# 이동 Ad-hoc 노드용 사전 키 분배 기법 및 경량 키 분배 프로토콜을 위한 보안관리 서버 시스템 설계 및 구현☆

# The Design and Implementation of a Security Management Server for Pre-Distributed Key Exchange Method and Lightweight Key Distribution Protocol for Mobile Ad-hoc Node

양 종 원* 서 창 호** 이 태 훈***
Jong-Won Yang Chang-Ho Seo Tae-Hoon Lee

## 요 약

이동 Ad-hoc 네트워크는 USN 기술의 핵심으로서 많은 노드들이 각자 수집한 환경정보들의 무선통신을 기반으로 하여, 중요 데이터를 multi-hop 에 걸쳐 원하는 목적지에 전달하는 최신 네트워크 기술이다. 최근 Ad-hoc 네트워크 관련 기술 개발 및 서비스가 활성화 되고 있으나, Ad-hoc 네트워크 상에서 무선으로 전송되는 패킷들에 대한 인증 및 암호화 등의 보안 기능 구현은 미흡한 상황이다. 본 논문은 이동 Ad-hoc 네트워크 상에서 키 교환, 키 관리, 개체 인증, 데이터 암호화 등의 시큐리티 서비스를 제공하고, 이동 Ad-hoc 네트워크에 특화된 보안 프로토콜을 처리 및 관리하기 위한 Ad-hoc 네트워크 보안 관리 서버 시스템을 설계하고 구현한다.

## Abstract

The Mobile Ad-hoc network does environmental information which an individual collects in nodes which are many as the kernel of the USN technology based on the radio communication. And it is the latest network description delivering critical data to the destination location desiring through a multi-hop. Recently, the Ad-hoc network relative technique development and service are activated. But the security function implementation including an authentication and encoding about the transmitted packets, and etc. is wirelessly the insufficient situation on the Ad-hoc network .This paper provides the security service of key exchange, key management, entity authentication, data enciphering, and etc on the Mobile Ad-hoc network. It implements with the Ad-hoc network security management server system design which processes the security protocol specialized in the Ad-hoc network and which it manages.

☞ ketyword : Ad-hoc, 타원곡선 알고리즘, 이동 네트워크

## 1. 서 론

이동 Ad-hoc 네트워크는 고정된 기반 망의 도움없이 이동 노드들간에 자율적으로 구성되는 망으로써, 네트워크에 자율성과 융통성을 부여한 네트워크이다. 그리고 이동 Ad-hoc 네트워크는 기지국(BS: Base Station)이나 엑세스포인트(AP: Access Point)와 같은 중재자(centralized coordinator)가 없이 이동 노드들간에 자체적으로 연결이 설정되므로 임시적 또는 즉흥적인 망의 구성이 가능하다.[1-3].

또한 이동 Ad-hoc 네트워크는 USN 기술의 핵심으로써 많은 노드들이 각자 수집한 환경정보들

* 정 회 원 : 공주대학교 바이오정보학과 정보보호 박사과정 nobody@kongju.ac.kr
** 정 회 원 : 공주대학교 응용수학과(정보보호전공) /바이오정보학과 부교수
*** 정 회 원 : 광주대학교 정보통신학과 교수 thlee@gwangju.ac.kr
[2007/05/21 투고 - 2007/05/30 심사 - 2007/07/23 심사완료]
☆ 이 논문은 2007년도 한국과학재단 특정기초사업의 지원에 의하여 연구되었음(R01-2005-000-10200-0)

을 무선통신을 기반으로 하며, 중요 데이터를 multi-hop 에 걸쳐 원하는 목적지에 전달하는 최신 네트워크 기술이다.

최근 이동 Ad-hoc 네트워크 관련 기술 개발 및 서비스가 활성화 되고 있으나, 이동 Ad-hoc 네트워크 상에서 무선으로 전송되는 패킷들에 대한 인증 및 암호화 등의 보안 기능 구현은 미흡한 상황이다.

따라서, 이동 Ad-hoc 네트워크 상에서 키 교환, 키 관리, 개체 인증, 데이터 암호화 등의 시큐리티 서비스를 제공하고, Ad-hoc 네트워크에 특화된 보안 프로토콜을 처리 및 관리하는 이동 Ad-hoc 네트워크 보안관리 서버에 대한 개발이 절실하게 요구되고 있다.

본 논문에서 이동 Ad-hoc 네트워크 보안 서버는 Ad-hoc 노드로 부터 수집된 데이터를 가공 처리하는 기능을 제공하는 것으로써, 임의의 Ad-hoc 노드와 신뢰 채널 생성이 요구되는 경우 두 통신 개체 사이의 신뢰 채널 생성을 위한 키 교환 기능을 제공하고, 키 교환 기능을 통해서 공유된 비밀키를 이용하여 Ad-hoc 노드와 암호화 통신을 수행한다.

또한, Ad-hoc 노트로부터 수집된 각종 데이터(온도, 습도, 조도, 초음파 등)들을 사전키 분배 기법 및 경량 키 분배를 통해 임의로 정해진 기간까지 수집된 데이터 저장 기능을 수행하는 포괄적인 관리 서버 역할을 담당한다. 위에 명시된 바와 같이 Ad-hoc 서버와 Ad-hoc 노드간 전송되는 데이터에 대한 보안 기능을 적용하기 위해 표준 문서에 명시된 시큐리티 계층 및 보안 알고리즘을 설계하고, 수집된 센서 정보들을 처리하기 위한 관리 서버시스템을 구현했다.

## 2. 타원곡선 암호 시스템(ECC)

공개키 암호시스템으로는 소인수 분해의 어려움에 근거한 시스템(RSA)[4]과 이산대수의 문제의 어려움에 근거한 시스템(DSA), 그리고 타원곡선 사의 이산대수 문제에 근거한 시스템(ECC)이 주로 사용된다. 이중 타원곡선 암호시스템 비트당 안전도가 가장 높은 암호 시스템으로 작은 사이즈의 키 값만으로도 높은 안전성을 보장한다. <표 1>은 RSA, DSA, ECC 의 비트당 안전성을 비교한 표이다[5].

〈표 1〉 RSA, DSA, ECC 안전성 비교

| Time to break in MIPS years | RSA/DSA key size | ECC key size | RSA/ECC key size ratio |
|---|---|---|---|
| $10^4$ | 512 | 106 | 5:1 |
| $10^8$ | 768 | 132 | 6:1 |
| $10^{11}$ | 1,024 | 160 | 7:1 |
| $10^{20}$ | 2,048 | 210 | 10:1 |
| $10^{78}$ | 21,000 | 600 | 35:1 |

모듈러 지수승 연산이 RSA의 성능을 좌우하듯이 ECC의 성능은 스칼라 곱셈 연산의 의하여 좌우된다. 스칼라 곱셈 연산은 임의의 랜덤수 $k$와 타원 곡선 위의 한점 $P$의 곱셈 연산으로 정의되며, 타원곡선 위의 점 $P$의 $k$번 덧셈연산으로 계산된다.

## 3. 이동 Ad-hoc 네트워크 보안 관리 서버모듈 설계

본 장에서는 본 논문에서 필요로 하는 Ad-hoc 네트워크 보안관리 시스템에 대한 설계 정보를 보인다.

Ad-hoc 네트워크 보안관리 서버에 요구되는 기능은 다음과 같다.

- 암호화, 키 교환, 인증 알고리즘
  - Sync Node와 통신을 위한 Serial Communication 모듈
  - $GF(p)$[6], $GF(2^m)$[6]상에서의 Finite Field Operation 모듈
  - AES, ARIA, SEED 등 대칭키 알고리즘과 각

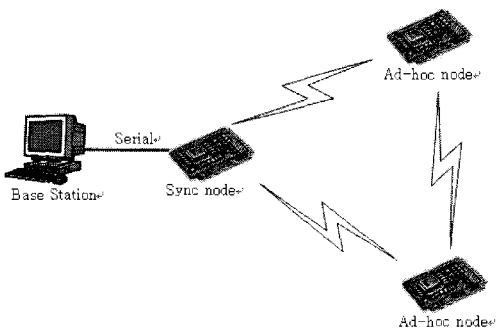
종 Mode-of-Operation(CBC, ECB 등) 을 통한 암·복호화 모듈
- ECDH, ECMQV, ECDSA, ECKCDSA, ECIES 알고리즘 모듈

- 신뢰 채널 생성을 위한 표준 보안 프로토콜
  - Ad-hoc 노드와의 보안 통신을 위한 SSL 모듈
  - Ad-hoc 노드와의 보안 통신을 위한 WTLS 모듈
- 수집된 센싱 데이터의 가공 처리 모듈로써 사용자 인터페이스를 통해 데이터 처리 및 운용 상태를 볼 수 있는 모듈
  - Mote 에 따른 온도, 습도, 조도, 초음파 데이터의 테이블식 표현 및, 2차원 공간에서의 mote위치에 따른 온도, 습도, 조도, 초음파 데이터 값 표시.
- 대칭키 기반 키 교환 및 키 관리를 위한 KDC(Key Distribution Center) 모듈

본 논문에서는 ECC기반 알고리즘(ECDSA, ECDHC)등 기술 표준을 정확하게 준수했다.

ECDSA는 ANSI X9.25[7]와 IEEE P1363[8] 표준 위원회에서 표준으로 채택되어지고 있으며, 또한 무선 환경에서 WPKI를 지원하기 위한 알고리즘의 커브 파라미터 등이 각각 WTLS[9], ANSI X9.62, FIPS 186-2[10]에서 권고하고 있다.

그림 1은 보안관리 서버 및 Ad-hoc 노드와의 시스템 구성을 보이고 있다.




(그림 1) Ad-hoc 네트워크 시스템 구성도

ECC은 여러가지 유한체 상에서 구현될 수 있으며, 본 시스템 구현에 사용되는 유한체는 다음과 같다.

- $GF(p)$ prime field
- $GF(2^m)$ binary field
- $GF(p^m)$ OEFs (p 는 mersenne prime)

특히 타원곡선 연산 구현상에 있어서 affile 좌표계를 사용하여 Addition 연산과 Doubling연산을 구현하게 되면 연산 중간에 유한체 inversion 연산을 사용되므로 전체적인 performance 가 떨어진다. 따라서 projective 좌표계를 이용하여 구현하면 Addition 연산과 Doubling연산이 단순히 유한체 square 연산과 multiplication 만으로 구현되어질 수 있으므로 빠른 연산 속도를 낼 수 있다.

이중에서 $GF(2^m)$ binary field가 현재 타원곡선 구현에 가장 널리 사용되고 있는 유한체이며, 특히 binary field는 사용되는 기저(basis)에 따라서 polynomial basis 와 normal basis로 일반적으로 나뉜다. normal basis는 타원곡선 암호시스템의 하드웨어 구현에 많이 사용되며, polynomial basis는 소프트웨어로의 구현에 주로 사용되고 있다. $2^m$를 m차 irreducible polynomial(기약 다항식) 이라 하고, 두 원소 $GF(2^m)$ 이라고 한다.

타원곡선 연산 구현에 필요한 $GF(2^m)$ 유한체 연산들은 다음과 같다.

- Addition, Subtraction 연산
  $\alpha + \beta = \alpha \oplus \beta$ (bitwise xor)
- Multiplication & Reduction 연산
  $\alpha * \beta \equiv \gamma \bmod f(x) \quad (\gamma \in GF(2^m))$
- Square 연산
  $\alpha^2 \equiv \gamma \bmod f(x) \quad (\gamma \in GF(2^m))$
- Inversion 연산
  $\alpha * \alpha^{-1} \equiv 1 \bmod f(x) \ (\alpha^{-1} \in GF(2^m))$

이와 같이, 네가지 유한체 연산을 구현해야하며 Multiplication, Square, Reduction, Inversion 연산은 가장 빠른 알고리듬을 이용하여 설계 및 구현해야 한다. 특히 reduction 연산은 $f(x)$가 pentinomial 또는 trinomial 인 경우에 빠른 구현이 가능하므로 이를 이용하여 빠른 reduction 연산을 구현해야 전체적은 performance 가 향상된다. 위의 유한체 연산을 이용한 타원곡선 연산은 다음과 같다.

$$E = (x, y) | y^2 + xy = x^3 + ax + b) \cup O$$

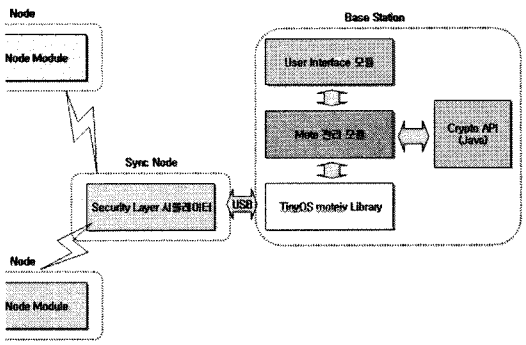
- 타원곡선 Addition연산(projective 좌표계)
  $P + Q = R(P, Q, R \in E$ 타원곡선 위의 점$)$
- 타원곡선 Doubling연산
  $2P = R(projective$ 좌표계 사용$)$
- 타원곡선 Scalar Multiplication연산
  $kP = R$ $(projective$ 좌표계의 사용$)$
- 타원곡선 좌표계의 상호 변화 연산
  $affine$ 좌표계 $\leftarrow \rightarrow projective$ 좌표

또한 Scalar Multiplication 연산은 일반적인 연산에는 Sliding Window method 또는 Montgomery method를 이용하여 계산하며, 키생성시에는 Fixed Based Comb method 를 이용한다. 본 논문에서는 타원곡선 암호 알고리즘들 중에서 ECDHC 과 ECDSA 적용하였다.

## 4. 이동 Ad-hoc 네트워크 보안 관리를 위한 보안서버 설계 및 구현

그림 2은 본 논문에서 제시한 Ad-hoc 네트워크 보안관리 서버 시스템의 전체 구성을 보여주고 있다.

구성별로 먼저 User Interface 모듈은 크게 두 가지로 나뉘며, 공통적으로 UI를 쉽고 편리하게 구성하기 위한 공통 UI 처리 모듈과 Ad-hoc 네트




(그림 2) Ad-hoc 네트워크 시스템 구성도

워크 보안관리 서버의 UI를 구성하기 위한 모듈(app)이 존재한다.

Crypto API 모듈은 ECC 알고리즘을 적절하게 제공하기 위하여 제공되는 보안모듈이며, Mote 관리 모듈은 TinyOS 에서 제공하는 모듈과 Mote를 제공받게 되며, 내부적으로 Mote와 통신을 하면서 하위 프로토콜을 처리하고, Mote를 제어하며, Mote의 응용단과 Base Station의 응용단을 연결시켜주는 역할을 수행한다.

### 4.1 구축환경

Base Station 프로그램을 설치하고 정상적인 서비스 운용을 위해서는 다음과 같은 환경이 구축되어 있어야 한다.

Microsoft Windows 계열
- Windows 2000/XP/2003
- TinyOS 2.x
- Java Virtual Machine (JDK 1.5.x)

Linux 계열
- TinyOS 2.x
- Java Virtual Machine (JDK 1.5.x)

또한, 이동 Ad-hoc의 node 인 mote를 제어하기 위해서는 TinyOS가 설치되어 있어야 함으로 프로

그램을 설치하기 전에 TinyOS가 시스템에 설치되어야 한다.

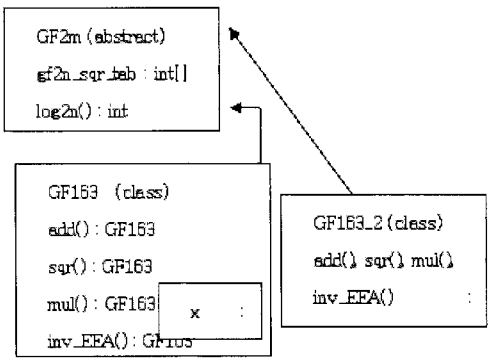
## 4.2 CrytoAPI 설계 및 구현

SUN 사의 자바언어 jdk1.4 에 포함되어있는 공개키 알고리즘으로는 RSA 와 DSA알고리즘이다. 그나마 jdk1.3에서는 포함되어있지 않았던 RSA알고리즘이 default 알고리즘으로 제공되어지고 있기는 하나 현재 WPKI 시스템이나 모바일 환경에서 사용되어지고 있는 ECC 알고리즘에 관해서는 key interface 조차 수출제한으로 포함되어있지 않은 실정이다. 자바로 타원곡선 알고리즘을 구현하려면 먼저 타원곡선 암호 알고리즘별 Key 클래스 및 Key Spec클래스와 그리고 크게 네 가지의 연산클래스 및 이러한 연산클래스를 중간에서 조율하는 provider class들로 분류하여 구현할 수 있다. 이렇게 연산 클래스와 provider class를 분리하여 구현하는 이유는 각 클래스들의 기능을 세분화 및 분류화 함으로써 각 기능들의 행동모델에 기반한 객체지향적인 설계를 위한 것이며 또한 연산 클래스의 유지보수를 쉽게 하기 위함이다. 먼저 연산 클래스는 아래와 같이 분류할 수 있다.

- GF2m(abstract), GF163, GF163_2 유한체 연산 클래스
- EC2m(interface), ECArithemtic, EC163, EC163_2 타원곡선 연산 클래스

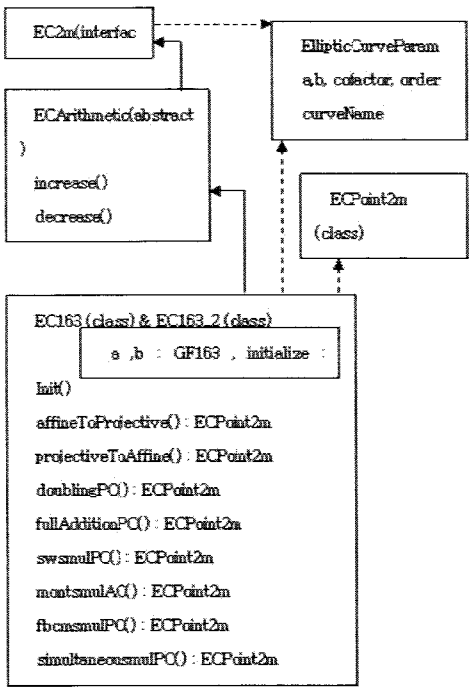
다음은 같은 163bit 길이 이지만 GF163과 GF163_2로 분류 하여 구현한 이유는 irreducible polynomial 서로 다르기 때문에 mod 연산을 최적화하기 위해서 이와 같이 설계하였다.

기본연산 클래스들 사이의 UML은 다음과 같다[그림3].




(그림 3) 기본 연산 클래스들 간의 UML

타원곡선 연산 클래스들에 대한 UML은 다음과 같다[그림4].




(그림 4) 타원곡선 연산 클래스들 간의 UML

이와 같이 EC2m이라는 interface를 선언함으로써 하나의 암호 알고리즘 연산 클래스에서 임의의 타원곡선 연산 객체를 호출해서 사용하기 위함이다. 즉 알고리즘 클래스들은 EC2m 형의 참

조 변수만을 선언해 놓고서 필요에 따른 적당한 타원곡선 연산 클래스(EC163 & EC163_2)의 객체를 할당해주면 된다.

그림 5는 소스의 일부분으로 EC2m형 참조변수를 이용하여 EC163 과 EC163_2 클래스내에 존재하는 8개의 연산 메소드를 사용하기 위해서 EC2m interface 내에는 위 8개의 연산 메소드들에 대한 abstract method 형태로 prototype을 선언해줘야 한다. 이러한 자바의 다형성을 이용하여 구현한다면 각각의 타원곡선 연산 클래스에 따른 여러 개의 같은 형태의 암호 알고리즘 클래스들을 만들 필요 없이 하나의 암호 알고리즘 클래스의 구현만으로도 여러 타원곡선 클래스를 이용할 수 있다는 장점이 있다. 그리고 여기서 타원곡선 연산 클래스를 이러한 다형성 특성을 이용하여 하나의 타원곡선 연산 클래스로 구현하지 않고 이렇게 EC163과 EC163_2로 분리하여 구현한 이유는 서로 다른 타원곡선 계수를 사용하여 fbcmsmulPC()이 메소드를 구현해야 하기 때문이다. 또한 서로 다른 precomputation point들을 저장해야 하며 또한 타원곡선 계수에 따라서 연산의 구현을 간략화 할 수 있기 때문에 전체적인 연산의 performance를 위해서 타원곡선 별로 따로 클래스를 나누어서 각 타원곡선에 최적화한 연산을 구현할 수 있다.

```
//PBEKeySpec.java
//2007. 1. 24.

package javacxt.crypto;

import java.security.spec.KeySpec;


public class PBEKeySpec
    implements KeySpec
{
    private char[]  password;

    public PBEKeySpec(
        char[]  password)
    {
        this.password = (char[])password.clone();
    }

    public final char[] getPassword()
    {
        return password;
    }
}
```

(그림 5) PBEKeySpec.java 일부분

Base Station 프로그램을 실행하려면, 기본적으로 mote 장비가 있어야 하며, mote 장비를 USB Port에 연결하고, TinyOS 환경에서 다음과 같은 명령을 통해 mote가 연결되었음을 감지하여야 한다[그림5].

```
$ motelist

SerialNum   PortName          Description

--------- ---------- ------------------------------

M4AA67FM    COM4              tmote sky
```

(그림 6) mote 연결상태 확인

이와 같이 motelist 명령에 의해서 시스템에 연결된 mote의 정보를 확인하고, 해당 mote가 Base Station을 위한 Sync Node임을 확인한다.

또한 MOTECOM을 통해 mote가 연결된 시리얼 포트의 정보를 지정하고, 연결 상태가 확인된 mote의 통신 포트를 지정해주면 해당 시리얼 포트에 Base Station이 연결하게 된다.

그림 6은 실제 이벤트 정보로 Base Station 과 각 Node간에 암호화 채널을 형성을 위한 키 교환, 암호화 데이터 통신 등의 이벤트 정보를 실시간으로 보여주는 기능을 제공한다.

(그림 7) 이벤트 처리화면

## 5. 결론 및 향후 연구

이동 Ad-hoc 네트워크 상에서 무선으로 전송되는 패킷들에 대한 인증 및 암호화 등의 보안 기능 구현은 미흡한 상황이다. 본 논문에서는 표준을 준용한 WTLS 보안 프로토콜을 통해 ECC 168

비트 키 생성 및 키 교환이 정상적으로 처리되는지, 상호 키 교환에 의해 동일한 세션키가 만들어지는가를 중점적으로 테스트 수행하였다.

또한 본 논문은 이동 Ad-hoc 네트워크 상에서 키 교환, 키 관리, 개체 인증, 데이터 암호화 등의 시큐리티 서비스를 제공했으며, ECC기반 ECDSA·ECDHC 알고리즘을 통해 사전 키 분배 기법과 경량 키 분배 프로토콜 기술을 적용하여 보안 관리 서버 시스템을 설계 및 구현하였다.

추후 통신 및 수집된 데이터의 가공처리를 위한 효율적인 사용자 인터페이스가 필요하며, 데이터의 저장 기능을 위한 시스템의 성능과 안정성이 균형을 이루기 위한 연구가 이루어져야 한다.

## 참 고 문 헌


[1] M.S. Corson and J.P. Macker, "Mobile Ad hoc Net-working(MANET): Routing Protocol Performance Issues and Evaluation Considerations," IETF RFC 2501, Jan. 1999.

[2] C.E. Perkins, Ad Hoc Networking, Addison-Wesley, 2001.

[3] C.K. Toh, Ad Hoc Mobile Wireless Networks : Protocols and Systems, Prentice Hall PTR, 2002.

[4] Rivest, R. L. Shamir, A., Adleman, L. M.: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21(2): pp. 120-126, 1978

[5] Certicom research, The Elliptic Curve Crypto-system, Certicom, April, 1997.

[6] Alfred J, Menezes, Paul C. van Oorschot, Scott A, Vanstone, Handbook of Applied Cryptography, CRC press, 1997.

[7] Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm(ECDSA) ANSI X9.62-1998, January, 1999.

[8] IEEE P1363a: Standard Specifications for Public Key Cryptography : Additional Techniques Draft 9, 2001.

[9] WAP WTLS version 05-Nov-1999, Wireless Application Protocol Wireless Transport Layer Security Specification.

[10] Digital Signature Standard (DSS), FIPS publication 186-2, National Institute of Standards and Technology, January, 2000.

## ◐ 저 자 소 개 ◑


**양 종 원(Jong-Won Yang)**
2003년 : 공주대학교 전자계산학과(학사)
2005년 : 공주대학교 일반대학원 컴퓨터공학과 (공학석사)
2005년 : 공주대학교 일반대학원 바이오정보학과 박사과정
2006년~현재 : 한국전자통신연구원 위촉연구원
<관심분야> 시스템 보안, 생체인식, 암호 알고리즘 등
e-mail: nobody@kongju.ac.kr

**서 창 호(Chang-Ho Seo)**
1990년 : 고려대학교 수학과(학사)
1992년 : 고려대학교 일반대학원 수학과 (이학석사)
1996년 : 고려대학교 일반대학원 수학과 (이학박사)
1996년~1996년 : 국방과학연구소 선임연구원
1996년~2000년 : 한국전자통신연구원 선임연구원, 팀장
2000년~현재 : 공주대학교 응용수학과(정보보호전공) 부교수
2001년~현재 : 공주대학교 바이오정보학과 부교수
<관심분야> 암호 알고리즘, PKI, 무선 인터넷 보호 등
e-mail: chseo@kongju.ac.kr

**이 태 훈(Tae-Hoon Lee)**
1982년 한국항공대학교 전자공학과 졸업(공학사)
1984년 아주대학교 대학원 전자공학과 졸업(공학석사)
1999년 아주대학교 대학원 전자공학과 졸업(공학박사)
1984년~1993년 한국전자통신연구원
1989년~1990년 일본 NTT연구소 객원연구원
1993년~현재 광주대학교 정보통신학과 교수
<관심분야> : Network Security, 멀티미디어 통신 및 서비스
e-mail: thlee@gwangju.ac.kr