ID 정보에 의한 회의용 암호키 분배방식

○ *손 기 욱, *이 경 호, *권 창 영, **이 인 숙, *원 동 호

* 성균관대학교 정보공학과
** 한국 통신 연구개발단

A Study on the Conference Key Distribution System based on ID-information

Ki-Wook Sohn, Kyoung-Ho Lee, Chang-Young Kwon
In-Sook Lee, Dong-Ho Won

* Sung Kyun Kwan University
Dept. of Information Engineering
** Korea Telecom. Research Center

요 약

암호 방식의 보안성은 암호키 보안에 커다란 영향을 받고 있어 암호 통신망 가입자가 상호간에 공유해야 하는 통신키 분배 문제가 암호학의 중요한 연구 분야가 되고 있다. 통신키를 분배 하는 방식은 크게 중앙 집중식 키 분배 방식과 공개키 분배 방식, 그리고 ID 정보에 의한 분배 방식으로 나눌 수 있다.

본 논문에서는 다자간 회의용 암호 통신키 분배 방식으로 사용할 수 있는 새로운 ID 정보에 의한 키 분배 방식을 제안하였다.

I. 서론

정보 시스템내에서 전송, 처리, 축적되는 정보는 전기적 현상을 이용하여 디지탈화, 대용량화 되고 있어 정보에 대한 적절한 보호 조치가 없으면 전송, 처리중 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 정보 보호를 위한 대책으로는 설비면에서의 물리적 대책, 관리 운영면에서의 인적 자원에 대한 대책, 기술면에서의 대책, 법과 제도면에서의 대책등이 있을 수 있으나 가장 경제적이면서도 보안 수준에 따라 효율적이면서도 계층적인 보안 대책을 제공할 수 있는 방법이 기술면에서의 대책인 암호 방식을 이용하는 방법이다.

암호 방식이란 보호하려는 정보를 작은 길이의 암호키로 관리하는 것이라 말할 수 있다. 따라서 암호 방식에서 효율적인 정보 보호를 위해서는 암호키를 안전하게 관리해야 한다.

암호키 관리는 키의 생성, 보관, 폐기 및 분배로 나누어 생각할 수 있는데 이중에서 가장 문제가 되는 것이 제 3자(해독자)에게 암호키를 노출되지 않게 분배하는 것이다.

암호키를 분배하는 방식은 크게 중앙 집중식 키 분배 방식, 공개키 분배 방식으로 나눌 수 있다. 중앙 집중식 키 분배 방식은 키 분배 센터와 가입자 사이에 터미날 키가 필요하며 공개키 분배 방식은 공개 화일을 갖추고 있어야 하는 불편이 있다.

이러한 단점을 극복할 수 있는 암호키 분배 방식으로 ID 정보에 의한 암호키 분배 방식이 있다. ID 정보에 의한 암호키 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, ROM등을 내장하고 있다.[4,5]

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

키를 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.

본 논문에서는 ID 정보에 의한 키 분배 방식을 새로이 제안하고 회의용키로 사용할 수 있음을 확인하였다.

Ⅱ. 제안한 ID 정보에 의한 암호키 분배 방식

이미 서론에서 언급된 바와 같이 기존의 공개 키 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 기존의 공개키 분배 방식에서와 마찬가지로 양자간의 비밀 통신키 생성 및 분배와 3인 이상이 서로 비밀 통신을 하기위한 회의용 키 분배 방식을 제안하였다. 이 회의용 키 분배 방식은 통신망에서 다수의 가입자들 사이에서 상호 비밀 통신에 사용될 수 있다.

모든 ID 정보에 의한 키 분배 방식은 두 단계를 통해 생성 및 분배된다. 첫 번째 단계에서 센터는 키 분배 시스템의 비밀 정보, 공개 정보 및 가입자의 ID 정보를 이용해서 각 가입자에 대한 비밀 정보를 생성한다. 이 가운데 가입자 공개 정보는 모든 가입자들이 알 수 있는 정보이고, 각 가입자의 비밀 정보는 안전한 채널(smart card)을 통해서 각 가입자에게 전달되며 이는 센터 및 각 가입자만이 알 수 있는 정보이다.

첫 번째 단계에서는 키 분배 시스템에 필요한 인자들이 카드 발급 센터에 의해 생성된다.

먼저 센터는 두 개의 큰 소수 p와 q를 선택하고 이들의 곱인 n을 생성한다. 이 때 p와 q는 256 bits 정도 길이를 갖는 소수가 선택된다. 이는 RSA 암호 방식에서 사용하는 인자들과 동일하게 생성된다.[3] 다음, 센터는 GF(p)상의 원시 원소이면서 GF(q)상의 원시 원소인 g를 생성한다. 또한 카드 발급 센터는 각 가입자의 공개 정보

인 id_i를 이용해서 비밀 정보인 s_i를 다음과 같은 조건이 성립하도록 생성한다.

$$s_i = id_i^{-1} \mod \Phi(n) \quad 단, \ \Phi(n) = (p-1)(q-1) \tag{1}$$

$$id_i \ id_i^{-1} = 1 \mod \Phi(n) \tag{2}$$

카드에 저장 각 가입자에게 전송되는 정보는 n, g, s_i가 되며 n과 g는 모든 가입자들에 대한 공개 정보이며 s_i는 가입자 i에 대한 비밀 정보이다.

두 번째 단계는 센터로부터 발급받은 정보와 각 가입자들의 공개 정보 id_i를 이용해서 각 가입자들이 공통키를 생성하는 통신 단계로, 가입자 i 및 j는 센터로부터의 전송 정보 및 자신이 선택한 난수를 이용하여 양자간의 통신키를 생성한다.

[protocol id-KDS]

step 1. : 가입자 i는 가입자 j에게 전송할 전송 정보 Y_i, Z_i 를 다음과 같이 생성한다.

$$Y_i = (id_j^{s_i} g^{r_i})^{id_j} \mod n \tag{3}$$

$$Z_i = g^{r_i \ id_i \ id_j} \mod n \tag{4}$$

가입자 j는 i로부터의 전송 정보를 통해 가입자 i의 사실 여부를 확인한 뒤 자신의 비밀 정보 및 자신이 선택한 난수를 이용해서 비밀 공통키를 다음과 같이 생성한다.

$$\begin{aligned} (Y_i)^{s_j id_i} &= (id_j^{id_i^{-1} id_j} g^{r_i id_j})^{id_j^{-1} id_i} \\ &= id_j \ g^{r_i \ id_i} \mod n \end{aligned} \tag{5}$$

$$\begin{aligned} (Z_i)^{s_j} &= (g^{r_i \ id_i \ id_j})^{id_j^{-1}} \\ &= g^{r_i \ id_i} \mod n \end{aligned} \tag{6}$$

이 경우 (5)식과 (6)식을 이용 가입자 j는 인증 과정을 통해 가입자 i라는 사실을 확인한다.

$$\left[id_j \, g^{r_i \, id_i} \; / \; g^{r_i \, id_i} \right] = id_j \quad \text{mod } n \qquad (7)$$

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

$$KEY = (Z_i)^{r_j}$$
$$= g^{r_i r_j id_i id_j} \quad \text{mod } n \qquad (8)$$

step 2. : 가입자 j는 가입자 i에게 전송할 전송 정보 Y_j, Z_j 를 다음과 같이 생성한다.

$$Y_j = (id_i^{s_j} \, g^{r_j})^{id_i} \quad \text{mod } n \qquad (9)$$

$$Z_j = g^{r_j \, id_i \, id_j} \quad \text{mod } n \qquad (10)$$

가입자 i는 j로부터의 전송 정보를 통해 가입자 j의 사실 여부를 확인한 뒤 자신의 비밀 정보 및 자신이 선택한 난수를 이용해서 비밀 공통키를 다음과 같이 생성한다.

$$(Y_j)^{s_i id_j} = (id_i^{id_j^{-1} id_i} \, g^{r_j id_i})^{id_i^{-1} id_j}$$
$$= id_i \, g^{r_j \, id_j} \quad \text{mod } n \qquad (11)$$

$$(Z_j)^{s_i} = (g^{r_j \, id_j \, id_i})^{id_i^{-1}}$$
$$= g^{r_j \, id_j} \quad \text{mod } n \qquad (12)$$

이 경우 (11)식과 (12)식을 이용 가입자 i는 인증 과정을 통해 가입자 j라는 사실을 확인한다.

$$\left[id_i \, g^{r_j \, id_j} \; / \; g^{r_j \, id_j} \right] = id_i \quad \text{mod } n \qquad (13)$$

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

$$KEY = (Z_j)^{r_i}$$
$$= g^{r_i r_j id_i id_j} \quad \text{mod } n \qquad (14)$$

이 후 가입자 i와 j는 공통키를 소유하게 되며 상대방과의 비밀 통신에 있어서 이 키를 사용한다.

Ⅲ. 회의용 암호키 생성 단계

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

[protcol id-CKDS]

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

$$Y_i = (id_{i+1}{}^{s_i} g^{r_i})^{id_{i+1}} \mod n \qquad (15)$$

$$Z_i = g^{r_i\, id_i\, id_{i+1}} \mod n \qquad (16)$$

step 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.

$$(Y_{i-1}{}^{id_{i-1}{}^{s_i}} / Z_{i-1}{}^{s_i}) = id_i * \prod_{2\le k\le j-1} id_{i-k} \mod n \qquad (17)$$

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, Z_i를 생성하여 가입자 i+1에게 전송한다.

$$Y_i = \left(\left(id_{i+1} \prod_{1\le k\le j-1} id_{i-k} \right)^{s_i} * g^{r_i \prod_{1\le k\le j-1} r_{i-k}\, id_{i-k}} \right)^{id_{i+1}} \mod n \qquad (18)$$

$$Z_i = g^{r_i\, id_i id_{i+1} \prod_{1\le k\le j-1} r_{i-k}\, id_{i-k}} \quad \bmod n \qquad (19)$$

그리고 가입자 i는 다음 step인 j+1을 수행한다.

step m : 가입자 i는 Y_{i-1}, Z_{i-1} 을 수신한다. 식 (17) 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.

이 때 회의용 암호키를 생성한다.

$$K = (Z_{i-1})^{r_i} \quad \bmod n \qquad (20)$$

실제 키의 값은

$$KEY = g^{\prod_{1\le k\le m} id_k\, r_k} \quad \bmod n \qquad (21)$$

이 된다.

Ⅳ. 결론

본 논문에서는 이산적 대수 문제 및 합성수의 소인수 분해 문제를 이용한 새로운 키 분배 방식을 제안하였다. 본 논문에서 제안한 키 분배 알고리즘의 특성은 일단 가입자가 센터로부터 정보를 받게된 후에는 다른 가입자와의 통신 및 키 생성 과정에서 센터의 서비스를 필요로 하지 않는다는 점이다. 이는 smart 카드를 이용한 암호 방식에서 반드시 이루어져야 할 부분이다. 또한 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 사전 동작이 필요하지 않으며 새로운 가입자가 네트워크에 가입하는 경우에도 기존의 가입자들이 소유한 공개 정보 및 자신의 비밀 정보를 갱신할 필요가 없다는 특성을 갖고 있다.

또한 키 생성 과정에서 상대방에게 전송되는 전송 정보를 통해 직접 인증(direct authentication)을 행함으로써 송, 수신 후 발생할 수 있는 가입자의 송,수신 부인을

봉쇄할 수 있다.

본 논문에서 제안한 키 분배 방식 알고리즘은 앞으로 다가올 화상 회의, 다자간 비밀 통신등에 효과적으로 적용되리라 사료되며 앞으로의 연구 방향은 보다 안전하고 효율적인 프로토콜 설계 [10,11,12], 적용 분야에 응용, 실제로 구현하는 것과 현재까지의 많은 ID 정보에 의한 키 분배 방식이 센터에 대한 의존도가 높은 것을 감안할 때 고신뢰 센터에 의존하지 않는 효율적인 프로토콜[13], ZKIP의 랜덤 정보(randomness information)를 이용한 키 분배 방식에 대한 연구[14,15,16]가 진행되어야 한다고 생각된다. 또한 ID 정보에 의한 키 분배 방식이 효과적으로 사용될 수 있는 폐쇄 group 내에서의 키 분배 방식에 대한 연구도 병행되어야 할 것이며 이를 통해 곧 도래할 smart 카드를 이용한 전자 송금, 신원 확인등에도 효과적으로 대처해 나가야 할 것이다.

V. 참고 문헌

1. W.Diffie, M.E.Hellman, "New Directions in Cryptography", IEEE Trans. IT-22, NO.6, pp.644-654, 1976.2.

2. 원동호, "암호 방식과 키분배", 한국 통신 정보 보호 학회지, 1권, 1호, pp.72-82, 1991.4

3. 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.

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. I.Ingemarson, D.Tang, C.K.Wong, "A Conference Key Distribution System", IEEE Trans. IT-28, NO.5, pp.714-720, 1982.

7. K.Koyama, K.Ohta, "Identity-based conference key distribution systems", Crypto87, pp.175-184, 1987.

8. Y.Yacobi, "Attack on the Koyama-Ohta identity based 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. Y.Yacobi, Z.Shmuely, "On Key Distribution System", Crypto 89. pp.334-355, 1989.

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

12. 이필중, 임채훈, "일반화된 Diffie-Hellman 키이 분배방식의 안전성 분석", 한국통신학회논문지, 91-7 vol.16, No.7, pp.575-597, 1991.

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

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

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

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