通信情報保護學會論文誌
第 1 卷, 第 1 號, 1991. 12

ID-Based 키 분배방식 및 회의용 키 분배방식

손기욱* · 권창영* · 양형규* · 원동호*

Identity-based key distribution system and conference key distribution system

Ki-Wook Sohn and Chang-Young Kwon and Hyung-Kyu Yang and Dong-Ho Won

요 약

본 논문에서는 ID 정보를 이용한 키 분배방식을 제안했다. 이 방식에서는 Diffie-Hellman 방식에서 사용하는 공개 화일 대신에 가입자의 ID 정보를 이용하였다. 이 방식은 키 분배를 위하여 센터는 아무런 역할을 하지 않으며, 공개 화일의 불법 변경 등의 공격에 대한 위험이 제거되는 장점을 가지고 있는 방식이다. 또한, 본 논문에서는 2명 이상의 회의용 키를 생성하는 ID 정보를 이용한 회의용 키 분배방식을 제안하였다. 가입자들은 링 네트워크(ring network)를 구성하고 있다고 가정하였다. 각 가입자들간의 전송정보들은 각 가입자의 ID 정보를 이용하여 인증된다. 제안한 방식의 안전성은 큰 수의 소인수 분해 및 이산대수 계산 문제에 근거한다.

Abstract

This paper proposes a key distribution system based on identification information. The system uses an individual user's identification instead of the public file used in the Diffie-Hellman system. It does not require any services of a center to distribute work keys and users to keep directory public file. We propose an identity-based key distribution system for generating a common secret conference key for two or more users. We assume users are connected in a ring network. Message among users authenticated using each user's identification information. The security of the our proposed system is based on the difficulty of both factoring large numbers and computing discrete logarithms over large finite fields.

* 성균관대학교 정보공학과

1. 서 론

정보 시스템내에서 전송, 처리, 축적되는 정보는 전기적 현상을 이용하여 디지탈화, 대용량화 되고 있어 정보에 대한 적절한 보호 조치가 없으면 전송, 처리 중 혹은 기억장치에 보관된 상태에서 정보의 불법 유출, 정보의 삭제 및 수정 등의 위험에 노출되기 쉽다[1,2,3]. 이러한 불법적인 사고로 인하여 개인 비밀이 침해될 뿐만 아니라 때에 따라서는 막대한 경제적 손실을 당하는 경우가 있어 정보 보호에 대한 관심이 고조되고 있다.

정보 시스템의 정보보호를 위한 대책으로는 설비면에서의 물리적 대책, 관리 운영면에서의 인적 자원에 대한 대책, 기술면에서의 대책, 법과 제도면에서의 대책 등이 있을 수 있으나 가장 경제적이면서도 보안 수준에 따라 효율적이면서도 계층적인 보안 대책을 제공할 수 있는 방법이 기술면에서의 대책인 암호방식을 이용하는 방법이다.

암호 방식이란 보호하려는 정보를 작은 길이의 키로 관리하는 것이라 말할 수 있다. 따라서 암호 방식에서 효율적인 정보 보호를 위해서는 키를 안전하게 관리해야 한다. 키 관리는 키의 생성, 보관, 폐기 및 분배로 나누어 생각할 수 있는데 이중에서 가장 문제가 되는 것이 제 3자(해독자)에게 키를 노출되지 않게 분배하는 것이다.

키를 분배하는 방식은 크게 중앙 집중식 키 분배 방식(centralized key distribution system), 공개키 분배 방식(public key distribution system)으로 나눌 수 있다[2]. 중앙 집중식 키 분배 방식은 키 분배 센터(KDC : key distribution center)와 가입자 사이에 터미날 키(terminal key)가 필요하며 공개키 분배 방식은 공개 화일(public file)을 갖추고 있어야 하는 단점이 있다.

이러한 단점을 극복할 수 있는 키 분배 방식으로 ID 정보에 의한 키 분배 방식(ID-based key distribution system)이 제안되었다. ID 정보에 의한 키 분배 방식은 Shamir와 Okamoto가 제안한 방식으로 공개 화일을 제거하기 위해 암호 통신망 가입자 모두가 smart 카드나 IC 카드를 이용하게 되며 카드에는 키의 생성과 전달에 필요한 마이크로 프로세서와 입/출력 포트, RAM, ROM 등을 내장하고 있다[4, 5].

ID 정보에 의한 키 분배 방식은 두 단계로 이루어지는데 첫번째 단계는 카드 발급단계로 각 가입자들에게 센터가 설정한 파라메터들을 카드에 저장, 발급하는 단계이며 두번째 단계는 카드의 내용과 가입자가 설정한 난수를 이용하여 가입자 상호간에 공통키를 생성하는 단계이다.

이 방식은 공개키 분배 방식에 근거를 두고 있으나 공개키 분배 방식에서는 공개 정보를 공개 화일에 등록하는데 반해 ID 정보에 의한 키 분배 방식에서는 가입자 ID 정보를 공개 정보로 하여 공개 화일 개념을 배제한다. 따라서 공개 화일에 대한 별도의 보호 조치가 필요하지 않으며 비밀 정보는 카드에 담아 분배되므로 비밀이 유지된다.

이미 언급된 바와 같이 기존의 공개키 분배 방식이나 ID 정보에 의한 키 분배 방식을 이용해서는 다수의 가입자를 위한 키 생성 및 분배가 어렵기 때문에 이에 대한 연구도 진행되었다[6,7,8,9].

본 논문에서는 ID 정보에 의한 키 분배 방식을 제안하였으며, 제안한 방식은 링 네트워크(ring network) 상의 통신망에서 2인 이상 다수 가입자들 사이의 상호 비밀 통신 즉, 다자간 회의용 키(conference key)로 사용할 수 있는 방식이다.

2. 제안한 ID-Based 키 분배 방식

제안한 ID-Based 키 분배 방식은 두 단계로 나누어 키 분배 과정을 수행한다. 첫번째 단계는 시스템 준비 및 카드 발행 단계이며 두번째 단계는 키 분배를 하기 위한 통신 단계이다.

2.1 시스템 준비 및 카드 발행 단계

첫번째 단계인 시스템 준비 및 카드 발행 단계

에서는 센터(center)는 자신의 비밀정보 및 공개 정보를 생성하고, 가입자의 ID 정보를 이용해서 각 가입자에 대한 비밀정보를 생성하여 안전한 채널(smart card 등)을 이용하여 각 가입자에게 전달한다.

순서 1. 시스템 준비(set up) 단계에서 센터는 두 개의 큰 소수 p와 q를 선택하고 이들의 곱으로 n을 생성한다. 이때 p, q는 256 비트 정도 길이를 갖는 소수를 선택하여야 하며 RSA 암호 방식에서 선택하여야 하는 인자들의 조건과 동일하게 생성된다[3]. 또한, 센터는 GF(p) 상의 원시 원소이면서 GF(q) 상의 원시 원소인 g를 생성한다.

$$p=2p'+1 \text{ 단, } p'\text{는 소수} \quad (1)$$
$$q=2q'+1 \text{ 단, } q'\text{는 소수} \quad (2)$$

순서 2. 카드 발행 단계에서 센터는 가입자 i의 정당성을 확인한 후 가입자 i의 개인 정보인 id_i를 이용해서 비밀 정보인 s_i를 다음과 같은 조건이 성립하도록 생성한다.

$$s_i=ID_i^{-1} \bmod \Phi(n) \text{ 단, } ID_i=(id_i \parallel 1) \quad (3)$$
$$ID_iID_i^{-1}=1 \bmod \Phi(n)$$
$$\text{단, } \Phi(n)=(p-1)(q-1) \quad (4)$$

센터는 가입자 i의 smart card에 시스템 전체의 공개정보인 n, g 및 가입자 i의 비밀 정보인 s_i를 저장하여 가입자 i에게 카드를 발급한다.

2.2 통신 단계

두번째 단계인 키 분배를 위한 통신 단계에서 가입자 i 및 가입자 j가 키(work key)를 생성하고자 할 경우 자신의 스마트 카드에 저장된 정보를 이용하여 아래와 같은 순서로 통신을 한다.

순서 1. 가입자 i는 가입자 j에게 전송할 전송정보 Y_i, Z_i를 다음과 같이 생성하여 time stamp T_i와 함께 전송한다.

$$Y_i=ID_j^{s_i} * g^{c_i r_i ID_j} \bmod n \quad (5)$$
$$Z_i=g^{ID_i ID_j r_i} \bmod n \quad (6)$$

단, $C_i=HASH(Z_i, ID_i, ID_j, T_i)$

순서 2. 가입자 j는 가입자 i에게 전송할 전송 정보 Y_j, Z_j를 다음과 같이 생성하여 time stamp T_j와 함께 전송한다.

$$Y_j=ID_i^{s_j} * g^{c_j r_j ID_i} \bmod n \quad (7)$$
$$Z_j=g^{ID_i ID_j r_j} \bmod n \quad (8)$$

단, $C_i=HASH(Z_j, ID_i, ID_j, T_j)$

순서 3. 가입자 i는 가입자 j로부터 전송 정보를 이용하여 아래와 같은 방법으로 송신자 j를 인증한다.

$$[Y_j^{ID_j} / Z_j^{c_j}]=ID_j \bmod n \quad (9)$$
$$(Y_j)^{ID_j}=ID_j * g^{c_j r_j ID_i ID_j} \bmod n \quad (10)$$
$$(Z_j)^{c_j}=g^{c_j r_j ID_i ID_j} \bmod n \quad (11)$$

가입자에 대한 인증이 이루어진 후에는 자신이 선택한 난수 r_i를 이용하여 비밀 통신키를 다음과 같이 생성한다.

$$WK=(Z_j)^{r_i}$$
$$=g^{r_i r_j ID_i ID_j} \bmod n \quad (12)$$

순서 4. 가입자 j는 가입자 i로부터의 전송 정보를 이용하여 아래와 같은 방법으로 송신자 i를 인증한다.

$$[Y_i^{ID_i} / Z_i^{c_i}]=ID_i \bmod n \quad (13)$$
$$(Y_i)^{ID_i}=ID_i * g^{c_i r_i ID_i ID_j} \bmod n \quad (14)$$
$$(Z_i)^{c_i}=g^{c_i r_i ID_i ID_j} \bmod n \quad (15)$$

가입자에 대한 인증이 이루어진 후에는 자신이 선택한 난수 r_j를 이용하여 비밀 통신키를 다음과 같이 생성한다.

$$WK=(Z_i)^{r_j} = g^{r_i r_j ID_i ID_j} \mod n \quad (16)$$

이 후 가입자 i와 j는 공통키를 소유하게 되며 상대방과의 비밀 통신에 있어서 이 암호키를 이용한다.

위 순서 3 및 순서 4에서의 인증 과정은 직접 인증(direct authentication)이며 만약 제 3자가 전송정보인 Y 또는 Z를 변경하면 해싱 함수의 결과값인 c의 값이 달라지므로 식(9) 및 식 (13)이 성립되지 않는다. 왜냐하면, c값은 전송정보 Z에 의존적(dependent)인 해싱 함수의 치역이기 때문이다. 또한, 제안한 방식에서 time stamp T_i를 사용하는 이유는 제 3자가 앞 번 통신시 전송된 정보 Y_i', Z_i'를 도청하여 정규의 가입자로 위장하는 행위를 방지하기 위함이다. 즉, 제 3자는 각 가입자의 비밀정보 s_i를 알지 못하므로 Y_i', Z_i'를 이용하여 인증 단계를 성공적으로 통과하는 Y_i, Z_i를 생성할 수 없다.

3. 회의용 키 생성단계

회의용 키 생성은 양 가입자 사이의 키생성시와 같은 전송 정보가 사용되며 본 논문에서는 가입자 m명이 원형 네트워크(ring network) 상에서 회의용 키(conference key)를 생성하는 방식을 제안하였다. 회의용 키 생성시 전송되는 정보의 순서를 보면 가입자 i는 반드시 가입자 i+1에게 정보를 전송하고 가입자 m은 가입자 1에게 정보를 전송한다. 결국 가입자들은 m−1회의 통신 후 다자간 회의용 키를 생성할 수 있다.

순서 1. 가입자 i는 임의의 난수 r_i를 생성하면 아래 식으로 Y_i, Z_i를 계산하여 가입자 i+1에게 전송한다.

$$Y_i^{(1)} = ID_i^{s_i} * g^{c_i r_i ID_{i+1}} \mod n \quad (17)$$

$$Z_i^{(1)} = g^{ID_i r_i ID_{i+1}} \mod n \quad (18)$$

단, $C_i = HASH(Z_i^{(1)}, ID_i, ID_{i+1}, T_i)$

순서 j($2 \le j \le m-1$) : 가입자 i는 Y_{i-1}, Z_{i-1}를 수신하여 Y_{i-1}, Z_{i-1}, ID_{i-1}, n을 이용하여 다음식의 만족여부를 검증한다.

$$(Y_{i-1}^{(1)\,id_{i-1}} / Z_{i-1}^{(1)\,c_i}) = \prod_{1 \le k \le j-1} id_{i-k} \mod n \quad (19)$$

만약 검증이 확인되면, 즉, 가입자 i가 수신한 메세지는 가입자 i−1, i−2, …, i−j+1로 부터 정상적으로 전송되었다는 것이 입증되면, 가입자 i는 $Y_i^{(j)}$, $Z_i^{(j)}$를 생성하여 가입자 i+1에게 전송한다.

$$Y_i^{(j)} = (ID_i \prod_{1 \le k \le j-1} ID_{i-k})^{s_i} * g^{c_i r_i ID_{i+1} \prod_{1 \le k \le j-1} r_{i-k} ID_{i-k}} \mod n \quad (20)$$

$$Z_i^{(j)} = g^{ID_i r_i ID_{i+1} \prod_{1 \le k \le j-1} r_{i-k} ID_{i-k}} \mod n \quad (21)$$

그리고, 가입자 i는 다음 단계인 순서 j+1을 수행한다.

순서 m : 가입자 i는 $Y_{i-1}^{(m-1)}$, $Z_{i-1}^{(m-1)}$을 수신한다. 식 (19)로 j=m인 경우에 대하여 검증한다. 검증이 확인되면 메세지가 가입자 i−1, i−2, i−3, …, i−m+1을 거쳐서 정상적으로 전송되었다는 것이

입증되는 것이다. 이때 회의용 키를 생성한다.

$$CK=(Z_{i-1})^{r_i} \quad \text{mod n} \qquad (22)$$

실제 회의용 키의 값은 아래와 같다.

$$CK=g^{\prod_{1\le k\le n} ID_k\ r_k} \quad \text{mod n} \qquad (23)$$

3.1 회의용 키 생성의 실제 예

4명의 가입자가 회의용 키를 생성하려 할 경우를 예로 들어 설명하여 보자. 회의용 키 생성시 전송되는 정보의 순서는 가입자 i를 중심으로 i는 반드시 i+1에게 정보를 전송한다. 결국 가입자들은 원을 형성하여 전송 정보를 통해 공통키를 생성한다. 그림 1은 4명의 가입자 사이에 회의용 키 생성시 전송 정보의 전송 방향을 표시한 것으로 가입자 1→2→3→4→1의 순으로 전송된다.

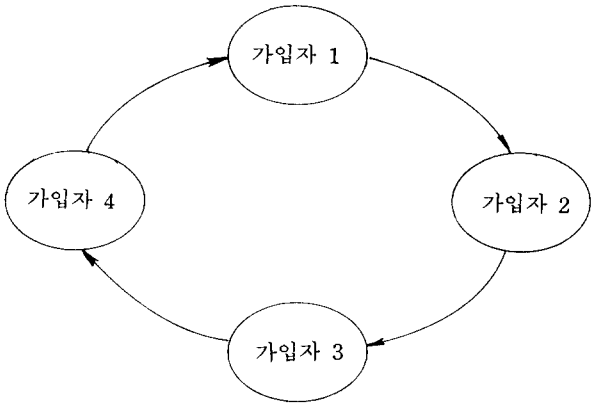


그림 1. 회의용 키 생성(4인)

순서 1에서의 가입자 1의 송신 정보는 식 (24), (25)로 표시되며 수신 정보는 식 (26), (27)로 표시된다.

$$Y_1^{(1)}=ID_1^{s_1} * g^{q_1 r_1 ID_2} \quad \text{mod n} \qquad (24)$$

$$Z_1^{(1)}=g^{ID_1 r_1 ID_2} \quad \text{mod n} \qquad (25)$$

$$Y_4^{(1)}=ID_4^{s_4} * g^{q_4 r_4 ID_4} \quad \text{mod n} \qquad (26)$$

$$Z_4^{(1)}=g^{ID_4 q_4 ID_4} \quad \text{mod n} \qquad (27)$$

순서 2에서 가입자 1의 인증과정은 가입자 4로부터의 수신 정보를 이용하여 식 (28)이 성립하는지 검증한다. 가입자 1은 인증 과정을 통해 송신자가 가입자 4라는 사실을 확인한다.

$$\{Y_4^{(1)}\}^{ID_4} / \{Z_4^{(1)}\}^{c_1}=ID_4 \qquad (28)$$

순서 2에서의 가입자 1의 송신 정보는 식 (29), (30)으로 표시되며 수신 정보는 시 (31), (32)로 표시된다.

$$Y_1^{(2)}=(ID_1\ ID_4)^{s_1} * g^{q_1 r_1 ID_2 r_4 ID_4} \quad \text{mod n} \qquad (29)$$

$$Z_1^{(2)}=g^{ID_1 r_1 ID_2 r_4 ID_4} \quad \text{mod n} \qquad (30)$$

$$Y_4^{(2)}=(ID_4\ ID_3)^{s_4} * g^{q_4 r_4 ID_1 r_3 ID_3} \quad \text{mod n} \qquad (31)$$

$$Z_4^{(2)}=g^{ID_4 r_4 ID_1 r_3 ID_3} \quad \text{mod n} \qquad (32)$$

순서 3에서 가입자 1의 인증과정은 가입자 4로부터의 수신 정보를 이용하여 식 (33)이 성립하는지 검증한다. 가입자 1은 인증 과정을 통해 송신자가 가입자 4라는 사실을 확인한다.

$$\{Y_4^{(2)}\}^{ID_4} / \{Z_4^{(2)}\}^{c_1} = ID_4\ ID_3 \qquad (33)$$

순서 3에서의 가입자 1의 송신 정보는 식 (34), (35)로 표시되며 수신 정보는 식 (36), (37)로 표시된다.

$$Y_1^{(3)} = (ID_1\ ID_4\ ID_3)^{s_1} * g^{q_1 r_1 ID_2 r_4 ID_4 r_3 ID_3} \mod n \qquad (34)$$

$$Z_1^{(3)} = g^{ID_1 r_1 ID_2 r_4 ID_4 r_3 ID_3} \mod n \qquad (35)$$

$$Y_4^{(3)} = (ID_4\ ID_3\ ID_2)^{s_4} * g^{q_4 r_4 ID_1 r_3 ID_3 r_2 ID_2} \mod n \qquad (36)$$

$$Z_4^{(3)} = g^{ID_{14} q_4 ID_1 r_3 ID_3 r_2 ID_2} \mod n \qquad (37)$$

순서 4에서 가입자 1의 인증과정은 가입자 4로부터의 수신 정보를 이용하여 식 (38)이 성립하는지 검증한다. 가입자 1은 인증 과정을 통해 송신자가 가입자 4라는 사실을 확인한다.

$$\{Y_4^{(3)}\}^{ID_4} / \{Z_4^{(3)}\}^{c_1} = ID_4\ ID_3\ ID_2 \qquad (38)$$

가입자 1은 최종적으로 회의용 키를 다음과 같이 생성한다.

$$CK = \{Z_4^{(3)}\}^{r_1} = g^{r_1 r_2 r_3 q_4 ID_1 ID_2 ID_3 ID_4} \mod n \qquad (39)$$

가입자 1, 2, 3 및 4는 각각 3회의 회의용 키 생성에 필요한 전송 정보를 전송한 후 공통키를 얻게되며 이는 가입자들 사이에서 비밀 통신 회의를 위한 키로 사용된다.

4. 제안한 방식에 관한 고찰

4.1 정수론적 고찰

본 논문에서 제안한 키 분배 방식에서 이용된 정수론적인 성질에 대해 살펴본다.

GF(p) 상의 원시 원소이며 GF(q) 상의 원시 원소인 g를 선택하는 이유는 유한체 상에서 원시 원소가 다음과 같은 성질을 갖고 있기 때문이다. 아래 식으로 표시되는 유한체 상에서의 멱승 함수를 생각하여 보자.

$$g^i = X \mod p \ (\text{단 } i = 0 \cdots n-1) \qquad (40)$$

이때 i를 0에서 n−1까지의 수로 멱승을 하면 그 치역은 i에 대해 유일한 값을 갖는다. 따라서 각 가입자들이 전송 정보 생성시 자신들의 개인 정보 ID와 난수 r_i로 g를 밑으로 하는 멱승 연산의 결과도 모두 유일하게 결정된다.

각 가입자의 비밀 정보 s_i를 생성할 때 mod $\Phi(n)$ 상에서 생성한 이유는 유한체상에서 지수부의 연산은 mod $\Phi(n)$에서 이루어지기 때문이다.

카드 발급 센터가 각 가입자의 비밀 정보를 위와 같이 선택한 후 해당 가입자에게만 분배하므로 다른 가입자들이 상대방의 비밀 정보를 계산 또는 유추해서는 안된다. 따라서 합성수 n의 선택도 신중히 이루어져야 한다. n은 두개의 큰 소수 p와 q의 곱으로 생성되며 소수 p와 q의 선택은 p−1 및 q−1의 인수가 적은 큰 소수를 선택하여야 계산적 안전성을 보장받는 암호계를 구성할 수 있다. 특히, 아래 식이 만족되는 소수를 선택하는 것이 안전하다[10,11].

$$p = 2p' + 1 \qquad (41)$$

$$q = 2q' + 1 \text{ 단, } p', q' \text{는 소수} \qquad (42)$$

이 경우의 $\Phi(n)$를 생각하면,

$$\Phi(n)=(p-1)(q-1)$$
$$=(2p'-1)(2q'-1)$$
$$=4p'q' \quad (43)$$

가 된다. 즉, $\Phi(n)$은 p', q' 및 4를 인수로 갖게 되므로 위에서 고려한 문제에 적합하다고 볼 수 있다. 각 개인의 s_i가 $\Phi(n)$ 상에서 생성되므로 s_i가 존재하기 위해서는 id 정보와 $\Phi(n)$이 서로소의 관계를 유지해야 한다.

$$\gcd(id_i, \Phi(n))=1 \quad (44)$$

이 때 각 id_i가 홀수이면서 p' 또는 q'를 인수로 갖지 않으면 위의 조건이 성립하게 된다. 이 경우 id와 $\Phi(n)$이 서로소가 아닐 확률은 식 (45)과 같이 매우 적다.

$$(p'+q'-1)/(p'q') \cong 2^{-400} \quad (45)$$

id 정보는 각 가입자의 개인 정보인 주민등록번호, 이름, 주소 등을 사용하므로 짝수일 확률이 1/2이다. 임의의 가입자의 id 정보가 짝수인 경우에는 id 정보가 $\Phi(n)$과 서로소가 안되므로 해당 가입자의 비밀 정보 s_i를 생성할 수 없는 문제점이 발생한다. 이 문제점을 해결하기 위해서는 모든 가입자의 id 정보를 홀수로 만들어 주면 된다. 즉, 각 가입자의 id 정보의 LSB에 1을 연접(concatenation)시켜 ID로 사용하면, 문제점을 해결할 수 있다.

4.2 안전성에 대한 고찰

가입자 i가 전송하는 전송 정보는 다음과 같이 구성되며 이를 구성하는 각각의 인수에 대한 안전성에 대해 고찰한다.

$$Y_i=ID_i^{s_i} * g^{c_i r_i ID_j} \mod n \quad (46)$$

$$Z_i=g^{ID_i ID_j r_i} \mod n \quad (47)$$

단, $C_i=HASH(Z_i, ID_i, ID_j, T_i)$

비밀 정보 s_i는 mod $\Phi(n)$에서 ID_i에 대한 곱셈 역원이므로 공개 정보 ID_i, n, g를 이용하여 계산하기는 어렵다. 왜냐하면, $\Phi(n)$은 센터만이 아는 비밀 정보이며 공개 정보 n을 통해서 $\Phi(n)$의 값을 얻어내는 것은 합성수의 소인수 분해 문제에 해당하게 되며 이에 대한 안전성은 이미 계산적으로 안전함이 입증되어 있다. 또한 Z_i를 통해 r_i의 값을 알아내는 것은 이산 대수 문제(discrete logarithm problem)에 해당되며 이 역시 합성수의 소인수 분해의 문제와 같이 그 안전성이 입증되었다[12]. 따라서 본 논문에서 제안한 ID-based키 분배 방식은 이산적 대수 문제 및 합성수의 소인수 분해의 어려움에 기반을 둔 안전한 키 분배 방식이라 할 수 있다. 또한 송, 수신 정보에 대한 직접 인증이 가능한 방식이기 때문에 가입자들이 정보 전송 후 송, 수신 정보의 부인을 봉쇄할 수 있는 방식이라 생각한다.

5. 결 론

본 논문에서는 이산적 대수 문제 및 합성수의 소인수 분해 문제를 이용한 새로운 ID-based 키 분배방식을 제안하였다. 본 논문에서 제안한 ID-based 키 분배 알고리즘의 특성은 일단 가입자가 센터로부터 정보를 받게된 후에는 다른 가입자와의 통신 및 키 생성과정에서 센터의 서비스를 필요로 하지 않는다는 점이다. 이는 smart 카드를 이용한 암호 방식에서 반드시 이루어져야 할 부분이다. 제안한 ID-based 회의용 키 분배 방식에서도 타 방식이 여러 가입자와 공통키를 생성하기 위하여 센터에 이들 가입자를 등록, 이에 대한 정보를 서비스 받는 것과는 달리 본 방식에서는 이러한 사전동작이 필요하지 않으며 새로운 가입자가 네트

워크에 가입하는 경우에도 기존의 가입자들이 소유한 공개 정보 및 자신의 비밀 정보를 갱신할 필요가 없다는 특성을 갖고 있다. 또한, 키 생성과정에서 상대방에게 전송되는 전송 정보를 통해 직접 인증(direct authentication)을 행함으로써 송, 수신 후 발생할 수 있는 가입자의 송, 수신 부인을 봉쇄할 수 있다. 그러므로 본 논문에서 제안한 키 분배 방식 알고리즘은 앞으로 다가올 화상 회의, 다자간 비밀 통신등에 효과적으로 적용되리라 사료된다.

향후 키 분배방식에서의 연구 방향은 보다 안전하고 효율적인 프로토콜 설계[13,14,15], 각종 적용 분야에 응용 및 구현, 현재까지의 많은 ID 정보에 의한 키 분배방식이 센터에 대한 의존도가 높은 것을 감안할 때 고신뢰 센터에 의존하지 않는 효율적인 프로토콜[16], ZKIP의 랜덤 정보(randomness information)를 이용한 키 분배방식에 대한 연구[17,18,19] 등이 진행되어야 한다고 생각된다. 또한, ID 정보에 의한 암호방식이 효과적으로 사용될 수 있는 smart 카드를 이용한 신분 확인, 전자 송금 등에도 효과적으로 대처해 나가야 할 것이다.

참 고 문 헌

1. W. Diffie, M.E. Hellman, "New Directions in Cryptography," IEEE Trans. IT-22, No. 6, pp. 644-654, 1976, 2.

2. 원동호, "암호방식과 키분배," 한국통신정보보호학회지, 1권, 1호, pp.72-82, 1991, 4.

3. R.L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Singatures and Public-Key Cryptosystems," CACM, Vol. 21, No. 2, pp. 120-126. Feb. 1978.

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

5. E. Okamoto, K. Tanaka, "Key Distribution System Based on Identification Information," Proc, GLOBECON 87, pp.108-111, 1987.

6. 손기욱, 이윤호, 권창영, 원동호, "ID를 기반으로 하는 키 분배방식," 대한 전공학회 하계 종합학술대회 논문집, 제 14 권, 제 1 호, pp.30-33, 1991, 6.

7. K. Koyama, K. Ohta, "Identity-based conference key distribution systems," Crypto 87, pp. 175-184, 1987.

8. Y. Yacobi, "Attack on the Koyama-Ohta identity baed key distribution scheme," Crypto 87, pp.429-433, 1987.

9. K. Koyama, K. Ohta, "Security of Improved Identity-based Conference Key Distribution System," EUROCRYPT 88, pp.11-19, 1988.

10. W. d. Jonge, D. Chaum, "Some veriations on RSA signature & their security," Crypto 86, pp. 49-59, 1986.

11. R.L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital signatures and Public-Key Cryptosystems," CACM, Vol. 21, No. 2, pp. 120-126, Feb, 1978.

12. J. Seberry, J. Pieprzyk, "Cryptography," Prentice Hall, pp.22-25, 1989.

13. Y. Yacobi, Z. Shmuely, "On Key Distribution System," Crypto 89. pp.334-355, 1989.

14. Y. Yacobi, "A Key Distribution : Paradox," Crypto 90, pp.245-255, 1990.

15. 이필중, 임채훈, "일반화된 Diffie-Hellman 키이 분배방식의 안전성 분석," 한국통신학회논문지, 91-7 Vol. 7, pp.575-597, 1991.

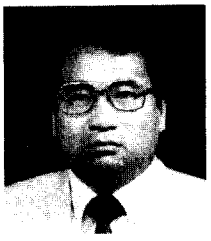
16. 박춘식, "고신뢰 센터를 고려하지 않은 강력한 개인 식별 방식," JCCI '91 논문집 제 1 권, pp.43-46, 1991.

17. T. Beth, "Efficient Zero-Knowledge Indetification Scheme for Smart Cards," EUROCRYPT 89, pp.29-37, 1989.

18. C.G. CUnter, "An identity-based key-exchange protocol," EUROCRYPT 89, pp.29-37, 1989.

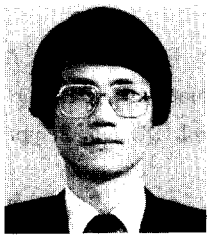
19. F. Bauspieβ, "How to keep Authenticity Alive in a Computer Network," EUROCRYPT 89, pp. 38-46, 1989.

□ 著者紹介



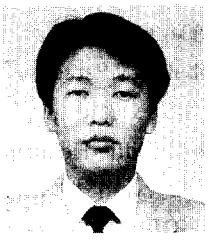
원 동 호(正會員)

1976年 성균관대학교 전자공학과 졸업(공학사)
1978年 성균관대학교 대학원 전자공학과 졸업(공학석사)
1988年 성균관대학교 대학원 전자공학과 졸업(공학박사)
1978~1980년 한국전자통신연구소 전임연구원
1985~1986년 일본 동경공대 객원연구원
1982~현재 성균관대학교 정보공학과 교수



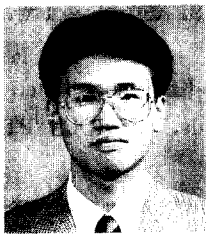
권 창 영(正會員)

1983年 성균관대학교 수학교육과 졸업(이학사)
1991年 성균관대학교 대학원 정보공학과 졸업(공학석사)
1991~현재 성균관대학교 대학원 정보공학과 박사과정 재학중
1982~1988 (주)KOLON 정보 SYSTEM실 팀장



양 형 규(正會員)

1983年 성균관대학교 전자공학과 졸업(공학사)
1985年 성균관대학교 대학원 전자공학과 졸업(공학석사)
1991~현재 성균관대학교 대학원 정보공학과 박사과정 재학중
1985~1991 삼성전자 컴퓨터 부문 선임연구원



손 기 욱(學生會員)

1990年 성균관대학교 정보공학과 졸업(공학사)
1990~현재 성균관대학교 대학원 정보공학과 석사과정 재학중