PCS의 호처리를 이용한 인증서 상태검증 모델 제안

A Proposal for Certificate Status Validation Using the Call Processing of PCS

이영교*, 이영숙**, 원동호*

성균관대학교 컴퓨터공학부*, 성균관대학교 정보통신대학원**

Young-Gyo Lee(ygee@dosan.skku.ac.kr)*, Young-Sook Lee(ysl472@yahoo.co.kr)**,
Dong-Ho Won(dhwon@dosan.skku.ac.kr)*

요약

이동통신 사용자들은 PKI를 기반으로 무선 인터넷을 통한 뱅킹, 증권거래, 전자 지불 등의 다양한 서비스를 이용하고 있다. 또한 이동통신 사용자간의 데이터 통신에 대한 필요성도 점차 증가하고 있다. 무선 PKI 환경에서 사용자들은 인증서를 이용하여 사용자 인증, 키 분배, 암·복호화 등을 수행할 수 있으며 그에 따라 이동통신 사용자간의 인증서상태 검증과정도 필요하게 되었다. 이미 개발되어 상용화되어 있는 이동통신용 교환기는 음성 통화를 위주로 설계되었으므로 이를 이용하여 데이터 통신을 하기 위해서는 음성호의 호처리 절차를 이용하여야 한다. 따라서 본 연구에서는 무선 PKI 환경을 이용한 이동통신 사용자간의 데이터 통신에 필요한 인증서상태 검증작업을 호처리 과정 내에서 효율적으로 처리할 수 있는 모델을 PCS(Personal Communication System)를 중심으로 제안하고자 한다.

■ 중심어 : | 인증서 | 인증서 상태 검증 | OCSP | PCS |

Abstract

With the rapid progress of research to offer a convenience of mobile communication, the mobile users can use not only the services of voice call but also the variety services of data communication using Internet. These include Internet Searching, Internet Shopping and Internet banking and Internet stock exchange and electronic payment and so on, based on PKI. Also, the need of data communication between the mobile users has been increased. As it is possible for mobile users to do user authentication, key distribution, encryption, decryption and so on, it is needed the certificate status validation between the mobile users. However due to the PCS(Personal Communication System) had been only designed and implemented for voice call between the mobile users, it is not easy to apply data communication between the mobile users on PKI. Therefore the study of for the data communication between the mobile users in PCS is a few. It is for the data transfer between the mobile users to communicate using call processing of PCS. So, we propose how to process the certificate status validation during call processing for data communication between the mobile users in the PCS.

■ keyword : | Certificate | Certificate Status Validation | OCSP | PCS(Personal Communication System) |

접수번호 : #041026-001
접수일자 : 2004년 10월 26일
심사완료일 : 2004년 11월 11일
교신저자 : 이영교, e-mail : yglee@dosan.skku.ac..kr

I. Introduction

The PCS(Personal Communication System) is a convenient mobile communication system to provide mobility for the mobile user. In the early times, the PCS had been designed to service voice call, SMS(Short Message Service) between mobile users. As the PCS is developed for wireless Internet, it can service the E-Commerce (Eletronic Commerce) using wireless Internet to the mobile user. In the most recent, the PCS is more developed to exchange a binary data between mobile users. Therefore the PCS is expected to service the E-Commerce between mobile users. Because the E-Commerce is almost processed on the PKI(Public Key Infrastructures) in nowadays, the E-Commerce between mobile users is processed on the wireless PKI. The certificate status validation of the other party is needed at the E-Commerce between mobile users on the wireless PKI. The computational performance and memory of a mobile station has smaller than terminal (PC). It is less efficient that the certificate status validation is processed in mobile station. The PCS use voice call processing for data exchange between mobile users.

In this paper, we propose that the certificate status validation is processed on PCX(Personal Communication eXchanger) during call processing for data exchanging between mobile users. This paper is consisted of five sections. In section 2, related work, we present a system component of PCS, the voice call processing and broadcast authentication processing in PCS. In section 3, we explain a new call processing with a certificate status validation and network configuration for it. In section 4, we analyze the characteristics and comparison of the proposed method. Finally, in section 5, we bring to a conclusion of this paper.

II. Related Works

1. The System Organization of PCS

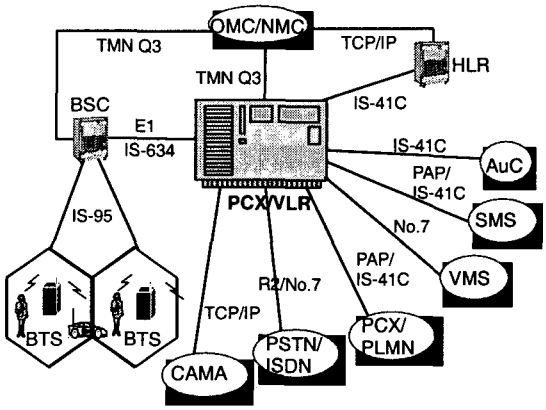

Fig. 1. System organization of PCS

Fig. 1 shows a total network organization of PCS. The PCX(Personal Communication eXchanger) is a center of the PCS network and its major role is a voice call exchanging between mobile users, a voice call connection between mobile user and user of PSTN(Public Switched Telephone Network), ISDN(Integrated Services Digital Network. In order to exchange voice call between mobile users, the PCX exchange user's information with the HLR(Home Location Register) / VLR(Visitor Location Register) that store it. In order to send/receive the signal, voice data with MS(Mobile Station), the PCX has a function interfacing with the BSC. The PCX has the control function of user's mobility, the control function of handoff between BSSs, the control function of handoff between PCXs. The HLR is a database management system that stores and manages a user's parameter and location information about all of the registered mobile station in PCS network. Also the access capability, the basic service, the extra service, etc are stored

in the HLR[1],[5],[6].

The HLR processes the routing function for the terminating call. The VLR is generally constructed in the PCX. Also, the VLR stores a user's information about the mobile user in itself zone. The VLR maintains user's information same with HLR. The BTS(Base station Tranceive System) has the function of wireless signal send/receive, wireless channel encoding/decoding, signal intensity/QoS(Quality of Service) measuring, base band signal processing, wireless resource management, self-maintain/repairing. The BSC (Base Station Controller) has the function of conjunction with BTS, handoff processing between cells, wireless resource management, equipment management, call control, etc.

The VMS(Voice Message System) provides a voice mailing service. The SMS(Short Message System) provides the short message service. The AuC(Authentication Center) is a equipment that processes the authentication about mobile user. The AuC stores the identification number about mobile user that prevent the illegal connection to PCX. The OMC(Operation and Management Center)/NMC is a center of network management that offers a centralized management and maintain/repair about all elements of network. The CAMA(Centralized Automatic Message Accounting) center is equipment that processes the collection/process of billing information transferred from the PCX[1],[5-7].

2. The voice call processing between mobile users in PCS

Fig. 2 shows normal mobile call processing between mobile users in PCS.

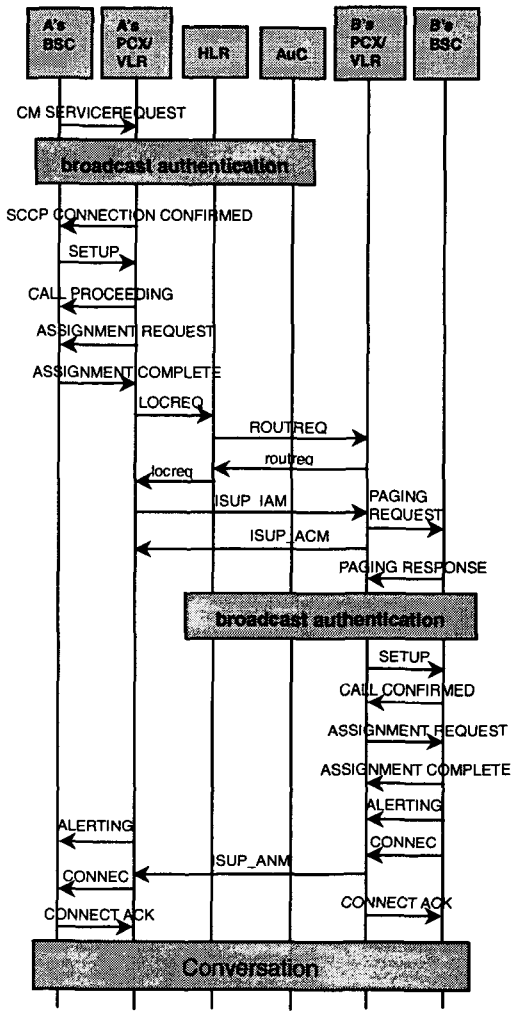

Fig. 2. Call processing of PCS

The mobile station A sends "CM SERVICE REQUEST(Connection Management SERVICE REQUEST)" to PCX A that mobile station A belongs to. The PCX A processes a broadcast authentication before call setup. If the result of broadcast authentication is success, the PCX A takes a mobile user A's information for call setup from VLR. If the mobile user A's information not exists in VLR, the PCX.

A take it from HLR. As the originating BSC

sends "SETUP" message to the PCX, the process for call setup begins. That message includes an information needed for call setup. The PCX sends "wireless channel allocation request message" to BSC. If the PCX receives "wireless channel allocation completion message" from BSC, it begins to analyze about terminating call number in "SETUP" message. In result of analysis about terminating call number, if the terminating number is mobile user, the PCX sends "LOCREQ(Location Request)" to HLR. The HLR sends "ROUTRQ(Routing Request)" message to a PCX that terminating user is location registered. The HLR transfer to originating PCX a TLDN value ofterminating user allocated by terminating PCX. The originating PCX begins to rout to terminating PCX. If the originating PCX receives "terminating status information" from terminating PCX, it sends "ALERTING" message to originating mobile station. At state of call transfer, if originating PCX receives "ISUP-ANM(ISDN User Part-ANswer Message)" from terminating PCX, it sends "CONNECT" message to originating mobile station. If the originating PCX receives "CONNECT ACK" message as response of this, it changes self's status to "conversation".

The authentication verifies a validity of mobile user that uses an IMSI (International Mobile Subscriber Identity). Also the authentication confirms a whether mobile station that use an ESN (Electronic Serial Number) is used or not used. In authentication process, parameters of RAND, AUTHR for confirmation of mobile station are transferred between network and mobile station. If the information of network is same as the information of mobile station, the authentication succeeds. The authentication classified into the broadcast authentication and the individual authentication. Fig. 3 shows the broadcast authentication that commonly is used in process of initial location registration, process of originating call and process of terminating call[1],[5-8].

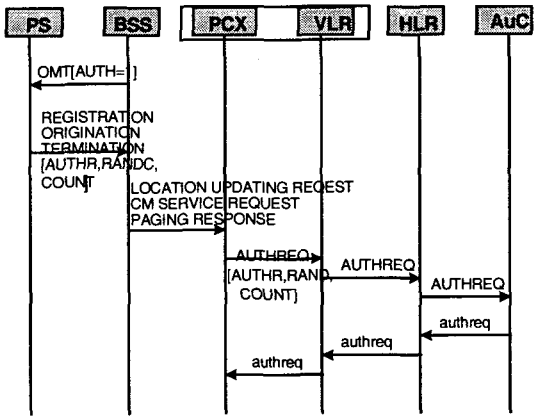

Fig. 3. Broadcast authentication of PCS

3. The certificate status validation for mobile communication

The mobile station continuously is designed to minimize and lighten in weight for portable. Therefore the mobile station has a smaller computational capability and memory than wire terminal. In wireless PKI(Public Key Infrastructure), mobile user not stores self's certificate in mobile station. The mobile user stores a URL(Uniform Resource List) that indicates a location of certificate in mobile station. At communication, the mobile user sends a URL to other party of communication. At communication between mobile users in wireless PKI, the mobile user that received a certificate of other party needs status validation of received certificate. The certificate status validation is a process that validates revocation, effectiveness of certificate. This process needs a CRL(Certificate

Revocation List) that the certificate authority publishes periodically. As mentioned above, the off-line method that downloads CRL and processes certificate status validation in mobile station is not suitable because mobile station has a small computational capability and memory. Thus on-line method that requests certificate status validation to a server is suitable for mobile station. There are OCSP(Online Certificate Status Protocol), SCVP (Simple Certificate Validation Protocol) in on-line method. The OCSP is at proposed state by RFC 2560 and the OCSP v.2 and SCVP are at Internet draft at now. Fig. 4 shows the certificate status validation using OCSP[2-4].

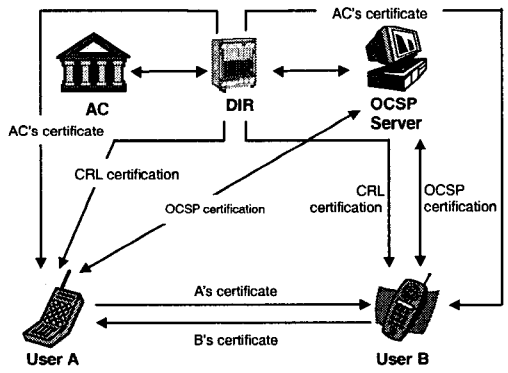

Fig. 4. Certificate status validation using OCSP

III. Proposed Scheme

In this section, we propose a new call processing that can provides certificate status validation of the other party in call processing.

1. Motivation

In data communication between mobile users in wireless PKI, the mobile user needs a certificate status validation of other party. The PCS is designed for voice call exchange between mobile users. As we have seen, the data communication between mobile users in wireless PKI has conditions the following.

① The mobile user sends self's certificate or certificate's URL to a other party \item The mobile user requests certificate status validation of other party to OCSP or SCVP server

② The data communication between mobile users must use voice call processing

③ The computational performance and memory of a mobile station has smaller than wire-line terminal(PC)

In particular, the PCS is designed for voice call exchange between mobile users. Also the IS-95 series protocol between MS and BTS supports the Circuit Switching method that allocates channel for voice call. Therefore for the data communication between mobile users, the data communication through voice channel is needed. It must use call processing for voice call In this paper, we propose a new call processing that can provides certificate status validation of the other party in call processing[7].

2. The proposed network configuration

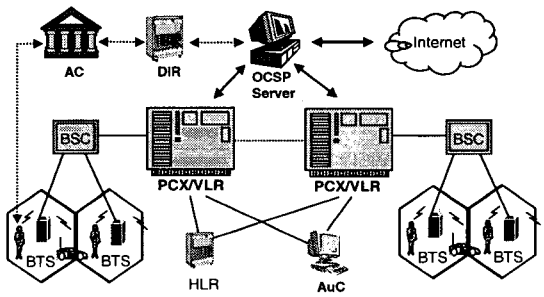

Fig. 5. Proposed network configuration

In this subsection, we propose a network configuration for new call processing. Fig. 5 shows a

network configuration for new call processing. In Fig.5, OCSP server is a computer that services a certificate status validation. If the OCSP server receives certificate status validation request including user's certificate URL from a PCX, it acquires user's certificate from Internet using URL at first. The OCSP server searches a serial number of requested certificate in CRL and sends a result of searching through the response to user' PCX. The mobile user receives certificate about public key, he stores certificate, private key.

The certification Authority stores the published certificate in directory. Also the certification Authority stores the published CRL periodically in directory. The OCSP server receives a CRL from directory and services certificate status validation to PCX.

3. The proposed call processing

In this subsection, we propose new call processing based on proposed network configuration. For satisfy given conditions, we propose call processing for data communication between mobile users in wireless PKI. Fig. 6 shows proposed call processing. The following is detailed procedure of proposed call processing.

① The mobile user A sends "CM SERVICE REQUEST" that involves URL of certificate to PCX through BSC.

CM SERVICE REQUEST

(+ user A's certificate URL)

② The PCX A requests certificate status validation(OCSPRequest) of mobile user A to OCSP server during broadcast authentication among PCX/VLR, HLR and AuC.

OCSPRequest(user A)

③ If OCSP server receives a OCSPRequest (user A) including A' URL, it acquires A's certificate from Internet using URL. OCSP server validates A's certificate status and sends its result to PCX A.

Certificate Status Validation of A

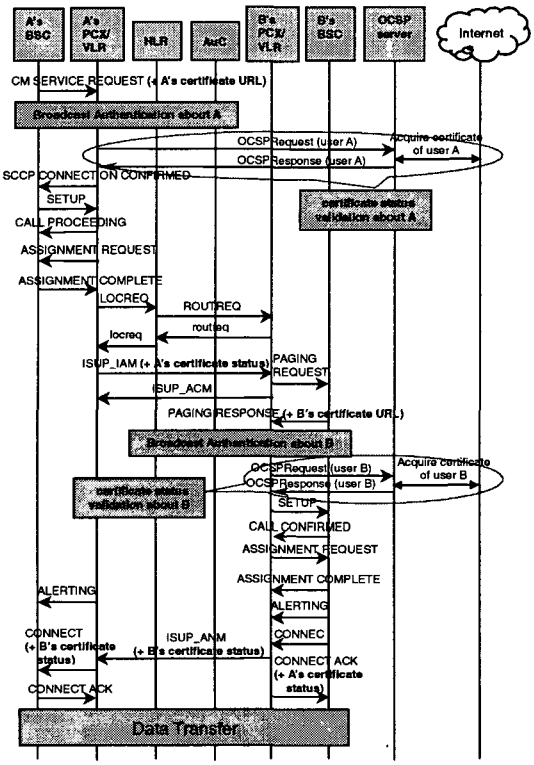

Fig. 6. Proposal of new call processing

④ If response(OCSPResponse) of certificate status validation about mobile user A is received, the PCX A stores its result.

OCSPResponse (user A)

⑤ If PCX B requests "PAGING REQUEST" to mobile user B, mobile user B responses "PAGING RESPONSE"that includes URL of certificate.

PAGING RESPONSE

(+ user B's certificate URL)

⑥ The PCX B requests certificate status

validation(OCSPRequest) of mobile user B to OCSP server during broadcast authentication between PCX/VLR, HLR and AuC.

OCSPRequest(user B)

⑦ If OCSP server receives a OCSPRequest(user B) including B' URL, it acquires B's certificate from Internet using URL. OCSP server validates A's certificate status and sends its result to PCX B.

Certificate Status Validation of B

⑧ If response of B's certificate status validation is received, the PCX B stores its result.

OCSPResponse(user B)

⑨ The PCX A sends a "ISUP-IAM" that includes result of A's certificate status validation to PCX B. The PCX B sends a "CONNECT ACK" that includes result of A's certificate status validation to mobile station B.

ISUP-IAM (+ A's certificate status)
CONNECT ACK (+ A's certificate status)

⑩ The PCX B sends a "ISUP-ANM" that includes result of B's certificate status validation to PCX A. The PCX A sends a "CONNECT" that includes result of B's certificate status validation to mobile station A.

ISUP-ANM (+ B's certificate status)
CONNECT (+ B's certificate status)

IV. Characteristics and comparison

The proposed method provides certificate status validation of users in PCS's call processing, circuit switching, for data communication. If certificate status validation is processed after call processing, each users stores a URL of other party in self MS at first. And each MS validates a certificate status of other party using new session. The connection for it inevitably is connected from MS to WAP(Wireless Application Protocol) server of Internet through BS, BSC, IWF(Inter Working Function). After MS acquires other party's certificate using its connection, MS request a certificate status validation to OCSP server. This method is inefficient because it needs a processing time for 2 connections.

methods	proposed	other
In where certificate status validation	in call processing	after call processing
processing method	parallel	serial
add of connection	x	2
OCSP server	add function	x
MS stores certificate other party	x	o
time save	o	x
modify call processing	small	x

Fig. 7. Comparison of the proposed method and other(other is a method that MS validate a certificate status of other party throuh BS, IWF using WAP)

1. Certificate status validation using voice call processing

The proposed call processing processes certificate status validation using voice call processing without much modification. The some request or responses are modified in its message format. Therefore the application of proposed call processing is easy and efficient for implementation.

2. Consideration of mobile station's resource

As we have seen, the mobile station has a small computational capability and memory. The proposed call processing not needs a download of the other party's certificate and CRL. Thus this

method prevents to use memory and calculate in mobile station.

3. Time save for certificate status validation

In proposed call processing, the certificate status validation and broadcast authentication are processed in parallel. Thus addition time for certificate status validation is not required. The certificate status validation is included in voice call processing. Therefore addition of a processing and a time for certificate status validation are not required.

4. Safety for result of certificate status validation

In proposed method, a result of certificate status validation is in PCX ar first and transfer to MS. Therefore safety in security is required. However PCX, BSC, and BS not need safety for it. If OCSP server responses to PCX after encrypts by self private key, MS decrypts a response using OCSP server's public key. Of course for it, each users must keep a public key of OCSP sever.

5. Model presentation of certificate status validation for mobile network

A proposed model can present a method of certificate status validation for mobile network. And it can help to development a efficient model for certificate status validation.

V. Conclusion

On this paper, we study the communication method including call processing, broadcast authentication in PCS and the certificate validation in OCSP. We propose a method of certificate status validation in call processing for data communication between mobile users based on PKI. Our method specially makes certificate status validation processing and broadcast authentication processing in parallel and considers MS that have a small memory and computational capability. Then it is able to avoid a time and a processing for certificate validation processing in addition. As mobile users have diverse service about Internet searching, payment system, E-commerce using wireless Internet, it will be needed the certificate status validation for data communication between the mobile users. The proposed method can give a convenience for mobile users and has more many advantages than possible other method that validates a certificate status through BS, IWF using WAP.

참 고 문 헌

[1] 성균관대학교 정보통신보호연구실, "무선 PKI 환경에서 보안 모듈의 활용 방안에 관한 연구", 한국전자통신연구원 최종연구보고서, 2002.

[2] 이승우, 곽진, 조석향, 원동호, 남길현, "실효율적인 인증서 검증 모델에 관한 연구", Information Technology Research Center 2002, 2002. 5.

[3] 곽진, 이승우, 조석향, 원동호, "온라인 인증서 상태 검증 프로토콜(OCSP)의 최근 영구 동향에 관한 연구", 한국정보보호학회지 제12권, 제2호, pp. 50-61, 2002.

[4] 서원호, 강철현, 박소현, 대우통신(주) 교환연구2실, "PCS 망에서 교환 및 이동성 관리 기술에 관한 연구", 제8회 통신정보합동학술대회 JCCI'98, 1998.

[5] 한국통신교환기술연구소, "개인통신교환기-기지국제어기간 접속규격", 1996.

[6] 한국통신교환기술연구소, "개인통신응용부 프로토콜 규격(안) Ver 2.0", 1996.

[7] C. Adams, P. Sylvestor, M. Zolotarev and R.

Zuccherato, "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols," IETF RFC 3029, 2001.

[8] R. Housley, W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC 2458, 1999.

[9] M. Myers, R. Ankney, A. Mappani, S. Galperin and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP," IETF RFC 2560, 1999.

[10] Qualcom, "CDMA Concepts and Terminology," 1996

[11] TIA/EIA/IS-41.C, "Cellular Radio Telecommunications Inter system Operations," 1995.

[12] TIA/EIA/IS-634.A, MSC-BSC Interface.

[13] Michel Cain etc, "Alternate Network Architectures for PCS," ICUPC, 1993.

저 자 소 개

이 영 교(Young-Gyo Lee) 정회원

- 1986년 : 한양대학교 전자공학과 졸업(학사)
- 1991년 : 한양대학교 전자공학과 졸업(석사)
- 2002년~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 박사과정(박사수료)
- 1993년~1998년 : 대우통신 종합연구소 선임연구원
- 1999년~2001년 : LG 전자/정보통신 중앙연구소 선임연구원
- 2002년~현재 : 인하공업대학 정보통신과 초빙전임강사

<관심분야> : 암호 프로토콜, 정보통신 보안, 네트워크 이론

이 영 숙(Young-Sook Lee) 준회원

- 1987년 : 성균관대학교 정보공학과 졸업(공학사)
- 2002년~현재 : 성균관대학교 정보통신대학원 정보보호학과(석사과정)
- 2002년~현재 : 두원공과대학 소프트웨어개발과 강사

<관심분야> : 정보통신 보안, 암호 알고리즘

원 동 호(Dong-Ho Won) 정회원

- 성균관대학교 전자공학과(학사, 석사, 박사)
- 한국전자통신연구소(ETRI) 전임연구원, 일본 동경공대 객원 연구원
- 성균관대학교 전산소장, 교학처장, 전기전자 및 컴퓨터공학부장, 연구처장
- 정보통신대학원장, 정보통신기술연구소장
- 국무총리실 국가정보화 추진자문위원회 자문위원
- 한국정보보호학회 이사, 회장, 부회장, 수석 부회장
- 현재 : 성균관대학교 정보통신공학부 교수, 정통부 지정 정보보호인증기술연구센터 센터장

<관심분야> : 암호학, 정보통신 보안, 암호알고리즘