http://dx.doi.org/10.14400/JDPM.2014.12.1.389

부인봉쇄 성질을 갖는 바이오메트릭 서명 위임 기법

윤성현*
백석대학교 정보통신학부*

The Biometric Signature Delegation Method with Undeniable Property

Sunghyun Yun*
Div. of Information & Communication Engineering, Baekseok University*

요 약 바이오메트릭 서명은 서명자의 바이로메트릭 키를 이용하여 서명하는 것으로 서명자는 서명에 앞서 본인임을 인증하는 과정이 필요하다. 바이오메트릭 인증은 매 서명 세션마다 이루어지기 때문에 전자상거래 쇼핑몰과 같이 대규모 서명이 요구되는 응용에는 적합하지 않다. 따라서 바이오메트릭 서명 기법의 실용화를 위해서는 신뢰할 수 있는 제 3자에게 서명 위임을 하여, 서명자의 업무량을 줄일 수 있는 기법이 필요하다. 본 연구에서는 대규모 서명에 적합한 바이오 서명 임대 기법을 제안한다. 제안한 서명 임대 기법은 바이오메트릭 키 생성, PKI 기반의 상호 인증, 서명 생성 및 검증 프로토콜로 구성된다.

주제어 : 바이오메트릭 서명, 디지털 서명 임대, PKI, 부인봉쇄 서명, 대규모 사용자 인증

Abstract In a biometric signature scheme, a user's biometric key is used to sign the document. It also requires the user be authenticated with biometric recognition method, prior to signing the document. Because the biometric recognition is launched every time the signature session started, it is not suitable for electronic commerce applications such as shopping malls where large number of documents to sign are required. Therefore, to commercialize biometric based signature schemes, the new proxy signature scheme is needed to ease the burden of the signer. In the proxy signature scheme, the signer can delegate signing activities to trustful third parties. In this study, the biometric based signature delegation method is proposed. The proposed scheme is suitable for applications where a lot of signing are required. It is consisted of biometric key generation, PKI based mutual authentication, signature generation and verification protocols.

Key Words : Biometric Signature, Proxy Signature, PKI, Undeniable Property, Large Scale Authentication

1. 서론

인터넷은 가상의 공간이기 때문에 사용자 인증이 비대면으로 이루어져 대리 인증이 가능하다. 로그인한 사용자가 실제 사용자인지 입증하려면 바이오메트릭 기반 기술의 접목이 필요하다. 바이오메트릭 인증은 사람마다 고유한 지문, 홍채 등의 데이터를 이용하여 본인임을 입증하는 기술로 사용이 편리하고 도난 및 분실의 위험이

Received 3 December 2013, Revised 3 January 2014
Accepted 20 january 2014
Corresponding Author: Myungju Chung(Busan National University)
Email: mjch@pusan.ac.kr

ISSN: 1738-1916

없다[1].

바이오메트릭 기반 기술의 실용화를 위해서는 바이오메트릭 데이터 입력에 필요한 스캐너의 보급과 사용자 프라이버시를 보장하는 기술이 선행되어야 한다. 현재 바이오메트릭 스캐너는 주로 공항, 연구소 등의 특정 분야에서 물리적 보안을 위한 신분 인증 용도로 활용되고 있다. 바이오메트릭 데이터는 사람마다 고유하고 그 개수가 제한되어 있어서 한 번 도용되면 다시 사용할 수 없는 프라이버시 문제를 야기한다[2].

스마트폰 사용자 인증은 터치를 이용한 패스워드 입력 또는 드래그 방식의 번호 연결 방법이 대표적이다. 단점은 입력시의 타이핑 오류, 패스워드 및 그림 패턴을 기억해야 하는 불편함 그리고 인증 정보를 남에게 빌려줄 수 있다는 것이다. 바이오메트릭 인증은 입력 오류, 기억에 대한 강박, 대리 인증 문제를 해결할 수 있다.

근래에 지문 스캐너가 내장된 스마트폰이 보급되면서 지문 인식 기반의 사용자 인증 인터페이스가 제공되고 있으며 향후 1-2년 이내에 대중화될 것으로 예측되고 있다. 스마트폰은 전화 기능과 컴퓨터 기능을 갖는 기기로 바이오메트릭 센서가 내장된 스마트폰의 보급은 바이오메트릭 기반 기술의 실용화를 위한 플랫폼 개발에 최적의 환경을 제공한다[3, 4].

바이오메트릭 기반 기술은 사용자가 매 세션 마다 참여하기 때문에 처리해야 할 데이터가 많아질수록 성능과 효율이 떨어지게 된다. 바이오메트릭 기반 기술은 컴퓨터가 아닌 사람의 속도에 비례하기 때문이다. 따라서 대규모 사용자와 데이터를 대상으로 하는 응용에는 적합하지 않다. 전자 투표에서의 투표권 인증, 쇼핑몰에서의 주문 및 결제 등이 대표적인 예로, 공통된 특징은 단순 반복되는 업무이고 바이오 서명을 적용하면 사용자 수가 많아질수록 처리 효율이 급감한다는 것이다. 따라서 대규모 응용에 적합하도록 인증 기능을 분산할 수 있는 새로운 서명 기법의 개발이 필요하다.

본 연구에서는 서명자가 자신이 신뢰하는 제 3자에게 서명 기능을 위임할 수 있는 서명 임대 기법을 제안한다. 제안한 기법은 바이오메트릭 키 생성, 서명 임대, 서명 생성 및 검증 프로토콜로 구성된다.

2 장에서 기존의 바이오메트릭 서명 및 대규모 인증 기술에 대해서 살펴본다. 3장에서 대규모 인증에 적합한 서명 임대 기법을 제안하고 4장에서 제안한 기법의 기능과 활용 방안에 대해서 기술한다. 5장에서 결론 및 향후 연구 과제를 제시한다.

2. 관련 연구 및 요구사항 분석

대규모 사용자를 대상으로 하는 바이오메트릭 인증이 왜 필요한지, 기존 바이오메트릭 기반 기술이 갖는 한계는 무엇인지, 대규모 인증을 위한 요구사항은 무엇인지 살펴본다.

2.1 대규모 사용자 인증

전자상거래 또는 전자정부와 같이 인터넷으로 대국민 서비스를 하는 응용은 대규모 사용자를 대상으로 하며 처리 결과의 법적 구속력이 확보되어야 한다. 대량의 데이터를 처리하기 때문에 서명 시간과 서명 크기가 시스템의 효율성을 결정하는 주요 지표가 된다.

PKI(Public Key Infrastructure)는 대규모 인증을 고려하여 개발된 대표적인 기술로 공개키와 키 소유자 간의 관계를 CA(Certificate Authority)가 입증해 주는 체계이다. Root CA는 CA 중의 최상위 기관으로 모든 사용자는 Root CA를 무조건 신뢰해야 한다. Root CA는 정부에서 지정하고 감독한다[2].

PKI는 대규모 사용자를 여러 도메인으로 나누어 그룹화 한다. Root CA의 권한을 하위 CA로 위임하여 각 도메인을 관리하도록 작업을 분산한다. 상위 CA와 하위 CA는 서명을 교환하여 법적 구속력을 확장해 나간다. 모든 사용자는 Root CA를 신뢰하기 때문에 Root CA로부터 확장된 모든 CA들 또한 사용자들이 신뢰하게 되는 인증 트리를 구성한다[2].

2.2 바이오메트릭 서명

바이오메트릭 키는 서명자 신체의 일부분인 바이오메트릭 데이터를 이용하여 생성된다[5]. 바이오메트릭 데이터는 서명자의 고유 정보이기 때문에 바이오메트릭 키는 그 자체로 법적 구속력을 갖는다. 일반 키는 키 소유자와의 종속성이 없기 때문에 제 3자가 피싱, 스미싱 공격으로 서명자를 가장하여 가짜키를 생성할 수 있다.

서명 생성은 키 생성과 독립적이기 때문에 일반 서명 생성 프로토콜과 비교하여 큰 차이점이 없다. 바이오메

트릭 키의 법적 구속력은 존재하지만 서명자가 다른 사용자에게 키를 임대할 수 있는 단점이 있다. 전자투표와 같이 투표권 인증에 서명자가 반드시 참여해야 하는 경우에는 대리 투표 및 매표의 위험이 있다[6]. 이 경우에는 바이오메트릭 인증이 접목된 서명 기법의 적용이 필수적이다.

〈Table 1〉 Biometric signature requirements

A. [Required] The signer's biometric key must be generated from his/her own biometric data.
B. [Optional] The biometric authentication should be done prior to signing.

표 1은 바이오메트릭 서명이 가져야 할 요구사항을 정리한 것이다. 요구사항 A는 서명키와 키 소유자의 바이오메트릭 데이터를 종속함으로써 키에 대한 법적 구속력을 확보한다. 요구사항 B는 바이오메트릭 인증과 서명이 동시에 필요한 선거, 심사, 회의 등과 같은 사회적 영역의 전자화에 필요하며, 실시간으로 서명자를 증명해야 하는 서명 기법에 적용된다.

2.3 대규모 인증을 위한 바이오메트릭 서명 요구사항

PKI는 법적 구속력이 요구되는 전자상거래를 비롯한 다양한 사회적 응용에 접목되고 있다. 하지만 인터넷과 같은 비대면 공간에서 PKI 인증서를 남에게 빌려 줄 수 있고 전자투표 또는 모바일 심사와 같은 응용에서는 인증서를 매매하는 것이 가능하다.

바이오메트릭 인증과 서명은 비대면 사용자의 신분 확인과 서명의 법적 구속력 확보를 위해서 사용되지만 매 세션마다 사용자가 직접 참여해야 하기 때문에 자동화된 인증 및 서명 솔루션 구현이 어렵다. 따라서 대규모 사용자를 대상으로 한 서비스에는 성능상의 문제로 적용이 쉽지 않다.

〈Table 2〉 Requirements of large scale user authentication and signature

A. Biometric key should have legal binding forces.
B. The job of generating biometric signature should be distributed.

표 2는 대규모 사용자 인증에 적합한 바이오메트릭 서명 요구사항을 보여준다. 바이오메트릭 키는 법적 구속력을 가져야 하고, 인증 및 서명 프로세스는 여러 서명자에게 분산하여 처리할 수 있어야 한다.

3. 바이오메트릭 기반 서명 위임 기법

제안한 바이오메트릭 서명 위임 기법은 인터넷에서 대규모 사용자를 대상으로 하는 인증 및 서명 서비스에 적용될 수 있다. 서명 작업을 분산하기 위하여 서명자 중심의 바이오메트릭 신뢰 체인을 생성한다. 검증 과정에서 신뢰 체인의 바이오메트릭 키를 확인함으로써 서명자와 위임자 간의 법적 구속력을 확보한다.

가정 1. 바이오메트릭 템플릿 BT는 도용될 경우에 취소하고 재등록할 수 있다[7].

바이오메트릭 템플릿은 사람의 고유 정보로 도용되면 다시 사용할 수 없다. 따라서 원본이 아닌 변형된 형태로 분배되어야 한다. 취소 가능한 템플릿은 이미 표준화된 기술이고 변형 함수를 사용하여 다양한 형태로 원본을 변환할 수 있다[5, 7]. 본 논문에서 사용되는 템플릿 BT는 가정 1과 같은 취소 가능한 성질을 갖는다.

가정 2. 가정 1의 바이오메트릭 템플릿 BT를 등록 및 관리하는 신뢰할 수 있는 센터가 존재한다.

PKI의 안전성은 CA를 전적으로 신뢰하는 것에 기반을 둔다. 마찬가지로, 바이오메트릭 템플릿 등록 및 관리를 위해서는 전적으로 신뢰할 수 있는 센터의 존재가 필수적이다. 본 논문에서 사용되는 센터는 가정 2와 같으며 모든 구성원들은 센터를 전적으로 신뢰한다.

정의 1. 암호학적으로 안전한 유한체 GF(p)

p는 큰 소수로 유한체 GF(p) 상에서 법 p에 대한 이산대수를 구하는 것이 계산상 불가능할 때 GF(P)를 암호학적으로 안전한 유한체라 정의한다[8].

〈Table 3〉 Key pairs of signer, delegate and center

User	Private key	Public key
CA	$SK_{CA} < p$	$PK_{CA} \equiv g^{SK_{CA}} \bmod p$
Center	$SK_R < p$	$PK_R \equiv g^{SK_R} \bmod p$
Signer	$SK_S < p$	$PK_S \equiv g^{SK_S} \bmod p$
Delegate	$SK_D < p$	$PK_D \equiv g^{SK_D} \bmod p$
· p : 큰 소수, g : 생성자, g < p		

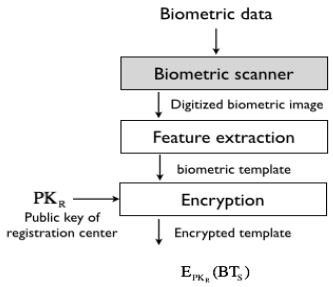
〈Table 4〉 Certificates of signer, delegate and center

User	Certificate
Center	$Cert_R = (PK_R \| ER_{SK_{CA}}(PK_R))$
Signer	$Cert_S = (PK_S \| ER_{SK_{CA}}(PK_S))$
Delegate	$Cert_D = (PK_D \| ER_{SK_{CA}}(PK_D))$

표 3은 CA, 센터, 서명자, 위임자의 공개키와 개인키 정보를 보여준다. 이 값들은 정의 1의 유한체 GF(p) 상에서 생성되며, 사용자들이 임의로 생성한 개인키는 서로 다른 값이어야 한다. CA는 사용자의 공개키를 인증하기 전에 같은 공개키가 등록되어 있는지 확인하고, 만약 같은 키가 존재하면 해당 사용자의 인증서 발급을 취소하고 키 생성을 다시 하도록 공지한다. 표 4는 CA가 발행한 인증서로 사용자 공개키에 CA가 서명을 하여 생성한다. 기타 본 논문에서 사용된 기호는 다음과 같다.

· ER: 공개키 암호 방식의 암호화 함수
· DR: 공개키 암호 방식의 복호화 함수
· E: 대칭키 암호 방식의 암호화 함수
· D: 대칭키 암호 방식의 복호화 함수

3.1 바이오메트릭 템플릿 등록



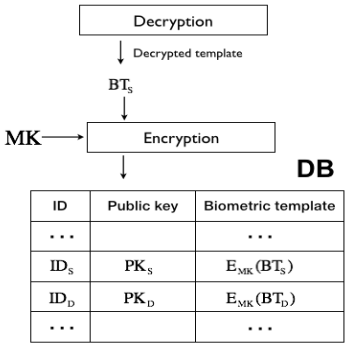
[Fig. 1] Biometric template generation

단계 1: 서명자는 스캐너로 자신의 바이오메트릭 데이터를 입력한다. 스캔된 이미지의 노이즈는 이미지 처리 프로그램을 이용하여 제거한다.

단계 2: 바이오메트릭 템플릿은 이미지 윤곽선에 있는 특징점들의 좌표와 방향 값으로 구성된다.

단계 3: 바이오메트릭 템플릿을 센터의 공개키로 다음과 같이 암호화한다.

$E_{PK_R}(BT_S)$, BT_S: 서명자의 바이오메트릭 템플릿



[Fig. 2] Bitmetric template registration

그림 2는 센터가 서명자의 바이오메트릭 템플릿을 등록하는 과정을 보여준다.

단계 1: 센터는 서명자가 보낸 암호화된 바이오메트릭 템플릿을 자신의 개인키로 다음과 같이 복원한다.

$$BT_S = D_{SK_R}(E_{PK_R}(BT_S))$$

단계 2: 센터는 CA의 공개키로 서명자 인증서에 있는 서명을 검증하여 서명자 ID를 인증한다.

단계 3: 센터는 서명자의 바이오메트릭 템플릿을 다음과 같이 마스터키로 암호화한다.

$$E_{MK}(BT_S)$$

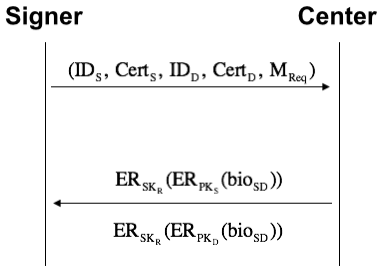
단계 4: 센터는 서명자 ID, 인증서, 암호화된 템플릿을 데이터베이스에 저장한다.

$$(ID_S,\ Cert_S,\ E_{MK}(BT_S))$$

3.2 서명 위임 키 생성

단계 1: 서명자는 서명자 ID, 서명자 인증서, 위임자 ID, 위임자 인증서, 서명 위임 요청 메시지를 센터로 전송한다.

$$(ID_S,\ ID_D,\ Cert_S,\ Cert_D, M_{Req})$$



[Fig. 3] Delegation key request

단계 2: 센터는 CA의 공개키를 이용하여 서명자와 위임자의 인증서를 검증하여 신분을 확인한다.

$$PK_S = DR_{PK_{CA}}(ER_{SK_{CA}}(PK_S))$$

$$PK_D = DR_{PK_{CA}}(ER_{SK_{CA}}(PK_D))$$

단계 3: 센터는 마스터 키를 이용하여 데이터베이스에 저장된 서명자와 위임자의 바이오메트릭 템플릿을 추출한다.

$$BT_S = D_{MK}(E_{MK}(BT_S))$$

$$BT_D = D_{MK}(E_{MK}(BT_D))$$

단계 4: 센터는 서명자와 위임자의 바이오메트릭 템플릿과 임의의 난수 R을 결합하고 이를 해쉬하여 바이오메트릭 시드(biometric seed)를 만든다. 난수 R은 재전송 공격을 방지하고 서명 임대 세션의 고유성을 확보하기 위하여 사용된다.

$$bio_{SD} = H(BT_S \| BT_D \| R)$$

단계 5: 센터는 바이오메트릭 시드를 서명자 및 위임자의 공개키로 각각 암호화하고 자신의 개인키로 서명한다. 센터는 서명자에게 바이오메트릭 시드를 전송한다.

$$ER_{SK_R}(ER_{PK_S}(bio_{SD})),$$
$$ER_{SK_R}(ER_{PK_D}(bio_{SD}))$$

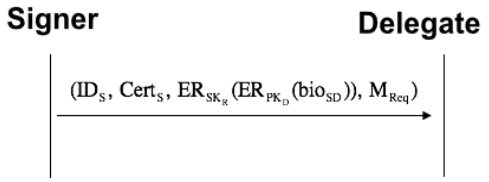
단계 6: 서명자는 센터의 서명을 검증하고 자신의 개인키로 암호화된 바이오메트릭 시드를 복원한다.

$$DR_{PK_R}(ER_{SK_R}(ER_{PK_S}(bio_{SD})))$$

$$bio_{SD} = DR_{SK_S}(ER_{PK_S}(bio_{SD}))$$

단계 7: 서명자는 서명자 ID, 서명자 인증서, 센터가 서명한 바이오메트릭 시드, 서명 위임 요청 메시지를 위임자에게 전송한다.

$$(ID_S, Cert_S, ER_{SK_R}(ER_{PK_D}(bio_{SD})), M_{Req})$$



[Fig. 4] Delegation key sharing

단계 8: 위임자는 센터의 서명을 검증하고 자신의 개인키로 바이오메트릭 시드를 복원한다.

$$DR_{PK_R}(ER_{SK_R}(ER_{PK_D}(bio_{SD})))$$

$$bio_{SD} = DR_{SK_D}(ER_{PK_D}(bio_{SD}))$$

단계 9: (서명자, 위임자) 상대방의 인증서를 검증하고 공개키를 추출한다.

$$PK_S = DR_{PK_{CA}}(ER_{SK_{CA}}(PK_S))$$

$$PK_D = DR_{PK_{CA}}(ER_{SK_{CA}}(PK_D))$$

단계 10: (서명자, 위임자) 디피-헬먼 키 교환 기법을 이용하여 공통 시드를 구한다.

$$seed_{SD} \equiv PK_D^{SK_S} \equiv g^{SK_D \cdot SK_S} \bmod p$$

$$seed_{SD} \equiv PK_S^{SK_D} \equiv g^{SK_S \cdot SK_D} \bmod p$$

단계 11: (서명자, 위임자) 다음과 같이 위임키를 생성한다.

$$SK_{SD} \equiv seed_{SD} \cdot bio_{SD} \bmod p$$

$$PK_{SD} \equiv g^{SK_{SD}} \bmod p$$

서명 생성 및 검증 프로토콜은 일반 서명 기법과 동일하다. 위임자는 위임 개인키를 이용하여 서명하고 검증자는 위임 공개키를 이용하여 서명을 검증한다. 위임 개인키에 포함된 공통 시드는 서명자와 위임자만이 만들 수 있고, 바이오메트릭 시드는 PKI 인증서와 사용자 바이오메트릭 데이터가 결합되어 법적 구속력이 확보된다.

4. 기능 비교 및 응용

제안한 기법과 다른 서명 기법들의 기능상의 차이점을 비교하고 응용 및 활용 방안에 대해서 기술한다.

4.1 기능 비교

〈Table 5〉 Comparison of main features of the proposed scheme with other signature schemes

	Ordinary Signature Scheme[1]	Biometric Signature Scheme[2]	Proposed Scheme
Can provide undeniable property?	O	O	O
Is it practical to sign to quite a lot of documents?	O	x	O
Is the signer has to participate to generate key pairs?	x	O	O
Can the signer delegate signing activities to other users?	O	O	O
Is there a legal relationship between the signer and delegates?	x	x	O

[1]: [8], [2]: [9, 10]

표 5는 일반 서명 기법, 바이오메트릭 서명 기법, 제안한 서명 위임 기법의 차이점을 보여준다. 부인봉쇄 기능은 서명 사실에 대해서 부인할 수 없는 법적 구속력을 갖도록 하는 것이다. 제안한 바이오메트릭 위임키는 서명자와 위임자의 바이오메트릭 데이터로부터 생성되며 PKI 인증서와 연동되기 때문에 부인봉쇄 기능을 만족한다.

더불어 제안한 기법에서는 PKI의 신뢰 구조와 유사한 바이오메트릭 기반의 신뢰 체인을 생성함으로써 서명자가 직접 법적 구속력을 갖는 위임자 그룹을 만들 수 있다. 서명 작업 분산이 가능하고 대규모 사용자를 대상으로 하는 인증 및 서명에 적용될 수 있다.

4.2 응용

제안한 기법은 대국민 서비스를 전자화하는 전자정부 실현을 위한 요소 기술로 활용될 수 있다. 전자정부 서비스는 대규모 사용자를 대상으로 하며, 공항이나 항만에서의 출입국 관리, 전자선거 등과 같은 서비스는 실 사용자 인증이 반드시 필요한 분야이다. 전자선거의 경우 매표를 방지하기 위해서 바이오메트릭 기반의 유권자 인증이 필수적이고, 유권자의 투표권은 법적 구속력을 확보하기 위해서 선거관리 센터의 서명을 받아야 한다. 일반 서명 기법을 적용하게 되면 피싱, 스미싱과 같은 공격으로 가짜 센터가 유권자 투표권에 서명하여 기권표를 만들 수 있다. 불특정 다수의 사용자들을 기존의 바이오 기술로 인증하는 것은 성능 상의 한계가 있다. 업무량을 분산하고 안전성 및 법적 구속력을 유지하려면 서명 위임 기법의 응용이 필수적이다.

5. 결론

본 연구에서는 바이오메트릭 기반의 서명 위임 기법을 제안하였다. 제안한 서명 위임 기법은 인증서 기반의 바이오메트릭 키 생성, 서명 위임, 서명 생성 및 검증 프로토콜로 구성된다. 서명 위임 기법과 기존 서명 기법과의 기능적 차이를 분석하였고 기대 효과 및 응용에 대해서 논하였다. 제안한 기법은 PKI와 같은 법적, 제도적 지원이 되는 환경에서 서명 기능 분산을 통하여 응용 시스템의 효율성과 실용화에 기여할 수 있다. 더불어 P2P와 같이 동적인 클라이언트를 대상으로 하는 인증 모델에서 인증 서버의 부하를 분산할 수 있도록 제안한 방법을 확장하는 것에 대한 연구가 추가적으로 필요하다.

REFERENCES

[1] Haizhou Li, Kar-Ann Toh, Liyuan Li, Advanced Topics in Biometrics, World Scientific, 2011.

[2] J. Tepandi, I. Tšahhirov and S. Vassiljev, “Wireless PKI Security and Mobile Voting,” IEEE Computer, vol. 43, no. 6, pp. 54-60, June, 2010.

[3] C. Vivaracho-Pascual, J. Pascual-Gaspar, "On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, pp. 1-10, 2011.

[4] Want, "iPhone: Smarter Than the Average Phone," IEEE Pervasive Computing, Vol. 9, No. 3, pp. 6-9, 2010.

[5] N. Ratha, J. Connell, R. Bolle, "Enhancing security and privacy in biometric-based authentication

systems," IBM Systems Journal, Vol. 40, No. 3, pp. 614 - 634, 2001.
[6] D. Evans and N. Paul, "Election Security: Perception and reality," IEEE Security & Privacy, vol. 2, no. 1, pp. 24-31, Jan. 2004.
[7] ITU-T X.1088, A Framework for biometric digital key generation, ITU-T, 2008.
[8] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, IT-31(4), pp. 469-472, 1985.
[9] P. Janbandhu and M. Siyal, "Novel biometric digital signatures for Internet-based applications," Information Management & Computer Security, Vol. 9, No. 5, pp. 205-212, 2001.
[10] P. Orvos, "Towards biometric digital signatures," Networkshop, Eszterhazy College, Eger, pp. 26-28, 2002.

윤 성 현(Yun Sunghyun)

- 1992년 2월 : 고려대학교 컴퓨터학과(이학사)
- 1994년 2월 : 고려대학교 컴퓨터학과(이학석사)
- 1997년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 1998년 3월 ~ 2002년 2월 : LG전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : 모바일 보안, 바이오메트릭 인증, DRM, 전자투표
- E-Mail : shcrpt@gmail.com