1/2)^2 + \cdots + (1/2)^n = 1 - (1/2)^n \quad (7)$$

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 3자 P*가 안다면, P*는 P로 위장할 가능성이 있다. 즉, 순서 1에서 제 3자 P*는 난수 r을 선택, $R = a^r/b \pmod p$를 계산하여 검증자 V에게 전송하고, 순서 3에서 제 3자 P*는 t 대신에 자신이 선택한 난수 r을 검증자 V에게 전송한다. 검증자 V는 순서 4에서 다음 식을 검증하게 되므로 항상 제 3자 P*를 증명자 P라고 확신하게 된다.

$$a^t = bR \pmod p \Leftrightarrow a^r = b(a^r/b) \pmod p \quad (8)$$

Ⅳ. 영지식 대화형 증명의 종류

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 영지식 증명이라고 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 어떤 정보도 노출 시키지않는다.

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, 공개 정보 I와 비밀 정보 S에 대하여 증명자 P는 'I에 대응하는 S를 갖는' 확률적 다항식 시간 Turing machine이고 다음 3가지 조건을 만족하는 것이 된다. 이것을 지식의 영지식 증명이라고한다.

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.

Yung은 지식에 의해 표현하지 못하는 범위로 확장하기 위하여 능력의 영지식 증명을 제안했다. 어떤 함수 f에 대하여 'f(x)로부터 $f^{-1}(f(x)) = x$를 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.

Ⅴ. Bit commitment

Bit commitment는 영지식 프로토콜[3,5], 개인 식별 방식[6], multiparty 프로토콜[7,8] 등에서 사용되어 왔으며, bit commitment의 개념은 여러가지 암호 프로토콜(cryptoprotocols) 구성시 매우 효과적이고 일반적인 primitive이다. Bit commitment의 목적은 A가 A의 도움없이는 누구도 한 bit의 값을 learning하지 못하며, A 또한 그 bit값을 변경하지 못하는 한 bit의 값을 B에게 commit하려는 것이다.

Bit commitment 프로토콜은 다음과 같이 두 단계로 구성된다.

〈Commit 단계〉

- A는 B에게 commit하고자 하는 한 비트 b를 갖고, B와 메세지를 교환한다.
- commit 단계 완료시 B는 b를 의미하는 어떤 정보를 갖는다.

〈Reveal 단계〉

- reveal 단계 완료시 B는 A가 commit하고자 하는 한 비트 b를 알게 된다.

이 프로토콜은 모든 확률적 다항식 시간 Bs에 대해서, 모든 다항식 p와 충분히 큰 안전 파라메타 n에 대해서 다음과 같은 특성을 갖는다.

① commit 단계 후에, B는 $1/2 + 1/p^{(n)}$보다 더 큰 확률로 b를 예측할 수 없다.

② A는 오직 하나의 가능한 값만을 reveal할 수 있다.
만약, A가 다른 값을 reveal하려고 하면, 적어도 $1 - 1/p(n)$의 확률로 발각된다.

Bit commitment 프로토콜이 따라야 할 성질을 정의할 때, B가 bit commit 프로토콜의 실행에 앞서 보다 더 큰 확률로 b를 예측할 수 없다고 가정하였다.

만약, 안전한 bit commitment scheme의 구성이 가능하면, 동전 던지기(coin flipping) 프로토콜은 쉽게 구현된다. 즉, A는 랜덤하게 선택한 bit를 B에게 commit하고 B는 이 bit의 값을 추측하여 자신이 추측한 값을 A에게 알린다. A는 B의 추측이 옳았는지 틀렸는지 검사하면 된다.

Bit commitment는 "blob"라고 불리는 도구인

primitive로 구현된다. Blob는 commitment로써 0 또는 1을 사용한다. 일반성을 갖게하기 위해서는 blobs의 특성에 어떤 제한을 둘 필요는 없다. "A commits to a blob"의 의미는 A가 마음 속으로 하나의 blob을 정하고, 그 blob를 프로토콜이 끝날 때까지 계속 고수한다는 것이다. 만약, blob가 가장 실제적인 bit string으로 표현될 수 있다면, commit할 blob를 명백하고 간단하게 보일 수 있을 것이다.

Blobs의 추상적인 정의에 의한 성질은 다음과 같다.

성질 1) A는 blobs를 commit할 수 있다. blob를 commiting 함으로써 A는 실제 한 bit를 commiting할 수 있다.

성질 2) A는 자신이 commit했던 어떠한 blob도 open할 수 있으며, A는 blob을 commiting할 때 사용한 실제 commiting했던 한 bit의 값을 B에게 증명할 수 있다. 그러나, A는 0 또는 1로 open할 수 있는 blob는 생성할 수 없다.

성질 3) B는 A가 commit했던 A만이 open할 수 있는 어떠한 unopened blob에서 아무 것도 learn할 수 없다.

성질 4) blobs는 "side information"을 포함하지 않는다. 즉, blobs들은 blobs들 사이 뿐만아니라, A가 commit하고 open하는 프로세스와 A가 B에게 비밀로 하려는 어떠한 것과도 상관관계가 없어야한다.

A가 한 bit를 commit하기를 원하는 경우(성질 1), A는 마루 위에 한 bit를 적고, 그것을 B에게 보여주기 전에 불투명한 테이프로 덮는다. 그렇게하면, B는 테이프밑에 어떤 bit가 감추어져 있는지 알 수 없으며, A는 그것을 변경할 수 없다(성질 3). "open the blob"하려면, A는 B에게 테이프를 떠고 감추어져 있던 bit를 보게한다(성질 2). 성질 4는 마루 위에 쓴 bit와 테이프 그리고, 그것들의 위치가 A가 B에게 비밀로 하려는 어떠한 것과 상관관계가 없게 함으로써 만족된다(성질 4).

1. 이산 대수 문제를 이용한 bit commitment

p는 큰 소수이고, α 는 정수 modulo p의 승산군(multiplication group) Z_P^*의 생성원(generator)이라 하자. 어떤 정수 y가 주어졌을 때, $\alpha^y \bmod p$를 계산하는 것은 쉬우나, 이 process의 역을 구하는 효과적인 알고리듬은 없으며 p-1의 소인수 분해를 안다고 해도 α, p, $\alpha^y \pmod p$로부터 y를 계산하는 것은 불가능(infeasible)하다고 가정하자.

처음에 A와 B는 그들이 p-1의 소인수를 아는 소수 p에 동의(agree)한다. 또한, Z_P^*의 생성원(generator) α를 동의한다. p-1의 인수에 대한 지식 때문에 그들은 p는 소수이고, α는 생성원이라는 확신으로 서로 검증(verify)할 수 있다[9].

파라메터 α 및 p는 공개할 수 있고, 가정에 의해 A는 $s = \alpha^e \pmod p$인 e를 계산할 수 없다. 이런 의미에서 bit commitment protocols에 참여하기를 원하는 모든 party들이 사용할 수 있다.

프로토콜 4. 이산 대수 문제를 이용한 bit commitment : $s=\alpha^e \pmod p$

순서 1. B는 난수 $s \in_R Z_P^*$ $(s \neq 1)$를 선택하여, A에게 전송한다.

순서 2. A는 어떤 bit b를 commit하기 위하여 난수 $y \in_R (0, p-2)$를 선택하고, blob인 $x = s^b \cdot \alpha^y \pmod p$를 계산하여 B에게 전송한다.
(단, y는 A가 x를 open하도록 허락하는 A의 witness임으로 B에게 는 비밀로 하여야한다.)

Z_P^*의 임의의 원소는 A가 0으로 commitment한 것처럼 사용될 수 있으며, 마찬가지로 1로 commitment한 것으로도 사용할 수 있다. (단지 임의의 원소에 대하여 A가 알고있는 지식에 대하여 의존적인) 더구나, Z_P^*의 임의의 원소는 일양확률분포(uniform probability distribution)인 프로세서에 의해서 A가 commit하려는 bit와는 독립적(independently)으로 얻어진다. 그러므로 성질 3은 무조건적(unconditionally)으로 만족된다. 즉, A에 의해서 commit된 blob는 A가 blob를 open하는 데 필요한 어떠한 정보도 포함하지 않는다. 성질 2는 계산적으로(computationally) 만족된다. 왜냐하면, A는 $\alpha^{y_1} = s \cdot \alpha^{y_2} \pmod p$인 y_0, y_1의 지식으로부터 (우리가 A에게 불가능하다고 가정했던) e를 쉽게 구할 수 있기 때문이다. 성질 4는 A가 랜덤하게 y를 선택했기 때문에 만족된다.

2. 의사 난수 생성기를 이용한 bit commitment

m(n)을 m(n) > n인 어떤 함수라 하자. 모든 다항식 p와 의사 난수 생성기의 출력과 truly 랜덤 수열을 구별하고자 하는 모든 확률적 다항식 시간 알고리듬 A에 대하여 $|Pr[A(y)=1] - Pr[A(G(s))=1] < 1/p(n)$ 이면, $G:\{0,1\}^n \rightarrow \{0,1\}^{m(n)}$는 의사 난수 생성기(pseudorandom generators) 이다. 단, 확률은 균일하게(uniformly) 임의로 선택된 $y \in \{0,1\}^{m(n)}$과 $s \in \{0,1\}^n$에 따라 좌우된다.

만일 의사 난수 생성기가 임의의 m(n) > n에 대해서 존재하면, 의사 난수 생성기는 all m polynomial in n 에 대해 존재한다고 알려져 있다[10]. 의사 난수 생성기는 지정되지 않은 길이의 수열을 출력하는 것을 다룰 수 있으며, 오직 일정한 prefix만을 조사할 수 있다. prefix의 길이는 seed 길이인 n의 다항식으로 표현된다.

어떤 의사 난수 생성기 G를 가정한다. n을 어떠한 실행 가능한 알고리듬도 seed 길이가 n인 의사 난수 생성기를 안전하다고 예측하는 안전 파라메타라고 하자. $G_l(s)$는 seed $s \in \{0,1\}^n$을 사용하여 의사 난수 수열의 처음 l비트들을 표기하기 위하여 사용하고, $B_i(s)$는 seed s일 때 의사 난수 수열의 i번째 비트를 표시하기 위하여 사용한다.

의사 난수 생성기에 의해서 생성된 의사 난수 수열은 다음 비트의 값에 대한 예측을 할 수 없게하는 특성을 갖는다. 즉, 의사 난수 수열의 처음 m개 비트가 주어진 상태에서 다음 비트를 예측하려고 시도하는 임의의 다항식 시간 알고리듬은 임의의 다항식 p(n)에 대하여 1/2 + 1/p(n)보다 적은 성공 확률을 갖는다. 본 절에서는 bit commitment를 얻기 위해서 이러한 특성을 적용한다.

Bit commitment 방식을 구성하기 위하여 다음과 같은 프로토콜을 생각해 보자.

프로토콜 5′. 의사 난수 생성기를 이용한 bit commitment

순서 1. A는 seed $s \{0,1\}^n$을 선택하고, $G_m(s)$와 $B_{m+1}(s) \oplus b$를 B에게 전송한다.

순서 2. A는 s를 B에게 전송한다.

순서 3. B는 순서 1에서 수신한 $G_m(s)$가 자신에게 보내진 것인지 확인하고,
$b = B_{m+1}(s)$ $(B_{m+1}(s) \oplus b)$을 계산한다.

위의 프로토콜은 A가 commit하려고 하는 비트 b를 1/2+ 1/poly(n)보다 큰 확률로 B가 예측할 수 없다는 특성을 갖는다. 왜냐하면 B는 의사 난수 수열을 예측할 수 있는 능력을 가지지 못하기 때문이다. 반면에 A는 B을 속일 수 있을런지 모른다. 만약 A가 $G_m(s_1) = G_m(s_2)$이고 $B_{m+1}(s_1) \neq B_{m+1}(s_2)$인 두개의 seed s_1과 s_2를 발견한다면 A는 자신이 원하는 임의의 비트를 reveal할 수 있다. 의사 난수 생성기의 정의에 그러한 쌍의 존재를 금지하는 것은 없다. 그러므로 임의의 의사 난수 생성기 G가 주어지면, 그러한 쌍을 가지는 다른 의사 난수 생성기 G′가 구성될 수 있다.

같은 수열을 생성하는 두개의 seed가 존재할 수 있기 때문에 A가 하나의 seed만 사용하도록 하는 방법은 없다. 그러므로 다음의 프로토콜의 목적은 A가 같은 의사 난수 수열만을 사용하도록 하거나 또는 A의 속이는 행위를 큰 확률로 발견할 수 있게 하는 것이다.

프로토콜 5. 의사 난수 생성기를 이용한 bit commitment

순서 1. B는 랜덤 벡터 $R=(r_1, r_2, \cdots, r_{3n})$을 선택하고, A에게 전송한다.
단, $r_i \in \{0,1\}$ for $1 \leq i \leq 3n$.

순서 2. A는 하나의 seed $s \in \{0,1\}^n$를 선택하고, 벡터 $D=(d_1, d_2, \cdots, d_{3n})$를 B에게 전송한다.

$$d_i = \begin{cases} B_i(s) & (r_i = 0\text{인 경우}) \\ B_i(s) \oplus b & (r_i = 1\text{인 경우}) \end{cases}$$

순서 3. A는 s를 B에게 전송한다.

순서 4. B는 모든 $1 \leq i \leq 3n$에 대해서, 만약 $r_i = 0$ 이면 $d_i = B_i(s)$인 지를 검사 하고, $r_i = 1$ 이면 $d_i = B_i(s) \oplus b$인 지를 검사한다.

이 프로토콜은 B가 비트 b에 대한 정보를 얻을 수 없다는 특성을 유지한다. 그렇지 않다면 B는 의사 난수 생성기의 출력과 truly 랜덤 스트링을 구별할 수 있는 능력을 가지게 될 것이다. 즉, 만약 A가 의사 난수 수열 대신에 truly 랜덤 수열을 선택했더라도, B는 b에 대한 어떠한 정보도 얻지 못할 것이다. 왜냐하면 모든 벡터 D는 b가 무엇이던지 간에 같아 보이기 때문이다.(이것은 B가 확률 q > 1/2로 b를 예측

할 수 있는 어떤 보조 입력을 가지는 일반적인 경우에도 사실이다.) 만약 A가 의사 난수 수열을 사용했을 때 b에 대한 정보를 얻을 수 있는 확률적 다항식 시간 B (B'로 칭함)가 존재한다면, B'는 G의 출력과 truly 랜덤 수열을 구별할 수 있는 distinguisher를 구성하는데 사용될 수 있다. 수열 x가 주어지고 A와 B'가 프로토콜의 commit 단계를 실행한다고 가정하자.(단, A는 랜덤 비트 b를 commit하고 의사 난수 수열을 생성하는 대신에 x를 사용) 이때 B'가 b를 예측하려 한다고 하자. 만약 B'가 올바르게 예측한다면 x는 의사 난수라고 결정될 것이고 그렇지 않으면 x는 truly 랜덤 수열이라고 결정될 것이다. Truly 랜덤 수열과 의사 난수 수열에서 그 수열이 의사 난수라고 결정될 수 있는 확률과 truly 랜덤 수열이라고 결정될 수 있는 확률과의 차이가 의미하는 것은 B'가 x가 의사 난수 수열인 경우에 b를 예측하는데 가질 수 있는 이점을 말한다.

A가 어떻게 하면 B을 속일 수 있는가? A가 속일 수 있는 기회는 $G_{3n}(s_1)$과 $G_{3n}(s_2)$가 r_i=0인 모든 i에서 같고 r_i=1인 모든 i에서 다른, 두 개의 seed s_1과 s_2가 존재한다면 A는 속일 수 있는 기회를 갖게 된다. 따라서 그러한 쌍은 R을 속일 수 있을 것이다.

Ⅵ. 영지식 대화형 증명 방식의 응용

1. 개인 식별 방식

개인 식별(identification) 문제는 암호학의 여러 분야에서 발생하는 매우 중요한 문제 중의 하나이다. 개인 식별은 가입자 A가 가입자 B와 협조하여 A는 B에게 자신이 A임을 증명할 수 있으나, 제 3자인 C는 A로 위장하여 B에게 자신이 A라고 속일 수 없는 사용자 인증(entity authentication) 기능에 가입자 B도 제 3자 D에게 자신이 A라고 증명할 수 없다는 조건이 추가된 기능이다. 일반적으로 개인 식별 방식이 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 매우 상통한다. Fiat, Shamir의 개인 식별 방식을 비롯한 전형적인 ID 정보 및 영지식 대화형 증명을 이용한 개인 식별 프로토콜들은 많은 변형이 가능하다. [6,11,12,13,14,15]

(1) 구체적인 예

Fiat-Shamir 개인 식별 방식은 ZKIP의 개념에 Shamir 자신이 제안한 ID 개념 [16] 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, id 번호, 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 6. FS 개인식별 방식 (순서 1에서 순서 4를 t회 반복한다.)

순서 1. 가입자 A는 $r \in_R Zn^*$ 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.

FS 방식의 문제점은 현재 스마트 카드 프로세서의 제약 조건들은 사용 알고리듬의 선택시 엄격한 제한을 수반하게 되는데 비해 반복(iteration) 횟수와 증

명자가 많은 메모리를 필요로 한다는 것이다. 또한, 만약 센터의 비밀 정보가 노출되는 경우 전혀 안전성이 보장되지 않으며, 센터와 특정 가입자 간의 결탁으로 임의의 가입자의 비밀 정보를 이용하여 부정한 행위를 행할 수 있는 가능성이 있다.

확장 Fiat-Shamir 개인 식별 방식(이하 확장 FS 방식)은 FS 방식의 효율성을 개선한 방식으로 FS 방식의 멱승 지수부를 기소수 L로 확장한 방식이다[11,12,13]. 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 사용자에게 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 1회로 줄일 수 shadowed identity J를 이용하였는데 ISO-DP 9796("digital signature scheme with shadow" 표준화)에 자세히 언급되어 있다.

프로토콜 7. 확장 FS 개인식별 방식 (순서 1에서 순서 4를 1회 반복한다.)

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

순서 2. 가입자 B는 $d \in_R Z_L$ 를 선택하여 가입자 A에게 d를 전송한다.

순서 3. 가입자 A는 $y = r \cdot s_i^d \pmod n$을 계산하여 가입자 B에게 전송한다.

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

FS 방식에서는 순서 1에서 순서 4를 t회 반복하는 데 반하여 확장 FS 방식에서는 순서 1에서 순서 4를 1회 행하므로 통신 효율을 개선하였다.

2. 키 분배 방식

영지식 대화형 증명[2]에서는 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 통신 정보 보호 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 indistinguishable하다. a는 고정 파라메터이고, g(R)은 영지식 증명을 이용하여 증 명자로부터 검증자에게 전송되는 하나의 메시지이다. 만약 g(f(r,a))와 g(R)의 분포 가 indistinguishable하다면, 영지식 증명은 가능하다. f(r,a)의 예인 a^r mod n 같은 함수는 identity-based key distribution 방식를 구성하는 데 사용할 수 있다. 또 다른 함수 bit commitment functions 들은 디지탈 서명 방식에 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 $1/s_{i,j} = (f(I_i,j))^{1/2} \pmod n$ (i=1,2, j=1,2, …,k)이다. 단, p, q는 소수이며, $p'=(p-1)/2$, $q'=(q-1)/2$ 역시 소수이고 n=pq이다. $g \in Zn^*$인 g의 order는 $p'q'$이며, lpl=$c_1$lnl, lql=$c_2$lnl (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 8. FS 개인식별 방식을 이용한 키 분배 (순서 1에서 순서 5를 t회 반복한다.)

순서 1. 가입자 A는 난수 $r_1 \in Zn$을 선택한다. 가입자 B에게 $x_1 = g^{2r1} \pmod n$ 을 전송한다.

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

가입자 A에게 전송한다.
가입자 B는 마찬가지로 난수 $r_2 \in Zn$을 선택한다.
가입자 A에게 $x_2 = g^{2r2} \pmod n$ 을 전송한다.

순서 3. 가입자 A는 가입자 B에게 y_1를 전송한다.

$$y_1 = g_{r1} \prod_j s_{1,j}^{e_{1,j}} \pmod n \quad (9)$$

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

순서 4. 가입자 B는 $x_1 = y_1^2 \prod_j f(I_{1,j})^{e_{1,j}} \pmod n$ 를 검증한다.
검증이 성립되면, K_1을 생성한다.

$$K_1 = x_1^{r_2} \pmod n \quad (10)$$

가입자 B는 가입자 A에게 y_2를 전송한다.

$$y_2 = g^{r_2} \prod_j s_{2,j}^{e_{2,j}} \pmod n \quad (11)$$

순서 5 : 가입자 A는 $x_2 = y_2^2 \prod_j f(I_{2,j})^{e_{2,j}} \pmod n$ 을 검증한다.
검증이 성립되면, K_1을 생성한다.

$$K_1 = x_2^{r_1} \pmod n \quad (12)$$

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

$$K = K_1 + K_2 + \cdots + K_t \pmod n \quad (13)$$

가입자 A와 가입자 B가 확장 FS 방식으로 개인 식별을 행하면, 키 분배를 행하는 프로토콜은 아래와 같다.

프로토콜 9. 확장 FS 개인 식별 방식을 이용한 키 분배

순서 1. 가입자 A는 $r_A \in_R Zn^*$를 선택하고 $x_A = (g^{r_A})^L \pmod n$을 계산하여 가입자 B에게 전송한다.

순서 2. 가입자 B는 $d_B \in_R Z_L$ 을 선택하여 가입자 A에게 d_B를 전송한다.
가입자 B는 $r_B \in_R Z_n^*$ 를 선택하고 $x_B = (g^{r_B})^L \pmod n$을 계산하여 가입자 A에게 전송한다.

순서 3. 가입자 A는 $y_A = ((g^{r_A}) \cdot S_A^{d_B} \pmod n$을 계산하여 가입자 B에게 전송한다.
가입자 A는 $d_A \in_R Z_L$ 을 선택하여 가입자 B에게 d_A를 전송한다.

순서 4. 가입자 B는 $y_A^L = x_A \cdot ID_A^{d_A} \pmod n$이 성립하는지 검증한다.
검증이 성립되면, 공통키 $K = x_A^{r_B}$를 생성한다.
가입자 B는 $y_B = (g^{r_B}) \cdot S_B^{d_A} \pmod n$을 계산하여 가입자 B에게 전송한다.

순서 5. 가입자 A는 $y_B^L = x_B \cdot ID_B^{d_B} \pmod n$이 성립하는지 검증한다.
검증이 성립되면, 공통키 $K = x_B^{r_A}$를 생성한다.

3. 디지탈 서명 방식

Fiat-Shamir 디지탈 서명 방식은 앞절에서 언급한 개인 식별 방식과 동일한 준비 과정을 행하며 증명자가 메시지 M에 대하여 서명을 만들어 확인자에게 전송해야 하므로 개인 식별 방식처럼 대화형 방식은 이용할 수 없다. 그러므로 증명자는 해쉬함수를 이용하여 서명하려는 메시지와 자신이 선택한 랜덤수에 의존하는 2진 벡터 {eij} 를 생성하여 이용한다.

프로토콜 10. FS 디지탈 서명 방식

순서 1. [디지탈 서명의 생성]

① 가입자 A는 $r_1,\cdots,r_t \in_R Zn^*$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 메시지 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, {eij} 및 y_i를 전송한다.

순서 2. [디지탈 서명의 검증]

① 가입자 B는 $v_j = f(ID_A, j)$ (1 j 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_{ik}와 동일한가 검증한다.

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

Ⅶ. 결 론

현대 사회는 고도 정보화 사회로 변화하는 과정에서 각종 암호화 프로토콜이 필요하다. 특히, 부가가치가 높은 '전자적인' 형태의 각종 서비스를 제공하기 위하여 안전하고 효율적인 암호화 프로토콜들이 필요하다. 본고에서는 암호화 프로토콜의 안전성을 학문적으로 엄밀하게 증명할 수 있는 방법을 제시하기 위한 모델인 영지식 대화형 증명 방식과 각종 암호화 프로토콜 구현시 사용되는 도구인 bit com-mitment 및 동전 던지기 프로토콜에 대하여 논하고, 그 각각의 구체적인 예를 들어 설명하였다. 또한, 영지식 대화형 방식을 이용한 개인 식별, 키 분배, 디지탈 서명 등의 응용 프로토콜에 대하여 구체적인 예를 들어 기술하였다.

영지식 대화형 증명 방식을 이용한 암호화 프로토콜들은 안전성을 증명할 수 있으나, 영지식 대화형 증명 방식을 구성하는 데 소요되는 통신 횟수 및 통신량이 많다는 단점을 갖고 있다. 그러므로 최근 이러한 단점을 극복하기 위하여 영지식 대화형 증명 방식과 관련한 이론적이고, 실제적인 관점에서의 의문점인 "round complexity의 최적 bound는 얼마인가 ?"하는 문제에 관한 연구가 활발히 진행되고 있다.[17] 즉, 영지식 대화형 증명을 이용하면, 안전한 암호화 프로토콜의 구성이 가능하므로 그 효율성을 극대화하려는 노력이다.

국내 정보 보호 관련 분야 연구에서도 영지식 대화형 증명 방식이 활발히 응용되어 고도 정보화 사회에서 요구되는 전자송금, 전자우편, 전자거래, 홈 쇼핑, 홈 뱅킹, 전자현금 등의 서비스 구현시 필요한 기반을 확고히 하여야 하겠다.

參 考 文 獻

[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] 원 동호, 양 형규, 권 창영 외, "ZKIP 이론에 관한 연구", 한국전자통신연구소 데이타 보호 기반 기술 연구과제 최종보고서, 성균관대, 1991.11.

[5] G.Brassard, D.Chaum, C.Crepeau, "Minimum disclosure proofs of knowledge" (revised version), Texchnical Report PM_R8710, Centre for Mathematics and Computer Science (CWI), Amsterdam, The Netherlands, 1987.

[6] A.Fiat, A.Shamir, "How to Prove Yourself : Practical Solutions to Identification and Signature Problems", *Proc.* CRYPTO' 86, pp. 186-194, 1986.

[7] O.Goldreich, S.Micali, A.Wigderson, "How to play any mental game", *Proc.* 19th ACM Symposium on Theory od Computing, pp.12-24, 1989.

[8] D.Chaum, I.B.Damgard, J.Van de graaf, "Multiparty computations ensuring privacy of each party's input and correctness of the result", Advances in Cryptology - CRYPTO' 87 Proceedings, Springer- Verlag, pp.87-119. 1988.

[9] Knuth,D.E. The Art of Computer Programming, vol.2 : Semi-numerical Algorithms, second edition, Addison-Wesley, Reading, MA, 1981.

[10] O.Goldreich, S.Goldwasser, S.Micali, "How to construct random functions",

Journal of the ACM, vol.33. pp.792-807, 1986.

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

[12] 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.

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

[14] K.Ohta, T.Okamoto, "A Modification of the Fiat-Shamir scheme", CRYPT '88, pp.233-243. 1988.

[15] T. Beth, "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Proc. EUROCRYPT' 88, pp.77-84, 1988.

[16] A.Shamir, "Identity-based Cryptosystems and Signature Schemes", CRYPTO '84, pp.47-53, 1984.

[17] 원 동호, 양 형규, 권 창영, 정 지원 외, "ZKIP의 round complexity와 응용 프로토콜에 관한 연구", 한국전자통신연구소 데이타 보호 기반 기술 연구과제 최종 보고서, 성균관대, 1992.11.

筆 者 紹 介

權 蒼 英
1957年 4月 22日生
성균관대학교 수학교육과 졸업
성균관대학교 대학원 정보공학과 졸업 (공학석사)
(주)KOLON 정보 SYSTEM실 팀장

현재 성균관대학교 대학원 정보공학과 박사과정 재학중
대유공업전문대학 사무자동화과 전임강사.

李 仁 淑
1957年 8月 22日生
이화여자대학교 수학과 졸업
이화여자대학교 대학원 수학과 졸업 (이학석사)
한국전자통신연구소 연구원
한국통신 연구개발단 선임연구원

현재 한국통신 통신망연구소 서비스진화연구실장

元 東 豪
1949年 9月 23日生
성균관대학교 전자공학과 졸업
성균관대학교 대학원 전자공학과 졸업 (공학박사)
한국전자통신연구소 연구원
일본 동경공대 객원연구원

현재 성균관대학교 정보공학과 교수
한국통신정보보호학회 편집이사