# 영지식증명을 이용한 키분배방식에 관한 연구

이윤호, 양형규, 장청룡, 원동호

성균관대학교 정보공학과

# A Study on the Key Distribution System based on the Zero-Knowledge Proof

Yun-Ho Lee, Hyung-Kyu Yang, Chung-Ryong Chang, Dong-Ho Won

SUNG KYUN KWAN UNIVERSITY

Department of Information Engineering

## 요 약

Fiat, Shamir의 ZKIP(zero knowledge interactive proofs) 방식[1]을 이용한 새로운 키분배방식을 제안한다. 본 방식은 평방잉여를 이용한 Fiat, Shamir의 ZKIP 방식을 이용하여 상호인증을 행하고 그 과정에서 교환되는 데이타를 사용하여 비밀통신용 공통키를 생성한다. 공통키생성 과정에 사용된 데이타가 인증 과정에서 사용된 데이타이고, 인증과정은 ZKIP 방식을 이용했으므로 제안한 키분배방식 역시 zero knowledge일 것으로 생각되며 ZKIP 방식은 인증 과정의 반복으로 인한 통신량이 많은 반면 제안한 방식은 인증과정에서의 반복횟수가 1이기 때문에 상대적으로 통신량이 적은 이점이 있다.

## 1. 서 론

급속한 컴퓨터기술의 발달과 사회 전반에 걸쳐 컴퓨터의 중요성이 증대됨에 따라 현

대사회는 고도 정보화사회로 접어들고 있다. 이로 인한 컴퓨터 통신망 가입자의 증가와 종합적인 정보시스템의 보급 확대로 통신망 가입자의 프라이버시 침해와 시스템 내에서 처리되는 중요 정보의 유출에 대한 우려가 높아지고 있어 이에 대한 대책 마련이 시급히 요구되고 있다.

컴퓨터 통신망에서 각 가입자의 프라이버시와 중요 정보 보호를 위한 가장 효율적이면서도 경제적인 방법으로 암호기법을 들 수 있다. 암호기법은 양 가입자 사이에 공통으로 소유해야 하는 암호키를 관리하는 것으로 볼 수 있는데 이러한 암호키 관리중에서도 가장 문제가 되는 것이 가입자들 간에 안전하게 암호키를 분배하는 것이다. 이와 함께 통신망 가입자간의 상호 인증 문제와 통신망으로의 불법적인 엑세스를 막기위한 사용자 인증 문제도 해결해야 할 중요한 과제이다.

상호 인증과 사용자 인증을 하는데 가장 안전하고 활발히 연구되고 있는 방법이 1985년 Goldwasser, Micali, Rackoff가 제안한 ZKIP 방식이다.[2] ZKIP이란 증명자(prover)가 검증자(verifier)에게 자신의 신분(identity)을 증명함에 있어서 불법적인 제삼자는 물론이고 검증자에게 조차도 증명의 타당성 이외에는 다른 어떤 정보도 유출시키지 않는 증명방법을 말한다.

또한 키분배방식에서도 1976년 Diffie, Hellman이 새로운 키분배방식[3]을 제안한 이래 1984년 Shamir가 제안한 ID(identification) 기반의 키분배방식에 이르기까지 보다 안전한 키분배방식을 위한 연구와 함께 이들 키분배방식의 안전성에 관한 연구도 활발히 진행되고 있다.

본 논문에서는 ZKIP 방식의 안전성을 이용하여 키분배에 ZKIP을 적용한 새로운 zero knowledge 키분배방식을 제안한다.

## 2. ZKIP 이론

1985년 Goldwasser, Micali, Rackoff가 ZKIP 개념을 발표하면서 시작된 ZKIP 이론은 증명자가 검증자에게 자신을 증명함에 있어서 증명의 타당성 이외의 어떠한 정보도 유출시키지 않는다는 것으로, 상대방인증 방식에 있어서 가히 혁신적인 것이었다.

이 후 많은 ZKIP 방식들이 발표되었으며 이러한 방식들은 P ≠ NP라는 가정하에 NP에 속하는 언어(language)들을 이용하여 상대방 인증을 행하는데, NP에 속하는 모든 언어

는 ZKIP에 이용될 수 있음을 Goldreich, Micali, Wigderson이 확인하였다.[4] 이러한 NP에 속하는 언어들로는 그래프 동형 문제(graph isomorphism), 그래프 비동형 문제(graph non-isomorphism), 만족도 문제(satisfiability)와 본 논문에서 제안한 방식에 이용한 평방잉여 문제(quadratic residue) 등이 있다.

ZKIP의 zero knowledge를 명확히 정의하기 위해서는 view라는 개념을 도입해야 한다. View는 검증자가 증명자로부터 받은 전송 데이타와 검증자 자신이 발생시킨 난수로 구성되며, 모든 다항식시간 검증자(polynomial time bounded verifier)에 대해서 증명자와의 통신 없이도 증명자와 검증자와의 상호통신 동안 만들어진 view를 똑같이 생성할 수 있는 다항식시간 시뮬레이터(simulator)가 존재한다면 그 프로토콜은 완전영지식(perfect zero knowledge)이라고 한다. 영지식에는 이러한 완전영지식과 함께 계산영지식(computational zero knowledge)이 있는데 이는 시뮬레이터가 만들어 낸 view와 실제 통신 동안 만들어진 view와의 구별이 다항식시간내에 불가능한(polynomially indistinguishable) 경우이다.

## 3. Fiat, Shamir의 ZKIP 방식

1986년 Fiat와 Shamir는 ZKIP의 개념과 Shamir 자신이 제안한 ID 개념을 이용하여 새로운 ZKIP 방식을 제안하였다. 이 방식은 충분히 큰 두 소수 p, q의 곱으로 이루어진 합성수 n을 modulus로 하는 법연산에서 n의 소인수분해를 모를 때, 제곱근(square root)을 찾는 문제는 어려운 문제(NP 문제)라는 점을 이용한 것으로 그 프로토콜은 아래와 같다.

(사전 준비 과정)

신뢰할만한 센터(center)는 가입자에게 카드를 발급하기 전에 modulus n과 임의의 string을 [0 , n)으로 대응시키는 pseudo random function f를 선택하고 이를 공개한다. 여기서 n은 충분히 큰 두 소수 p, q의 곱이며, 이 p, q는 센터만이 아는 비밀정보이다.

(카드발급 과정)

합법적인 사용자에게 카드를 발급할 때 센터는 그 사용자에 관한 정보(이름, ID 번호, 주소, 주민등록번호 등)와 카드에 관한 정보(유효기간 등)를 담고 있는 I를 준비하

고 아래의 과정을 수행한다.

1) $v_j = f(I, j)$ $(j = 1,\ldots,m)$ 을 구한다.

2) 이 중에서 k개의 평방잉여를 골라 각각의 $v_j^{-1}$의 가장 작은 제곱근 $s_j$를 mod n 상에서 계산한다.

3) I와 k개의 $s_j$, 그리고 각각의 j값을 카드에 담아 사용자에게 발급한다.

(인증과정)

| 증명자(A) | | 검증자(B) |
|---|---|---|
| 자신의 I와 k를 전송한다. | $\xrightarrow{I,\ k}$ | $v_j = f(I, j)$ $(j = 1,\ldots,k)$를 계산한다. |
| - 다음의 과정을 t회 반복한다. $(i = 1,\ldots,t)$ | | |
| 임의의 난수 $r_i$를 선택해서 $x_i = r_i^2 \bmod n$을 전송한다. | $\xrightarrow{x_i}$ | k개의 random binary vector $e_i = (e_{i1}, e_{i2},\ldots,e_{ik})$를 전송한다. |
| $y_i = r_i \prod_{e_{ij}=1} s_j \bmod n$를 계산해서 전송한다. | $\xrightarrow{y_i}$ | $x_i = y_i^2 \prod_{e_{ij}=1} v_j \bmod n$ 인지를 검사한다. |

위의 프로토콜로부터 다음을 알 수 있다.

1) B는 A의 비밀정보 $s_j$ $(j = 1,\ldots,k)$에 관한 어떠한 정보도 얻을 수 없다.

2) polynomial time내에 평방잉여인 어떤 수의 제곱근을 구할 수 없는 임의의 증명자 A'는 $2^{-kt}$의 확률로 B에게 자신이 A인 것처럼 증명할 수 있다. 그러나 이 확률은 매우 작은 확률이다.

3) 임의의 제삼자 C는 A에서 B로 가는 어떠한 전송데이타에서도 증명자 A의 비밀정보인 $s_j$를 알아낼 수 없다.

4) 위의 방식은 zero knowledge이다.[1)]

따라서 $y_i$는 검증자 B의 coin toss에 대해 증명자 A만이 만들 수 있는 인증된 전송데이타이며 또한 이 $y_i$로부터 제삼자 및 B는 증명자에 대한 어떠한 정보도 얻지 못함을 알 수 있다. 본 논문에서 제안한 키분배방식에서는 이 인증된 데이타 $y_i$를 키분배에 이

용한다.

# 4. 제안한 Zero Knowledge 키분배방식

ZKIP을 이용한 키분배방식으로는 1989년 Fritz Bauspieß가 제안한 방식이 있다.[5] 이 방식은 1988년 Beth가 제안한 ZKIP 방식[6]을 키분배에 이용한 것으로 이산대수의 어려움을 이용했다. Beth의 ZKIP 방식을 보면 Diffie-Hellman이 최초로 제안한 키분배방식에서 발생되는 키와 거의 비슷한 부분이 있으며, Fritz Bauspieß는 이를 이용해서 Diffie-Hellman 방식과 비슷한 zero knowledge 키분배방식을 제안했다.

이 방식에서 인증과정 이외에 공통키생성시 한 번의 통신이 더 필요한 점은 제안한 방식과 마찬가지이지만 Bauspieß의 방식에서는 양 가입자 모두에게 두 개의 키가 생성되며, 키의 인증을 위해 두 번의 통신을 통한 확인과정을 거쳐야 하는 단점이 있으나 제안한 방식에서는 이러한 과정이 필요 없으며 Bauspieß의 키분배방식이 이산대수의 어려움에 근거한 반면 제안한 키분배방식은 평방잉여 문제의 어려움을 이용했다.

위의 Fiat, Shamir의 ZKIP 방식에서 반복횟수 t가 1인 경우를 생각해 보자. 먼저 센터는 f함수를 가입자의 ID에 적용한 결과가 평방잉여인 하나의 k개의 $v_i(i = 1,\ldots,k)$를 찾아서 그에 해당하는 가장 작은 $sqrt(v_i^{-1})$를 구한다.

양자간에 공통키를 생성하기 위해서는 서로를 인증해야 하며 따라서 인증방식은 상호대칭적(symmetric)으로 진행되어야 한다.

다음이 키분배에 Fiat, Shamir의 ZKIP을 이용한 새로운 키분배방식이다.

## 4.1 사전 준비 과정

신뢰할만한 센터는 modulus n과 임의의 string을 [0 , n)의 범위로 대응시키는 일방향 함수(oneway function) f를 정하고 이를 공개한다. 여기서 n은 충분히 큰 두 소수 p, q의 곱으로 이루어지며, p와 q는 센터의 비밀 정보이다.

## 4.2 가입자 등록 과정

가입자 B가 등록을 요청했을 때 센터는 가입자의 신분을 확인한 후 가입자 고유의 정보 $I_B$를 이용해서 다음의 과정을 수행한다.

1) $v_j = f(I_B, j)$ $(j = 1,\ldots,m)$을 구하고, 이 중에서 평방잉여가 되는 $v_j$를 k개 찾고 각각의 가장 작은 $s_j = \mathrm{sqrt}(v_j^{-1})$를 구한다.

2) $I_B$와 함께 k개의 $s_j$ 및 각 $s_j$의 j값을 B에게 전송한다.

### 4.3 통신 과정

아래의 사용자 인증 및 공통키의 생성을 위해 필요한 프로토콜은 사용자 A, B간에 서로 대칭적으로 진행된다. 편의상 k개의 j를 $i = 1,\ldots,k$로 나타낸다.

1) 인증 과정 (authentication phase)

| 사용자 A | | 사용자 B |
|---|---|---|
| 자신의 $I_A$와 k를 전송. | $\xleftarrow{I_A}$ | 자신의 $I_A$와 k를 전송. |
| $v_{Bi} = f(I_B, i)(i=1,\ldots,k)$. | $\xrightarrow{I_B}$ | $v_{Ai} = f(I_A, i)(i=1,\ldots,k)$. |
| 난수 $r_A \in (1,N)$를 선택하고 | | 난수 $r_B \in (1,N)$를 선택하고 |
| $x_A = r_A^2 \bmod n$ 계산. | $\xleftarrow{x_A}$ | $x_B = r_B^2 \bmod n$ 계산. |
| 임의의 k개의 비트 $R_{Ai}$를 | $\xrightarrow{x_B}$ | 임의의 k개의 비트 $R_{Bi}$를 |
| 택해서 전송. | $\xleftarrow{R_{Ai}(i=1,\ldots k)}$ | 택해서 전송. |
| $y_A = r_A \prod_{R_{Bi}=1} s_{Ai} \bmod n$ | $\xrightarrow{R_{Bi}(i=1,\ldots k)}$ | $y_B = r_B \prod_{R_{Ai}=1} s_{Bi} \bmod n$ |
| 을 계산해서 전송. | $\xleftarrow{y_A}$ | 을 계산해서 전송. |
| | $\xrightarrow{y_B}$ | |

A 측에서의 검증 과정

$x_B = y_B^2 \prod_{R_{Ai}=1} v_{Bi} \bmod n$ 인지를 검사한다.

B 측에서의 검증 과정

$x_A = y_A^2 \prod_{R_{Bi}=1} v_{Ai} \bmod n$ 인지를 검사한다.

2) 공통키 생성 과정 (common key generation phase)

편의상 아래의 정의를 이용한다.

$$\prod_{R_{Bi}=1} s_{Ai} \bmod n = S_A, \qquad \prod_{R_{Ai}=1} s_{Bi} \bmod n = S_B$$

사용자 A　　사용자 B

난수 $z_A \in (1,n)$를 선택.　　난수 $z_B \in (1,n)$를 선택.

$t_A = \left(\frac{r_A \cdot x_B}{y_B} + S_A\right) \cdot z_A$　　$t_B = \left(\frac{r_B \cdot x_A}{y_A} + S_B\right) \cdot z_B$

$t_A \longrightarrow$

$\longleftarrow t_B$

A 측에서 키 $K_A$를 생성하는 과정

$$K_A = t_B \cdot S_A \cdot z_A$$
$$= ((r_A \cdot r_B) / S_A + S_B) \cdot z_A \cdot S_A \cdot z_B$$
$$= (r_A \cdot r_B + S_A \cdot S_B) \cdot z_A \cdot z_B \bmod n$$

B 측에서 키 $K_B$를 생성하는 과정

$$K_B = t_A \cdot S_B \cdot z_B$$
$$= ((r_B \cdot r_A) / S_B + S_A) \cdot z_B \cdot S_B \cdot z_A$$
$$= (r_B \cdot r_A + S_B \cdot S_A) \cdot z_B \cdot z_A \bmod n$$

# 5. 안전성의 검토

## 5.1 인증과정에서의 안전성

제안한 키분배방식의 인증과정은 Fiat, Shamir의 ZKIP방식에서 반복 횟수인 t가 1인 특수한 경우이다. 따라서 제안한 인증과정의 안전성은 임의의 비트열 $R_{Ai}$, $R_{Bi}$ (i = 1,...k)에 의해 좌우된다. 보통 $2^{-20}$ 정도의 확률로 불법인증이 가능하다면 안전하다고 볼 수 있기 때문에 반복 횟수가 1인 본 인증과정에서는 t가 20이상이어야 한다. Fiat, Shamir의 ZKIP방식에서와 마찬가지로 임의의 사용자 C가 A인 척 하려면 B로부터 전송되는 $R_{Bi}$를 받기 전에 이 $R_{Bi}$를 정확히 예측해서 변형된 $x_A'$를 전송해야 하는데 k = 20일 경우, 이 확률은 $2^{-20}$이 된다.

또한 제안한 인증과정이 대칭적으로 진행되기는 하나, A가 B를 인증하는 경우와 B가 A를 인증하는 경우는 서로 독립적이기 때문에 인증과정이 대칭적으로 진행된다 해도 문제점은 없다고 할 수 있다.

## 5.2 평방잉여를 이용한 키분배방식에서의 전송정보

위의 방식은 크게 인증 과정과 공통키생성 과정으로 나누어 생각할 수 있다. 인증 과정에서 사용된 방식은 이미 zero knowledge임이 증명되었으므로, 문제될 수 있는 것은 공통키생성 과정이다. 따라서 이 부분이 안전함을 보이는 것은 곧 제안한 zero knowledge 키분배방식이 안전함을 보이는 것과 같게 된다.

평방잉여를 이용한 키분배방식에서는 제곱의 형태는 알려져 있지만 modulus n의 소인수분해 p, q를 알지 못하면 그 제곱근을 구하는 것은 어렵다는 점을 이용하여 상대방 인증과 키분배를 행한다. 다음은 평방잉여를 이용한 zero knowledge 키분배방식에서 전송되는 데이타의 안전성을 고찰한 것이다.

정의) C : 누구에게나 알려져 있는 값. (예 : $x_A$와 같은 전송데이타 및 공개정보)

K : 제곱의 형태만이 알려져 있는 값. (예 : $S_B$, $r_B$는 알려지지 않았으나 $S_B^2$인 $v_B$와 $r_B^2$인 $x_B$는 알려진 것과 같은 경우)

U : 누구에게도 알려져 있지 않은 값. (예 : 위의 프로토콜에서 $z_A$, $z_B$가 이에 해당되며 이는 자신만이 아는 난수이다.)

아래의 전송정보 형태를 고려해보자.

1) $C_1 = K_1 + K_2 \cdot C_2$

2) $C_1 = K_1 \cdot K_2$

3) $C_1 = (K_1 \cdot C_2 + K_2) \cdot U_1$

1) 의 경우는 아래와 같은 방법으로 $C_1$과 $C_2$로부터 $K_1$과 $K_2$를 쉽게 구할 수 있다.

$$K_1 = (C_1^2 + K_1^2 - (K_2 \cdot C_2)^2) \; / \; 2 \cdot C_1$$

이로부터 $K_2$도 쉽게 구할 수 있다. 즉 직접적으로 제곱근을 구하지 못한다하더라도 $K_1, K_2$를 구하는 것이 가능하다. 따라서 이러한 형태의 전송데이타는 적합하지 못하다.

2) 의 경우는 $C_1$으로부터 $K_1$이나 $K_2$를 구하는 것은 불가능하다. 이 경우 알려질 수 있는 형태는 $K_1 / K_2$, $K_2 / K_1$ 등이 있다. 이러한 형태의 전송데이타는 인증과정에서 사용된 것으로 $y_A$ 및 $y_B$가 이에 해당된다. 따라서 $y_A$ 나 $y_B$로부터 $r_A$와 $S_A$ 혹은 $r_B$와 $S_B$를 분리하는 것은 불가능하다.

3) 의 형태가 제안한 프로토콜의 공통키 생성과정에서 이용된 것이다. 이 형태의 전송데이타에서 1)과 다른 점은 발생자 이외의 누구에게도 알려지지 않은 난수 $U_1$이 첨가되었다는 것이며, 이로 인해서 전송데이타 $(K_1 \cdot C_2 + K_2)$가 감춰진다.

제안한 키분배방식의 공통키 생성과정에서는 키생성을 위해 한 번의 통신을 더 행하

는데, 문제가 되는 것은 이 첨가된 과정에서 유출되는 정보가 있는가 하는 점이다. 그러나 2)의 전송정보 형태와 비교해 볼 때 3)의 형태 역시 안전할 것으로 생각되며 따라서 유출되는 정보도 없을 것으로 생각된다.

### 5.3 Known Key Attack하에서의 안전성

공통키를 생성하기 위해 필요한 factor 들을 살펴보면 고정되어 있는 것은 아무것도 없다. $r_A$, $r_B$, $z_A$, $z_B$ 모두 매번 통신할 때 마다 바뀌는 난수이고, $S_A$, $S_B$ 역시 k개의 $R_{Ai}$, $R_{Bi}$에 의해 매번 바뀌게 된다. 따라서 과거의 공통키가 알려졌더라도 공통키 자체가 임의의 수들의 곱이므로 현재의 공통키를 구하는데 아무런 도움이 안된다. 따라서 제안한 방식은 known key attack하에서도 안전할 것으로 생각된다.

## 6. 결론

제안한 키분배방식은 Fiat, Shamir의 ZKIP 방식을 이용한 인증과정에서의 데이타를 이용해 키분배를 행하는 것이다. 따라서 제안한 키분배방식 역시 zero knowledge일 것으로 생각되며 인증과정에서의 전송데이타를 이용해서 키분배를 하여도 첨가된 것은 임의의 난수뿐이기 때문에 공통키생성 과정에서 역시 누출되는 정보는 없을 것이다.

본 방식을 이용했을 경우, 기존의 키분배방식보다 안전함은 물론이고 효율적일 것으로 생각되며 ZKIP 방식이 통신량이 많은 반면, 제안한 방식은 반복함이 없이 단 한번씩에 전송이 되므로 실제로 응용할 때 통신량의 부담없이 사용될 수 있을 것이다. 단지 센터가 각 사용자의 비밀정보를 모두 알고 있기 때문에 당연한 말이지만 센터는 신뢰할 만 해야 한다. 그러나 이러한 경우는 실제의 통신에 있어서 극히 드문 경우이기 때문에 문제될 것은 없을 것이다.

## 7. 참고 문헌

1. A. Fiat, A. Shamir, "How to Prove Yourself : Practical Solutions to

Identification and Signature Problems", Proc. Crypto'86, pp. 186-194, 1986.

2. S. Goldwasser, S. Micali, C. Rackoff, "Knowledge Complexity of Interactive Proofs", Proc. 17th STOC, 1985, pp. 291-304.
3. W. Diffie, M.E. Hellman, "New Directions in Cryptography", IEEE Trans. IT-22, No. 6, pp. 644-654, 1976.
4. O. Goldreich, S. Micali, A. Wigderson, "Proofs that Yield Nothing But their Validity", Proc. Crypto'86, pp.171-185, 1986.
5. F. Bauspieß, "How to Keep Authenticity Alive in a Computer Network", Eurocrypt'89, 1989.
6. Th. Beth "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Proc. Eurocrypt'88, pp. 77-84, 1988.