ElGamal 암호알고리듬을 이용한 메세지 전송 영지식 증명 방식

*엄화영, 0염흥열, *이만영

*한양대학교 전자통신공학과, 0순천향대학교 전자공학과

Message Sending Zero-Knowledge Interactive Proof System Using ElGamal Cryptographic Algorithm

*Hwa Young UM, 0Heung Youl YOUM, *Man Young RHEE

*Dept. of Electronic communication Eng. Hanyang Univ.

0Dept. of Electronics Eng. Sooncheonhyang Univ.

요약

영지식 대화증명은 인증자(prover)가 비밀정보를 노출시키지 않으면서, 검증자(verifier)와 대화를 통해서 이 비밀정보을 알고 있음을 검증자에게 증명하는 방법이다. 본 논문에서는 ElGamal 암호 알고리듬을 이용하여 메세지 전송과 개인 인증이 동시에 가능한 순방향 영지식 증명 프로토콜과 역방향 영지식 증명 프로토콜을 제안한다. 그리고 전송효율을 송신한 전비트와 정보비트와의 비로 정의하여 각각의 프로토콜의 전송효율을 계산한다.

1. 서론

영지식 대화증명(zero-knowledge interactive proof)은 1985년 개념이 제안된 이래 계산량이론, 암호이론의 발전에 있어서 중요한 역할을 담당하였다. 영지식 대화증명은 인증자(prover)가 비밀정보를 노출시키지 않으면서, 검증자(verifier)와 대화를 통해서 이 비밀정보을 알고 있음을 검증자에게 증명하는 방법이다. 영지식 대화증명은 영

지식 대화증명을 구성할 수 있는 문제의 범위를 특징 짓는 방향으로 이론적인 연구가 진행되어, 최근에는 다항식 영역에서 표현 가능한 문제는 대화증명으로 증명할 수 있다고 최종적으로 결론지어졌다.[1][2]

한편, 응용면에서는 개인인증 프로토콜을 중심으로 발전하였다. 메세지 전송 프로토콜에 대한 연구가 미흡했으나 1987년 Desmedt, Goutier 그리고 Bengio(DGB)는 FS(Fiat-Shamir) 기법을 기반으로 하여 메세지 전송이 가능한 프로토콜을 제안하였다.

본 논문에서는 2절에서 FS 기법을 제시하고 3절에서 DGB 기법을 분석하여, 4절에서 FS기법과 DGB 기법을 결합한 개량된 DGB기법을 상세히 설명한다. 그리고 5절에서는 ElGamal 암호알고리듬을 이용하여 메세지 전송이 가능한 순방향 영지식 증명 프로토콜을 제안하고 6절에서는 역방향 영지식 증명 프로토콜을 제안한다.

2. FS 기법[3]

이 방식은 충분히 큰 두 소수 p,q의 곱으로 이루어진 합성수 n을 법으로 하는 연산에서 n의 소인수를 모르는 경우 제곱근(square root)을 구하는 문제는 NP문제 라는 점을 이용한 것이다. 센터는 충분히 큰 두 소수 p,q를 선택하여 비밀로 유지하면서, 이것들의 곱 $n(=p \cdot q)$과 임의의 스트링(string)을 [0,n)으로 대응시키는 의사난수(pseudo-random) 함수 f를 선택하여 공개한다. 사용자 j는 네트워크 가입시에 센타로부터

$$ID_j = s_j^2 \mod n \qquad \text{(식. 1)}$$

인 s_j를 얻어서 비밀로 한다. 여기서 ID_j는 j의 ID정보(이름, 주소, 주민등록번호, 전화번호 등)이며 s_j의 평방잉여 이다.

검증자(verifier) V가 인증자(prover) P를 인증하고자 하는 경우, 인증자는 "s_j"를 알고있다는 것을 검증자에게 보이면 된다. 그림 1에 나타나 있다.

인증 프로토콜은 이하의 step 1~4를 t회 반복한다. 단, t는 n의 비트수 이다.

step 1. P는 난수 r을 선택, x를 계산해서 V에게 보낸다.

$$x = r^2 \mod n \qquad \text{(식. 2)}$$

step 2. V는 임의로 e(= 0 또는 1)를 선택하여 전송한다.

step 3. P는 y를 계산하여 V에게 전송한다.

$$y = \begin{cases} r & e=0\text{인 경우.} \\ r \cdot s_j \mod n & e=1\text{인 경우.} \end{cases} \qquad \text{(식. 3)}$$

step 4. V는 다음이 성립하는가 검사한다.

$$y^2 = \begin{cases} x & e=0\text{인 경우.} \\ x \cdot ID_j \mod n & e=1\text{인 경우.} \end{cases} \qquad \text{(식. 4)}$$

3. DGB 기법[4]

FS 기법에 의해서는 P가 V에게 난수 만을 전송한다. (즉, "s_j"를 알고있다는 사실만을) DGB는 메세지 전송이 가능한 기법을 다음과 같이 제안하였다. 그림 2에 나타나 있다.

<u>인증과정</u>

step 1. C를 A가 B에게 전송하는 암호문이라 하자. A는 난수 r을 선택, x를 계산해서 B에게 전송한다.

$$x = (C \cdot r^2)^2 \mod n \qquad \text{(식. 5)}$$

step 2. B는 임의로 e(= 0 또는 1)를 선택하여 전송한다.

step 3. A는 y를 계산하여 B에게 전송한다.

$$y = \begin{cases} C \cdot r^2 & e=0\text{인 경우.} \\ Cr^2 \cdot s_A \mod n & e=1\text{인 경우.} \end{cases} \qquad \text{(식. 6)}$$

step 4. B는 다음이 성립하는 검사한다.

$$y^2 = \begin{cases} x & e=0\text{인 경우.} \\ x \cdot ID_A \mod n & e=1\text{인 경우.} \end{cases} \qquad \text{(식. 7)}$$

step 5. A는

if e=1, goto step 1.

if e=0, $x = r^2 \mod n$ 을 B에게 전송한다.

step 6. FS 기법 (step 2 ~ 4)을 행한다.

step 7. goto step 1.

위 프로토콜에서 사용자 B가 암호문을 복구하는 방법은 다음과 같다. e=0인 경우, B는 $y=C \cdot r^2$ 과 $x=r^2$ 을 받게 되므로 다음식에 의해 암호문 C를 복구할 수 있다.

$$C = \frac{y}{x} \mod n = \frac{C \cdot r^2}{r^2} = C \qquad \text{(식. 8)}$$

이 DGB 기법에서는 사용자 B가 e를 "0"으로 하여 사용자 A에게 보내지 않는 한 절대로 step 6 을 넘어갈 수 없으므로, 반드시 e=0인 경우가 발생하며 그때 암호문 C를 복구할 수 있다. 그리고 사용자 A는 e=1인 경우 반드시 새로운 임의의 난수를 생성해야 한다.

[정의] 전송효율 R을 다음과 같이 정의 한다.

$$R \triangleq \frac{\text{A에서 B로 보낸 정보 비트수}}{\text{A에서 B로 송신한 전체 비트수(평균)}}$$

e가 처음에 "0"일 확률 $p(e_1=0)=½$ 이므로 $e_1=0$ 일때 보내야 할 최소블럭은 4블럭이다. e가 두번째 "0"일 확률은 $p(e_1=1) \cdot p(e_2=0)=¼$ 이므로 $e_2=0$ 일때 보내야 할 최소블럭은 6블럭이다. 이런식으로 평균 전송블럭을 계산해 보면 다음과 같다.

$$E[N] = 4\times½ + 6\times¼ + 8\times⅛ + \cdots$$
$$= 6 \qquad \text{(식. 9)}$$

따라서 DGB 기법에서의 평균 전송효율 $R = 1/E[N] = 1/6$ 이다.

4. DGB 기법의 개량[5]

본 장에서는 DGB 기법의 전송효율을 개선하는 방법을 제시한다. 그림 3에 나타나 있다. A가 B에게 전송하는 i번째 메세지 쌍을 C_{1i}, C_{2i}라 하자.

<u>인증과정</u>

for i = 1,…,t

for j = 1,2,…

step 1. A는 난수 r을 선택, x를 계산해서 B에게 전송한다.

$$x = (C_{2i}(C_{1i} \cdot r_{ij}^2)^2)^2 \mod n \qquad (식.10)$$

step 2. B는 임의로 e_{ij}(= 0 또는 1)를 선택하여 전송한다.

step 3. A는 y를 계산하여 B에게 전송한다.

$$y = \begin{cases} C_{2i}(C_{1i} \cdot r_{ij}^2)^2 & e=0인 경우. \\ C_{2i}(C_{1i} r_{ij}^2) \cdot s_A \mod n & e=1인 경우. \end{cases} \qquad (식. 11)$$

step 4. B는 다음이 성립하는 검사한다.

$$y^2 = \begin{cases} x & e=0인 경우. \\ x \cdot ID_A \mod n & e=1인 경우. \end{cases} \qquad (식. 12)$$

step 5. A는

if e=1, ① j=j+1.

② r_{ij} 선택.

③ goto step 1.

if e=0, step 6로 뛴다.

for j' = j, …

step 6. A는 $x=(C_{1i} \cdot r_{ij}^2)^2$ 을 B에게 보낸다.

step 7. B는 임의로 e_{ij}'(= 0 또는 1)를 선택하여 전송한다..

step 8. A는 다음의 y를 계산하여 B에게 전송한다.

$$y = \begin{cases} C_{1i} \cdot r_{ij}'^2 & e_{ij}'=0 \\ C_{1i} \cdot r_{ij}'^2 \cdot s_A & e_{ij}'=1 \end{cases} \qquad \text{(식. 13)}$$

step 9. B는 다음이 성립하는 가를 검사한다.

$$y^2 = \begin{cases} x & e_{ij}'=0 \\ x \cdot ID_A & e_{ij}'=1 \end{cases} \qquad \text{(식. 14)}$$

step 10. A는

if $e_{ij}'=1$, ① $j'=j'+1$.

② r_{ij}' 선택.

③ goto step 1.

if $e_{ij}'=0$, ① A는 $x=r_{ij}'^2 \mod n$ 을 B에게 전송한다.

② goto step 11.

step 11. FS 기법을 행한다.

step 12. goto step 1.

위의 개량된 DGB 기법에서 암호문 C_{2i}는 step 5와 step 6에서 얻은 x와 y로부터 다음식에 의해 복구할 수 있다.

$$C_{2i} = \frac{y}{x} = \frac{C_{2i}(C_{1i} \cdot r_{ij}^2)^2}{(C_{1i} \cdot r_{ij}^2)^2} \mod n \qquad \text{(식. 15)}$$

암호문 C_{1i}는 step 8과 step 10에서 얻은 x와 y로부터 다음식에 의해 복구할 수 있다.

$$C_{1i} = \frac{y}{x} = \frac{C_{1i} \cdot r_{tj}^2}{r_{tj}^2} \mod n \qquad \text{(식. 16)}$$

step 1-5를 KS phase라 하고 step 6-10까지를 DGB phase라 하면, KS phase를 빠져나오기 위한 평균 블럭수 $E[N_1]$은 다음과 같이 된다.

$$E[N_1] = 2\times\frac{1}{2} + 4\times\frac{1}{4} + 6\times 1/6 + \cdots = 4 \qquad \text{(식. 17)}$$

또, DGB phase를 빠져나오기 위한 평균 블럭수 $E[N_2]$은 다음과 같이 된다.

$$E[N_2] = 2\times\frac{1}{2} + 4\times\frac{1}{4} + 6\times 1/6 + \cdots = 4 \qquad \text{(식. 18)}$$

또한 FS phase를 빠져나오기 위한 평균 블럭수 $E[N_3]$는 2이다.

따라서, 전송효율 R은,

$$R = \frac{2}{E[N_1]+E[N_2]+E[N_3]} = \frac{2}{4+4+2} = \frac{1}{5} \qquad \text{(식. 19)}$$

암호문을 k개로 확장하는 경우에는,

$$R = \lim_{k\to\infty} \frac{k}{4k+2} = \frac{1}{4} \qquad \text{(식. 20)}$$

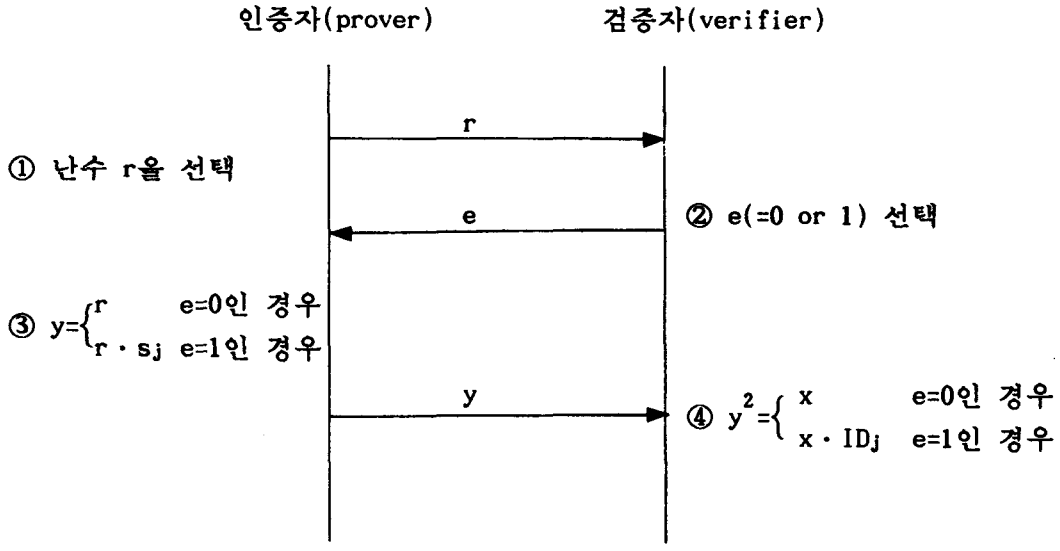

그림 1. FS 기법

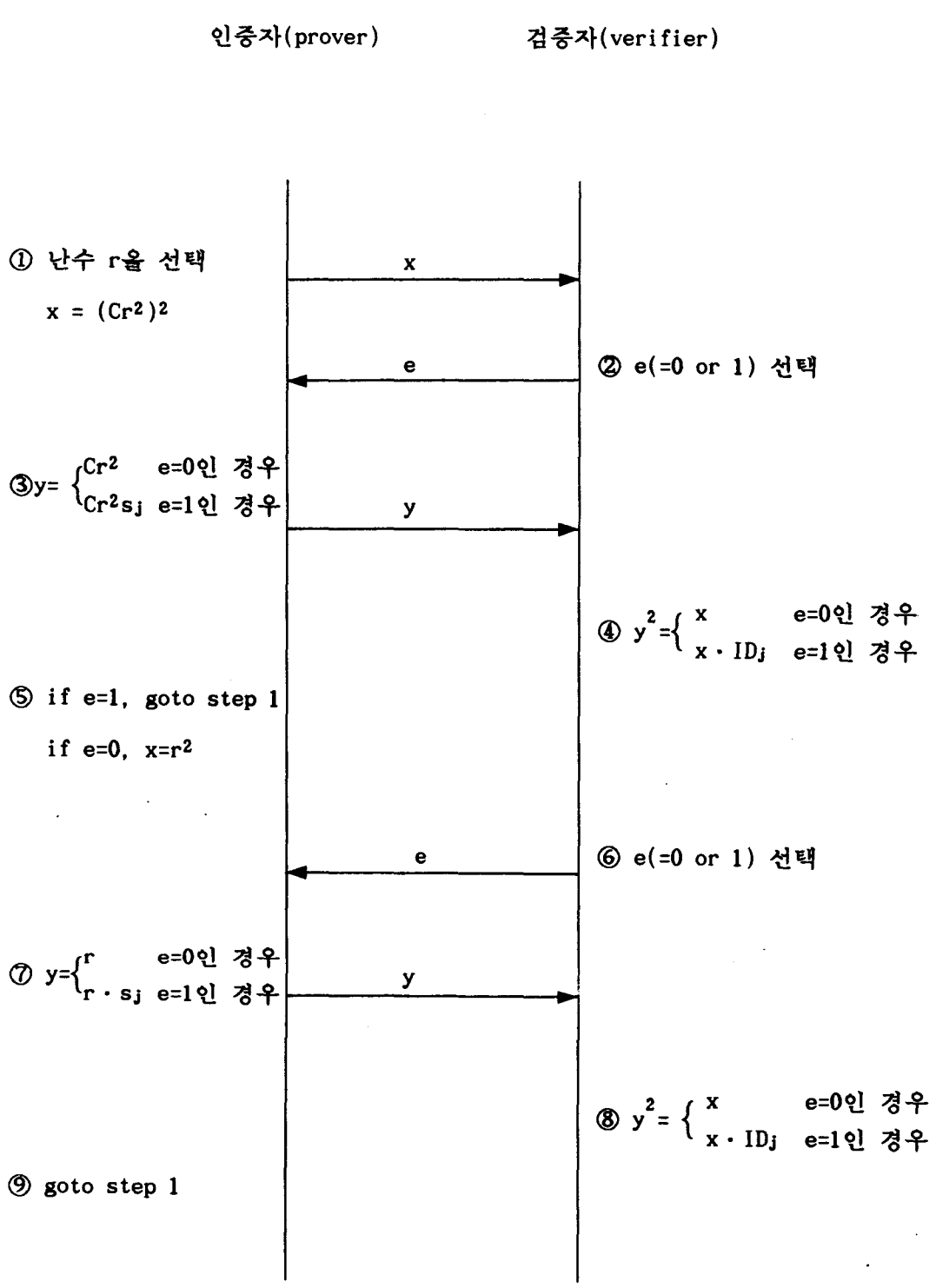
인증자(prover)
검증자(verifier)
① 난수 r을 선택
x = (Cr²)²
x
e
② e(=0 or 1) 선택
③y= {Cr² e=0인 경우 / Cr²sj e=1인 경우
y
④ y² ={ x e=0인 경우 / x · IDj e=1인 경우
⑤ if e=1, goto step 1
if e=0, x=r²
e
⑥ e(=0 or 1) 선택
⑦ y={r e=0인 경우 / r · sj e=1인 경우
y
⑧ y² = { x e=0인 경우 / x · IDj e=1인 경우
⑨ goto step 1

그림 2. DGB 기법

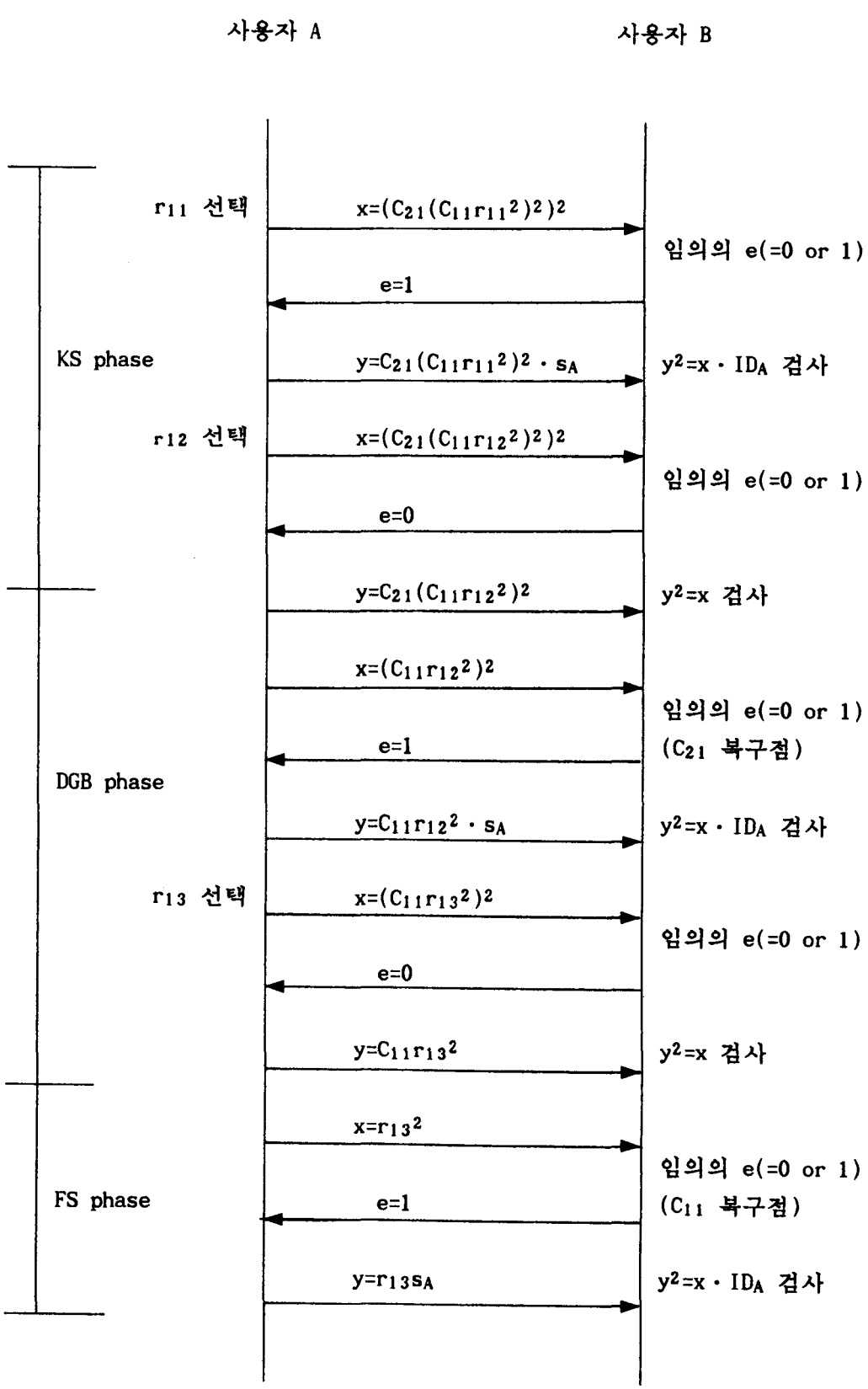
사용자 A
사용자 B
r11 선택
x=(C21(C11r11²)²)²
임의의 e(=0 or 1)
e=1
KS phase
y=C21(C11r11²)² · sA
y²=x · IDA 검사
r12 선택
x=(C21(C11r12²)²)²
임의의 e(=0 or 1)
e=0
y=C21(C11r12²)²
y²=x 검사
x=(C11r12²)²
임의의 e(=0 or 1)
(C21 복구점)
e=1
DGB phase
y=C11r12² · sA
y²=x · IDA 검사
r13 선택
x=(C11r13²)²
임의의 e(=0 or 1)
e=0
y=C11r13²
y²=x 검사
x=r13²
임의의 e(=0 or 1)
(C11 복구점)
FS phase
e=1
y=r13sA
y²=x · IDA 검사

그림 3. DGB 개량 기법

5. ElGamal 암호알고리듬을 이용한 영지식 증명

본 절에서는 ElGamal 암호알고리듬을 이용하여 메세지 전송과 사용자 인증을 동시에 수행하는 방식을 제안하였다.[6] 본 방식은 ID 기본 암호알고리듬을 기반으로 하여 구성한다. 먼저 5.1절에서는 순방향 영지식 증명 방법을 제안하고, 5.2절에서는 역방향 영지식 증명 방법을 제안한다. 그리고 제안한 두 방식의 전송효율을 계산한다.

5.1 순방향 영지식 증명

순방향 영지식 증명인 경우에는 인증자가 암호문을 보내는 통신 주체이고 검증자가 암호문을 받는 주체이다. 인증 프로토콜은 다음과 같다. 여기서 $N=p \cdot q$이고 C_i'을 사용자 A에서 사용자 B에게 전송되는 암호문이다. 그림 4에 나타나 있다.

<u>인증 과정</u>

step .1 B는 N의 원시원(primitive element)인 R_1과 난수 R_2를 선택한 후 다음과 같이 C_1, C_2, C_3를 계산하여 A에게 전송한다.

$$C_1 = g^r \qquad \text{(식. 21)}$$

$$C_2 = R_1 \cdot (y_A)^r \qquad \text{(식. 22)}$$

$$C_3 = R_1 + R_2 \qquad \text{(식. 23)}$$

step 2. A는 N의 원시원(primitive element)인 R_1과 난수 R_2를 복구한다.

이하의 과정을 t회 반복한다.

step 3. A는 암호문 $X(=C_{11}', C_{12}')$를 B에게 전송한다.

$$C_{11}' = g^r \mod p \qquad \text{(식. 24)}$$

$$C_{12}' = m_1 \cdot (y_B)^r \mod p \qquad \text{(식. 25)}$$

$$\text{단, } y_B = \prod_{i=1}^{n} y_i^{EID_{Bi}} \quad \begin{cases} EID_B = (ID_B)^e \\ y_i\text{는 공개정보} \end{cases}$$

$$= g^{k_B} \qquad \text{(식. 26)}$$

step 4. B는 임의의 비트 e(=0 or 1)를 선택하여 A에게 보낸다.

step 5. A는 아래의 식을 이용해서 서명문 (r,s)를 만들어 B에게 전송한다.

$$r \equiv R_1^{R_2} \pmod{p} \qquad \text{(식. 27)}$$

$$C_1' \equiv k_A \cdot r + R_2 \cdot s \qquad \text{(식. 28)}$$

step 6. B는 다음의 식이 성립하는지 검사한다.

$$R_1^{C_{11}'} \equiv (y_A)^{r_{11}} \cdot r_{11}^{s_{11}} \qquad \text{(식. 29)}$$

$$R_1^{C_{12}'} \equiv (y_A)^{r_{12}} \cdot r_{11}^{s_{12}} \qquad \text{(식. 30)}$$

암호문 C_{11}'과 C_{12}'구조에서 메세지 m_1을 복구하는 방법은 다음과 같다.

① $C_{11}'' \equiv (C_{11}')^{k_B} \bmod p \equiv (g^r)^{k_B}$

② $(C_{11}'')^{-1} \cdot C_{12}' \equiv \left[(g^r)^{k_B}\right]^{-1} \cdot m_1 \cdot (y_B)^r \equiv r$

영지식 증명 동안의 전송효율을 계산해 보면 다음과 같다.

$$\text{전송효율} = \frac{\text{A에서 B에게 전송한 정보 비트수}}{\text{A에서 B로 전송한 전체 비트수}} = \frac{1(\text{block})}{8(\text{blocks})}$$

5.2 역방향 영지식 증명

역방향 영지식 증명인 경우에는 검증자가 암호문을 보내는 통신 주체이고 인증자가 암호문을 받는 주체이다. 인증 프로토콜은 다음과 같다. 여기서 $N=p \cdot q$이고 C_i을 사용자 B에서 사용자 A에게 전송되는 암호문이다. 그림 5에 나타나 있다.

<u>인증 과정</u>

step .1 B는 N의 원시원(primitive element)인 R_1과 난수 R_2를 선택한 후 다음과 같이 C_1, C_2, C_3를 계산하여 A에게 전송한다.

$$C_1 = g^r \qquad \text{(식. 31)}$$

$$C_2 = R_1 \cdot (y_A)^r \qquad \text{(식. 32)}$$

$$C_3 = R_1 + R_2 \qquad \text{(식. 33)}$$

step 2. A는 N의 원시원(primitive element)인 R_1과 난수 R_2를 복구한다.
이하의 과정을 t회 반복한다.

step 3. B는 암호문 난수 r를 선택해서 $X(=(C_{11}r^2) \cdot C_{12})$를 A에게 전송한다.

step 4. A는 임의의 비트 e(=0 or 1)를 선택하여 B에게 보낸다.

step 5. B는 아래의 식을 이용해서 서명문 (r,s)를 만들어 A에게 전송한다.

$$r \equiv R_1^{R_2} \pmod p \qquad \text{(식. 34)}$$

$$C_1' \equiv k_A \cdot r + R_2 \cdot s \qquad \text{(식. 35)}$$

step 6. A는 다음의 식이 성립하는지 검사한다.

$$R_1^X \equiv (y_B)^r \cdot r^s \qquad \text{(식. 36)}$$

본 방식에서 암호문 C_{11}, C_{12}를 복구하는 방법은 DGB 개량 기법과 같다.

영지식 증명 동안의 전송효율을 계산해 보면 다음과 같다.

① Initializing phase : 3 blocks.

② KS phase를 빠져 나오기 위한 평균 블럭 수 $E[N_1]$

$$E[N_1] = 4\times1/2 + 8\times1/4 + 12\times1/6 + \cdots$$
$$= 8 \qquad \text{(식. 37)}$$

③ DGB phase를 빠져 나오기 위한 평균 블럭 수 $E[N_2]$

$$E[N_2] = 4\times1/2 + 8\times1/4 + 12\times1/6 + \cdots$$
$$= 8 \qquad \text{(식. 38)}$$

④ FS phase $E[N_3]$

$$E[N_3] = 4 \qquad \text{(식. 39)}$$

$$\therefore \text{전송효율} = \frac{\text{A에서 B에게 전송한 정보 비트수}}{\text{A에서 B로 전송한 전체 비트수}}$$

$$= \frac{1}{E[N_1]+E[N_2]+E[N_3]+3} = \frac{1}{23} \qquad \text{(식. 40)}$$

k개의 암호문으로 확장했을 경우의 전송효율을 계산해 보면 다음과 같다.

$$\text{전송효율} = \frac{k/2}{E[N_1]+E[N_2]+\cdots+E[N_k]+7} = \frac{k/2}{8k+7}$$

$$\therefore R = \lim_{k\to\infty} \frac{k/2}{8k+7} = \frac{1}{16} \qquad \text{(식. 41)}$$

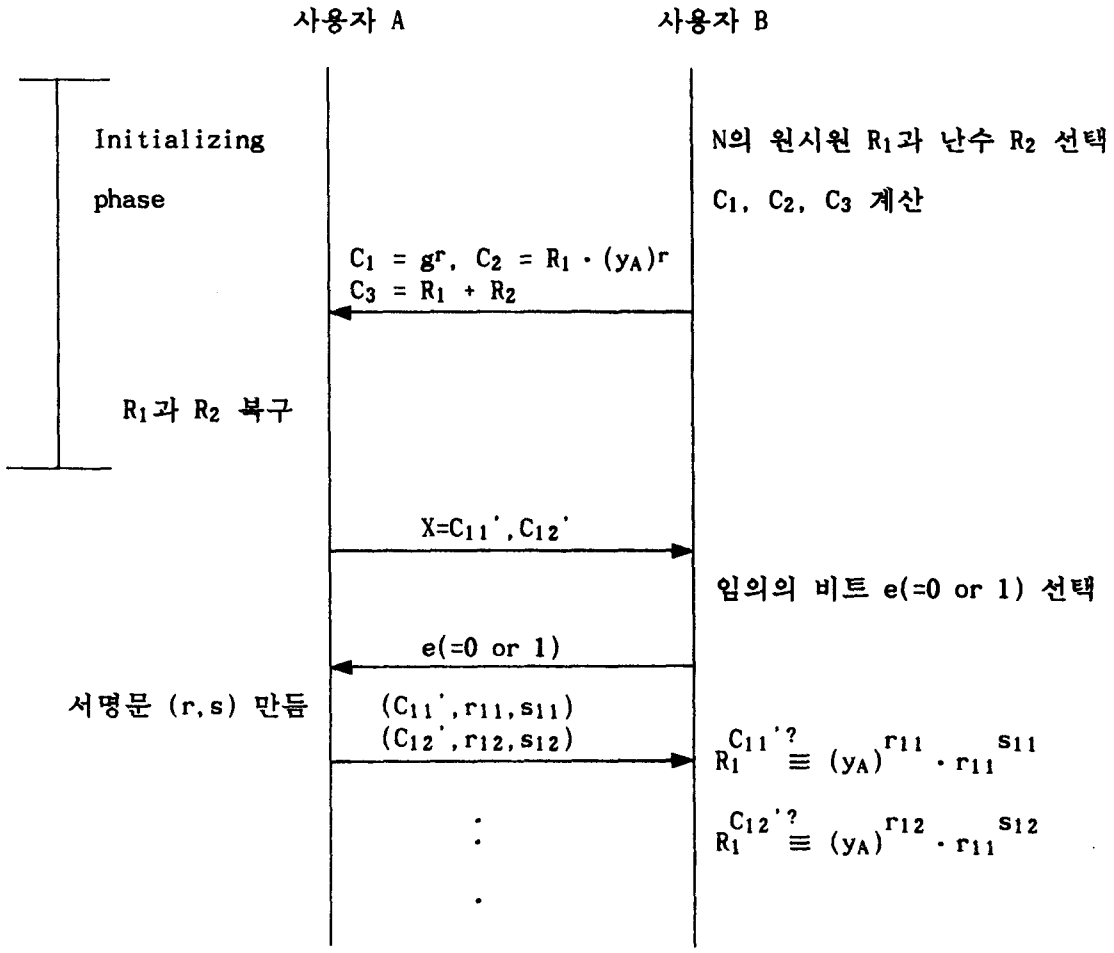

그림 4. ElGamal 암호를 이용한 순방향 영지식 증명

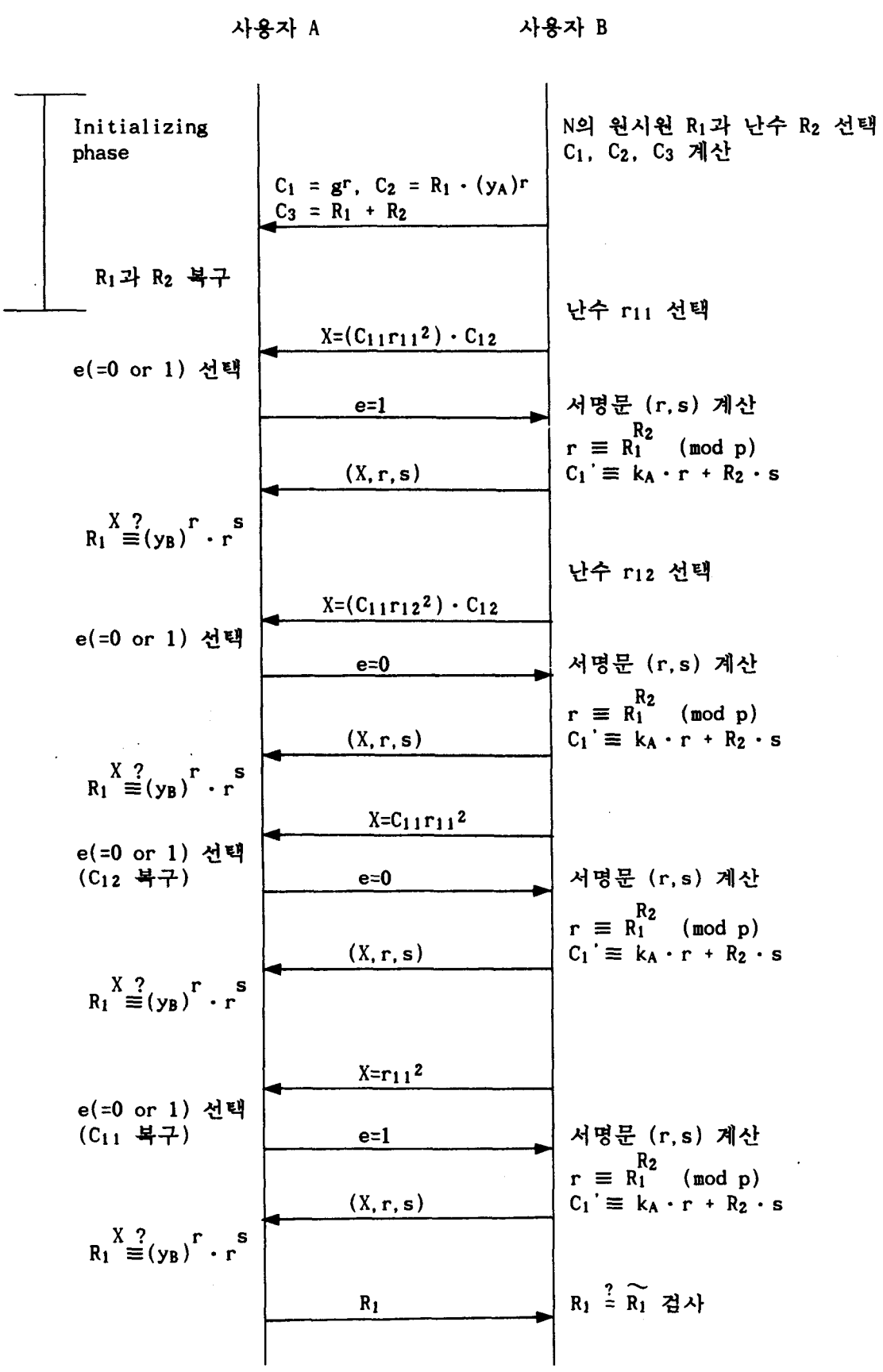

그림 5. ElGamal 암호를 이용한 역방향 영지식 증명

6. 결론

본 논문에서는 DGB 기법을 분석하여 개량된 DGB기법을 제시하였고 전송효율이 1/6에서 1/4로 향상됨을 보였다. 그리고 ElGamal 암호알고리듬을 이용하여 메세지 전송이 가능한 프로토콜을 제안하였다. 전송효율이 순방향 영지식 증명인 경우는 1/8이고 역방향 영지식 증명인 경우에는 1/16임을 보였다.

향후 ElGamal 암호알고리듬이 국제 표준으로 될 가능성이 매우 크므로 이 알고리듬을 이용한 프로토콜에 대한 연구가 활성화 되리라 사료된다.

참고문헌

[1] 이만영, "암호의 역사적 고찰," 한국통신정보보호학회, vol.1, no.1, pp.11-23, 1991.4.

[2] Goldwasser, S., Micali, S. and Rackoff, C.,"The Knowledge Complexity of Interactive Proof Systems," Proc. of STOC'85, pp.291-302, 1985.

[3] A. Fiat and A. Shamir, "How to Prove Yourself : Practical solution to identification and Signature Problem," Proc. Crypto'86, pp.186-194, 1986.

[4] Desmedt, Goutier and Bengio, "Special uses and abuses of the Fiat-Shamir passport protocol," Crypto'87, 1987.

[5] Karou KUROSAWA and Shigeo TSUJII, "On the transmission rate of zero knowledge proof systems," SCIS90-7D, 1990

[6] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithm," IEEE Trans. Inform. Theory, vol.IT-31, pp.469-472, 1985.