通信情報保護論文誌
第9券 第2號 1999. 06

무선통신 환경에서 사용 가능한 고차잉여류 문제에 기반을 둔 자체 인증방식

이 보영*, 최 연이**,주 미리*, 원 동호*

An efficient ID-based authentication scheme based on the γ^{th}- residuosity problem in wireless environment

Bo-young Lee*, Yeon-yi Choi**, Mi-ri Joo*, Dong-ho Won*

요 약

이동하는 모빌노드(mobile node)의 인증 기법 중에, 홈 에이전트(home agent)와 모빌노드, 외부 에이전트(foreign agent)를 거치는 triangle 인증 기법이 있다. 이 기법의 문제점은, 모빌노드의 이동이 빈번하게 발생되면 인증 절차 또한 비례적으로 이루어져야 하므로 무선통신 환경상의 통신 오버헤드가 증가하게 된다. 이러한 문제점을 개선하기 위해서 본 논문에서는, 고차잉여류의 개념에 근거한 다중서명방식을 이용하여 모빌노드가 이동할 때마다 필요했던 홈 에이전트와 외부 에이전트간의 인증을 생략한 자체 인증 방식을 제안하고자 한다.

Abstract

In an open network computing environment, a host cannot to identity its users correctly to network services. In order to prevent this thing, we present the design of a authentication scheme that using the notion of γ^{th}- residuosity problem and discrete logarithm problem which is proposed by S. J. Park et al.. The proposed scheme described here is efficient method for mutual authentication without leakage of users identity in mobile communication system that ensure user anonymity and untraceability.

* 성균관대학교 전기·전자 및 컴퓨터 공학부 정보통신보호연구실, ** 신성대학 정보통신학과

I. 서 론

현대사회는 정보의 생성, 저장, 처리, 가공, 검색 기능이 상호 연결된 다양한 통신망 환경에서 여러가지 형태의 정보와 서비스에 대하여 이루어지고, 통신사업의 고속성장으로 인해 인터넷이 전세계적으로 널리 사용되고 있다. 또한, 컴퓨터분야의 많은 발전으로 소형, 무선 컴퓨터를 이용하여 사용자가 언제, 어디서나, 누구와도 데이터통신과 원격(tele-)통신이 가능하게 되었다. 이러한 통신 네트워크가 가져온 분산구조는 무선(wireless) 또는 모빌(mobile)통신을 현실화 시켰다. 그러나 무선통신망의 전송매체는 공중파를 사용하므로, 유선을 이용하는 통신보다 쉽게 정보의 유출이나 정보의 불법사용, 수정 등이 가능하다. 이를 방지하기 위한 방법으로는 암호시스템의 이용이라 할 수 있다. 현재 많은 무선통신 시스템에서 인증 및 암호 기능을 제공하기 위해 비밀키 암호 방식(conventional or private key cryptosystem)을 채택하고 있다. 이는 security 서비스의 제공으로 인한 시스템에 미치는 부하(load)의 증가, 단말기의 소형화에 따른 계산 능력의 문제점등을 고려함이다. 반면, 비밀키 암호방식에 의한 security 서비스의 제공에 대한 취약점을 개선하기 위하여, 공개 키 암호방식을 이용한 각종 방안들이 제시되고 있다. 이들은 비록 시스템의 부하(load)를 증대시키는 등 실현이 용이하지 않은 부분도 있으나, 앞으로의 하드웨어의 발달이나 소형화 기술, 그리고 계산능력의 향상에 따라 많은 발전이 있으리라 예상된다[2].

인증에 대해서는, 1980년대 후반 유럽 이동통신의 표준인 GSM(Group Special Mobile)이 발표된 후, CDPD(Cellular Digital Packet Data), UPT(Universal Personal Telecommunication) 등 많은 표준안에서 인증을 포함한 security 기능을 권고하고 있다. 무선(이동) 통신에서의 security 기능에는 인증(authentication), 부인방지(non-repudiation), 위임과 책임(authorization and accountability), 기밀성(confidentiality), 익명성(anonymity), 데이터 무결성(data integrity), 기록(logging), 침입탐지(intrusion detection)등이 있다.

인증 프로토콜에는 초기의 GSM과 CDPD내의 인증 프로토콜이 있고, 공개키 암호를 이용하여 이동통신의 인증의 기능을 제공하는 TMN(Tatebayashi, Matsuzaki, Neuman)방식과 1993년 Beller, Chang & Yaccobi가 제안한 BCY방식, 1994년 Aziz 와 Diffie가 제안한 LAN에서의 프로토콜, Molva, Samfat & Tsudik의 프로토콜[3]등 이있고, 가장 최근의 방식은 Yuliang Zheng이 제안한 방식[4]이 있다.

임의의 모빌노드가 자신이 등록되어있는 홈 에이전트에서 외부 에이전트로 이동하는 경우, 모빌노드와 외부 에이전트, 외부 에이전트와 홈 에이전트간의 인증이 이루어지고 나서 모빌노드는 서비스를 받기 시작된다. 그러나, 모빌노드가 빈번하게 이동할 때에는 이와 비례하게 인증 또한 이루어져야 하므로 통신상의 오버헤드가 증가한다. 이러한 문제점을 개선하기 위해서, 본 논문에서는 고차잉여류 개념에 근거한 다중서명 방식을 이용하여 모빌노드가 이동 할때마다 홈 에이전트와의 인증을 실행하는 것 대신에 홈 에이전트가 서명한 인증서를 갖고 다니면서 모빌노드가 이동하는 외부 에이전트들에게 인증서에 서명을 하게 함으로써 홈 에이전트를 거치지 않고 모빌노드와 외부 에이전트 사이의 인증을 수행한다.

본 논문은 다음과 같이 구성된다. 서론에 이어 2장에서는 무선통신시스템에 대한 일반적인 내용과 인증방식을 소개하고, 3장에서는 제안한 논문의 기본 개념인 자체인증 개인식별정보 방식에 대해 언급한다. 4장에서는 제안하는 고차잉여류 문제에 기반을 둔 자체인증 방식에 대해 기술하고 5장에서 결론으로 끝맺는다.

II. 무선통신 시스템

2.1 무선통신시스템 구성 및 기능

무선통신 시스템은 크게 교환국, 기지국, 이동국으로 구성되어 있으며 전체적인 구성과 설명은 표 2.1에 기술하였고, 본 논문에서 사용되는 단어의 의미는

표 2.1 무선 통신 시스템 구성표

구성 요소	기 능
MS(Mobile Station)	· 이동 단말기로서 이동 통신서비스를 제공받기 위한 단말기능을 보유하고 있으며, 아날로그 방식 이동국과 다른 특징으로는 송신 전력의 제어가 빠르고 정확하게 수행하기 위한 전력 제어 기능과 다경로 페이딩(fading)환경에서 양질의 링크 품질을 보장하기 위한 rake 수신기를 가지고 있다.
BTS(Base Tranceiver system)	· 기지국 무선 장치로서 RF 접속을 통하여 이동국과의 무선 접속 및 이동국과 기지국 제어장치간의 유/무선 접속 기능을 수행한다.
BSC(Base Station Controller)	· 기지국 제어장치로서 기지국과 이동 통신 교환기 사이에 위치하여 기지국관리 및 제어를 담당한다.
MSC(Mobile Switching Center)	· 이동 단말기에게 이동통신 서비스를 제공하기 위한 이동 통신 교환기로서 가입자간 회선교환, 가입/출 중계호 처리, 핸드오프(hand off), 페이징 및 로밍(roaming)기능 등을 갖으며, VLR 데이터베이스를 관장한다.
HLR(Home Location Register)	· 이동국의 현재 위치 정보를 비롯하여 이동 가입자의 상태, 통계 및 각종 서비스 관련 정보를 관리하는 데이터베이스 센터이다.
OMC(Operation Maintenance Center)	· 이동 통신망에 대한 망운용의 효율화, 보전 서비스 향상, 고품질 통신 서비스를 제공하기 위한 운용 및 유지 보수를 담당한다.

Table 2.1 Wireless communication system table

다음과 같다.

- 모빌 노드(Mobile Node)
  하나의 네트워크나 서브 네트워크에서 다른 위치로 연결점을 변경하는 호스트 또는 라우터
- 홈 에이전트(Home Agent)
  모빌 노드의 홈 네트워크의 라우터를 말하며, 모빌 노드가 홈에서 외부로 이동했을 때, 데이터 그램은 터널을 통해 전달하고, 모빌 노드의 현재 위치 정보를 유지한다.
- 외부 에이전트(Foreign Agent)
  모빌 노드가 방문한 네트워크의 라우터를 말하며, 터널 해제를 통해 모빌 노드로 데이터 그램을 전달하고, 모빌 노드의 기본 라우터가 된다.
- Agent Advertisement
  Router advertisement 메시지를 확장하여 구성한다.
- 이동 에이전트(Mobility Agent)
  홈 에이전트 또는 외부 에이전트를 가리킨다.
- 터널(Tunnel)
  데이터그램을 암호화하여 전달하는 경로이다.

2.2 무선통신상의 인증 방식

무선통신에서 인증이란 통화초기에 설정된 비밀 정보를 가입자, 즉 모빌노드가 서비스 제공자인 네트워크에 증명하여 정당한 가입자임을 밝히는 절차이다. 이는 모빌노드의 불법 사용을 방지하기 위한 대책이다. 모든 공중 통신망에서는 사용에 따른 요금부과가 가입자에게 징수되어야 하지만, 제공된 서비스에 대한 과금이 제대로 수행되지 않게 되거나, 다른 사람에게

그림 2.1 Triangle Mobile node의 인증 절차

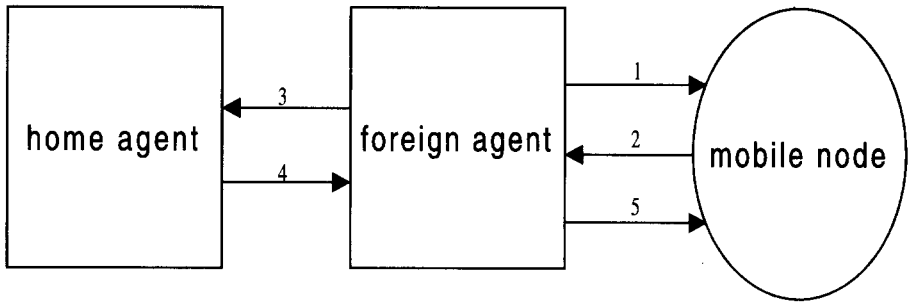

Fig 2.1 Authentication procedure of triangle mobile node

과금이 되도록 하는 불법 행위들이 일어날 수 있다. 이러한 위조나 불법 사용에 대한 보호 대책을 위해 모빌노드의 신분확인이 반드시 이루어져야 한다. 이러한 인증 작업은 인증 알고리즘과 인증 프로토콜에 의해서 이루어 질 수 있다[2]. 그 절차는 그림 2.1과 같다.

〔절차〕

1. Agent Advertisement message
   모빌노드(mobile node)가 외부 에이전트(foreign agent)로 이동하면, 외부 에이전트는 모빌노드에게 advertisement 메시지를 보낸다.
2. Registration Request (모빌노드와 외부 에이전트간)
   모빌노드는 외부 에이전트에게 자신의 등록 요구 메시지를 보낸다.
3. Registration Request(외부 에이전트와 홈 에이전트간)
   외부 에이전트는 홈 에이전트에게 등록 요구와 응답을 서로 교환한다.
4. Registration Reply
   요구를 받은 홈 에이전트는 그 요청에 대한 허가 또는 거부를 응답으로 보내준다.
5. Registration Reply
   외부 에이전트는 모빌 노드에게 응답을 전달한다.

III. 자체인증 개인식별정보에 기반을 둔 방식

1994년 박성준 등은 자체인증 공개키 방식을 개인식별정보에 기반을 둔 방식에 적용하여 만든 새로운 개념인 자체인증 개인식별정보(self-certified identity information)방식을 제안하였다.[11]

자체인증 개인식별정보 방식은 자체인증 공개키 방식에서 인증자의 역할을 하는 공개키가 바로 개인식별 정보인 경우를 말한다. 이 방식은 효율성을 개선하기 위해, 사용자의 비밀키 중 인증센터에 의해 생성된 i와 x를 공개키로 사용함으로써 자체인증 공개키 방식으로 변환시킬 수 있다. 제안된 방식의 안전성은 고차잉여류 문제(γ^{th}-잉여류 문제)와 이산대수 문제의 어려움에 기반을 두고 있다.

〔정의〕

• 고차잉여류 문제

: 양의 정수 γ, n이 주어질 때, 정수 z가 다음의 조건을 만족하면, z를 법 n에 대해 γ^{th}-잉여류라 한다.

(조건)

gcd(z, n) = 1이고 $z \equiv x^{r} \bmod n$ 을 만족하는 x가 존재한다.

위의 조건을 만족하지 않는 z는 법 n에 대하여 γ^{th}-비잉여류라 한다.

고차잉여류 문제(γ^{th}-residuosity problem)란 주어진 gcd(z, n) = 1인 양의 정수 $z \in Z_n^*$ 가 γ^{th}-잉여류인지 γ^{th}-비잉여류 인지를 결정하는 문제이다. 고차잉여류 문제의 계산 복잡도는 γ가 다항식 크기일 때

n의 소인수 분해 문제와 동치이고 γ가 지수적 크기일 때는 n의 소인수 분해 문제보다 어렵다고 간주되고 있다.

• 이산대수 문제

: 소수 p가 주어지고 $y = g^x \bmod p$인 경우, 역으로 $x = \log_g y \bmod p$ 인 x를 계산 하는 문제로서 여기서 x를 법 p상의 y의 이산대수라 한다. 소수 p가 매우 크고(2^{512} 이상), g의 위수(order) k가 2^{140} 이상인 경우, 다항식 시간 내에 x를 찾는 효율적인 알고리즘은 존재하지 않는다.

• Acceptable triple (n, γ, y)

: (n, γ, y)가 아래의 3가지 조건을 만족할 때 acceptable triple 이라 한다.

(조건1)

$n = n_1 n_2 \cdots n_t$, 여기서 각 n_i는 홀수의 소수이다.

(조건2)

γ는 $1 \le l \le t$인 하나의 l에 대해 $\gcd(\gamma, \phi(n_l)) = \gamma$이고, 나머지 $i(\neq 1)$에 대해 $\gcd(\gamma, \phi(n_l)) = 1$인 2보다 큰 홀수이다.

(조건3)

$y = h_1^{b_1^{\gamma}+e} \prod_{j=2}^{t} h_j^{b_j} \bmod n$, 여기서 모든 $i \neq 1$, $1 \le j \le t$에 대해 $0 < e < \gamma$, $\gcd(e, \gamma) = 1$, $1 \le b_j \le \phi(n_j)$ 이고, $\langle h_1, h_2, \cdots, h_t \rangle$는 Z_n^*의 생성벡터이다.

• 잉여류 지수

: Acceptible triple (n, γ, y)과 임의의 $z \in Z_n^*$가 주어졌을 때, $z = y^i u^r$를 만족 하는 유일한 i가 존재한다. 이때 i를 z의 잉여류 지수로 정의한다.

〔시스템의 초기화〕

신뢰 센터는 acceptable triple (n, γ^d, y)를 선 택한다. 단, $n = p \cdot q = (2\gamma^d f p' + 1) \cdot (2fq' + 1)$, 여기서 f, p', q'는 서로 다른 소수이고, $\gcd(\gamma, q') = 1$, $\gcd(\gamma, p') = 1$ 이다.

y는 modulus n 상에서 $(\gamma^d)^{th}$-비잉여류이고, b는 modulus p와 modulus q상에서의 위수(order)가 f인 Z_n의 원소로 법 n상에서의 위수(order)가 f이다. 신뢰 센터의 공개키는 (n, γ^d, y, b, f)이고 비밀키는 (p', q')이다.

이러한 성질을 이용하여 센터는 개인식별정보 ID를 갖는 사용자의 비밀키를 다음과 같이 생성한다.

단계1)

홈 에이전트 H는 자신만의 비밀키 정보 $0 < s < f$를 생성하고 자신의 개인식별 정보 I와 $b^s \pmod n$을 센터에게 전송한다.

단계2)

센터는 H를 확인한 뒤, $(Ib^s)^{-1} \bmod n$ 의 잉여류 지수 i와 $(Ib^s y^i)^{-1}$의 γ^d근 x를 계산한다. 즉, $ID = b^{-s} y^{-i} x^{-\gamma^d} \pmod n$을 만족하는 i와 x를 계산하여 홈 에이전트 H에게 안전하게 전송한다.

단계3)

홈 에이전트 H는 (s, i, x)를 자신의 비밀키로서 관리한다.

여기서 각 홈 에이전트의 비밀키는 (s, i, x) 이나, 신뢰 센터는 사용자가 선택한 비밀키 s를 알 수 없다.

〔인증 및 키분배절차〕

자체인증 개인식별정보 개념을 사용한 인증방식으로 Schnorr방식과 유사하다.

홈 에이전트 H가 모빌노드 M과 통신하고자 할 경우의 인증 프로토콜은 다음과 같다.

단계1)

H는 〔0, f-1〕상에 있는 랜덤수 r_H을 선택하고, z_H를 계산한다.

$$z_H = r_H - s_H \bmod f$$

단, $r_H \in_R [0, f-1]$

단계2)

H는 I_H, z_H, i_H, x_H 를 센터에 전송 한다.

단계3)

센터는 b_{r_H} 를 계산한다.

$$b_{r_H} = I_H b^{z_H} y^{i_H} x_H^{r^d} = b^{r_H} \bmod n$$

단계4)

센터는 모빌노드 M에게 b_{r_H} 를 전송한다.

단계5)

M은 [0, f-1]상에 있는 랜덤수 r_M을 선택하고, z_M를 계산한다.

$$z_M = r_M - s_M \bmod f$$

단, $r_M \in_R [0, f-1]$

단계6)

M은 I_M, z_M, i_M, x_M 를 센터에 전송한다.

단계7)

센터는 b_{r_M} 를 계산한다.

$$b_{r_M} = I_M b^{z_M} y^{i_M} x_M^{r^d} = b^{r_M} \bmod n$$

단계8)

센터는 홈 에이전트 H에게 b_{r_M} 를 전송한다.

단계9)

H와 M은 세션키 K를 다음과 같이 계산한다.

$$K = b_{r_M}^{r_H} = b_{r_H}^{r_M} = b^{r_H r_M} \bmod n$$

[인증서에 대한 서명의 생성]

홈 에이전트 H가 인증서 m을 모빌노드 M에게 서명하고자 할 경우의 서명 프로토콜은 다음과 같다.

단계1)

H는 v, e를 계산한다.

$$v = b^{r_H} \bmod n$$

$$e = h(v, m)$$

여기서 h는 안전한 해쉬 함수이다.

단계2)

H는 다음의 z를 계산한다.

$$z = r_H - se \bmod f$$

단계3)

인증서 m의 서명문은 (z, e)이다.

단계4)

H는 (z, i, x, e)을 M에게 전송한다.

[서명의 검증]

단계1)

M은 다음의 v를 계산한다.

$$(Iy^i x^{r^d})^e b^z \pmod n = v$$

단계2)

M은 $e = h(v, m)$를 검증한다.

IV. 고차잉여류 문제에 기반을 둔 다중인증 방식

4.1 다중인증방식의 개요

지금까지 개발되어 온 대부분의 전자서명은 문서에 한 사람이 서명하는 단순서명(Single Signature) 방식이었다. 그러나 이런 단순서명 방식을 실제 생활에 적용하기에는 여러 가지 문제점이 있다. 이런 문제중에 하나가 결재와 서명, 계약의 경우와 같이 여러 사람이 한 문서에 서명하는 경우이다. 단순서명을 반복해서 적용하면 서명의 길이가 늘어나고 서명을 검증하려면 서명자의 수만큼 검증과정을 거쳐야 하기 때문에 서명자가 많은 경우 시간이 오래 걸린다는 단점이 있다. 이러한 단순서명 방식의 문제점을 해결하기 위해 나온 개념이 다중서명(Multisignature) 방식이다. 다중서명 방식은 같은 메시지를 서명자들이 순차적으로 서명하는 순차 다중서명방식(Sequential multisignature scheme)과 서명자들이 메시지에 동시에 서명하는 효과를 갖게하는 동시 다중서명방식(Simultaneous multisignature scheme)으로 나눌 수 있다. 최초의 다중서명 방식은 소인수 분해 문제를 이용한 RSA 단순서명 방식에 기반을 둔 순차다중서명 방식이다. 그러나 RSA 방식이 연산수가 많기 때문에 이것을 해결하고자 잉여류 문제에 바탕을 둔 Fiat-Shamir 단순서명 방식을 기반으로 하는 다중서명 방식이 개발되었다. Fiat-Shamir방식은 연산수가 RSA비해 적고 ID-based 방식이어서 키 디렉토리가 필요없는 장점이 있지만, 통신횟수가 많다는 단점이 있다. 후에 이산대수 문제를 이용한 ElGamal 단순서명 방식을 기반으로 하는 다중서명 방식들이 개발되었다. 이산대수 문제를 기반으로 하는 경우, Fiat-Shamir 단순서명 방식을 이용하는 다중서명 방식보다 기본 연산수는 많

지만 서명자의 수에 영향을 적게 받는다는 장점이 있다.

본 논문에서는 신뢰 센터가 사용자의 비밀키를 생성하는 과정에서 고차 잉여류를 이용한 공개키 암호 시스템의 복호화 과정이 요구되는 다중인증 방식을 제안하였고 그 절차는 다음절에서 기술된다.

4.2 시스템의 초기화

시스템의 초기화 절차는 앞에서 언급한 자체인증 개인식별방식과 같다. 신뢰 센터는 홈 에이전트 H를 확인한 후, $ID_H = b^{-s_H} y^{-i_H} x_H^{-\gamma^d} \pmod n$을 만족하는 i_H와 x_H를 계산하여 홈 에이전트 H에게 안전하게 전송한다. 여기서 각 홈 에이전트의 비밀키는 (s_H, i_H, x_H)이나, 신뢰 센터는 홈 에이전트가 선택한 비밀키 s_H를 알 수 없다[12].

4.3인증서에 대한 서명생성

모빌노드가 소지하고 있는 인증서 m에 대해 각 외부 에이전트가 다중서명문을 생성하는 과정은 다음과 같다. 여기서 서명자란, 모빌노드가 이동하는 외부 에이전트를 의미한다.

[절차 1 : 난수 생성 단계]
단계1)
서명자$_i$는 랜덤수 $0 < r_{i,1} < f$, $0 < r_{i,2} < \gamma^d$, $0 < r_{i,3} < n$을 선택하고, v_i를 계산한다.

$$v_i = (b^{r_{i,1}} y^{r_{i,2}} r_{i,3}^{\gamma^d}) \cdot v_{i-1} \pmod n$$

단, $v_0 = 1 \pmod n$ 이다.
단계2)
서명자$_i$는 v_i를 서명자$_{i+1}$에게 전송한다. 만약 서명자가 마지막 서명자(서명자$_n$)이면 v_n를 홈 에이전트(즉, 서명자$_1$)에게 보낸다.

[절차 2 : 서명 생성 단계]
단계1)
서명자$_i$는 인증서 m의 해쉬값 $e = h(v_n, ID_{cn}, m)$을 계산한다.
단계2)
서명자$_i$는 다음의 $z_{i,1}$, $z_{i,2}$, $z_{i,3}$를 계산한다.

$$z_{i,1} = r_{i,1} - s_i e + z_{i-1,1} \pmod f$$
$$z_{i,2} = r_{i,2} + i_i e + z_{i-1,2}$$
$$z_{i,3} = x_i e \cdot r_{i,3} \cdot z_{i-1,3} \pmod n$$

단, $z_{0,1} = 0 \pmod f$, $z_{0,2} = 0$, $z_{0,3} = 1 \pmod n$ 이다.
단계3)
서명자$_i$는 인증서 m에 대한 서명 (ID_{cn}, v_n, $z_{i,1}$, $z_{i,2}$, $z_{i,3}$)을 서명자$_{i+1}$에게 전송한다. 만약 서명자가 마지막 서명자(서명자$_n$)이면 다중서명 (ID_{cn}, e, $z_{i,1}$, $z_{i,2}$, $z_{i,3}$)을 검증센터로 보낸다.

4.4 다중서명의 검증

각 서명자와 검증센터는 다음의 절차에 따라 인증서 m에 대한 다중서명을 검증하게 된다.

[서명자$_i$ (단, $2 \le i \le n$)의 서명 검증]
단계1)
서명자$_i$는 인증서 m의 해쉬값
$e = h(v_n, ID_{cn}, m)$을 계산한다.
단계2)
서명자$_i$는 다음의 수식이 만족되는지 확인한다.

$$v_{i-1} \stackrel{?}{=} \left(\prod_{\text{서명자}=1}^{i-1} ID_{\text{서명자}}\right)^e \cdot b^{z_{i-1,1}} \cdot y^{z_{i-1,2}} \cdot z_{i-1,3}^{\gamma^d} \pmod n$$

[검증센터의 서명 검증]
단계1)
검증센터는 다음의 v_n을 계산한다.

$$v_n = \left(\prod_{\text{서명자}=1}^{n} ID_{\text{서명자}}\right)^e \cdot b^{z_{n,1}} \cdot y^{z_{n,2}} \cdot z_{n,3}^{\gamma^d} \pmod n$$

단계2)
검증센터는 다음의 수식이 만족되는지 확인한다.

$$e \stackrel{?}{=} h(v_n, ID_{cn}, m)$$

단계3)
검증센터는 인증서 m에 대한 다중서명 (ID_{cn}, e, $z_{n,1}$, $z_{n,2}$, $z_{n,3}$)을 저장 보관한다.

4.5 성능 분석

제안된 방식은 난수 생성 단계와 생성된 난수를 바탕으로 서명을 생성하는 단계로 구성되어 있다. 이 방식은 다중서명의 길이가 증가되지 않고 고속처리와 ID에 근거하기 때문에 RSA에 근거한 서명방식보다 효율적이다. 또한 개인식별정보에 기반을 둔 방식이면서도 센터가 각 사용자의 비밀키를 알 수 없다. 그러

나, 이 방식은 n개의 외부 에이전트가 다중서명을 수행하고자 할 때 (2n-1)번의 통신을 수행해야하고, 서명자는 첫 번째 라운드에서 생성한 난수를 두 번째 라운드 즉, 메시지를 직접 서명할 때까지 보관해야 하며 또한 첫 번째 라운드와 두 번째 라운드의 서명자 순서가 다른 경우 중간 서명자는 앞 서명자의 서명을 확인할 수 없다.

V. 결 론

본 논문에서는 고차잉여류 개념에 근거한 다중서명 방식을 이용하여 모빌노드가 이동 할때마다 홈 에이전트와의 인증을 실행하는 것 대신에 홈 에이전트가 서명한 인증서를 갖고 다니면서 모빌노드가 이동하는 외부 에이전트들에게 인증서에 서명을 하게 함으로써 홈 에이전트를 거치지 않고 모빌노드와 외부 에이전트사이의 인증을 수행하였다. 제안된 방식은 모빌노드가 빈번하게 이동하여도 인증서 m에 대한 다중서명의 길이가 일정하고, 서명 처리속도가 빠르며, ID에 근거하기 때문에 RSA에 근거한 인증방식 보다 효율적이다. 특히 제안된 방식은 자체인증 특성을 갖는 공개키 방식으로 인해 세션키 분배시 특별한 인증 절차를 필요로 하지 않는 장점과 계산량이 적고 안전성을 검증할 수 있는 특성을 갖는다.

참 고 문 헌

[1] W. Diffie and M. Hellman, "New Direction in Cryptography", IEEE Trans. Inform. Theory, Vol. IT-22, pp. 644-654, 1976.

[2] 박춘식, "디지틀 이동 통신을 위한 안전 대책", *Telecommunications Review* Vol. V, No. 5, pp. 122-141, 1995.

[3] R .Molva, D .Samfat, G. Tsudik, "Authentication of Mobile Users", IEEE Network Magazine, Special issue on Mobile Communications, March/April 1994.

[4] Y. Zheng, "An Authentication and Security Protocol for Mobile Computing"

[5] T. Kiesler and L. Harn, "RSA blocking and multisignature schemes with no bit extension", Electronic Letters, Vol. 26, No. 18, pp. 1490-1491, 1990.

[6] K. Ohta and T. Okamoto, "A digital multisignature scheme based on the Fiat-Shamir scheme", Proc. of Asiscrypt'91, pp. 75-79, 1991.

[7] L. Harn, "New digital signature scheme based on discrete logarithm", Electronic Letters, Vol. 30, No. 5, pp. 396-398, March 1994.

[8] Y. Zheng, T. Matsumoto, and H. Imai, "Residuosity Problem and its Application to Cryptography", Trans. IEICE, vol. E71, No. 8, pp. 759-767, 1988.

[9] Y. Y. Choi, S. J. Kim, S. J. Park, and D. H. Won, "A Paradoxical ID-Based Key Distribution Protocol for Mobile Communication System", MDMC'96, 1996.

[10] B. Y .Lee, S. J. Kim and D. H. Won, "ID-based Multisignature Scheme based on the High Residuosity Problem", JWISC'97, pp. 227-230, 1997.

[11] S. J. Park and D. H. Won, "A paradoxical identity-based scheme based on rth- residuosity problem and discrete logarithm problem", KIISC vol.4, No. 2, pp. 113-118, 1994.

[12] 이보영, 박택진, 원동호, "고차잉여류 문제에 기반을 둔 다중서명 방식", 정보처리학회 논문지, 제6권 3호, 1999.

[13] S. J. Park, B. Y. Lee, and D. H. Won, "A Generalized Public Key Residue Cryptosystem and Its Applications", IEEE GLOBECOM'95, Singapore, pp. 1179-1182, 1995.

□ 著者紹介

이 보 영(Bo-young Lee) **정회원**

1989년 2월 :성균관대학교 정보공학과 졸업
1995년 8월 :성균관대학교 정보공학과 석사
1996년 3월 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정

최 연 이(Yeon-yi Choi) **정회원**

1993년 2월 :한림대학교 화학과 졸업
1995년 2월 :성균관대학교 산업과학대학원 석사
1996년 3월 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정
1997년 3월 ~ 현재 신성대학 정보통신과 교수

주 미 리(Mi-ri Joo) **정회원**

1996년 2월 :성균관대학교 정보공학과 졸업
1998년 2월 :성균관대학교 정보공학과 석사
1999년 3월 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정

원 동 호(Dong-ho Won) **정회원**

1976년 2월 :성균관대학교 전자공학과 졸업
1978년 2월 :성균관대학교 전자공학과 석사
1988년 2월 :성균관대학교 전자공학과 박사
1978년 ~ 1980년 한국전자통신연구원 연구원
1985년 ~ 1986년 일본 동경공대 객원연구원
1996년 ~ 현재 성균관대학교 공과대학 전기전자 및 컴퓨터공학부 정교수

〈관심분야〉 암호이론, 정보이론