論 文

공개키 분배방식에 관한 연구

正會員 권 창 영* 正會員 원 동 호*

A Study on Public Key Distribution System

Chang Young KWON* Dong Ho WON* *Regular Members*

要 約 본 논문에서는 기존의 제안된 여러가지 공개키 분배방식을 정리하고, 3인 이상 다수 가입자의 공유 비밀 회의용 키로 사용할 수 있는 새로운 공개키 분배방식을 제안하였다.

본 방식은 모든 연산이 큰 소수 p에 관한 법연산이 적용되는 멱승 함수를 이용하였으며 GF(p)상에서 승산역원을 계산하기 위한 새로운 방법을 고안하였다. 또한, 기존의 방법과 달리 공통 암호화키를 분배하기 위한 사전 분배정보는 일방향 통신만으로 가능하다.

본 방식의 안전성은 유한체 GF(p)상에서 이산 대수의 이려움에 근거하며, DH(Diffie-Hellman) 공개키 분배방식 보다 강하다.

ABSTRACT This paper summarizes previously proposed several public key distribution systems and proposes a new public key distribution system to generate a common secret conference key for public key distribution systems three or more user.

The new system is based on discrete exponentiation, that is, all operations involve reduction modulo p for large prime p and we study some novel characteristics for computing multiplicative inverse in GF(p). We use one-way communication to distribute work keys, while the other uses two-way communication.

The security of the new system is based on the difficulty of determining logarithms in a finite field GF(p) and stronger than Diffie-Hellman public key distribution system.

I. 서 론

최근 컴퓨터 산업의 발전과 전기통신의 대중화로 정보화 사회가 급속하게 도래하고 있다. 이에 따라 정보의 축적, 처리, 전달이 고도화 다양화되어 정보 시스템의 이용은 산업, 경제, 교육의 분야와 행정기관을 비롯한 공공기관의 업무처리 등 사회 모든 분야로 확대되고 있다.

이러한 정보 시스템내에서 처리, 축적, 전달되는 정보는 불법유출, 내용변경, 미확인 발신자 및 수신자등의 위협을 내포하고 있어 정보 보호에 대한 관심이 고조되고 있다.

정보 시스템에서 요구하는 정보의 보호 수준에

*成均館大學校 情報工學科
Dept. of Information Telecommunication Eng.,
Sung Kyun Kwan University.
論文番號：90-99(接受1990. 10. 17)

따라 효율적이며 계층적인 보안대책을 제공하기 위해서는 암호계를 이용하는 것이 매우 효과적이다.

암호계는 키의 분배와 관리 방법에 따라 관용 암호방식 (conventional cryptosystem)과 공개키 암호방식(public key cryptosystem)으로 나눌 수 있다. 이중 관용 암호방식은 암호화키와 복호화키를 공통으로 사용하는 방식으로 암호계 이용자는 사전에 키를 비밀리에 나누어 갖고 있어야 한다. 따라서 관용 암호방식을 이용한 비밀 통신망에서는 공통 암호화키를 제삼자에게 알려지지 않게 분배해야 하는 문제가 발생한다. 이러한 문제 해결을 위해 Merkle은 비보호 통신로에서의 암호화키 전송 및 비밀통신에 관하여 논문을 발표하였으며[1] 이러한 개념의 구체적인 예로는 유한체 상에서 멱승의 가환성과 이산대수 문제를 이용한 최초의 공개키 분배 방식(PKDS : public key distribution system)인 Diffie-Hellman 방식(DH 방식)이 있다[2]. 그러나 DH 방식은 특정 가입자 2인 사이의 암호화키가 항상 일정한 문제점을 갖고 있어 이를 개선한 Yamamoto-Akiyama 방식(YA 방식), Okamoto-Nakamura 방식(ON 방식), Matsumoto-Takashima Imai 방식(MTI 방식) 등이 제안되었다[3,4,5].

이들 방식은 DH 방식의 암호화키(MK : master key)를 이용하여 메세지 통신용 암호화키(WK : work key)를 얻는 방법과 암호화키 WK를 직접 얻는 방식으로 대별되며 WK키를 교환하는 과정에서 사전 분배 정보의 교환과 많은 계산량을 필요로 한다[6].

본 논문에서는 보다 개선된 새로운 공개키 분배방식을 제안하고 타방식과의 차이점을 비교 연구하였다. 특히, 제안한 방식은 3인 이상의 다수 가입자 사이에 공유키(CKDS : conference key distribution system)로 사용할 수 있는 특징을 갖고 있다.

Ⅱ. 이산대수 문제

이산대수는 유한체 GF(p)상의 대수를 말하며 유한체 상에서 이산대수를 계산하는 문제를 이산대수 문제(discrete logarithm problem)라 한다. 실수 연산 체계에서 대수를 계산하는 문제는 매우 큰 수인 경우에도 간단하나 유한체상의 연산 체계에서 대수를 계산하는 문제는 매우 어렵다[2].

이산대수 문제는 정수의 이산대수 문제와 다항식의 이산대수 문제로 대별된다. 본 논문에서는 정수의 이산대수 문제를 이용하였으므로 이 문제에 관하여 기술한다.

이산대수 문제는 유한체상의 멱승관계이므로 먼저 유한체 GF(p)상의 멱승 성질을 살펴본다. GF(p)상의 0 이외의 원소 x, y에 대하여 다음 식이 성립한다.

$$(h)^{xy}=(h^{y})^{x} \tag{1}$$

$$h^{x}*h^{y}=h^{x+y} \tag{2}$$

$$h^{x}=h^{x \bmod(p-1)} \tag{3}$$

GF(p)상의 임의의 원소 g, z에 대하여 다음 식이

$$y=g^{z} \bmod p \tag{4}$$

성립할 때 z를 구하는 경우, z를 y의 이산대수라 하며 z는 식(5)로 나타낼 수 있다.

$$z=\log_{g} Y \tag{5}$$

이 때 g가 GF(p)상의 원시원소 (primitive element)이면 z값에 따라 서로 다른 y값을 갖게 된다.

유한체의 위수(order)가 작은 경우에는 원시원소 g를 멱승한 값을 미리 계산하여 대수표를 작성하면 이산대수를 구하는 문제는 간단히 해결된다.

그러나 유한체의 위수가 큰 경우에는 이산대수

를 계산하는 것은 상당히 어려운 문제이다. 이와 같은 복잡성을 이용하여 공개키 분배방식을 구성하였다.

Ⅲ. 공개키 분배방식

임호통신망 가입자가 자기의 비밀 정보 x_i와 공개 화일에 등록된 상대 가입자의 등록정보 y_j 로부터 공유정보를 계산하여 공통키로 사용하는 방식으로 이 방식을 이용하면 관용 암호계의 암호화키를 비보호 채널을 이용하여 분배할 수 있다.

이러한 방식을 공개키 분배방식이라 하며 그 알고리즘은 그림 1과 같다.

각 가입자가 상대가입자의 등록 정보와 자기의 비밀정보로 부터 공통 암호화키를 얻기 위한 알고리즘은 다음 조건이 만족되어야 한다.

조건1) $C(X_i, R(X_j))=C(X_j, R(X_i))$이 임의의 X_i, X_j에 대하여 성립하여야 한다.

조건2) 함수 R, C의 계산량이 적어야 한다.

조건3) 모든 (x_i, x_j)에 대하여 (R, C, $R(x_i)$, $R(x_j)$)와 부대정보 SI로부터 $C(x_i, R(x_j))=C(x_j, R(x_i))$를 얻기 위한 계산량이 충분히 커야 한다.

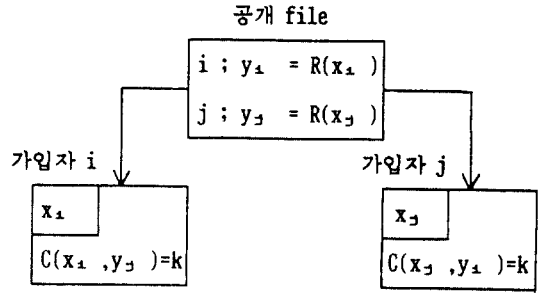


그림 1. 공개키 분배방식
Fig. 1. Public-key distribution system.

조건1), 2)를 만족하는 알고리즘을 공개키 분배방식이라 하며 부대정보 SI에 대하여 공개키 분배방식 (R, C)가 조건 3)를 만족할 때 (R, C)는 SI에 대하여 안전하다고 한다. 이러한 공개키 분배방식은 1976년 Diffie와 Hellman이 처음 이산대수 문제를 이용하여 구성하였다[2]. 이 방식은 그림 2와 같이 GF(p)상의 원시원소 g를 선택하여 각 가입자는 자신의 비밀정보 x_i를

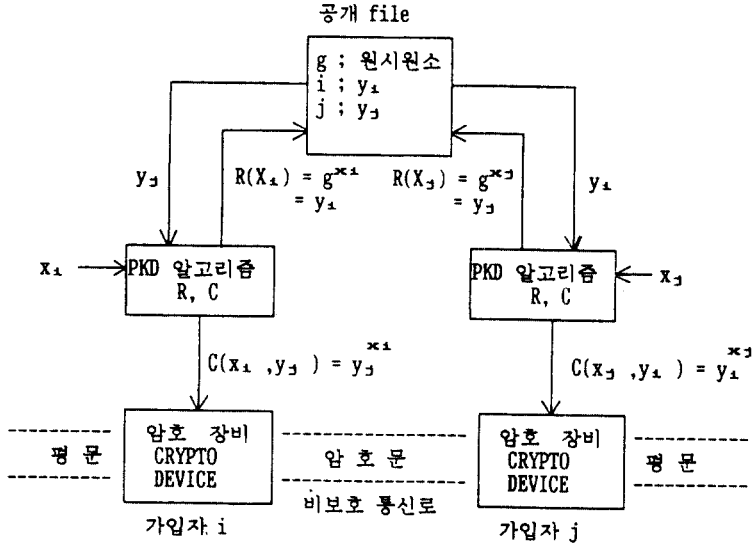


그림 2. D-H 공개키 분배방식
Fig. 2. D-H Public-key distribution system.

이용하여 등록정보 y_I를 계산하여

$$y_I=R(x_I)=g^{x_I} \quad (6)$$

을 공개 화일에 등록한다. 가입자 i와 가입자 j 사이에 비밀 통신을 하는 경우 공통키는 상대방의 등록정보에 자신의 비밀정보를 멱승하여 계산한다.

i, $$C(x_I, R(x_J))=(g^{x_J})^{x_I}=g^{x_Jx_I} \quad (7)$$

j, $$C(x_J, R(x_I))=(g^{x_I})^{x_J}=g^{x_Ix_J} \quad (8)$$

이 방식은 각 가입자의 비밀정보의 변경이 없는 한 공통 암호화키는 항상 일정하다. 이는 비밀통신에서 커다란 취약점이 된다. 이를 개선하기 위한 몇가지 방식이 제안되었다.

1. 기존의 공개키 분배방식

1.1. Yamamoto-Akiyama의 공개키 분배방식[3].

YA 공개키 분배방식은 DH 방식의 분배점을 극복하기 위해 가입자 i, j는 DH 방식의 공통키를 마스터 키(MK : master key)로 해서 가입자 i와 가입자 j는 각각 난수 R_I, R_J를 발생시켜 식(9), 식(10)과 같이 분배정보 Z_{IJ}, Z_{JI}를 생성하여 가입자 i는 j에게 Z_{IJ}를, 가입자 j는 i에게, Z_{JI}를 각각 양방향으로 전송한 다음, 가입자 i는 상대가입자 j의 분배정보 Z_{JI}에 난수 R_I를 멱승하여 암호화키(WK : work key) WK_I를 생성하며 가입자 j는 같은 방법으로 분배정보 Z_{IJ}로 부터 암호화키 WK_J를 생성한다.

1) $Z_{IJ}=MK^{R_I}$ (9)

2) $Z_{JI}=MK^{R_J}$ (10)

3) $WK_I=Z_{JI}^{R_I}$ (11)

4) $WK_J=Z_{IJ}^{R_J}$ (12)

단, $MK=g^{x_Ix_J}$

이 방식은 가입자 i와 j가 먼저 MK를 계산한 다음 각자 생성한 난수 R_I, R_J를 MK에 멱승하여 WK계산을 위한 분배 정보를 상대방에 전송해야 한다.

1.2. Okamoto-Nakamura 공개키 분배방식[4].

ON 공개키 분배방식은 YA 방식과 유사한 방법이나 MK를 경유하지 않고 별도의 분배정보를 교환하여 공통 암호화키를 생성하는 방식으로 ON(1)과 ON(2)가 있다.

ON (1)

1) $Z_{IJ}=y_I^{R_I}$ (13)

2) $Z_{JI}=y_J^{R_J}$ (14)

3) $WK_I=(Z_{JI}*y_J^{R_I})^{x_I}$ (15)

4) $WK_J=(Z_{IJ}*y_I^{R_J})^{x_J}$ (16)

ON(2)

1) $Z_{IJ}=y_J^{R_Ix_I}$ (17)

2) $Z_{JI}=y_I^{R_Jx_J}$ (18)

3) $WK_I=(Z_{JI})^{R_I}$ (19)

4) $WK_J=(Z_{IJ})^{R_J}$ (20)

ON 공개키 분배방식은 암호통신할 때마다 새로운 난수를 이용하므로 암호화키가 동일하지 않다.

ON(2) 방식은 YA 방식의 암호화키 생성 결과와 동일하다.

1.3. Matsumoto Takashima-Imai 공개키 분배

방식[5].

MTI 공개키 분배방식은 분배정보 생성이 간단하다는 것이 특징이다. MTI 방식의 일부는 공개 화일에 등록된 공개키의 지수부 즉, 가입자 i의 비밀키인 X_i의 mod P-1에서의 승산역원인 X_i^{-1}를 이용하였다. 이 방식은 앞에서 언급한 여러가지 공개키 분배방식에 비하여 비밀키 X_i를 선택하는데 제약이 있다. 이는 GF(p)상의 임의의 원소 X_i가 p-1을 법으로 하는 연산에서 승산역원이 항상 존재하는 것이 아니기 때문이다.

MTI(1)

1) $Z_{ij}=g^{R_i}$ (21)

2) $Z_{ji}=g^{R_j}$ (22)

3) $WK_i=Z_{ji}^{X_i}*y_j^{R_i}$ (23)

4) $WK_j=Z_{ij}^{X_j}*y_i^{R_j}$ (24)

MT1(2)

1) $Z_{ij}=y_j^{R_i}$ (25)

2) $Z_{ji}=y_i^{R_j}$ (26)

3) $WK_i=Z_{ji}^{X_i^{-1}}*g^{R_i}$ (27)

4) $WK_j=Z_{ij}^{X_j^{-1}}*g^{R_j}$ (28)

MTI(3)

1) $Z_{ij}=y_j^{R_i}$ (29)

2) $Z_{ji}=y_i^{R_j}$ (30)

3) $WK_i=Z_{ji}^{X_i^{-1}R_i}$ (31)

4) $WK_j=Z_{ij}^{X_j^{-1}R_j}$ (32)

MTI(4)

1) $Z_{ij}=g^{R_i}$ (33)

2) 없음

3) $WK_i=y^{(i^{X_i+R_i})}\quad y_j^{(X_i+R_i)}$ (34)

4) $WK_j=(Z_{ij}*y_i)^{X_j}$ (35)

2. 제안한 공개키 분배방식

Diffie-Hellamn의 공개키 분배방식 발표 이후 앞절에서 언급한 여러가지 형태의 공개키 분배방식이 제안되었으나 이 방식들은 3인 이상이 동시에 공유하는 암호화키를 공유할 수 없다. 뿐만 아니라 암호화키 분배를 위한 사전 계산량의 개선을 볼 수 없으며 MTI 방식은 비밀키 X_i의 선택에 문제가 있음을 알 수 있다. 즉, GF(p)상의 모든 원소가 mod p-1 상에서 승산역원을 갖지 못하므로 비밀키 X_i 선택 범위가 적어진다[8].

본 논문에서는 분배정보가 일방향이고, 3인 이상이 암호화키를 공유할 수 있는 새로운 공개키 분배방식을 제안한다.

제안한 공개키 분배방식의 구성 순서는 다음과 같다.

순서 1) 가입자 i는 난수 R_i로 식(36)과 같이 분배정보 Z_{ij}를 생성하여 가입자 j에 전송하고 WK를 식(37)과 같이 계산한다.

$$Z_{ij}=y_j^{X_i}*g^{R_i} \quad (36)$$

$$WK_i=g^{R_i} \quad (37)$$

순서 2) 가입자 j는 분배정보 Z_{ij}를 수신하여 식(38)과 같이 WK를 계산한다.

$$WK_j=Z_{ij}*(y_i^{X_j})^{-1} \quad (38)$$

제안한 방식의 가입자 i, j의 공통 암호화키 WK는 g^R이다.

분배정보 Z_{ij}와 $WK=g^R$의 계산량에 대하여 알아보자. 분배정보 Z_{ij}는 가입자 i가 상대가입자 j의 공개정보 y_j를 자신의 비밀정보 x_i로 멱승한 결과와 GF(p)상의 원시원소 g를 가입자 i 자신

이 선택한 난수 R_I를 누승한 결과를 곱하여 얻으므로 분배정보의 계산은 2회의 멱승과 1회의 승산이 필요하다.

공통 암호화키의 계산은 가입자 i의 경우는 분배정보 Z_{IJ} 계산시 이미 완료되며 가입자 j의 경우에는 수신한 분배정보 Z_{IJ}에 가입자 i의 공개정보 y_I를 x_J로 멱승한 결과의 승산역원을 구하여 곱하면 구할 수 있으므로 가입자 j의 공통 암호화키 계산은 멱승 1회와 승산 역원 계산 1회, 승산 1회가 필요하다.

따라서 제안한 공개키 분배방식의 공통 암호화키 분배시 총계산량은 '멱승 3회+승산 2회+승산역원 계산 1회'이다. 이 계산량중 가장 문제가 되는 것이 승산역원 계산이다. GF(p)상의 승산역원을 구하는 방법은 유한체 성질을 이용하여 p-2승을 하는 방법과[7] 유크리드 알고리즘(Euclid's algorithm)을 이용하는 방법이 있으나 본 논문의 경우는 다음 정리를 이용하면 $g^{x_Ix_J}$의 승산역원을 간단히 구할 수 있다.

[정리] g가 GF(p)상의 원시원소일 때 식(39)과 식(40)을 만족하는 GF(p)상의 임의의 원소 y_I, x_J, y_J 값을 알고 x_I값을 모를 때

$$y_I=g^{x_I} \bmod p \tag{39}$$

$$y_J=g^{x_J} \bmod p \tag{40}$$

GF(p)상의 원소 $g^{x_Ix_J}$의 승산역원 $(g^{x_Ix_J})^{-1}$은 식(41)과 같이 계산할 수 있다.

$$(g^{x_Ix_J})^{-1}=(g^{x_I})^{(p-1)-x_J} \bmod p \tag{41}$$

(증명) p, x_J를 알고 있으므로 $(p-1)-x_J$는 간단히 계산되며 y_I값을 알고 있으므로 식(42)이 계산 가능하다.

$$k=(y_I)^{(p-1)-x_J} \bmod p \tag{42}$$

다시 식(42)는 다음과 같이 변형된다.

$$\begin{aligned} k&=(y_I)^{(p-1)-x_J} && \bmod p\\ &=(g^{x_I})^{p-1-x_J} && \bmod p\\ &=g^{x_I(p-1)-x_Ix_J} && \bmod p\\ &=(g^{p-1})^{x_I}*g^{-x_Ix_J} && \bmod p\\ &=g^{-x_Ix_J} && \bmod p\\ &=(g^{x_Ix_J})^{-1} && \bmod p \end{aligned} \tag{43}$$

따라서 $g^{x_Ix_J}$의 승산 역원은 식(41)로 계산 가능하다.(증명완료)

위 정리를 이용하면 제안한 공개키 분배방식에서 암호화키 분배시에 필요한 계산량은 '멱승 3회+승산 2회+감산 1회'로 감소된다.

3. 3인 이상의 공유키 분배방식

비밀 통신망에서 다수 가입자가 동보통신을 할 때, 다수 가입자가 암호화키를 공유하여 통신을 하면 보다 효과적이다. 다수 가입자 간에 암호화키를 공유하지 않고 동보통신을 하려면 송신자는 평문을 각기 다른 n-1개의 암호화키로 (n-1)회 암호화하여 n-1명의 가입자에게 서로 다른 암호문을 전송해야 한다. 이러한 단점을 동보통신을 하려는 다수 가입자의 암호화키를 공유하게 하는 공유키 분배방식(CKDS : conference key distribution system)을 이용, 해결할 수 있다. 제안한 공개키 분배방식을 이용하면 간단히 공개키 분배를 할 수 있다.

이러한 공유키 분배 방식의 과정은 다음과 같다.

순서 1) 소수 p와 GF(p)상의 원시원소 g를 가입자 n인에게 공개한다.

순서 2) 각 가입자 i($1\leq i\leq n$)는 1…p-1 범위의 원소 x_I를 무작위로 선택 비밀키로 한다.

순서 3) 각 가입자는 원시원소 g와 자신의 비밀키 x_I를 이용하여 공개키 y_I를 생성하여 공개 화일에 등록한다.

$$y_I=g^{x_I} \tag{44}$$

순서 4) 송신가입자 i는 1…p-1 범위의 난수 R를 선택 분배정보를 생성한다.

$$Z_{ij}=y_j^{x_i} * g^R$$
$$=g^{x_i x_j} * g^R$$
$$=g^{x_j x_i \cdot R} \quad (45)$$

송신가입자 i는 분배정보를 각 가입자 j(i≠j)에 전송하고 공유키 CK(conference key)를 생성한다.

$$CK=g^R \quad (46)$$

순서 5) 각 가입자 j는 분배정보 Z_{ij}로부터 공유키를 생성한다.

$$CK=Z_{ij} * (y_i^{x_j})^{-1}$$
$$=g^{x_j x_i + R} * (g^{x_i x_j})^{-1}$$
$$=g^R \quad (47)$$

Ⅳ. 타 방식과 비교

1. 암호화키 생성시 필요한 계산량과 특징

GF(p)상의 원소의 멱승의 평균계산량을 [^], 승산의 계산량을 [*]로 표시하고 mod p−1에서의 감산의 계산량을 [−], 가산의 계산량을 [+], 승산 계산량을 [.]로 표시하면 각 공개키 분배방식의 암호화키 변경시 필요한 계산량은 표1과 같다.

표 1에서 알 수 있는 바와 같이 암호화키 분배를 위한 사전계산량은 DH 방식이 제일 적으나 암호화키가 항상 일정한 단점이 있다.

공통 암호화키를 통신할 때마다 변경할 수 있는 개선된 방식들은 모두 사전 분배정보가 필요하며 대부분 6~8회의 사전 계산이 필요하다. 특히, MTI(2), MTI(3) 방식은 비밀정보 선택시 GF(p) 상에서 mod p−1의 승산역원을 갖는 원소를 선택해야 하므로 비밀정보 선택에

표 1. 각 공개키 분배방식의 키 변경시 필요한 계산량
Talbe 1. Computation for exchange of a key on several PKDS

분배방식		전송정보 생성시	암호화키 생성시	특징	난수 생성 횟수 및 분배정보 통신횟수
DH	i	0	[^]	공통 암호화키 동일	0
	j	0	[^]		0
YA	i	2[^]	[^]	MK를 경유	2
	j	2[^]	[^]		2
ON(1)	i	[^]	2[ ]+[*]		2
	j	[^]	2[ ]+[*]		2
ON(2)	i	[^]+[.] [^]	[^]	YA 방식과 결과 동일	2
	j	[^]+[.] [^]	[^]		2
MT1(1)	i	i [^]	2[^]+[*]		2
	j	[^]	2[^]+[*]		2
MTI(2)	i	i [^]	2[^]+[*]	비밀정보 선택 제한.	2
	j	[^]	2[^]+[*]		2
MTI(3)	i	i [^]	[^]+[.]	비밀정보 선택 제한.	2
	j	[^]	[^]+[.]		2
MTI(4)	i	i [^]	[^]+[+]	분배정보 1회	1
	j	0	[^]+[*]		1
제안한 분배방식	i	2[^]+[*]	0	공유키 분배방식 가능	1
	j	0	[^]+[*]+[−]	분배정보 1회	1

제한이 있다. 한편 이미 제안된 공개키 분배방식들은 모두 동보통신을 위한 공유키 분배방식으로 이용할 수 없으나 본 논문에서 제안한 공개키 분배방식은 공유키 분배방식으로 사용할 수 있는 장점이 있다.

2. 암호화키 위조시 필요한 계산량

제안한 공개키 분배방식의 안전성을 검토하기 위하여 제3자가 공개 화일에 등록된 공개 정보와 입수 가능한 각종 정보를 이용하여 암호화키 WK를 위조하려고 할 때 필요한 계산량을 제안한 방식에서의 공통 암호화키 강도로 채택하였다.

기존의 방식과 비교하기 위해 DH 공개키 분배방식의 암호화키 위조에 필요한 계산량을 [DH]로 표시하여 제안한 방식과 비교 검토하였다.

DH 공개키 분배방식에서 암호화키를 위조하는 함수 DH를 식(48)로 정의하자.

$$DH(g ; g^{xI}, g^{xJ})=g^{xIxJ} \tag{48}$$

식(48)에서 g^{xI}, g^{xJ}는 공개 화일의 공개 정보이다.

함수 DH는 식(49) 및 식(50)이 성립한다.

$$DH(g^{xI} ; g, g^{xIxJ})=g^{xJ} \tag{49}$$

$$DH(g ; g^{xIxJ}, g^{-1})=g^{xIxJ} \tag{50}$$

또한, 제안한 공개키 분배방식에서 공개 화일의 공개 정보와 비보호 통신로의 분배 정보를 이용하여 암호화키를 위조하는 함수 KW를 식(51)로 정의하자.

$$\begin{aligned} WK&=KW(g ; y_I, y_J, Z_{IJ})\\ &=KW(g ; g^{xI}, g^{xJ}, g^{xIxJ\cdot R})\\ &=g^{R} \end{aligned} \tag{51}$$

식(51)에서 g^{xI}, g^{xJ}는 공개 화일의 공개 정보이며 $g^{xIxJ\cdot R}$은 비보호 통신로에서 입수 가능한 분배정보이다.

식(48), (49), (50)을 이용하여 제안한 공개키 분배방식의 암호화키를 위조하는 함수 KW를 DH 공개키 분배방식의 암호화키를 위조하는 함수 DH로 나타내면, 식(52) 같이 된다.

$$\begin{aligned} &KW(g ; g^{xI}, g^{xJ}, g^{xIxJ+R})\\ &\quad=DH(g ; DH(g ; g^{xI}, g^{xJ}), g^{-1})*g^{xIxJ+R}\\ &\quad=DH(g ; g^{xIxJ}, g^{-1})*g^{xIxJ+R}\\ &\quad=g^{xIxJ}*g^{xIxJ+R}\\ &\quad=g^{R} \end{aligned} \tag{52}$$

따라서 제안한 방식에서 암호화키를 위조할 때 필요한 계산량은 DH 방식에서 암호화키를 위조할 때 필요한 계산량 [DH] 보다 승산역원 계산 및 승산이 필요함을 알 수 있다.

한편, 임의로 선택한 난수가 $R=x_Ix_J$인 경우에는 식(53) 같이 된다.

$$\begin{aligned} &KW(g ; g^{xI}, g^{xJ}, g^{2xIxJ})\\ &\quad=DH\ (g ; g^{xI}, g^{xJ})\\ &\quad=g^{xIxJ} \end{aligned} \tag{53}$$

이 경우의 발생 확률은 $1/p-1$이므로 발생될 가능성이 극히 적으나 위조에 필요한 계산량은 DH 공개키 분배방식에서의 암호화키 위조시 필요한 계산량인 [DH]와 동일하다.

따라서 제안한 공개키 분배방식에서의 암호화키 위조에 필요한 계산량은

$$[DH]\leqq[KW]\leqq[DH]+[\text{승산역원}]+[*] \tag{54}$$

의 관계를 갖는다. 즉, 제안한 공개키 분배방식의 암호화키 위조시 필요한 계산량은 DH 공개키 분배방식의 암호화키 위조시 필요한 계산량 보다 많이 소요되므로 제안한 방식의 암호화키 강도가 DH 방식의 암호화키 강도 보다 강함을 알 수 있다.

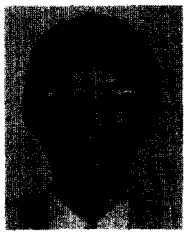
V. 결 론

본 논문에서는 Diffie, Hellman의 공개키 분배 방식을 개선하여 암호화키를 임의로 변경할 수 있는 새로운 공개키 분배방식을 제안하였다. 제안한 방식은 사전의 분배 정보가 송신 가입자로부터 수신 가입자에게 1회 일방향성으로 전송되며 공통 암호화키 변경시 계산량이 이미 제안된 타방식 보다 적다. 또한 암호강도는 제3자가 입수 가능한 정보 g, g^{X_I}, g^{X_J}, $g^{X_I X_J \cdot R}$로 부터 계산할 경우 DH 방식보다 강하다.

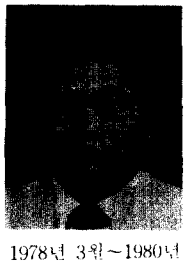
특히, 제안한 공개키 분배방식은 3인 이상의 동보 비밀통신에 이용할 수 있는 공유키로도 사용할 수 있는 특징을 갖고 있어 비밀통신에 널리 이용되리라 사료된다.

參 考 文 獻

1. Merkle, R. : "Secure communication over an insecure channel", communication of ACM, vol. 21, No. 4, pp. 294~299, Apr. 1978.
2. Diffie, W. Hellman, M. E. : "New direction in cryptography", IEEE Trans. on Inform. Theory, vol. IT-22, No. 6, pp. 644~654, Nov. 1976.
3. Yamamoto, T, Akiyama, R, : "A Data Encryption Device Incorporating Fast PKDS", Proc. of IEEE Gloval Telecommunication Conference, pp. 1,085~1,090, Nov. -Dec. 1985.
4. 岡本榮司, 中村勝洋 : "公開鍵配送方式の一檢討", 昭和59年度 電子通信學會 通信部門 全國大會 講演論文集 [分冊 1] No. 15 (Oct. 1984).
5. 松本勉, 高嶋洋一, 今井秀樹 : "公開鍵配送方式の關する二つの考察", 電子通信學會 技術研究報告, IT 84-40, 1985.
6. 松本勉, 高嶋洋一, 今井秀樹 : "古典的 PKDS と新しい PKDS", 電子通信學會 技術研究報告 IT 85-19, 1985.
7. 장기태, 박광식, 권창영, 원동호, "GF(p^m)상의 정규기저를 이용한 고속 승산역원 계산 알고리즘에 관한 연구", 한국통신학회 추계학술발표회 논문집, pp. 232~235, 1989.
8. 권창영, 손기욱, 김형수, 원동호, "이산적 대수 문제를 이용한 새로운 공개키 분배방식", 한국통신학회 하계학술발표회 논문집, pp. 804~808, 1990.



권 창 영(Chang Young KWON) 정회원
1957년 4월 22일생
1983년 2월 : 성균관대학교 수학교육과 졸업(이학사)
1989년 3월~현재 : 성균관대학교 대학원 정보공학과 석사과정
1982년 12월~1988년 9월 : (주)KOLON 정보 SYSTEM실 팀장



원 동 호(Dong Ho WON) 정회원
1949년 9월 23일생
1976년 2월 : 성균관대학교 전자공학과 졸업(공학사)
1978년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학석사)
1988년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학박사)
1978년 3월~1980년 4월 : 한국통신기술연구소 연구원
1985년 9월~1986년 8월 : 일본 동경공대 객원연구원
1982년 3월~현재 : 성균관대학교 정보공학과 부교수