論文93-30A-8-1

WH와 WI를 이용한 4-move ZKIP과 그 응용

(4-Move ZKIP Using WH and WI and Its Applications)

梁 亨 圭*, 李 仁 淑**, 元 東 豪*

(Hyung Kyu Yang, In Sook Lee and Dong Ho Won)

要 約

본 논문에서는 NP-Complete 문제와 관련된 ZKIP 방식에서 필수적인 bit-commitment 방식과 임의의 프로토콜의 병렬 합성시에도 안전한 특성을 유지하는 WH와 WI를 이용하여 SAT 문제의 최적 round를 6-move ZKIP에서 4-move ZKIP으로 구성하고, claw-free pairs of functions 하에서 5-move ZKIP을 같은 함수하에서 4-move ZKIP으로 구성 제안하였다. 제안된 방식들의 안전성 즉, 영지식성을 증명하고, 제안한 방식이 계산량 및 통신량 측면에서 Fiat와 Shamir가 제안한 방식보다 효율적임을 보이며, 또한 본 방식을 이용하여 효율적이고, 선택 암호문 공격에 안전한 개인식별 방식을 제안하였다.

Abstract

In this paper, we will propose 4-move ZKIP and its application. Using bit-commitment scheme that is necessary to organize the ZKIP related to NP-Complete problem and WH and WI preserving the property for security under parallel composition of protocols, we will show that the proposed ZKIP is 4-move ZKIP of SAT comparing to 6-move ZKIP of SAT proposed by Brassard, Chaum and Yung, and under claw-free pairs of function the proposed ZKIP is also 4-move ZKIP comparing to 5-move ZKIP proposed by Goldreich and Krawczyk under the same assumption. Moreover we will show the efficiency of the proposed scheme better than Fiat and Shamir's scheme at the points of computational complexity and communication complexity, and also propose the efficient and secure identification scheme against the chosen ciphertext attack, using the proposed scheme.

Ⅰ. 서론

1985년 Goldwasser, Micai와 Rackoff가 ZKIP (Zero-Knowledge Interactive Proof Sytems)에 대한 개념을 최초로 제안했으며[1], Goldreich, Micali와 Wigderson는 안전한 bit-commitment 방식이 존재한다는 가정하에서 모든 NP 문제는 ZKIP 방식을 갖는다는 사실을 증명함으로써 ZKIP을 확장하였다.[2] ZKIP과 관련한 이론적이고 실제적인 관점에서의 의문점은 ZKIP의 round complexity의 최적 bound는 얼마인가 하는 문제이다.[3] 최근에 Goldreich와 Krawczyk는 이 문제에 대한 결론을 얻었다.[4] 즉, "만약 임의의 언어 L이 3-move black box simulation ZKIP을 갖는다면,

*正會員, 成均館大學校 情報工學科
(Dept. of Information Eng., Sungkyun kwan Univ.)
**正會員, 韓國通信 通信網研究所
(Korea Telcom Telecommunication Networks Research Lab)
接受日字: 1993年 1月 11日

언어 L은 BPP에 속한다" 라고 증명하였다. 다시 말하면 "BPP 이외의 언어는 4-move 이상의 ZKIP을 구성할 수 있다"라는 의미로 해석할 수 있다. 따라서 기존의 ZKIP 방식을 갖는 예들(Quadratic Residue, Certified Dicrete Logarithm Assumption, Graphic Isomorphism)은 round 수가 제한되지 않았다. 그 예로 Brassard, Crepeau와 Yung은 "CDLA 가정하에서 모든 NP 문제를 6-move ZKIP으로 구성할 수 있다"라고 증명하였고[5], Fiat와 Shamir는 "같은 가정하에서 모든 NP 문제를 4-move ZKIP으로 구성할 수 있다"라고 증명하였으며[6], Bellare, Micali와 Ostrovsky는 "모든 RSR (Random Self Reducibility) 언어를 5-move ZKIP으로 구성할 수 있다" 라고 증명하였다.[7] 위의 결과들을 정리하면 다음과 같다.

ZK [3] = BPP ([3])
ZKAM [3] = BPP ([3])
PZK [4] ⊇NP ([5])
PZK [5] ⊇RSR ([6])

단, (P)ZK [n] : n-move로 구성이 가능한 black-box simulation (perfet)ZKIP을 갖는 언어들의 class를 의미.
round : 2 move

참고문헌 [7] 의 6-move ZKIP을 구성하기 위해 사용된 주요 개념은 trapdoor bit-commitment 방식으로 검증자(verifier)가 임의로 자신의 도전 비트(challenge bits)을 생성하는 것을 방지하는 것이다. 따라서 증명자(prover)와 검증자는 증명자의 첫 번째 message의 값에 의존하게 된다.

본 논문에서는 NP-Complete 문제와 관련된 ZKIP 방식에 중요한 bit-commitment 방식과 WI (witness indistingushable) 그리고 WH(witness hiding)을 이용하여, SAT 문제의 최적 round를 [7] 의 6-move ZKIP에서 4-move ZKIP으로 구성하였으며, claw-free pairs of functions 하에서 [4] 의 5-move ZKIP을 같은 함수하에서 4-move ZKIP으로 구성하였다. 또한, 제안한 방식이 계산량 및 통신량 측면에서 [6] 이 제안한 방식보다 효율적임을 보이고, 본 방식을 이용하여 효율적이고 선택 암호문 공격(chosen ciphertext attack)에 안전한 개인식별(identification) 방식을 제안하였다.

Ⅱ. Bit-commitment 방식

Bit-commitment 방식은 NP-Complete 문제들과 관련한 모든 상호 프로토콜(interactive protocols) 구성시 매우 중요한 역할을 한다. Bit-commitment 방식의 목적은 임의의 프로토콜이 병렬로 수행될 때, 이 프로토콜이 영지식을 만족하기 위한 방법을 제공하는데 있다. Bit-commitment 방식은 검증자는 증명자의 도움 없이는 숨긴(commitment) 비트의 값 즉, 0 혹은 1에 대한 값을 알 수 없도록 하고, 증명자 자신이 이미 선택된 비트의 값을 변경하는 것을 방지하기 위해서 증명자 자신이 생성한 bit의 값을 숨기는 것(commitment)을 허락하는 방식이다. 증명자(A)와 검증자(B)간에 일어나는 bit-commitment 방식은 두 단계 즉, commit 단계와 reveal 단계로 구성된다.

Commit 단계 : 상호간 메세지가 교환된 후 검증자는 증명자의 비밀 비트 b를 의미하는 임의의 정보를 얻는다.
Reveal 단계 : 검증자는 b의 값을 알게 된다.

정의 2.1 Trapdoor bit-commitment 방식은 commit 단계와 reveal 단계로 구성되고 다음의 특성들을 만족한다.

1. 완전성(completness): 임의의 A는 임의의 비트 b(0 혹은 1)에 대해서 commit할 수 있다.
2. 건전성(soundness) : A는 자신이 프로토콜 종료 후 두 가지의 가능한 방법으로 0 과 1을 의미하는 commitment를구성할 수 있는 확률은 거의 0이다.
3. 안전성(security) : 임의의 B가 commit된 비트의 값을 예측할 수있는 확률은 거의 0이다.
4. 함정성(trapdoor) : trapdoor 정보를 통해서 B는 A의 commitment와는 구별할 수 없는 commitment를 구성할 수 있다.

정의 2.1의 trapdoor 특성은 Brassard, Chaum과 Crepeau가 발표한 minimum disclosure 개념에서의 chameleon 특성과 유사하다.[8] Trapdoor 특성은 증명자만이 임의의 비밀 즉, trapdoor 정보을 알고 있다면 자신만이 알고 있는 임의의 비밀을 이용하여 증명자가 원할 때마다 자신의 commitment를 검증자에게 속이는 것을 가능하게하는 특성을 말한다. 다시 말하면, 이러한 trapdoor 정보에 대한 지식은 증명자에게 0과 1을 의미하는 commitment를 위조(즉, 1C⇒0로 0⇒1)할 수 있는 방법을

제공하게 되고 이러한 위조된 commitment들은 원래의 commitment들과는 정보 이론적으로 구별 불가능 (information theoretically indistingushable)하게 된다. 이러한 특성 때문에 trapdoor 특성을 갖는 bit-commitment 방식들은 영지식 특성을 갖게 되며, constant round ZKIP을 구성하는데 필수적인 도구가 된다. [9] 본 논문에서 제안한 ZKIP방식 역시 trapdoor 특성을 이용한다.

Ⅲ. 영지식 상호 증명 방식

본 논문에서 제안한 영지식 상호 증명 방식의 증명자 P와 검증자 V는 확률적 다항식 계산 능력을 갖는 상호 Turing 기계이며, P와 V의 공통 입력은 | x | 로, 그 길이(length)는 x = n으로 표시된다. 각각의 Turing 기계는 임의의 입력 테이프를 소유하고, 테이프로부터의 P와 V의 임의의 입력을 각각 w, y로 표시한다. $\nu(n)$은 어떤 다항식 함수의 역수보다 빠르게 감소하는 임의의 함수로 정의한다. 즉, 다음의 식으로 표시할 수 있다.

$$\forall k, \exists N s.t. \forall n \rangle N, \nu(n) \langle 1/n^k \qquad (1)$$

무시할 수 있는 확률이란 $\nu(n)$처럼 표시되는 확률을 의미하고, 압도적인 확률이란 $1-\nu(n)$처럼 표시되는 확률을 의미한다.

A(x)는 입력 x에 대한 확률적 알고리즘 A의 출력이며 랜덤 변수이다. $V_P(x)$는 공통 입력 x에 대해서 P와 대화한 후 V의 출력이다. M(x;A)(단, A는 P 혹은 V 중의 하나이다)는 입력 x에 대한 알고리즘 M의 출력을 표시한다. 단, M은 알고리즘 A를 서브루틴으로 사용한다.

정의 3.1. L을 다항식 시간 비결정적(nondeterministic) Turing기계 M_L에 의해 서 수락된 NP 언어라 하자. 계산 경로(computation path)는 M_L이 만 든 일련의 비결정적 선택들이다. 입력 x∈L에 대해서 M_L이 수락한 계산 경로의 집합을 x의 witness 집합이라 하고 w(x)로 표기한다.

정의 3.2. NP 언어 L에 대한 지식의 상호 증명 방식은 다음의 조건을 만족하는 하나의 알고리즘의 쌍 (P,V)이다.

1. 완전성 : 임의의 입력 x∈L 과 임의의 w∈w(x)에 대해서, $V_{P(x,w)}(x)$는압도적인 확률로 증명을 받아 들인다. 수식적으로 표현하면 다음과 같다.

$$\forall x \in L \forall w \in w(x) \Pr ob\left(V_{p(x,w)}(x) acceots\right) \rangle 1 - \nu(n) \qquad (2)$$

단, 확률은 P와 V의 동전 던지기 (coin tosses)와 관련된다.

2. 건전성 : 임의의 x와 임의의 P′에 대해서, P′가 x∈L에 대한 witness을실질적으로 알아야지만 P′는 V에게 증명을 확인시킬 수 있다. 평균 다항식 시간 지식 추출기(knowledge extractor) E는 witness를 계산할 수 있는 P′의 능력을 표현하기 위해서 사용된다. 수식적으로 표현하면 다음과 같다.

$$\exists M, \forall P', \forall x, \forall w'$$
$$\left(\Pr ob\left(V_{p'(x,w')}(x) accepts\right) - \Pr ob\left(E(x, P'(x,w')) \in w(x)\right)\right) \qquad (3)$$
$$\langle \nu(n)$$

단, 확률 : V와 M의 동전 던지기와 관련, E : P′를 서브루틴으로서 사용할 수 있다.

정의 3.3. I를 무한한 스트링들의 집합이라 하고 E_1과 E_2를 두 개의 확률 앙상블(probability ensembles)이라 하자. (단, 임의의 x∈I에 대해서, $E_1(x)$와 $E_2(x)$는 랜덤 변수이다.) 임의의 알고리즘 D에 대해서 D가 입력 x와 확률분포 $E_1(x)$에 따라서 선택된 원소를 입력으로 해서 1을 출력하는 확률을 $P_1^D(x)$로 표기하자. 만약 임의의 비균일(nonuniform)한 다항식 시간 구별자(distingusher) D에 대해서, $|P_1^D(x) - P_2^D(x)| \langle \nu(n)$이면, 앙상블 E_1와 E_2는 다항식 시간 구별 불가능(indistingushible)하다.

정의 3.4. 증명 방식이 다음의 조건을 만족하면 L에 대해서 영지식이다.

조건) 임의의 확률적 다항식 시간 V′와 witness w와 관련된 입력 x∈L 과, V′에 대한 임의의 입력 y에 대해서, 두 개의 앙상블 $V'_{P(x,}$

$_{W}$)(x,y)와M(x,V′(x,y))가 다항식 구별 불가능한 앙상블 M(x,V (x,y))를 평균 다항식 시간내에 생성할 수 있는 시뮬레이터 M이 존재한다.
단, M은 V′를 서브루틴으로서 사용할 수 있다.

Ⅳ. CDL 가정하에서 4-move ZKIP

본 절에서는 CDL(certified discrete logarithm)을 이용하여 CDL 가정하에서 SAT 문제의 최적 round를 6-move ZKIP에서 4-move ZKIP으로 구성해 본다. 그리고 증명자와 검증자 모두는 다항식 시간 계산 능력을 갖고 있으며[10,11], 영지식을 증명하기 위해서 black-box simulator를 사용한다.[12] 우선 SAT 문제에 대한 참고문헌 [8] 의 프로토콜을 생각해보자.

프로토콜 1. 공통 입력 : Boolean formula Ψ(진리표 T_m, $1 \le m \le h$을 가진 h개의 논리 게이트들과 연결선들로 구성)
〈증명자 P는 자신의 비밀 테이프에 witness 즉, satisfying assigment H를 보관한다〉

Move 1-1. P는 연결선당 임의의 값인 c_j를 사용하여 $T_m = (b_{i,j})_m$의 행들을 다음과 같이 계산한다.

$$T_m' = (b_{i,j} \oplus c_j)_m \quad (4)$$

1-2. P는 치환 Π를 사용하여 T_m'의 열들을 치환하여 다음과 같이 계산한다.

$$T_m'' = (b_{\pi(i),j} \oplus c_j)_m \quad (5)$$

1-3. P는 T_m''의 각 비트를 "commit"한다.

Move 2. V는 랜덤하게 도전 비트 q를 선택해서 P에게 보낸다.

Move 3-1. 만일 q = 0이면, P는 V에게 모든 commitment들을 오픈하고 모든 계산에 사용된 비트들 즉, c_j를 오픈한다.

3-2. 만약 q = 1이면, P는 각 진리표 T_m''의 한 열에 대응하는 commitment들만 오픈한다.

Move 4. V는 대응되는 commitment들이 올바른가 즉, "commit"의 결과들과 진리표의 내용들이 일치하는가를 검사한다.

프로토콜 1은 순차적으로 k(단, security number)번 반복하면 다음과 같은 특성을 만족한다.

1. 완전성 : 정직한 P와 V는 항상 프로토콜을 성공적으로 수행한다.
2. 건전성 : 사용한 commitment 방식이 건전하므로 프로토콜을 성공시킬 수 있는 제삼자 P′의 능력이란 것은 satisfying assigment H를 알고 있다는 것을 의미한다.
3. 영지식 : 사용한 commitment 방식이 안전하다면 blackbox simul-ator에 의해서 증명된다.

그러나 만일 병렬로 수행된다면 이 프로토콜은 더 이상 영지식을 만족시키지 못한다.(SAT∈BPP가 아니라면[4]) 프로토콜 1에서는 사용된 bit-commitment 방식에 대해서 정확히 밝히지 않았으나, 본 논문에서는 WI와 WH를 이용한 bit-commitment 방식을 사용한다. 이와는 별도로 [2] 는 probabilistic encryption functions을 사용한 bit-commitment 방식을 제안하였다. 다음은 SAT 문제의 최적 round를 6-move ZKIP에서 4-move ZKIP으로 구성하는데 필요한 프로토콜을 WI와 WH를 이용하여 다음처럼 구성할 수 있으며, 이 프로토콜은 프로토콜 1의 bit-commitment 방식을 구성하는데 사용된다.

프로토콜 2. P는 x_1 혹은 x_2 둘 중의 하나에 대한 discrete log를 안다는 사실을 증명하는 프로토콜이다. 공통 입력은 CDLA를 기반으로 하는 IG (invulnerable generator)에 의해서 생성되는데 이것은 입력이 두 개의 witness를 소유하게 한다.

공통 입력 : (p, g, c, x_1, x_2)
단, p : 소수 , g : Z_p^* 상의 원시 원소
c : p, g에 대한 certificate[12]

$$x_1 = g^{w1} \mod p \quad (6)$$
$$x_2 = g^{w2} \mod p \quad (7)$$

Move 1. P는 랜덤하게 그리고 독립적으로 r_1, r_2를 비밀리에 선택하고, 다음의 식을 계산한다.

$$y_1 = x_1 \cdot g^{r1} \mod p \quad (8)$$
$$y_2 = x_2 \cdot g^{r2} \mod p \quad (9)$$

P는 랜덤 순서로 위의 값들을 V에게 보낸다.

Move 2. V는 랜덤 비트를 P에게 보낸다.

Move 3-1. 만일 P가 0을 받으면 P는 r_1과 r_2를 V에게 보낸다. 이 때 , V는 y_1과 y_2가 올바르게 구성됐는 가를 검사한다.
($y = x \cdot g^r \bmod p$)

3-2. 만약 P가 1을 받으면 P는 y값들 중의 오직 하나에 대한 discrete log(w + r(mod p-1))을 V에게 보낸다. 이 때, V는 대응되는 값을 검사한다.

정리 4.1. 이 프로토콜은 CDL 가정하에서 WH를 만족한다.

정리 4.1의 증명은 참고문헌 [5] 의 증명과 유사하다.

최종적으로 SAT 문제의 4-move ZKIP을 구성하여 보자. 우선 6-move ZKIP을 구성하고, 다음에 이 프로토콜을 이용하여 4-move ZKIP이 성립됨을 밝히겠다.

프로토콜 3. SAT 문제에 대한 지식의 완전 영지식 상호 증명. 프로토콜 3은 프로토콜 1과 프로토콜 2의 순차적 합성이다.

공통 입력 : Boolean formula Ψ

P의 witness: satisfying assigment H

Move 1. V는 프로토콜 2에 대한 입력 I = (p,g, c,x_1,x_2)를 생성하기 위해서 약간 수정된 IG를 사용한다. V는 프로토콜 2에서 증명자처럼 행동한다. 또한, V는 w_1과 w_2 둘 중에 하나를 랜덤하게 선택해서 버리고 나머지는 자신의 비밀입력 즉, witness로서 보관한다. V는 I를 P에게 보낸다.

Null Move. P는 p가 소수이고 g가 원시원소인지 검사하기 위해서 certificate c를 사용한다. 만약, 검사가 실패하면 P는 중지한다.

Move 1~3. V와 P는 입력으로서 I를 가지고 프로토콜 2를 수행한다.

〈이 서브 프로토콜에서는 서로의 역할이 상반된다. 즉, V는 비밀 입력을 가지는 증명자이고 P는 검증자이다.〉

Null Move: 만약 프로토콜 2가 성공적으로 수행되면 P는 V가 I에 대한 witness를 알고 있다고 확신한다. 그렇지 않으면 P는 중지한다.

Move 4~6. P와 V는 공통 입력 Ψ를 가지고 프로토콜 1의 병렬합성을 수행한다. 이 때 P의 비밀 입력은 H이다. bit- commitment로서 P는 입력으로 Ψ를 가지고 프로토콜 2의 절차를 사용한다.

Move 4-1. P는 연결선당 임의의 값 cj를 사용하여 $T_m = (b_{i,j})_m$의 행들을 다음과 같이 계산한다.

$$T_m' = (b_{i,j} \oplus c_j)_m \tag{10}$$

4-2. P는 치환 π를 사용하여 T_m'의 열들을 치환하여 다음과 같이 계산한다.

$$T_m'' = (b_{\pi(i),j} \oplus c_j)_m \tag{11}$$

4-3. P는 T_m''의 각 비트에 대해서 다음과 같이 계산한다. . T_m''= 0이면 r_1과 r_2를 랜덤하게 선택해서 y_1과 y_2를 랜덤한 순서로 V에게 보낸다.

$$y_1 = x_1 \cdot g^{r_1} \bmod p \tag{12}$$
$$y_2 = x_2 \cdot g^{r_2} \bmod p \tag{13}$$

. T_m''= 1이면 r_k(k = 0 혹은 1)와 w를 선택해서 y_1과 y_2을 V에게 보낸다.

$$y_1 = x_k \cdot g^{r_k} \bmod p \tag{14}$$
$$y_2 = g^w \bmod p \tag{15}$$

Move 5. V는 랜덤하게 도전 비트 b_m를 선택해서 P에게 보낸다.

Move 6-1. 만일 b_m = 0이면 P는 V에게 모든 commitment들을 오픈하고 모든 계산에 사용된 비트들 즉, cj를 오픈한다.

6-2. 만일 b_m = 1이면 P는 각 진리표 T_m''의 한 열에 대응하는 commitment들만 오픈한다.

Null Move. 만약 프로토콜 1이 성공적으로 수행됐다면, V는 P의 witness를 수락한다.

프로토콜 3은 6-move로 구성됐으나 이것을 4-move로 줄이기 위해서 위 프로토콜을 다음처럼 수정한다.

프로토콜 4. SAT 문제에 대한 지식의 완전 영지식 상호 증명. 이 프로토콜은 정확히 프로토콜 3처럼 수행한다. 그러나 6-move를 4-move로 재구성함에 따라 프로토콜 2와 프로토콜 1을 병렬로 수행한다.

Move 1. (1)
Move 2. (2,4)
Move 3. (3,5)
Move 4. (6)

정리 4.2. CDLA하에서 프로토콜 4는 SAT를 만족하는 satisfying assigment H에 대한 지식의 완전 영지식 상호 증명 방식이다.

〈 증 명 〉

1. 완전성: 정직한 P와 V는 항상 프로토콜을 성공적으로 수행한다.
2. 건전성: 평균 다항식 시간(expected polynomial time)내에 중지하는 지식 추출기 E와 이것이 SAT의 satisfying assignment H를 출력하는 확률은 P′(제 삼자 포함)가 정직한 V에게 H를 확신시킬 수 있는 확률과 같다 라는 것을 보여주면 된다.
   1) E는 랜덤하게 w_1과 w_2를 선택하고 $x_1 = g^{w_1} \bmod p$, $x_2 = g^{w_2} \bmod p$를 계산해서 x_1과 x_2를 랜덤 순서로 P′에게 보낸다. 이 후, E는 충실하게 V의 역할을 시뮬레이션함으로써 나머지 프로토콜(P′,V)을 수행한다.
   2) E는 반복적으로 P′를 프로토콜의 move 4로 리셋(reset) 시키고 새로운 랜덤 비트 $\{b_m\}$(move 5를 의미)를 선택한다. 그리고 P′가 이러한 랜덤 비트를 사용하여 성공적으로 프로토콜을 완성할때까지 반복한다.
   3) 두 개의 성공적인 수행에서, 만약 첫번째 진리표와 두번째 진리표가 move 4에서 일치하면(P′는 같은 방법 즉, 프로토콜을 따라서 commitment들을 오픈한다), E는 비밀 즉, satis-fying assigment H를 알 수 있다. 왜냐하면 move 6에서 E는 치환된 진리표와 각 행과 계산된 비트 값, 그리고 H를 만족하는 진리표의 치환된 열들을 동시에 알기 때문에 이러한 두 개의 성공적인 수행으로부터 H를 추출할 수 있다.
   4) 두 개의 성공적인 수행에서, 만약 첫번째 진리표와 두 번째 진리표가 move 4에서 다르다면(P′는 다른 방법 즉, 프로토콜과 다르게 commitment들을 오픈한다), 이것은 P′가 이미 w를 알고있다는것을 의미하므로 E는 이러한 두 개의 성공적인 수행으로부터 H를 알 수 있다.
   5) E는 H를 얻을 때까지 위의 과정을 반복한다.

건전성 증명에서 3)은 trapdoor 특성을 의미하는 것이고, 4)는 bit commit-ment의 건전성을 의미하는 것이다.

3. 영지식: 임의의 V′에 대해서 평균 다항식 시간내에 프로토콜의 view와 구별 할 수 없는 V′의 view를 생성할 수 있는 시뮬레이터 M을 구성한다. 시뮬레이터 M은 처음에 move 1~3에서 P의 역할을 수행한다.
   만일 V′가 성공적으로 이러한 서브 프로토콜을 완성시키지 못하면 M은 멈추고, 그렇지 않으면 M은 V′가 한번 더 자신의 도전 비트를 성공적으로 만족시킬 때까지 매번 다른 도전 비트를 사용하여 move 2를 반복 수행한다. 두 개의 성공적인 수행으로부터 M은 w를 발견할 수 있다. V′가 올바르게 대답할 수 있는 오직 한 세트의 도전 비트들이 있는 경우에 무한한 실행을 방지하기 위해서 M은은 스스로 소모적(exhaustive)탐색을 사용해서 w를 발견하기 위해 병렬로 계산한다.
   M이 w를 발견하면 M은 자기가 0 그리고 1로써 모두를 오픈할 수 있는 trapdoor commitment의 예들(instances)을 생성할 수 있다. 이 것은 M이 move 4~6에서 H를 몰라도 P의 역할을 수행하는 것을 허락하게 된다. 따라서 M이 생성한 view와 실제의 P와 수행했을 때 생성된 V′의 view는 완전한 구별이 불가능하다. 왜냐하면 프로토콜 2는 완전 WI하기 때문이다.

제안된 프로토콜 4는 Boyar와 Peralta의 "circuit-based proofs"방식을 사용하면 [6] 이 제안한 방식보다 계산량 및 통신량 측면에서 매우 효율적이다.[14] 즉, 통신량 측면에서 고찰해 보면 [6] 의 방식은 $CC_k(N) \in O(k \cdot N^2)$인데 반해 본 방식은 $CC_k(N) \in O(k \cdot N)$이 된다.

단, $CC_k(N)$: 영지식을 증명하는데 통신되는 비트의 수

N : SAT의 입력의 크기

계산량은 "commit"할 비트의 수가 (N+4S)/(N+13S)만큼 줄어들기 때문에(약 1/3) 계산량 측면에서도 효율적이다.(단, N은 입력들의 수이고 S는 게이트들의 수이다)그리고 [5] 의 방식은 "commit"할 비트의 수가 n^3(단,n은 입력의 크기)인데 반해, 본 방식은 $k \cdot n$에 비례한다.

Ⅴ. Claw free pairs of function을 이용한 4-move ZKIP

본 절에서는 claw free pairs of fuction을 이용하여 ZKIP의 최적 round를 5-move ZKIP에서 4-move ZKIP으로 구성해 보겠다. 증명자와 검증자의 계산 능력은 4장에서와 같으며, 영지식을 증명하기 위해서 같은 시뮬레이터를 사용하며, 기본 프로토콜으로 프로토콜 1을 사용한다.

프로토콜 5. P는 x_1 혹은 x_2 둘 중의 하나에 대한 평방근를 알고 있다는 사실을 증명하는 프로토콜이다.

공통 입력 : (N, x_1, x_2) 단, N :큰 두 소수의 곱

$$x_1 = w_1^2 \bmod N \quad (16)$$
$$x_2 = w_2^2 \bmod N \quad (17)$$

Move 1. P는 랜덤하게 그리고 독립적으로 r1,r2를 비밀리에 선택 하고 다음의 식을 계산한다.

$$y_1 = x_1 \cdot r_1^2 \bmod N \quad (18)$$
$$y_2 = x_2 \cdot r_2^2 \bmod N \quad (19)$$

P는 랜덤한 순서로 위의 값들을 V에게 보낸다.

Move 2. V는 랜덤 비트를 P에게 보낸다.

Move 3-1. 만일 P가 0을 받으면 P는 r_1과 r_2를 V에게 보낸다. 이 때 V는 y_1과 y_2가 올바르게 구성됐는 가를 검사한다.

$$(y = x \cdot r^2 \bmod N)$$

3-2. 만약 P가 1을 받으면, P는 y값들 중의 오직 하나에 대한 평방근$((w \cdot r) \bmod N)$을 V에게 보낸다. 이 때, V는 대응 되는 값을 검사한다.

관계 $R = \{(x,w)\}$가 주어졌을 때 다음의 조건을 만족하면 R^2이라 하자.

단, $(x_1, x_2, w) \in R^2$

조건) $(x_1, w) \in R$ 혹은 $(x_2, w) \in R$

R에 대한 생성기(generator) G가 주어진다면, G를 독립적으로 두 번 적용시킨 다음 두 개의witness 중 하나를 랜덤하게 버림으로써 R^2에 대한 생성기 G^2를 얻는다.[15] 따라서 다음과 같은 정리를 얻는다.

정리 5.1. 위의 프로토콜은 WH을 만족한다.

정리 5.1의 증명은 참고문헌 [6] 의 증명과 유사하다.

최종적으로 4-move ZKIP을 구성해본다. 우선 6-move ZKIP을 구성하고 다음에 이 프로토콜을 이용하여 4-move ZKIP이 성립됨을 보이겠다.

프로토콜 6. SAT 문제에 대한 지식의 완전 영지식 상호 증명. 프로토콜 6은 프로토콜 1과 프로토콜 5의 순차적 합성이다.

공통 입력 : Boolean formula Ψ

P의 witness: satisfying assigment H

Move 1~3. 프로토콜 3과 같다.

Move 4~6. P와 V는 공통 입력 Ψ를 가지고 프로토콜 1의 병렬 합성을 수행한다. 이 때, P의 비밀 입력은 H이다.

bit-commitment로서 P는 입력으로 Ψ를 사용하여 프로토콜 2의 절차를 사용한다.

Move 4-1. 프로토콜 3과 같다.

4-2. 프로토콜 3과 같다.

4-3. P는 T_m''의 각 비트에 대해서 다음과 같이 계산한다.

.T_m''= 0이면 r_1과 r_2를 랜덤하게 선택해서 y_1과 y_2를 랜덤한 순서로 V에게 보낸다.

$y_1 = x_1 \cdot r_1^2 \bmod N$ (20)
$y_2 = x_2 \cdot r_2^2 \bmod N$ (21)

$T_m'' = 1$이면 r_k (k = 0 혹은 1)와 w를 선택해서 y_1과 y_2를 V에게 보낸다.

$y_1 = x_k \cdot r_k^2 \bmod N$ (22)
$y_2 = w^2 \bmod N$ (23)

Move 5. V는 랜덤하게 도전 비트 b_m을 선택해서 P에게 보낸다.

Move 6-1. 만일 $b_m = 0$이면, P는 V에게 모든 commitment를 오픈 하고 모든 계산에 사용된 비트들 즉, c_i를 오픈한다.

6-2. 만일 $b_m = 1$이면, P는 각 진리표 T_m''의 한 열에 대응하는 commitment만 오픈한다.

Null Move: 만약 프로토콜 1이 성공적으로 수행됐다면, V는 P의 witness를 수락한다.

프로토콜 6은 6-move로 구성됐으나 이것을 4 move로 줄이기 위해서 위 프로토콜을 다음과 같이 수정한다.

프로토콜 7. SAT 문제에 대한 지식의 완전 영지식 상호 증명. 이 프로토콜은 정확히 프로토콜 6처럼 수행한다. 그러나 6-move를 4-move로 재구성함으로써 프로토콜 5와 프로토콜 1을 병렬로 수행한다.

Move 1. (1)
Move 2. (2,4)
Move 3. (3,5)
Move 4. (6)

정리 5.2. Claw free pairs of fuction을 이용한 프로토콜 6는 SAT를만족하는 satisfying assigment H에 대한 지식의 완전 영지식 상호 증명 방식이다.

〈 증 명 〉

4 장에서의 증명 방법과 유사하다. 그러나 영지식을 간단히 살펴보면, 생성되어진 view는 실제의 P와 수행했을 때 생성된 V′의 view와 완전하게 구별 불가능하다. 왜냐하면 프로토콜 5는 완전 WI하기 때문이다.

Ⅵ. 응 용

이 장에서는 수동적 공격하에서 안전하고, 메세지와 서명(signature) 두 쌍의 데이타가 오직 공개키를 사용했을 때 균일하게 분포되는 임의의 디지탈 서명 방식을 사용한 개인식별 방식을 구성해보자. 예로써 RSA 방식은 수동적 공격에 대해서 안전하고 데이타가 균일하게 분포되는 디지탈 서명 방식이다. 왜냐하면 균일하게 s를 선택해서 $m = s^e \bmod n$와 같이 계산함으로써 (m,s)는 균일하게 생성되기 때문이다. (단, m: 메세지, s: m의 서명, (e,n) : 공개키) 다음과 같이 개인식별 방식을 구성해 본다.

프로토콜 8 : 개인식별 방식

step 1. (키 생성과 등록)

1-1. 먼저 위의 디지탈 서명 방식의 존재를 가정한다.

1-2. P는 비밀키 a_p와 공개키 b_p를 생성하고 자신의 이름과 함께 공개키를 공표한다.

1-3. 서명 방식의 메세지 크기는 t로 한다.

1-4. 이 step은 P가 개인식별 방식에 참여할 때만 행한다.

1-5. 공통입력 : (p,g,c,y) 단, $y = g^s \bmod p$, s : P의 witness

step 2. V는 비밀리에 랜덤하게 w_1과 w_2를 선택해서 다음을 P에게 보낸다.

$x_1 = g^{w1} \bmod p$ (24)
$x_2 = g^{w2} \bmod p$ (25)

V는 t_1, t_2를 선택해서 다음처럼 계산하고, 랜덤 순서로 P에게 보낸다

$c_1 = x_1 g^{t1}$ (26)
$c_2 = x_2 g^{t2}$ (27)
V -〉 P : (x_1, x_2), c_1, c_2

step 3. P는 랜덤 비트 b와 e_s, r_1, r_2, w를 선택하고, 다음을 계산한다.

$$BC(e_s, r_1, r_2) = \begin{cases} y_1 = w_1 g^{r_1}, y_2 = w_2 g^{r_2} & if\ e_s = 0 \\ y_1 = w_k g^{r_k}, y_2 = g^w & if\ e_s = 1 \end{cases} \quad (28)$$

단, k는 1 혹은 2

P는 랜덤 스트링 v_i를 선택해서, 다음을 계산한다.

$Z = g^{vi} \bmod p$ (29)

P -> V : b, BC(e_s,r_1,r_2), Z

step 4. V는 P에게 다음을 보낸다.

만일 b = 0이면, t_1 ,t_2를 보낸다.

만일 b = 1이면, c의 이산대수 값중의 하나(w+t)를 보낸다.

V는 e_{ri}를 랜덤하게 선택해서 보낸다.

V -> P : (t_1, t_2) 혹은 (w+t), e_{ri}

step 5. P는 c_1, c_2를 검사한다.

P는 n 개의 비트 스트링 m = ($e_{s1} \oplus e_{r1} \cdots e_{sn}$ e_{sn})을 계산 하고, P는 자신의 비밀키 a_p를 사용해서 m에 대한 자신의

서명 s을 생성한다.

P는 다음을 계산해서 보낸다.

$$d_i = \begin{cases} v \bmod p & if\ e_{si} + e_{ri} = 0 \bmod 2 \\ v + s \bmod p & if\ e_{si} + e_{ri} = 1 \bmod 2 \end{cases} \qquad (30)$$

$$P \rightarrow V: m, s, d_i$$

step 6. V는 d_i를 검사하고, P의 공개키 b_p를 사용해서 s가 m의 타당한서명인지를 검사한다.

정리 6.1 : 위의 개인식별 방식은 영지식을 만족한다.

위의 개인식별 방식에 대한 증명은 정리 4.2, 5.2의 증명과 유사하다. 일반적으로 선택 암호문 공격에 대한 안전성을 얻기 위한 중요한 도구로 ZKIP 방식을 사용한다. 즉, 만약 f_i가 일방향 함수이고 y는 둘 다에게 알려진 어떤 값이라 한다면, 증명자는 검증자에게 자신은 y의 pre-image 즉, 관계 $f_i(x) = y$를 만족시키는 x를 알고 있다는 사실을 x와 관련된 정보는 누설시키지 않고 확신시킬 수 있는 특성때문에 ZKIP 방식이 사용된다. 따라서 프로토콜 8은 영지식을 만족하므로 선택 암호문 공격에 안전하며, 최적 round방식이므로 효율적이다. 또한 위 방식을 이용하여 선택 암호문 공격에 안전하고, 효율적인 메세지 인증 방식을 구성할 수 있다.

Ⅶ. 결 론

본 논문에서는 constant round ZKIP 방식에서 필수적인 bit-commitment 방식에 대해서 고찰하였으며, 임의의 프로토콜의 병렬 합성시에도 안전한 특성을 유지하는 WI와 WH를 이용하여 SAT 문제에 대한 지식의 완전 영지식 상호 증명 방식을 최적 round인 4-move ZKIP으로 제안하였으며, 또한 claw-free pairs of function 하에서 5-move ZKIP을 같은 함수하에서 WI와 WH를 이용하여 4-move ZKIP으로 제안하였다. 제안한 방식은 참고문헌 [5] , [6] 그리고 [8] 이 제안한 방식보다 계산량 및 통신량 측면에서 매우 효율적임을 알 수 있다. 즉, 통신량 측면에서 고찰해 보면 [6] 의 방식은 $CC_k(N) \in O(k \cdot N^2)$인데 반해, 본 방식은 $CC_k(N) \in O(k \cdot N)$이 된다.

또한, 본 논문에서 제안한 최적의 4-move ZKIP을 이용하여 효율적이고, 선택 암호문 공격에 안전한 개인식별 방식을 구성하였다.

參 考 文 獻

[1] S. Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proof Systems," The 17th ACM STOC, pp.291-304, 1985.

[2] O. Goldreich,S. Micali, and A. Wigderson, "Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero Knowledge Proofs," Tech. Rep.#544,Israel Institute of Technology,Department of Computer Science (Mar. 1989).

[3] 양형규,권창영,원동호, "ZKIP의 round complexity와 응용프로토콜에 관한 연구," 데이타 보호 기반 기술 WORKSHOP 논문집 pp.193-217, 1992.

[4] O. Goldreich and H. Krawczyk, "On the composition of Zero Knowledge Proof Systems," Proc. of ICALP'90 pp. 268-282, 1990.

[5] G. Brassard,C. Crepeau, and M. Yung, "Everything in NP Can Be Argued in Perfect Zero knowledge in a Bounded Number of Rounds," Proc. of ICALP '89 pp.123-136, 1989.

[6] U. Feige and A.Shamir, "Zero Knowledge Proofs of Knowledge in Two Rounds," CRYPTO' 89 pp.526-544, 1989

[7] M. Bellare,S. Micali, and R. Ostrovsky, "Perfect Zero Knowledge in

constant Rounds," The 21th ACM STOC pp.482-493, 1990.
[8] G. Brassard, D. Chaum, and C. Crepeau. "Minimum Disclosure Proofs of Knowledge," JCSS, vol.37, no.2, pp. 156-189, 1988.
[9] G. Brassard and M. Yung. "One-Way Group Actions." CRYPTO '90 pp.85-98, 1990.
[10] M. Tompa and H. Woll. "Random Self-Reducibility and Zero Knowledge Interactive Proofs of Possession of Information," The 31th IEEE FOCS pp. 472-482, 1987.
[11] U. Feige, A. Fiat, and A. Shamir. "Zero knowledge Proofs of identity," The 19th ACM STOC pp.210-217, 1988.
[12] O. Goldreich and Y. Oren. "Definitions and Properties of Zero Knowledge Proof Systems," Tech. Rep.#610, Israel Institute of Technology, Department of Computer Science (Feb. 1990).
[13] V. Pratt. "Every prim has a succint certificate," SIAM J. Computing pp. 214-220, 1975.
[14] J. Boyar and R. Peralta. "On the Concrete Complexity of Zero-Knowledge Proofs," CRYPTO' 89 pp.507-525, 1989
[15] U. Feige and A. Shamir. "Witness Indistingushable and Witness Hiding Protocols," The 21th ACM STOC pp. 416-426, 1990.

著者紹介

梁 亨 圭(正會員)
1983年 성균관 대학교 전자공학과 졸업 (공학사). 1985年 성균관 대학교 대학원 전자공학과 졸업 (공학석사). 1991年~현재 성균관 대학교 대학원 정보공학과 박사과정 재학중. 1985年~1991年까지 삼성전자 선임 연구원.

李 仁 淑(正會員)
1979年 이화여자대학교 수학과 졸업(이학사). 1985年 이화여자대학교 대학원 수학과 졸업(이학석사). 1979年~1984年 한국전자통신 연구소 연구원. 1991年~현재 성균관 대학교 대학원 정보공학과 박사과정 재학중. 1984年~현재 한국통신 통신망연구소 선임연구원.

元 東 豪(正會員)
1976年 성균관 대학교 전자공학과 졸업 (공학사). 1978年 성균관 대학교 대학원 전자공학과 졸업 (공학석사). 1988年 성균관 대학교 대학원 전자공학과 졸업 (공학박사). 1978年~1980年 한국전자통신연구소 연구원. 1985年~1986年 일본 동경공대 객원연구원. 1982年~현재 성균관 대학교 정보공학과 조교수, 부교수, 교수.