수정된 ID 기본 암호시스템을 이용 1대 N 그룹통신에 적합한 키 분배방법

임 웅 택, 김 화 수
국방대학원 전자계산학과

A Key Distribution Scheme for 1 TO N Group Communication Using Modified ID-Based System

Ung-Taeg Lim, Hwa-Soo Kim
Dept. of Computer Science, National Defense College

요 약

ID 기본 암호시스템은 1984년 Shamir에 의해 제안되어 기존의 암호시스템이 가지고 있는 공개키 관리에 대한 문제점을 해결하였다. ID기본 암호시스템은 두 사용자간 암호통신에 적합 하지만 이를 1 대 N 그룹통신에 적용 할경우 N개의 각 사용자에 대한 대화키(Session Key)를 생성하여 N번의 암호화로 각 사용자와 암호통신을 해야 하는 문제점이 대두되므로, 본 논문은 지금까지 발표된 ID기본 암호시스템을 바탕으로 1 대 N 그룹통신에 적합 하도록 수정된 ID 기본 암호시스템을 제안한다. 제안된 ID 기본 암호시스템은 암호통신을 하고자하는 사용자가 임의의 사용자 그룹을 선정하여 각 사용자와 핸드쉐이크 과정을 통하여 상호 인증을 실시하며, 핸드쉐이크 과정에서 전달된 각 사용자의 비밀키가 포함된 자료를 이용 그룹 공통의 대화키를 생성한다.

제안된 ID 기본 암호방식의 특징은 (i)암호통신을 위한 사용자 그룹은 둘이상 임의로 선정 가능하고, (ii)상대방 인증을 위해 별도의 해쉬함수를 사용하지 않으며, (iii)그룹은 하나의 공통 대화키를 사용한다는 점이다.

I. 서 론

현대 사회가 고도의 정보화 사회로 발전 함에 따라 수많은 자료가 컴퓨터를 통하여 저장 및 처리되고 많은 사용자는 컴퓨터 통신망을 이용하여 다른 사용자와 빈번한 정보교환을 하고있다. 이에따라 중요하고 가치있는 정보가 통신 도중에 제삼자에게 노출되거나 불법적인 침입자에 의해 도청 및 변조에 대한 보안대책이 요구되고 있다.

정보보호를 위해 가장 효율적인 수단은 암호를 이용하는 방법으로 암호방식은 암호키의 분배와 관리방법에 따라 개인키 암호시스템과 공개키 암호시스템으로 나눌수 있다[1]. 개인키 암호시스템은 암호키와 복호화키를 공통으로 사용하는 방식으로 통신망 가입자는 상대방과 암호통신을 하기위해 상대방과 자신을위한 비밀키를 갖고 있어야한다. 따라서 이 방식은 각 사용자가 다른 사용자 수 만큼의 비밀키를 가지고 있어야 한다는 문제점이 있다. 한편 공개키 암호시스템은 암호키와 복호키를 분리하여 사용 하는데 각 사용자는 자신의 복호키를 비밀리에 간직하고, 모든

사용자의 암호키는 중앙의 키 디렉토리(key directory)에 공개키로 유지하는방식이다[2]. 이 방식은 개인키 암호시스템이 갖는 비밀키보유에 의한 메모리낭비의 문제점은 해결 했지만 키 디렉토리가 신뢰성 있게 관리되야 한다는 문제점이 있다.

1984년 Shamir[3]는 이러한 문제점을 해결하는 방안으로 ID 기본 암호시스템을 제안하였다. 이 방식은 공개키로서 사용자를 식별할 수 있는 ID를 사용하므로 별도의 공개키 관리가 요구되지 않으며, ID에 의해 상대방을 인증한다. 이방식은 지금까지 발표된 여러가지 방식중 가장 주목을 받는 방식으로 많은 사람에 의해 연구되어지고 있다. 그러나 이 방식은 두 사용자간 암호통신에 안전성과 효율성을 제공 하지만 1 대 N 의 그룹통신을 할경우 전문 발송자는 N개의 대화키를 생성하여 동일한 전문을 서로다른 N개의 대화키로 암호화하여 각 사용자에게 전송해야 하는 비효율성이 발생한다.

컴퓨터 통신망이 대형화되고 국가적으로는 국가 기간 전산망 사업이 추진중에 있어 통신망가입자가 늘고 컴퓨터 통신망에 대한 의존도가 증가되는 시점에서 그룹에 의한 암호통신을 위한 안전성 있고 신속한 암호시스템이 요구되고 있지만 이에대한 연구는 저조한 실정이다.

따라서 본 논문에서는 ID 기본 암호시스템을 정의 및 분석하고, 이를 바탕으로 1 대 N 그룹통신에 효율적으로 적용 될수 있도록 수정된 ID 기본 암호시스템 알고리즘을 제시한다.

Ⅱ. 키 분배 및 암호방식

암호 시스템은 암호통신을 하고자하는 두 당사자 사이에 안전한 대화키를 생성 및 분배하여, 정보를 암호화 하고 복호화 하는 과정으로 구성된 시스템을 말하는 것으로 키 분배(key distribution) 또는 키 관리(key management)방식에 따라 개인키 암호시스템과 공개키 암호시스템으로 대별하며 이들 두 방식의 문제점을 보완한 ID 기본 암호시스템이 있다.

2.1 개인키 암호시스템

두 통신당사자가 암호화 키와 복호화 키를 공통으로 사용하는 것으로 모든 사용자간의 암호통신을 위한 대화키를 유지하는 중앙의 키 관리센타(KMC: Key Management Center)를 두어 암호통신시 대화키를 분배하는 중앙집중식 키 분배 방식과 미리 사용자에게 대화키를 분배 하여 사용자가 직접 대화키를 관리하는 분산식 키 분배 방식이 있다.

2.1.1. 중앙 집중식 키분배

중앙에 KMC를 두어 사용자의 요구에 따라 대화키를 분배하는 방식으로 대화키를 해당 사용자에게 분배하기위한 별도의 비밀키가 각 사용자마다 하나씩 필요하게 된다. 그림 1 은 사용자 A와 B가 암호통신을 하기위해 KMC로 부터 대화키를 분배 받는 절차이다. 여기에서 K_a, K_b는 KMC와 사용자 A, B간에 대화키를 전달 하기위한 별도의 비밀키 이며, SK_a, SK_b는 A와 B간의 대화키이다. $f(I_b)$는 상대방을 확인 하기위한 해쉬함수(hash function)이다.

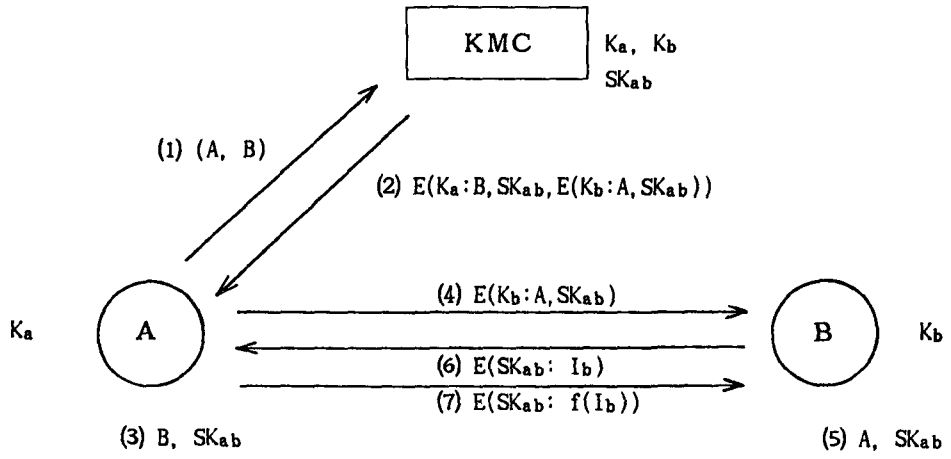

그림 1. 중앙 집중식 키분배

중앙 집중식 키 분배방식에는 몇가지 문제점이 있다. 첫째, 대화키 분배를 위한 또 하나의 비밀키를 유지 해야하며, 중앙 키분배 센타는 충분히 신뢰할 수 있게 관리 되어져야 한다는 점이다. 둘째, 하나 이상의 가입자가 동시에 타 가입자에게 메세지를 전송 하려할때 KMC에 대한 교통량의 증가로 병목현상(bottle neck)을 초래할 가능성이 있다. 세째, KMC가 마비 될경우 전체 통신망은 대화키를 배당받지 못하므로 암호 통신을 할수 없게 되는 치명적인 문제점이 있다. 네째, 대화키를 생성 하기위한 사전 통신절차가 매우 복잡하다.

2.1.2 분산식 키 분배

이 방식은 각 사용자가 통신망 내의 다른 사용자와 암호통신을 위한 대화키들을 모두 유지하고 있는 방식이다. 두 통신 당사자 간의 암호통신은 이미 공유 하고있는 비밀키로 직접 수행될 수 있으므로, 중앙 집중식 키분배 방식에서와 같이 대화키를 얻기위한 KMC의 키 생성과 분배에 관한 오버헤드가 제거될 수 있다.

그러나, 전체 통신망 내의 사용자 수가 N개 일때 각 사용자는 (N-1)개의 비밀키를 유지하게 되고, 통신망내의 전체적인 비밀키의 수는 N*(N-1)/2 개가 필요하게 된다[4]. 따라서, 이 방식의 문제점은 각 사용자가 많은 수의 비밀키를 유지해야 하고, 통신 당사자 상호간에 비밀키 관리를 위한 안전한 절차가 요구된다는 점이다.

2.2 공개키 암호시스템

개인키 암호 방식에서의 키분배는 대화키 분배를 위한 별도의 비밀키를 유지해야 하며, KMC로부터 대화키를 분배 받아야 하는 사전통신의 문제가 있다. 공개키 분배 방식은 이러한 문제점을 해결하기 위해 암호키와 복호키를 다르게 구성하여 암호키는 공개키로서 중앙의 키 디렉토리(key directory)에 유지, 관리하고 복호키는 각 사용자가 비밀키로 간직하는 방식이다.

공개키 분배 방식은 이산대수(discrete logarithm) 문제를 이용하여 실현되어 지는데, 1976년

Diffie 와 Hellman[2]에 의해서 발표 된것이 대표적인 방식이다. 이 방식의 특징은 키를 분배할 필요성이 없고 관리할 키의 갯수가 적다는점과 디지틀 서명이 가능 하다는 점이다[2] [4].

사용자 B와 통신하고자 하는 사용자 A는 KMC에 있는 B의 공개키에 자신의 비밀키로 멱승하여 대화키를 얻고 B는 A의 공개키에 자신의 비밀키를 멱승하여 대화화 키를 얻는다. A와 B 두 통신 당사자간 암호통신을 위한 대화키 생성 절차는 그림 2 와 같다.

여기에서 N과 g는 최초 공개키를 생성하기위해 KMC측에서 선택하는 수이다. N은 큰 소수 p와 q에 의하여 N=p*q로 구해지며, g는 p를 법으로 하는(mod p) 잉여류의 유한체(galois field, finite field) GF(p)상 임의의 원시원소이다. 여기서 유한체란 가감승제를 할 수 있는 유한개의 원소를 지니는 체(Field)를 말한다[4].

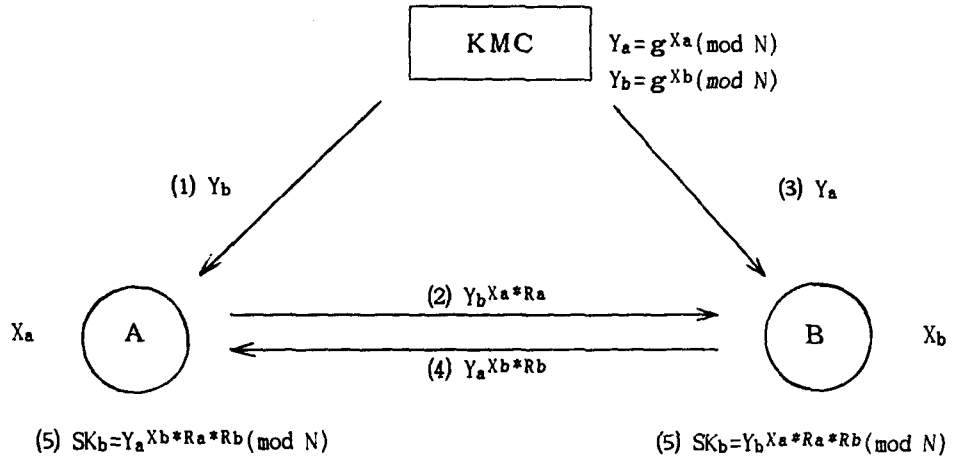

그림 2. 공개키 분배

공개키 분배방식은 개인키 분배방식에서의 키분배문제와 추가적인 비밀키관리 문제점을 해결하였으나, 어떤 사용자의 비밀키가 유출될 경우 공개키가 새로이 변경 되어야 하고, 불법 침입자에의해 공개키가 거짓으로 등록된후 사용되는 것을 방지할 수 있도록 신뢰성있게 공개키가 관리되어져야 한다는 문제점이 있다.

2.3 ID 기본 암호시스템

지금까지 살펴본 키 분배방식은 암호통신을 하기위해 KMC로부터 대화키를 제공 받거나 자신이 직접 관리해야 하며, 공개키의 경우도 KMC에 의해 공개키가 관리되어져야 한다는 문제점이 있다.

이러한 문제점을 해결하기 위한 ID 기본 키 분배방식이 Shamir에 의해 1984년에 제안되었다. 이 방식은 각 사용자가 사전에 카드발급센타(CIC: Card Issue Center)로 부터 대화키 생성에 필요한 공개정보와 자신의 비밀키가 수록된 IC카드를 발급받는 단계부터 시작되는데 상대방과 암호통신을 할때마다 각 가입자들 간에 직접 대화키를 생성한다.

이 방식의 특징은 ID를 공개키로 사용하기 때문에 공개키를 인증할 필요성이 없어지고, 따라서 공개키 관리를 위한 키 디렉토리 관리가 필요 없다는 점이다[4].

이 방식은 최초 사용자가 자신의 ID를 키 센타에 등록하여 공개키와 자신의 비밀키가 수록된

카드를 발급 받아야하며, 실제 상대방과 암호통신할 때마다 대화키를 생성해야 한다.

2.3.1 키 카드 발급

최초 사용자는 자신의 ID를 CIC에 등록하고 대화키 생성에 필요한 공개키와 자신의 비밀키가 수록된 IC 카드를 발급 받는다. 키 카드 발급 절차는 그림 3 과 같다[6].

여기에서 CIC는 큰 소수 p,q를 선정하여 N=p*q를 구하고 e*d(mod (p-1)*(q-1))=1 을 만족하는 e와 d를 계산하며, p의 유한체 GF(P)로 부터 g를 선택한다. 이중 N, g, e는 공개키로서 사용자에게 공개하며, p, q, d는 비밀리에 간직하여 새로운 통신망 가입자가 있을때, 비밀키를 생산 하는데 사용한다.

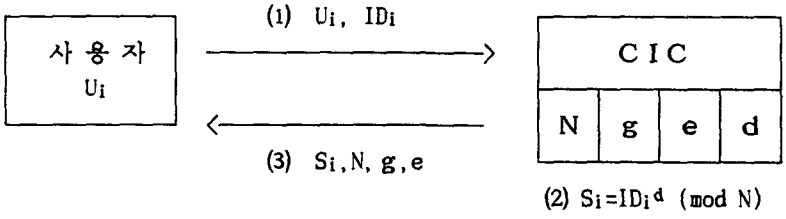

그림 3. 키 카드 분배

⊙ 카드 분배절차

순서 1. Ui ——→ CIC : Ui, IDi

순서 2. CIC : Si=IDi^d (mod N)

순서 3. CIC ——→ Ui : Si,N, g,e

2.3.2 대화키 생성

암호통신을 원하는 두 사용자는 공개키와 자신의 비밀키로 상대방을 인증한후 안전하게 대화키를 생성하는 과정으로 그 절차는 그림 4 와 같다. 여기에서 T는 Timer로부터 얻은 정수이며, Ra, Rb는 사용자 A와 B가 선택한 난수이다. 또한 Ca, Cb는 사용자 A와 B가 공용하는 일 방향성 해쉬 함수(hash function)에의해 결정되며 Ca=Cb 이다.

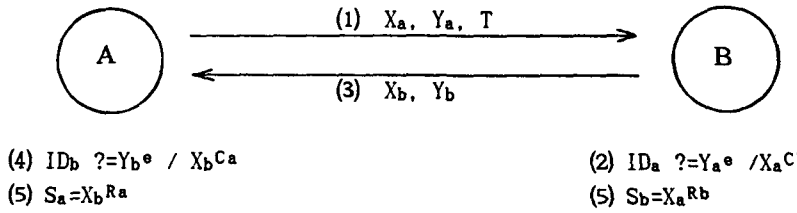

그림 4. 대화키 생성

3.1 키 카드 발급

최초 통신망 가입자는 자신의 ID를 CIC에 등록하고, 자신의 비밀키와 대화키생성시 필요한 공개키가 수록된 IC 카드를 발급 받는다. CIC는 새로운 통신망 가입자를 위해 계속 존속하며, 신뢰할 수 있는 기관에 의해 안전하게 관리 되어져야 한다. 카드 발급절차는 앞절의 그림3과 같다.

3.2 1 대 N 암호통신

1 대 N 그룹통신의 간단한 예로 사용자 I가 A, B, C에게 전문을 발송하고자 할때의 1 대 3 그룹통신에서, 상대방 인증 및 대화키 생성절차를 살펴보자.

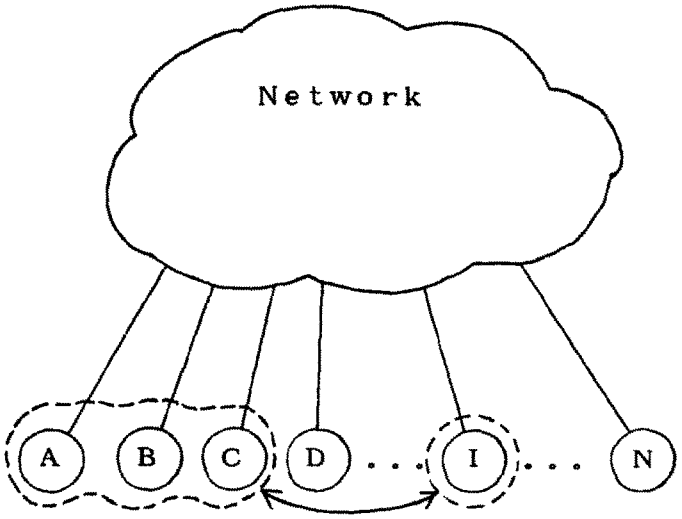

그림 5. 1 대 3 그룹선정

⊙ 인증 및 대화키생성 알고리즘

순서 1. 사용자 I는 Timer로부터의 T_i와 자신의 비밀키로 계산된 신호로 A, B, C에게 암호통신을 요구한다.

$I \longrightarrow A, B, C : REQ_i, T_i$

$[\ REQ_i = g^{Si*Ti*}(\mathrm{mod}\ N)\ ]$

순서 2. 암호통신을 요구받은 각 A, B, C는 자신을 I에게 인증시키기위해 자신의 비밀키로 계산된 신호로 I 에게 응답한다. T_a, T_b, T_c는 timer로부터 얻은 수.

$A \longrightarrow I : ACK_a, X_{ai}, Y_{ai}$

$[\ ACK_a = g^{Sa*Ti}(\mathrm{mod}\ N)$

$X_{ai} = CHK_a^{e*Ta},\quad Y_{ai} = S_a * CHK_a^{Ta*CHKa}\ ]$

$B \longrightarrow I : ACK_b, X_{bi}, Y_{bi}$

$[\ ACK_b = g^{Sb*Ti}(\mathrm{mod}\ N)$

$X_{bi} = CHK_b^{e*Tb},\quad Y_{bi} = S_a * CHK_b^{Tb*CHKb}\ ]$

⊙ 인증 및 대화키 생성 알고리즘

순서 1. A ——→ B : X_a, Y_a, T

$$[\ X_a = g^{e*Ra} \pmod N,\quad Y_a = S_a * g^{Ra*Ca} \pmod N$$

단, $C_a = f(X_a, ID_a, ID_b, T)$]

순서 2. B : $ID_a \stackrel{?}{=} Y_a^{e} / X_a^{Cb}$

$$= S_a^{e} * g^{e*Ra*Ca} \pmod N / g^{e*Ra*Cb} \pmod N$$

$$= ID_a^{d*e} \pmod N * g^{e*Ra*Ca} \pmod N / g^{e*Ra*Cb} \pmod N$$

$$= ID_a^{d*e} \pmod N$$

$$= ID_a$$

단, $C_b = f(X_b, ID_a, ID_b, T) = C_a$

순서 3. B ——→ A : X_b, Y_b

$$[\ X_b = g^{e*Rb} \pmod N,\quad Y_b = S_b * g^{Rb*Cb} \pmod n\ ]$$

순서 4. A : $ID_b \stackrel{?}{=} Y_b^{e} / X_b^{Ca}$

순서 5. A : $SK_a = X_b^{Ra} = g^{e*Ra*Rb} \pmod N$

B : $SK_b = X_a^{Rb} = g^{e*Ra*Rb} \pmod N$

ID 기본 암호방식은 암호통신을 위한 별도의 키 관리센타를 둘 필요가 없고 두 당사자가 핸드쉐이크 과정을 통하여 공통의 대화키를 생성하므로 개인키 분배방식 및 공개키 분배방식에서 나타나는 문제점들을 ID 기본 암호시스템이 가장 잘 해결하고 있음을 알 수 있다. 그러나, 이와같은 ID 기본 암호시스템은 1 대 1 통신에 적합하므로, 본 논문에서는 ID 기본 암호시스템을 기초로한 1 대 N 그룹통신을 위한 키 분배 방식을 제III장에서 제안하였다.

Ⅲ. 제안된 ID 기본 암호시스템

1 대 N 암호통신을 할경우 기존의 ID 기본 암호방식을 적용하면 N개의 대화키를 생성하여 N번의 암호화 전송이 이루어져야 하므로, 본 논문에서는 이러한 비효율성을 해결 하고자 핸드쉐이크 과정을 통해 각사용자가 상대방을 인증하고, 그룹 공통의 대화키를 생성해 한번의 암호화를 통해 N명의 사용자에게 자료 전송이 가능하도록 대화키 생성 절차를 제안하였다.

제안된 ID 기본 암호방식은 기존의 방식과 비교하여 다음 몇가지 특징을 갖는다.

(i)암호통신을 위한 사용자 그룹은 둘이상 임의로 선정할 수 있다, (ii)상대방 인증을위해 별도의 해쉬함수를 사용하지 않는다, (iii)그룹은 하나의 공통대화키를 사용한다, (iv)새로운 통신망 가입자를 위해 CIC는 존속 시킨다.

C ——> I : ACK_c, X_{ci}, Y_{ci}

[$ACK_c = g^{Sc*Ti} (mod\ N)$

$Xci = CHK_c^{e*Tc}$, $Y_{ci} = S_c * CHK_c^{Tc*CHKc}$]

단, $CHK_a = REQ_i^{Sa} = g^{Si*Sa*Ti} (mod\ N)$

$CHK_b = REQ_i^{Sb} = g^{Si*Sb*Ti} (mod\ N)$

$CHK_c = REQ_i^{Sc} = g^{Si*Sc*Ti} (mod\ N)$

순서 3. 사용자 I는 A, B, C로부터 접수한 각 신호에 자신의 비밀키로 각 A, B, C를 인증한다.

I : $ID_a ?= Y_{ai}^e * (X_{ai}^{CHKia}) - 1$

$= S_a^e * CHK_a^{e*Ta*CHKa} * (CHK_a^{e*Ta*CHKia})^{-1}$

$= S_a^e$

$= ID_a^{d*e} (mod\ N)$

$= ID_a$

$ID_b ?= Y_{bi}^e * (X_{bi}^{CHKib}) - 1$

$ID_c ?= Y_{ci}^e * (X_{ci}^{CHKic}) - 1$

단, $CHK_{ia} = ACKa^{Si} = g^{Si*Sa*Ti} (mod\ N) = CHK_a$

$CHK_{ib} = ACK_b^{Si} = g^{Si*Sb*Ti} (mod\ N) = CHK_b$

$CHK_{ic} = ACK_c^{Si} = g^{Si*Sc*Ti} (mod\ N) = CHK_c$

순서 4. 사용자 I는 인증된 사용자만을 그룹으로 간주하여 난수 R_i를 이용해 자신을 상대방에게 인증시키고, 그룹 공통대화키를 계산할 수 있는 기초자료를 전송한다.

I ——> A : X_{ia}, Y_{ia}

[$X_{ia} = g^{e*Ri*Ti*CHKia'} (mod\ N)$

$Y_{ia} = S_i * ACK_a^{Ri*CHKabc} = S_i * g^{Sa*Ri*Ti*CHKabc} (mod\ N)$]

I ——> B : X_{ib}, Y_{ib}

[$X_{ib} = g^{e*Ri*Ti*CHKib'} (mod\ N)$

$Y_{ib} = S_i * ACK_b^{Ri*CHKabc} = S_i * g^{Sb*Ri*Ti*CHKabc} (mod\ N)$]

I ——> C : X_{ic}, Y_{ic}

[$X_{ic} = g^{e*Ri*Ti*CHKic'} (mod\ N)$

$Y_{ic} = S_i * ACK_c^{Ri*CHKabc} = S_i * g^{Sc*Ri*Ti*CHKabc} (mod\ N)$]

단, $CHK_{abc} = CHK_a * CHK_b * CHK_c$

$CHK_{ia'} = CHK_b * CHK_c$

$CHK_{ib'} = CHK_a * CHK_c$

$CHK_{ic'} = CHK_a * CHK_b$

순서 5. 각 사용자 A, B, C는 자신의 비밀키를 이용해 I를 인증한다.

A : $ID_i ?= Y_{ia}^e * (X_{ia}^{Sa*CHKa}) - 1$

$= S_i^e * g^{e*Sa*Ri*Ti*CHKabc} * (g^{e*Sa*Ri*Ti*CHKia'*CHKa})^{-1}$

$= S_i^e = ID_i^{d*e} (mod\ N) = ID_i$

B : $ID_i ?= Y_{ib}^{e} * (X_{ib}^{Sb*CHKb})^{-1}$

C : $ID_i ?= Y_{ic}^{e} * (X_{ic}^{Sc*CHKc})^{-1}$

순서 6. 그룹내 각 사용자는 자신의 비밀키로 그룹공통의 대화키를 계산한다.

I : $SK_i = g^{e*Ri*Ti*CHKabc} \pmod N$

A : $SK_a = X_{ia}^{CHKa} = g^{e*Ri*Ti*CHKia'*CHKa} = g^{e*Ri*Ti*CHKabc}$

B : $SK_b = X_{ib}^{CHKb} = g^{e*Ri*Ti*CHKib'*CHKb} = g^{e*Ri*Ti*CHKabc}$

C : $SK_c = X_{ic}^{CHKc} = g^{e*Ri*Ti*CHKic'*CHKc} = g^{e*Ri*Ti*CHKabc}$

3.4 분석 및 평가

이상에서 살펴본 1 대 N 사용자 그룹을 위한 암호통신 절차는 ID 기본 암호방식을 기본으로 한 것으로, 기존의 방식이 1 대 N 그룹 암호통신에 적용 되었을때 발생하는 비효율성을 극복하기 위해 제안 되었다.

이러한 기존 방식의 비효율성과 제안된 방식의 특성을 중심으로 몇가지 비교 분석을 하면 다음과 같다.

첫째, 대화키 생성에 있어서 기존의 방식은 1 대 1 암호통신을 반복 함으로써 그룹통신을 실현해야하나, 제안된 방식은 선정된 그룹 사용자간에 핸드쉐이크 과정을 통하여 그룹 공통의 대화키를 생성 하여, 전문 발송자는 단 1회의 암호화로 그룹내의 사용자 들에게 전문을 발송할 수 있으므로 암호통신 시간을 줄일수 있다..

둘째, 안전성 문제로 제안된 방식은 그룹내 사용자 상호간에 인증 과정을 거치며, 이과정에서 기존 방식과 달리 해쉬함수를 사용하지 않는다. 따라서 제삼자가 불법으로 임의의 비밀키를 만들어 도청하는 위험성을 제거하기위해 전문 발송자와 각 수신자가 자신들의 비밀키로 핸드쉐이크 하여 상호 인증을 하도록 하였으며, 공통의 대화키는 그룹의 모든 사용자의 개인 비밀키가 개입되므로 안전성은 더 강해졌다 할수 있다.

셋째, 전문 발송자는 수신자 그룹을 임의로 선정할 수 있으며, 각 수신자에게 암호통신 할것을 통보한후 응답이 있는 사용자들로만 그룹을 재구성 할수 있는 유연성이있다.

끝으로 제안된 방식에서는 CIC를 키 카드 분배후 폐쇄 시키지 않고 계속 존속 시켰다. 이는 새로운 통신망 가입자에대한 키 카드 지원을 위한 것으로, 별도로 신뢰성있는 기관에 의해서 CIC가 관리 되어야 한다는 문제점을 갖고있다.

이러한 수정된 ID 기본 암호방식을 이용한 키 분배방식은 많은 사용자와 그룹통신을 해야하는 메세지 처리시스템(Message Handling System)에 적용하여 사용할 수 있다[5].

Ⅳ. 결 론

본 논문에서는 유한체에서의 이산대수문제에 기초를 둔 ID기본 암호 시스템을 정의하고, 1 대 N 그룹통신에 적용하기위한 상대방 인증 및 대화키 생성 알고리즘을 제안 하였다.

제안된 알고리즘은 1 대 N의 임의 사용자 그룹에 대한 암호통신시 상호 핸드쉐이크 과정을 거

쳐 상대방을 인증하고 그룹 공통의 대화키를 생성 함으로써 전문 전송자는 1회의 암호화 만으로 N의 사용자 그룹에게 암호화 전문을 발송 할수 있게 하였다.

그룹통신은 많은 사용자와 핸드쉐이크 과정을 통하여 인증과 대화키를 생성 하므로, 보다 신속한 상대방 인증과 대화키 계산을 위해서는 병렬처리 기법에 의한 암호통신 연구가 계속 되어 져야 할 것이다. 특히 국가 5대 기간 전산망 사업이 추진 중에 있고, 컴퓨터 통신망에의한 정보교환의 필요성이 증대되고 있는 현 시점에서 그룹에의한 암호통신은 계속적으로 연구 되어져야 할 것이다.

V. 참고문헌

1. D.E.Denning, Cryptography and Data Security, Addision Wesley, 1982.
2. W.Diffie and Hellman, "New direction in cryptography", IEEE Trans. Inform. Theory, Vol. IT-22, PP.644-654, 1976
3. A.Shamir, "Identity-based cryptosystem and signature scheme", in Proc. of Crypto'84, pp.47-53, 1984
4. 한국전자통신연구소, "현대 암호학", pp.125-182, 1991
5. P.Schicker, "Message Handling System and Distributed Application", North-Holland, 1989
6. R.L.Rivest, A.Shamir, and L.Adleman, "Amethod for obtaining digital signatures and public-key cryptosystem," Comm. ACM,Vol.21,pp120-126,1978