DBpia

論 文

개인통신서비스를 위한 인증 및 키분배방식 연구

正會員 丁 仙 伊* 正會員 鄭 鎭 旭*

A Key Distribution Protocol with User Authentication for Mobile PCS

Sun Ny Jung*, Jin Wook Chung* *Regular Members*

요 약

본 논문은 개인통신서비스(PCS)의 운영에 있어 필수적인 요소로 부상하고 있는 개인식별 기능을 갖는 두가지 키분배 방식을 제안하였다. PCS를 위한 서비스절차와 안정성 요구분석을 수행하고, 기존에 제안된 디지탈 이동통신을 위한 키분배방식의 안전성을 검토하였다. 특히 기존 방식중 Park 등이 제안한 ElGamal변형방식이 이용자 인증과정에 있어서 능동적 공격자에 대해 취약함을 입증하였다. 본 제안방식 I, II는 Rabin과 ElGamal암호계를 변형, 혼합한 것으로, PCS 운영에 있어서 빈번히 요구되는 인증시 계산량을 감소시켰고 이용자의 제한된 계산능력을 고려하여 이용자의 계산량을 줄였으며, PCS 안전성 요구사항을 만족시킨 것이다. 타 방식과 비교분석한 결과, 안전성 및 효율성 특히 이용자의 계산량에 있어서 제안방식이 더 개선되었음을 확인하였다.

ABSTRACT

Two types of key distribution protocols with user authentication are proposed for PCS(Personal Communication Service) and digital mobile communication systems. In this paper, we investigate the service procedure and security requirement for PCS, also discuss the security problems of KDPs previously proposed for digital mobile communication, and show that Park's type II among the schemes is easily broken by an impersonation attack. Our proposed I, II are based on the modified cryptosystem of Rabin and ElGamal, and reduce the amount of computation for user authentication. Such a reduction is good solution coped with the limited capability of user terminal on PCS. As a result of making a comparison between our schemes and the previously presented schemes, we can know ours are more secure and efficient for PCS.

*成均館大學校 情報工學科
Dept. of Infor. Eng., Sungkyunkwan Univ.
論文番號 : 93-194

I. 서 론

2000년을 향한 통신서비스로서 개인통신망(PCN :

www.dbpia.co.kr

Personal Communication Network)상에서의 개인통신서비스(PCS : Personal Communication Service)가 최근 각 분야의 관심을 모으고 있다. 가장 두드러지는 개인통신서비스의 특징으로는 무엇보다도 각 이용자의 고유한 식별번호에 의한 서비스 제공이라 할 수 있다. 즉 개인통신은 발착호절차 및 과금 등의 관리가 현재 운영되고 있는 PSTN이나 이동전화 통신망과 같이 가입자선이나 각 단말기에 부여된 식별번호(ID : identification)가 아니라, 실제로 통신을 행하는 각 이용자ID 의해서 이루어진다. 또한 각 이용자는 필요에 따라서 장소나 시간에 구애받지 않고 통신서비스를 받을 수 있어, 언제 어느 단말기에서나 자신의 ID를 등록하여 네트워크에 자신의 소재를 알려둠으로써, 자신과의 통신을 원하는 상대와 통신을 할 수 있게 된다[*1].

이렇듯 PCS가 단말기 중심체제로 부터 이용자 중심체제로 탈바꿈하게 됨에 따라, 기존의 이동무선통신서비스보다 더 안전한 서비스 제공이 요구되고 있다. 고의적인 불법사용자에 대한 방지나 다른 합법적 이용자의 식별번호를 도용한 불법사용, 부정하게 네트워크내에 접속하는 위험성 및 다른 사람에게 착호되는 정보의 부정 취득 등과 같은 제반 안전성 문제가 항상 존재하기 때문이다. 특히 개인통신 서비스 가운데 무선채널을 이용하는 무선 PCS는 개인통신의 특징을 가장 잘 발휘할 수 있는 특징을 갖는 반면, 무선자원의 이용에 의한 정보의 노출이 더욱 심각한 안전성 문제를 안고 있다.

또한 PCS에서는 이용자가 스마트카드와 휴대단말기를 이용하기 때문에, 안전성 서비스 제공을 위해 요구되는 계산능력에 한계를 갖게 된다. 따라서 안전성 제공을 위한 프로토콜 채용에 있어서 고려되어야 할 또다른 특징으로는 이용자측에서의 계산량을 최소화하여야 한다는 점이다.

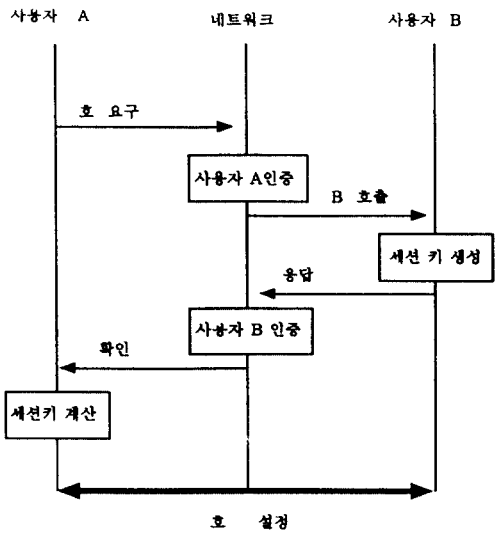
따라서 본 논문에서는 PCS와 같은 디지탈 이동통신에 있어서 요구되는 안전성과 효율성의 상반된 문제(trade-off)를 고려, Rabin암호계와 ElGamal암호계를 변형, 혼합함으로써 사용자식별자에 의한 인증기능을 갖는 효율적인 키분배 프로토콜을 제안하였다. 먼저 2장에서는 무선 PCN에 의한 발착호 절차를 살펴보고, 이에 따른 안전성 요구사항을 분석하였다. 3장에서는 이동체 및 무선통신을 위한 기존의 키 분배방식에 대해 그 절차를 설명하고 각각의 안전성을 살펴보았다. 특히 Park 등이 제안한 방식이 이용자 인증과정에 취약점을 갖고 있어 능동적 공격자에 의해 가장(impersonation)에 의한 네트워크 접속이 가능함을 보였다. 4장에서는 Rabin과 ElGamal의 안전성에 기반을 둔 제안방식을 개인통신서비스 절차에 따라 설명하고, 5장에서는 제안방식과 기존 방식을 안전성과 효율성의 관점에서 비교분석하였다.

Ⅱ. 무선 PCS와 안전성 요구분석

개인통신서비스는 발호, 착호, 과금관리의 대상이 각 이용자의 식별번호가 되므로, 실제 이동중에 서비스를 받기 위해서는 발호 및 착호시에 개인식별번호의 확인작업이 선행되어야만 한다[*2]. 본장에서는 무선 PCS를 위한 서비스절차를 살펴보고, 여기에 수반되어야 할 안전성 서비스 제공을 위한 요구분석을 수행한다.

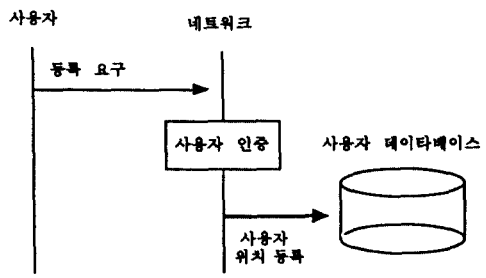
1. PCS의 서비스 절차

PCS의 서비스절차는 그림 1에서 보듯이 크게 두가지로 대별할 수 있다. 먼저 호를 설정하여 원하는 상대와 통신하기 위한 발호 및 착호시 호설정절차와, 자신으로 도달하는 호를 이동중에 있어서도 착호할 수 있도록 데이터베이스에 이용단말을 등록하는 이용단말의 등록절차가 그것이다. 이들 각 절차는 다음과 같다.



(a) 호설정 절차(발호 및 착호 절차)
(a) Call Establishment Procedure

www.dbpia.co.kr



(b) 이용단말의 등록 절차
(b) Registration Procedure of User Terminal

그림 1. PCS의 서비스 절차
Fig 1. Service Procedure of PCS

(1) 호설정 절차(발호 및 착호 절차)

① 발호 절차

먼저 발호를 원하는 이용자는 IC카드 등에 저장된 자신의 개인식별정보를 네트워크 센터로 보내, 자신이 그 네트워크의 합법적인 이용자임을 확인시킨 다음, 센터에 의해 착호자로의 호연결이 이루어진다. 물론 네트워크 센터는 다음 착호절차에서 언급하듯이, 착호자가 현재 위치해 있는 단말기 정보를 데이터베이스로 부터 검색하여 해당 단말기로 착호자의 개인식별자를 전송함으로써, 연결을 설정하게 된다. 물론 과금부과기능은 호의 설정과 동시에 해당 이용자의 개인식별번호에 대해 동작된다.

② 착호 절차

특정 이용자로 걸려온 호에 대해 네트워크 센터는 먼저 동 이용자의 데이터베이스를 검색하여 동 이용자의 위치정보(즉 등록단말기의 위치정보)를 인지할 수 있으면 그 단말기로 호를 연결하게 된다. 이때 센터는 그 단말기를 이용하는 이용자가 수명일 경우의 혼잡을 피하기 위해 어느 이용자에게 걸려온 신호인지를 식별할 수 있도록 착호자의 ID를 단말기에 디스플레이할 수 있어야 한다. 그 다음, 착호자는 자신의 IC카드 등을 통해 네트워크 센터에 자신이 올바른 이용자임을 인증시킨 다음 호를 받게 된다.

위 절차에 의해 두 이용자간의 호가 설정된다.

(2) 이용단말기의 등록절차

앞서도 언급했듯이, PCS는 이동중에도 언제 어디서나 자신으로의 도착신호를 수신할 수 있도록 하기 위해서 자신이 이용하게 될 이용단말기를 네트워크 센터의 자신의 데이터베이스에 등록하여 둠으로써, 자신을 호출하는 호에 대해서 네트워크센터가 연결할 수 있도록 하여야 한다. 물론 이 과정에서도 정당한 네트워크 이용자임을 네트워크 센터에 입증하게 된다.

이동중인 이용자는 자신으로 호를 착호하기 위해서 자신이 현재 이용할 수 있는 단말기 정보를 자신의 데이터베이스에 등록하여야 한다. 먼저 이용단말의 등록을 원하는 이용자는 IC카드 등에 저장된 자신의 개인식별번호를 이용, 네트워크 센터에 자신이 네트워크의 합법적 이용자임을 확인시킨다. 그 다음, 네트워크 센터는 이용자의 데이터베이스에 단말기의 정보를 기록하여 두고, 이동중인 이용자의 위치정보를 등록된 단말기의 위치정보로써 가름하여 관리하게 된다. 물론 이 과정은 특정 이용자를 찾는 신호에 대해 현재 이용자가 어디에 위치하고 있는가를 검색하기 위한 것이다.

이러한 과정을 통해 무선 개인통신서비스가 실현되는 것이다. 이 과정은 완전한 개인식별정보에 의한 발착호 절차를 예시한 것으로, 실제 서비스시에는 각 상황에 따라 보다 간단히 할 수도 있다. 또한 PCS에서는 단말기에서 자신을 이용하는 이용자가 누구인지를 기억해두지 않도록 하는 것이 각 이용자를 보호한다는 측면에서 요구되고 있다.

2. PCS를 위한 안전성 요구분석

앞에서 설명한 절차에 의해서 수행되는 개인통신서비스의 제공을 위해서는 어떠한 방법에 의해서든지 이용자의 정당성이 네트워크 센터에 의해 정확히 확인되어야 함이 강력히 요구되고 있다. 특히 PCS가 무선환경하에서의 이용형태가 주류를 이룰 것으로 예측됨에 따라, 유선의 경우보다 정보의 안전성(secrecy)과 개인의 프라이버시(privacy) 노출문제가 더욱 취약한 것은 당연하다. 따라서 개인통신서비스의 실현을 위해서는 이용자의 인증기능을 비롯한 제반 안전성 서비스가 함께 제공되어야 할 것이다[*3].

본 절에서는 개인통신서비스 제공을 위해 요구되는 안전성을 분석한다.

(1) 개인식별기능

네트워크 센터는 발착호 및 과금권리를 위해 네트워크를 이용하고자 하는 모든 이용자에 대해 정당한 이용자인지를 정확히 확인함으로써, 비인가된 불법 이용자가 네트워크로 접속하는 것을 방지해야 한다.

www.dbpia.co.kr

PCS에서는 이용자가 네트워크 센터에게 호설정을 요구할 때와 이용단말의 등록시 및 착호시에 이용자 식별기능이 요구된다.

이용자 인증방법으로는 패스워드 등과 같은 각 개인의 비밀 식별정보를 센터에게 제시하고, 센터는 이 정보를 자신이 갖는 데이터베이스와 비교하는 간단한 방법도 있으나, 이러한 방법은 전송중에 이를 감시하는 부정한 자에 의해 도용될 가능성이 많으므로, 안전성의 관점에서 적합하지 않다.

따라서 각 이용자의 개인식별정보는 네트워크 센터와의 전송시에 암호화 방법을 취해줌으로써 부정한 자에 의한 정보노출로 부터 보호되어야 한다. 현재 공통키 암호를 사용한 인증방법[4]을 비롯하여, Fiat-Shamir법[5]을 이용한 여러가지 변형 및 영지식 증명을 이용한 안전한 상호인증방법[6]등이 제시되고 있다.

(2) 불법공격자로 부터의 보호

정보의 노출이 유선보다 더욱 심각한 무선환경을 이용하는 PCS에서는 불법 공격자로 부터의 정보의 보호가 절실히 요구되고 있다.

이용자와 네트워크 센터, 이용자와 이용자간에 전송되는 각 이용자의 인증정보를 포함한 모든 정보는 이를 도용하려는 공격(passive attack)으로부터 보호되어야 한다. 이를 위해서는 전송되는 모든 정보에 대해 통신당사자만이 유효정보를 취할 수 있도록 공통키 및 공개키 암호시스템 등에 의해 암호화된 암호통신이 이루어져야 한다.

또한 이들 정보는 변경(modification), 재사용(replay attack), 위장(impersonation) 등에 의한 공격(active attack)에 의해서도 보호되어야 한다. 일반적으로 재사용에 의한 공격은 시간날인(time stamp) 메카니즘에 의해 보완될 수 있으며, 변경이나 위장 등에 의한 공격은 암호화 기법 및 비밀정보의 노출 방지 등에 의해 막을 수 있게 된다.

(3) 합법적 이용자에 의한 공격

만일 수명의 합법적 이용자의 협잡이나, 특정 이용자로의 의도적인 수회의 통신 등에 의해 복적하는 이용자의 비밀정보를 취하려는 합법적 이용자의 공격에 대해서도 모든 이용자의 비밀정보는 보호되어야 한다. 즉, 협잡이나 수회의 통신에 의해 이용자의 비밀정보가 노출되어서는 안된다.

또한 단일 네트워크가 아닌 여러 통신사업자가 혼재된 네트워크에서는 네트워크 센터에 의한 정보노출도 방지되어야 할 것이다. 만일 이용자간의 정보를 보호하기 위해 생성된 세션키(session key)가 네트워크 센터에 노출된다면, 현재 사회적으로 문제시 되고 있는 네트워크 센터의 도청 등 센터에 의한 부정행위를 야기시키게 된다. 따라서 이용자간의 정보를 보호하기 위한 세션키는 네트워크 센터에 대해 보호되어야 한다.

(4) 공개정보 화일의 제거

네트워크 센터나 이용자는 안전성 서비스를 위해 매 호설정시마다, 타 이용자들에 대한 공개정보를 저장하는 화일이나 데이터베이스를 각자가 저장한다거나 참조하는 번거로움을 가능한 피해야 한다.

즉, 매 이용자 인증시마다 인증정보를 위해 네트워크 센터가 각 이용자의 데이터베이스를 참조하여 비교하는 것은 시간지연 및 통신량의 증대를 유발시키게 될 뿐만아니라, 이용자가 급증하는 경우, 공개 정보를 저장하기 위한 메모리의 낭비도 무시할 수 없게 된다. 또한 각 이용자가 타는 이용자와의 비밀 통신을 위해 네트워크내의 모든 이용자의 공개정보를 저장하는 것 역시 네트워크의 확장이나 변경 등에 유연하게 대처할 수 없게 될 뿐만아니라 메모리의 비효율성을 가져오게 된다. 따라서 가능한 공개정보를 위한 화일이나 데이터베이스의 참조는 억제되어야 한다.

(5) 트래픽 및 계산량의 최소화

앞절에서 살펴본 바와 같이 PCS는 발호, 착호 및 이용단말의 등록시 등 무선채널상에서의 빈번한 이용자의 인증기능이 요구될 뿐만아니라, 향후 소형 휴대단말기 및 스마트 카드 등에 의존해 이들 서비스가 수행됨을 고려할 때, 이용자 인증을 위한 계산능력과 안전성 서비스를 위해 부가되는 정보량은 가능한 최소화되어야 한다. 또한 이용자의 인증기능과 이용자간의 비밀통신을 위한 세션키 분배기능 역시 가능한 한번의 네트워크 센터를 거친 이용자간 통신(two-way handshake)에 의해 이루어져야 한다.

이용자 인증기능과 세션키 분배를 위해 소요되는 계산량, 트래픽 횟수 및 트래픽당 안전성 서비스를 위해 부가되는 정보량(overhead)의 크기를 최소화하여야 한다. 물론 통신의 효율성과 안전성은 서로 상반되는 관계이므로, PCS의 특성을 고려한 최적점을 찾아야 될 것이다.

www.dbpia.co.kr

Ⅲ. 기존의 제안방식과 안전성 분석

1. Tatebayashi의 키분배방식

Tatebayashi 등에 의해 제안된 키분배방식(KDP : Key Distribution Protocol)들[*7]은 디지탈 이동통신을 위해 네트워크 센터에 의한 키관리기능을 제거하고, 제한된 계산능력을 갖는 휴대단말기를 이용하여 효율적인 시간내에 세션키를 분배할 수 있도록 공개키와 단순 대치암호를 혼합한 암호시스템을 채용하고 있다.

먼저 Tatebayashi의 KDP1은 이용자로 부터 네트워크 센터로의 전송시에는 센터의 공개키 값(e)을 3으로 하는 공개키 시스템을 채용하고 있으며, 세션키(r2)는 착호자에 의해 생성되어 발호자의 생성정보인 r1과 단순 모듈러 합연산을 취하여 다시 발호자에게로 전송되는 단순 대치암호를 이용하고 있다. 본 방식은 센터의 공개키의 값을 3으로 함으로써 이동단말에서의 계산량을 최소하였으나, 이미 Simmons[*8]에 의해 그 안전성 문제가 제기된 바 있듯이, 합법적 이용자와 네트워크 센터간에 교환되는 r_i^3정보를 취한 두명의 네트워크 이용자의 협잡에 의해 모든 이용자간의 세션키가 노출될 수 있다. 이러한 취약성(weakness)은 RSA 암호시스템의 모듈러 곱연산에 대한 교환성질에 기인한 것이다. 또한 동 방식은 이미 사용된 정보의 재사용에 의해 다른 이용자를 가장할 수도 있으며, 네트워크 센터에 대해 이용자간의 세션키가 노출될 뿐만아니라 PCS에 있어서 가장 중요한 인증기능이 결여되는 문제점을 안고 있다. 따라서 Tatebayashi는 그림 2와 같이 재사용 공격(replay attack)에 대비, 시간날인 메카니즘을 채용하고, KDP1에서와 같이 2명의 협잡에 의한 정보노출을 방지하며, 네트워크 센터에 의한 합법적 사용자의 인증기능을 갖는 KDP2를 제안하였다. 그러나 동 방식은 KDP1과 마찬가지로 네트워크 센터에 대해 이용자간의 세션키가 노출되는 문제를 그대로 안고 있을 뿐만 아니라, 센터의 공개키로서 지수값 3을 이용하기 때문에 $(t_i//S_i//r_i)^3$의 정보로 부터 이미 t_i와 r_i의 정보를 알고 있는 통신당사자중 어느 한쪽의 의도에 의해 동일 상대와 3번만 통신을 하게 되면 그 이용자의 비밀정보인 S_i를 취할 수 있어, 그 이후 그 이용자임을 자처하여 네트워크 센터에 자신을 부정하게 인증시킴으로써 과금시비 등의 문제를 유발할 수 있게 된다.

이 공격은 이미 Park의 논문[*9]에서 밝혀진 바와 같이, $(t_i//S_i//r_i)^3$의 정보는 //이 연접을 나타태므로, 일련의 2진 비트열로서 표현될 수 있다. 따라서 다른 사람의 비밀정보를 취하고자 하는 의도적인 통신자는 목적하는 동일 통신상대자와 3번만 통신을 수행한다면, 통신과정에서 ti와 ri의 정보는 매번 구할 수 있으므로, 타인의 비밀정보 Si에 대한 3차 방정식 3개를 만들 수 있게 된다. 그러므로 단지 미지수가 Si 하나뿐인 3개의 3차 방정식으로 부터 쉽게 Si정보를 취할 수 있다.

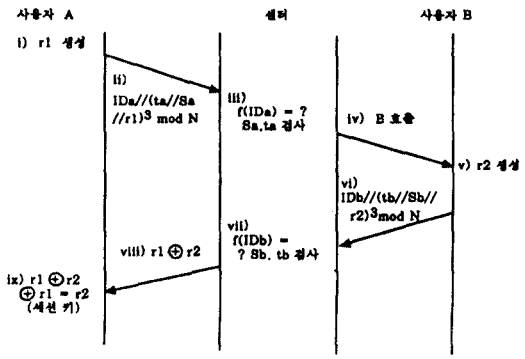


그림 2. Tatebayashi의 KDP2
Fig 2. Tatebayashi's KDP2

2. Park 등의 제안방식

Tatebayashi의 KDP2가 동일 이용자와 3회의 통신에 의해 쉽게 비밀 식별정보를 취할 수 있는 문제점을 해결키 위해 Park과 Kurosawa는 Rabin암호계와 ElGamal암호계에 기반을 둔 키분배방식을 제안하였다[*9].

이들이 제안한 Rabin 암호계[*10]에 기반을 둔 방식은 이동체 데이터통신의 특징인 키관리의 문제점, 계산능력의 최소화 등의 관점에서는 기존의 방식이 갖는 문제점을 해결하는 상당히 효율적인 방식이다. 특히 단순 대치암호의 취약성에 따른 세션키의 손쉬운 노출을 강화하기 위해 발호자측에서 두개의 랜덤수를 생성함으로써, 수명의 협잡이나 반복적인 집중공격으로 부터 각 이용자의 비밀 식별정보와 세션키를 보호하도록 하였다. 그러나 동 방식은 센터에 대해 세션키가 노출되는 안전성 문제를 여전히 안고 있다.

그림 3은 Park 등이 앞의 프로토콜이 갖는 세션키의 네트워크 센터로의 노출문제를 해결키 위해 Diffie-Hellman/ElGamal암호계[*11, *12]에 기반하여 제안한

www.dbpia.co.kr

안전한 인증기능을 갖는 키분배 프로토콜이다. 특히 신뢰할 수 있는 네트워크 센터에 의해 사전에 각 이용자에게 분배된 비밀정보는 실제 네트워크를 운영하는 운영센터에서도 노출되지 않도록 인증 및 키분배 기능이 제공될 수 있는 안전성을 유지한다. 그림3의 Yi와 Si는 각각 이용자별 공개정보와 비밀정보로서 네트워크 센터가 가입단계에서 큰 소수 P에 의해 생성하며, $Yi = g^{Si} \pmod P$의 관계를 갖는다.

그러나 동 방식은 이용자의 가입단계에서 신뢰할 수 있는 네트워크 센터와 네트워크 운영센터가 필요하며, 네트워크 운영센터는 모든 가입자에 대한 공개정보를 저장하거나 해당 데이터베이스로의 접속을 매 인증시마다 수행해야 한다. 또한 가장 큰 단점으로는 계산량의 복잡도로서, 향후 휴대 단말기나 스마트카드 등을 이용한 계산을 고려할 때 해결되어야될 과제로 남게 된다.

또한 이 방식은 다음에서 보듯이 특정 이용자간의 통신을 1회 도청한 다른 공격자에 의해 합법적 이용자로의 위장에 의한 네트워크 접속이 가능하다.

〈위장에 의한 네트워크의 불법 접속〉

그림 3에서 보듯이 두 이용자간에 전송되는 정보를 감시하던 공격자는 네트워크내의 모든 이용자에 대한 공개정보 Y_i를 취득할 수 있다. 그 후, 공격자는 언제든지 다음 과정을 통해 자신이 원하는 상대와 다른 이용자의 인증기능을 통해 네트워크에 접속할 수 있게 된다.

step 1) 합법적 이용자 A를 가장하여 네트워크에 접속하고자 하는 위장자 A'는 A의 공개정보 Ya를 이용하여 다음 정보를 생성, 네트워크 센터로 (Ta', ra'//ta')를 전송한다.

$Ta' = Ya^{ra'//ta'} \mod P$

step 2) 센터는 수신된 정보에 의해 다음을 체크하여 합법적 이용자 A임을 확인하고, 상대 이용자 B를 (Ya, $g^{ra'}$, ra') 정보와 함께 호출한다.

$Ya^{ra'//ta'} = ?\ \ Ta'$

step 3) 위장자는 센터에서 B로 전송되는 정보중 Ya를 자신의 공개정보 Ya'로 변경한다. 즉 착호자로의 전송정보는 (Ya', $g^{ra'}$, ra')가 된다.

step 4) B는 수신된 정보를 이용, $(g^{ra'})^{Sb}$, $(Ya')^{ra'+Sb} \oplus SK$를 계산하여, 센터로 전송한다.

step 5) 센터는 $(g^{ra'})^{Sb}$가 $Yb^{ra'}$임을 확인함으로써, 이용자 B를 인증한다.

step 6) 센터는 $Yb * g^{ra'}$와 $(Ya')^{ra'+Sb} \oplus SK$를 위장자 A'에게 전송한다.

step 7) 위장자 A'는 수신된 정보로 부터 다음 계산에 의해 세션키를 취득한 다음, 원하는 이용자 B와 호출 설정하게 된다.

$(Yb * g^{ra'})^{Sa'} \oplus (Ya')^{ra'+Sb} \oplus SK = g^{(Sb+ra')Sa'} \oplus g^{Sa'(ra'+Sb)} \oplus SK = SK$

센터의 인증기능은 매번 이용자에 의해서 새로이 생성되는 랜덤수와 시간날인정보에 의해서만 확인된다. 따라서 특정된 타 이용자의 공개정보만 알고 있다면 교환법칙에 의해 $(g^{ra/ta})^{Si} = (g^{Si})^{ra/ta} = Yi^{ra/ta}$가 성립되므로, 위장자는 언제든지 자신이 생성한 랜덤수와 시간날인정보로서 Ta'의 정보를 계산하여 위 step 1)과 2)에 의해 다른 이용자인 척 네트워크에 접속할 수 있게 된다.

또한 위장자는 step 3)부터 step 7)의 과정과 같이 수행함으로써, 이용자 A를 가장하여 네트워크에 접속하여 키분배와 함께 호를 설정할 수 있게 된다. 이에 따라 네트워크는 이용자 A에게 과금을 하게 되므로, 요금시비 등의 문제를 갖는다. 즉 Park 등의 ElGamal변형 프로토콜은 이용자의 인증시, 메시지 변경에 따른 위장 공격에 취약점을 갖음을 알 수 있다.

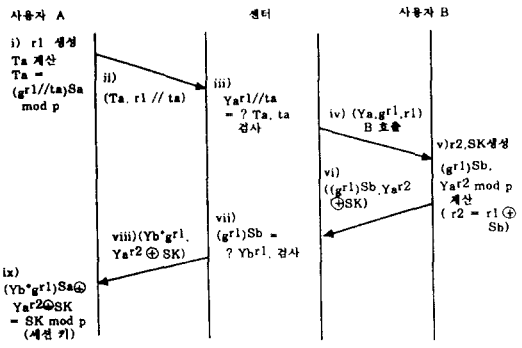


그림 3. ElGamal암호계에 기반한 Park의 키분배 프로토콜
Fig 3. A Park's KDP based on ElGamal Cryptosystem

3. Cho 등의 제안방식

그림 4는 Cho 등에 의해서 제안된 키분배 프로토콜로서, 이용자로 부터 네트워크 센터로는 RSA암호화 방식을, 센터로 부터 이용자로는 Diffie-Hellman의 변형방식을 이용하여, 인증기능과 동시에 키분배 기능을 수행하고 있다. 그림에서 각 이용자의 비밀정보를 생성하는 f( )함수는 센터만이 알고 있는 polyra-

www.dbpia.co.kr

ndom함수이다[*13].

동 방식은 랜덤수에 의한 세션키 생성시 발생되는 비도문제를 해결키 위해 이산대수의 난도를 이용한 암호화 기법에 의해 키를 분배함으로써, 안전성을 강화하고 있다. 이 방식은 앞에서 제기된 안전성 서비스를 만족시킬 수 있으나, 5장에서 살펴보는 바와 같이 Park 등이 제안한 ElGamal변형에 비해 계산량이 개선되지는 않고 있다.

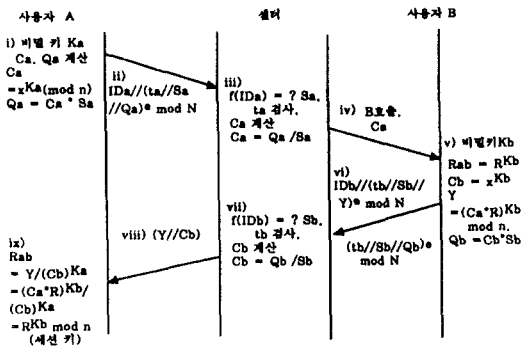


그림 4. Cho 등의 키분배 프로토콜
Fig 4. A KDP proposed by Cho

Ⅳ. 본 논문의 제안방식

2장에서 살펴본 바와 같이 PCS는 이용단말의 등록, 착호, 발호시 등 3단계에 걸쳐 이용자의 인증기능이 요구되며, 호설정시에는 이용자간의 비밀데이터 전송을 위한 세션키의 분배도 동시에 이루어져야 한다.

따라서 본 논문에서는 인증기능과 세션키의 분배기능을 분리하여, 서로 상반된 관계에 있는 안전성과 효율성 문제를 모두 고려, 다음과 같이 두가지 방식을 제안하였다.

제안방식 I, II는 기본적으로는 이용자로부터 네트워크 센터로의 인증을 위해서는 계산량이 비교적 적은 Rabin암호계를 채용하였으며, 호 설정시의 세션키 분배를 위해서는 ElGamal 변형 암호계를 채용하였다. 특히 Rabin 암호계 채용에 있어서는, Rabin암호계가 복호시 4 : 1의 ambiguity 복호의 문제점을 갖으므로, 네트워크 센터측에서 정확한 메시지의 일의 복호를 위해 부가적인 정보로서 timestamp와 각 이용자의 비밀정보를 이용하였다.

방식 I은 3.2절에서 분석된 Park방식의 문제점을 해결한 것으로, 네트워크 센터에서의 이용자 인증기능과 두 이용자간의 세션키 분배기능을 완전히 분리하여 센터의 이용자 인증기능과 세션키 분배기능을 제공토록 하였다.

방식 II에서는 네트워크 센터에서의 이용자 인증뿐만 아니라 두 이용자간의 상호인증 기능을 갖는 키분배 프로토콜을 제안하였다.

1. 제안방식 I

(1) 네트워크 가입단계

신뢰할 수 있는 네트워크 센터는 먼저 세션키의 분배를 위해 큰 솟수 P를 생성하여 GF(P)상에서의 원시원소 g를 결정한 다음, P와 g를 각 이용자가 세션키의 생성을 위한 파라미터로서 이용할 수 있도록 공개한다(키분배를 위한 암호계 생성). 또한 네트워크 센터는 이용자 인증을 위해서 또다른 큰 솟수 p와 q를 구하여 이의 합성수인 $N = p*q$를 만든 다음, p와 q는 센터만의 비밀정보로서 간직하고 N은 공개한다(인증을 위한 암호계 생성).

그후, 이용자가 네트워크에 가입코자 할 때 이용자 i가 제시한 이용자 ID_i를 기반으로 다음 함수에 의해 각 이용자의 인증을 위한 비밀정보(즉, 과금 등의 관리를 위한 개인식별정보 : PID)를 생성한다.

$S_i = H(f(ID_i))$

여기서 f( )는 pseudo random함수이며, H( )는 해쉬함수로서 센터만의 비밀함수이다. 센터는 IC카드 등에 (ID_i, P, g, N, S_i)의 정보를 안전하게 기록하여 이용자 i에게 전달한다. 이 가운데 S_i는 네트워크 센터와 가입자 i만이 알고 있는 이용자 인증을 위한 비밀정보이며, P, g, N 등은 공개정보이다.

(2) 서비스단계(인증 및 키분배 과정)

이용자의 네트워크 센터에 의한 인증과 이용자간의 세션키 분배단계는 착호을 위한 이용자의 이용단말 등록단계와 호설정을 위한 발착호 단계로 분류하여 살펴본다.

① 이용단말 등록절차

이용자 A는 자신이 이동중에 자신으로의 호를 수신하기 위해서 현재 위치를 네트워크 센터에 등록해 두어야, 센터에 의한 착호서비스를 받을 수 있게 된다.

따라서 이용자 A는 자신의 위치등록을 위해 먼저 단말기에 자신의 IC카드를 넣고 그림 5와 같이 자신

www.dbpia.co.kr

이 합법적인 네트워크 이용자임을 센터에 확인시키고 자신이 이용하는 단말을 등록시킴으로써 이용자 위치정보를 센터에게 인지시키도록 한다.

step 1) 이용자 A는 먼저 랜덤수 r1을 생성하여 센터의 공개키인 e=2를 이용, 다음을 계산하여 센터에게 자신의 IDa와 함께 전송한다.

$(ta//r1//Sa)^2 \mod N$

(여기서 ta는 replay attack 방지를 위한 time-stamp이며, //는 연접(concatenation)을 나타낸다.)

step 2) 센터는 자신이 수신한 암호문으로 부터 Rabin의 복호과정을 통해 mod p와 mod q상에서 모두 4개의 해를 구한다. 또한 이용자의 IDa를 이용하여 f( ), H( )를 수행한 결과치인 Sa를 구한다.

센터는 4개의 해 가운데에서 이용자의 비밀정보 Sa와 timestamp정보를 갖는 해가 존재하는지를 확인하여, 만일 이들 정보를 갖는 해가 존재하면, 센터는 동 이용자가 네트워크의 합법적 이용자임을 인증하고, 동 이용자의 데이터베이스에 현재의 위치정보를 이용중인 단말의 위치정보로서 등록하여, 이를 관리하게 된다.

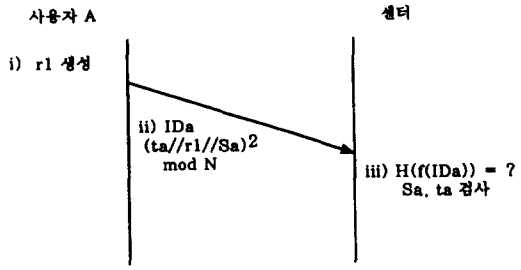


그림 5. 제안방식의 이용단말 등록절차

Fig 5. Registration Procedure of User Terminal of the Proposed Scheme

② 호설정을 위한 발착호 절차

이용자 A가 이용자 B와 호설정을 하고자 할 때의 A, B 이용자인증과 키분배 절차는 그림 6에서 보듯이 다음 절차에 의해 이루어진다.

step 1) 이용자 A는 랜덤수 ra, r1을 생성하여, Ya와 Za를 계산한다.

$Ya = g^{ra} \mod P$

$Za = (ta//r1//Sa)^2 \mod N$

step 2) 이용자 A는 IDa//Ya//Za를 센터에게 전송한다.

step 3) 센터는 앞의 이용단말 등록절차 step 2)에서와 동일한 과정을 통해, Za를 복호하여 이용자 A를 확인한다. 만일 A가 정당한 이용자이면 이용자 B의 데이터베이스를 검색하여 B가 현재 위치하고 있는 단말기로 이용자 B의 호출과 동시에 Ya정보를 전송한다. 인증에 실패하면 센터는 호를 단절한다.

step 4) 이용자 B는 네트워크 센터의 호출에 대응해, 랜덤수 rb, r2를 생성하고, 자신을 호출한 이용자 A와의 데이터보호를 위한 세션키 SK를 생성한다.

다음으로 Yb, Zb, T를 계산한다.

$Yb = g^{rb} \mod P$

$Zb = (tb//r2//Sb)^2 \mod N$,

$T = Ya^{rb} \oplus SK \mod P$

step 5) 이용자 B는 센터에게 IDb//Yb//Zb//T를 전송한다.

step 6) 센터는 step 3과 마찬가지로 Zb를 복호하여 tb//r2//Sb를 취한 다음, 이용자 B를 인증한다. 만일 성공하면 이용자 A에게 (Yb, T)를 전송하고, 실패하면 호를 단절한다.

step 7) 이용자 A는 수신된 정보로부터 다음과 같이 모듈러 합연산에 의해 세션키 SK를 취한다.

$$Yb^{ra} \oplus T = Yb^{ra} \oplus Ya^{rb} \oplus SK$$
$$= g^{rarb} \oplus g^{rarb} \oplus SK \ (\mathrm{mod}\ P)$$
$$= SK$$

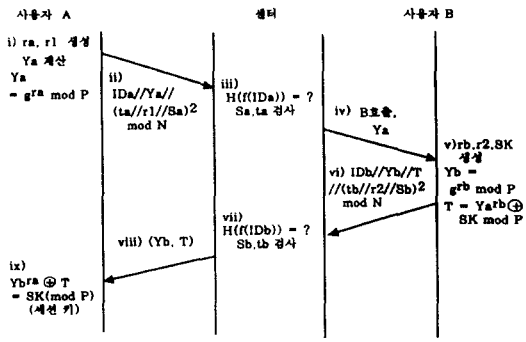


그림 6. 제안방식 I의 호설정을 위한 인증 및 키분배 절차

Fig 6. Call Establishment Procedure of the Proposed Scheme I

www.dbpia.co.kr

2. 제안방식 II

제안방식 II는 네트워크 가입단계와 호설정 단계가 제안방식 I과 완전히 동일하다. 다만 제안방식 I에서 결여된 두 이용자간의 상호인증기능을 부가하기 위해, 세션키의 생성시 각 이용자의 비밀정보를 이용하도록 하였다.

제안방식 II는 방식 I의 step 1)과 4)에서 각 이용자가 Yi의 값을 $g^{(ri+Si)}$로 취하도록 하였으며, step 4)에서는 T값을 $Ya^{(rb+Sb)} \oplus SK$로 대치하였다. 따라서 step 7)에서는 다음 연산에 의해 세션키 SK를 구할 수 있게 된다.

$$Yb^{(ra+Sa)} \oplus T = Yb^{(ra+Sa)} \oplus Ya^{(rb+Sb)} \oplus SK$$
$$= g^{(rb+Sb)(ra+Sa)} \oplus g^{(ra+Sa)(rb+Sb)} \oplus SK \pmod P$$
$$= SK$$

즉, 제안방식 II는 세션키의 분배시 두 이용자의 비밀정보를 이용하여 이용자간의 묵시적 상호인증기능을 부가한 것이다.

V. 안전성 및 효율성 분석

1. 안전성 검토

네트워크 센터에 의해 수행되는 합법적 이용자인지에 대한 발착호 및 과금관리를 위한 이용자 인증기능은 Rabin암호계를 이용하여, 이용자로부터 센터로의 인증정보가 전송되므로, 합성수 N의 소인수 분해의 난이도에 기인한 모듈러 N에서의 제곱근을 구하는 복잡도에 그 안전성을 의존한다. 따라서 합성수 N이 큰 경우, 이는 계산적 안전도를 갖게 된다.

무선채널상에 전송되는 정보인 Ya와 Za는 암호문으로서, 센터의 비밀키와 각 이용자가 생성한 랜덤수를 알지 못하는 공격자는 이들 정보로 부터 유용한 정보를 얻을 수 없으며, replay attack은 시간날인 메카니즘의 채용에 의해 해결하도록 하였다.

기존 방식중 안전도가 비교적 높은 것으로 제안된 Parks'의 ElGamal변형방식은 시간날인메카니즘을 사용하였지만, 3.2절에서 살펴본 바와 같이 랜덤수와 시간정보의 노출 등에 의해 누구든지 쉽게 다른 이용자를 가장하여 센터에 접속할 수 있게 되어 인증상의 문제를 갖고 있다.

반면 제안방식 I, II는 모두 센터에서의 인증시 Si 정보를 이용하므로, 이 정보를 알고 있는 이용자와 센터 이외에는 다른 이용자를 가장하여 센터에 접속할 수 없게 된다. 특히 방식 II는 세션키 생성시 Yi 정보에 상대 이용자의 비밀 인증정보를 이용토록 함으로써, 두 이용자 상호인증이 수행된다.

또한 제안방식은 랜덤수 발생에 의해 Za 내부의 미지수를 2개로 함으로써, 수명의 합법적 네트워크 이용자간의 협잡에 의해서도 각 이용자의 비밀 인증정보 S_i를 취할 수 없도록 하였다. Park 등의 Rabin 암호계 변형방식이 갖는 취약점인 네트워크 센터의 부정 가능성은, 이용자가 발생한 랜덤수를 알지 못하는 센터가 단순 대치암호로 암호화된 정보인 T로부터 세션키 SK를 취할 수 없다는 사실에 의해 방지될 수 있으며, 세션키는 매번 이용자 임의대로 변경할 수 있는 one-time키로 하였다. 물론 이 경우, 세션키와 Y_i는 의미를 갖지 않는 비트열로서 다루어져야만 exhaustive attack에 대해서 안전하다.

본 방식은 인증을 위해 안전한 해쉬함수를 사용하도록 함으로써, 네트워크 센터가 안전성 서비스를 위해 별도의 이용자 공개정보 화일을 저장하거나 데이터베이스에 접속할 필요성을 제거하였다.

한편, 제안방식 I과 II는 키의 분배시 Yi정보를 공격자가 변경함으로써 이용자 B가 생성한 세션키는 취득할 수 있을지라도 공격자가 변경한 암호문때문에 이용자 A는 올바른 키를 생성할 수 없게 되어, 결국 공격자는 세션키의 취득에 의해 두 이용자간의 암호통신을 해독할 수 없게 된다. 단지 두 이용자간의 키분배만을 방해할 뿐인 것이다.

이상, 본 제안방식들은 안전성의 관점에서 살펴볼 때 이산대수와 소인수분해의 난도에 의존한 계산적

표 1. 안전성 비교
Table 1. Comparison of Security

분류 / 방식		이용자 인증	키 분배	재사용 방지	상호 인증	협잡 방지	센터부 정방지	위장접속방지	공개화일 존재유무
Tate	KDPI	×	○	×	×	×	×	×	무
	KDPII	○	○	○	×	×	×	○	무
Park	I	○	○	○	×	○	×	○	무
	II	○	○	○	○	○	○	×	유
Chos'	방식	○	○	○	×	○	○	○	×
제안	I	○	○	○	×	○	○	○	무
방식	II	○	○	○	○	○	○	○	무

*○, ×는 해당 기능의 유무를 나타낸다.

www.dbpia.co.kr

상도를 갖으며, 디지탈 이동무선통신망상에서 제안된 3장의 타 방식에 비해 PCS가 요구하는 제반 안전성 요구사항을 모두 만족시킴을 알 수 있다.

표 1은 앞의 3장에서 이미 분석된 기존 방식들의 안전성과 본 절의 제안방식 I, II의 안전성을 비교한 것이다.

2. 효율성 검토

제안방식들은 PCS가 빈번한 인증을 요구한다는 특징에 기인하여 안전한 키분배를 위한 복잡한 지수계산이 매 인증시마다 사용되지 않도록, 인증을 위한 암호계와 안전한 키분배를 위한 암호계를 분리하였다. 따라서 인증서버스에서는 간단한 제곱계산을 수행하는 Rabin암호계를 채용하였으며, 키분배를 위해서는 네트워크 센터에서의 세션키 노출을 방지하기 위해 많은 지수계산을 수행하는 ElGamal암호를 변형하였다. 또한 호설정시에는 인증과 키분배가 two-way handshake에 의해 함께 수행되도록 하였으며, 인증기능과 키분배기능을 결합함으로써, 불법 공격자의 변경에 의한 가장에도 안전하도록 하였다.

특히 제안방식은 디지탈 이동통신의 경우, 스마트카드나 휴대단말기 등에 계산을 의존해야 하는 이용자의 계산능력을 고려, 가능한 이용자의 계산량을 최소화 하도록 하는데 중점을 두었다.

본 절에서는 기존의 방식중 제안방식과 안전도 수준이 유사한 Park 등이 ElGamal암호의 변형방식과 Cho등의 방식을 대상으로 계산량의 관점에서 비교분석한다(표 2).

2장에서 살펴본 바와 같이 서비스의 절차를 이용자의 이용단말등록시와 호설정시로 나누어, 각 방식에서 요구되는 계산량과 데이터베이스 및 해쉬함수의 수행횟수, 그리고 서비스제공을 위해 요구되는 네트워크센터의 수를 비교하여 표 2에 보였다. 비교의 단순화를 위해 P나 N 모듈러스 연산에 의한 복잡도는 고려하지 않았으며, 단순 제곱연산은 곱셈연산으로 간주하였다.

이용자가 다른 이용자와 하나의 호를 설정하기 위해서는 단말등록단계와 호설정 단계가 모두 필요하므로, 이때의 계산량은 표 2에서 보듯이 새로운 제안방식I과 II가 다른 방식들에 비해 복잡한 지수연산의 횟수가 더 감소되었음을 알 수 있다. 특히 제안방식들은 이용자측에서의 계산횟수를 줄임으로써, 이용자의 연산 능력이 다른 네트워크에 비해 열악한 PCS상에서의 채용에 더 효율적임을 확인하였다.

표 2. 효율성 비교

Table 2. Comparison of Efficiency

분 류		계산 횟수				DB참조 및 해쉬수행	센터수
		지수	곱셈	나눗셈	덧셈		
Parks'	사용등록시	2(1)	1(1)			DB 1회	2
	호설정시	7(4)	2(1)		3(3)	DB 2회	
Chos'	사용등록시	3(2)	1(1)			해쉬1회	1
	호설정시	10(7)	3(3)	3(1)		해쉬2회	
제안 방식 I	사용등록시	1(0)	1(1)			해쉬1회	1
	호설정시	6(4)	2(2)		2(2)	해쉬2회	
제안 방식 II	사용등록시	1(0)	1(1)			해쉬1회	1
	호설정시	6(4)	2(2)		4(4)	해쉬2회	

* 주) ( )의 숫자는 센터를 제외한 이용자 측에서 수행되는 계산횟수임.

또 센터에서 수행되는 과정중 인증을 위해 이용자 공개정보를 취하기 위한 데이터베이스 참조는 Parks' 방식에서만 요구되며, 다른 두 방식은 네트워크가 갖는 해쉬함수의 수행에 의해 공개정보의 저장이나 참조없이 인증을 수행할 수 있다. 또한 Parks'방식은 반드시 완전하게 신뢰할 수 있는 네트워크센터와 운영센터 등 2개의 독립적인 센터가 필요한 반면, 다른 두 방식은 동일 센터로서 서비스될 수 있다.

따라서 본 논문에서 제안된 방식이 가입단계에서 타 방식에 비해 네트워크 센터가 P와 N의 2개 모듈러스 연산을 위해 더 많은 공개 및 비밀정보를 생성해야 한다는 부담을 안고 있지만 이는 운영과정에서는 무시할 수 있어 실제 서비스단계에서는 타 방식에 비해 더 효율성을 갖는 것으로 판단된다.

Ⅵ. 결 론

본 논문은 향후 개인통신망 환경에서의 안전성 서비스 제공을 위한 인증기능을 갖는 효율적인 키분배 방식에 대한 연구이다. 개인통신서비스는 반드시 이용자의 네트워크센터에서의 빈번한 인증기능이 요구되며, 스마트카드나 휴대단말기를 이용함에 따른 이용자의 계산능력의 제한을 갖고 있다. 따라서 본 논문은 이러한 관점에서 간단한 제곱지수연산을 수행하는 Rabin암호계를, 네트워크 센터의 부정방지를 위해 키분배시에는 ElGamal방식의 변형을 채용하는

www.dbpia.co.kr

혼합암호계를 채용함으로써, 이용자의 계산량을 개선한 안전한 인증기능을 갖는 키분배 방식 I, II를 제안하였다.

먼저 개인통신서비스의 제공을 위한 서비스절차를 살펴보고, PCS를 위한 제반 안전성 및 효율성 요구사항을 분석하였다. 다음으로 기존에 디지탈 이동무선통신을 위해 제안된 여러가지 키분배 프로토콜을 본 제안방식 I, II와 안전성 및 효율성의 관점에서 비교 분석하였다.

그 결과, 제안방식들이 PCS가 요구하는 안전성을 모두 만족시키면서도 계산량의 관점에서 기존의 방식에 비해 더 개선되었음을 확인하였다.

참 고 문 헌

1. S. Ginn, "Personal Communication Services : Expanding the Freedom to Communicate," IEEE Communication Magazine, pp.30-39, Feb. 1991.
2. H. Tsubakiyama, M. Obhashi, K. Koga, "A study on Information Security for Radio Personal Telecommunications," 日本 電子情報通信學會 技術研究報告, CS91-19, pp.15-22, 1991.
3. Akiyama, Sasaki, "Authentication and Encryption in a Mobile Communication System," 43rd IEEE Vehicular Technology Conference, pp.927-930, 1993.
4. 花岡他, "Digital 移動通信網에 있어서 認證方式," 1990年 日本 電子情報通信學會 秋季 全國大會 講演論文集, B-232, 1990.
5. A. Fiat, A. Shamir, "How to Prove Yourself : Practical Solutions to Identifications and Signature Problems," in Advances in Cryptology-Crypto86, Proceedings, Springer-Verlag, pp. 186-194, 1987.
6. T. Beth, "Efficient Zero Knowledge Identification Scheme for Smart Cards," Proc. Eurocrypt'88, pp.77-84, 1988.
7. M. Tatebayashi, N.Matsuzaki, D.Newman Jr., "Key Disribution protocol for Digital Mobile Communication Systems," Advances in Cryptology : Proceedings of Crypto'89, Springer-Verlag, pp.324-333, 1990.
8. G. J. Simmons, "An Impersonation-proof Identity Verfication Scheme," Advances in Cryptology : proceedings of Crypto'87, Springer-Verlag, pp. 211-215, 1988.
9. C. Park, K.Kurozawa, "Key Distribution Protocols for Mobile Communication Systems," 日本 電子通信學會 信學技報 ISEC92-48, pp.17-23, 1992.
10. M. Rabin, "Digital Signatures and Public Key Functions as Intractable as Factorization," In Technical Reprt MIT/LCS/TR-212, MIT, 1979.
11. W. Diffie, M.HEllman, "New Directions in Cryptography," IEEE Trans. on Info. Theory, Vol. IT-22, No.6, pp.644-654, 1976.
12. T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," IEEE Trans. on I.T., Vol.IT-31, pp. 469-472, 1985.
13. 윤장근, 문태욱, 조성준, "이동통신시스템을 위한 키분배방식에 대한 연구," 통신정보합동 학술대회 논문집 제3권 pp.357-360, 1993.

丁 仙 伊(Sunny Jung) 정회원

1981년 2월 : 한국항공대학 통신공학과 학사

1991년 2월 : 성균관대학교 정보공학과 석사

1991년 3월 ~ 현재 : 성균관대학교 정보공학과 박사과정 재학중

1981년 2월 ~ 1988년 10월 : 월간 전자과학 편집장

※주관심분야 : 네트워크 보안, 고속무선 통신프로토콜

鄭 鎭 旭(Jin Wook Chung) 정회원

1974년 2월 : 성균관대학교 전기공학과 학사

1979년 2월 : 성균관대학교 전자공학과 석사

1991년 2월 : 서울대학교 계산통계학과 박사

1973년 9월 ~ 1981년 12월 : 한국과학기술연구소 연구원

1982년 1월 ~ 1985년 2월 : 한국과학기술연구소 실장

1981년 9월 ~ 1982년 8월 : Racal-Milgo Co. 객원연구원

1985년 3월 ~ 현재 : 성균관대학교 교수

1992년 1월 ~ 1993년 1월 : 미국 Maryland대 객원교수

※주관심분야 : 네트워크 보안, 네트워크 관리, 고속 및 무선 통신 프로토콜

www.dbpia.co.kr