http://dx.doi.org/10.14400/JDC.2014.12.2.243

이동성과 프라이버시를 제공하는 모바일 회의 인증 기법

윤성현*
백석대학교 정보통신학부*

The Mobile Meeting Authentication Scheme Providing Mobility and Privacy

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

요 약 스마트폰의 보급으로 여러 사용자가 그룹을 만들어 함께 대화하는 메신저 서비스에 대한 관심이 급증하고 있다. 모바일 회의는 회의 참석자가 스마트폰 메신저를 이용하여 장소에 구애받지 않고 회의에 참가하여 토론하는 것을 의미한다. 모바일 회의의 실용화를 위해서는 회의 참석자의 이동성과 프라이버시가 보장되어야 한다. 이동성은 장소에 구애받지 않는 것으로 회의 참석자 대신 다른 사람이 회의에 참석할 수 없어야 한다. 프라이버시는 회의 참석자들이 회의 결과에 동의하고 그 내용에 대해서 부인할 수 없는 것을 의미한다. 본 논문에서는 이동성과 프라이버시를 제공하는 모바일 회의 인증 기법을 제안한다. 제안한 기법은 회의 그룹 생성, 그룹 공통키 생성, 그룹 서명 생성 및 검증 프로토콜로 구성된다. 도전-응답 방식의 그룹 서명 검증은 회의 참석자가 모두 참여해야만 검증이 가능하다. 따라서 제안한 방법은 이해 관계에 있는 참석자들의 공모 공격에 대해서 안전하다.

주제어 : 모바일 회의, 이동성, 프라이버시, 그룹 서명, 바이오메트릭 키

Abstract The demand for messenger service goes on growing rapidly with widespread use of smartphones. Generally, the smartphone messenger provides group communication functions in which users can make the group and communicate with each other. In the mobile meeting, the attendees can participate in the meeting with use of smartphone messengers wherever they are. To make the mobile meeting put to practical use, the mobility and privacy should be ensured to attendees. To satisfy the mobility requirement, the user which is not belong to the group members should not be able to participate in the meeting. To ensure the privacy requirement, the attendees should have not to repudiate the meeting results. In this study, the mobile meeting authentication scheme is proposed which provides mobility and privacy. The proposed scheme consists of meeting group creation, group key generation, group signature and verification protocols. All attendees should have to participate in the signature verification because it is based on the challenge-response type protocol. Thus, it's not possible to collude with malicious attendees to change the meeting results.

Key Words : Mobile Meeting, Mobility, Privacy, Group Signature, Biometric Key

Received 10 January 2014, Revised 10 February 2014
Accepted 20 February 2014
Corresponding Author: Sunghyun Yun(Baekseok University)
Email: shcrpt@gmail.com

ISSN: 1738-1916

1. 서론

SNS(Social Network Service)는 온라인으로 사회적 관계를 형성해 주는 서비스로 특정한 주제나 목적을 가진 사람들 간의 모임을 가능하게 한다. 특히 스마트폰과 Wi-Fi의 보급으로 카카오톡과 같이 그룹 대화가 가능한 메신저 서비스에 대한 수요가 급증하고 있다[1]. 메신저의 그룹 대화 기능은 여러 사람이 모여서 회사의 안건을 토의하는 업무 회의의 효율을 높일 수 있다.

회의는 정해진 시간과 정해진 장소에 회의 구성원들이 모여서 안건을 토의하는 것이다. 하지만 중요한 안건을 심의해야 하는 회의에서 회의 참석자가 지리적으로 먼 지역에 있을 경우에는 참석하기 어려운 단점이 있다. 온라인으로 화상 회의를 하려면 화상 통신 장비를 갖춘 장소가 있어야 하고, 특히 안건 심의 및 의결 과정에서 비밀 투표가 불가능하여 많은 제약이 따른다. 지식 기반 사회에서 신속한 의사 결정과 실행은 사업의 성공을 위해서 매우 중요한 요소이다.

스마트폰과 같은 모바일 기기를 이용한 메신저 서비스는 새로운 회의 문화를 위한 적합한 대안이 되고 있다. 메신저 기반의 회의는 장소에 구애받지 않기 때문에 회의 시간 및 회의 참석자의 스케줄 조정이 용이하다. 더불어 긴급한 사안을 심의해야 할 경우에 신속히 대처할 수 있다.

스마트폰 메신저는 대화 기능과 인증 기능으로 구분된다[1]. 대화 기능은 네트워크를 통하여 메시지를 주고 받는 것으로 무선 네트워크의 특성 상 스니핑 공격의 위험이 높다. 대화 내용을 인증할 수 있는 정보보호 기법의 적용이 필수적이다.

카카오톡과 같은 스마트폰 메신저에 대한 인증은 SMS로 전송된 인증코드를 이용한다[1]. 단점은 인증코드와 기기가 서로 독립적이기 때문에 본 기기가 아닌 다른 기기의 메신저로 등록이 가능하다는 것이다.

따라서 스마트폰과 메신저를 함께 인증하려면 기기 자체의 고유정보를 이용해야 한다. 스마트폰 USIM은 사용자 개인 정보와 기기 고유 정보가 내장되어 있어서 인증코드 방식의 단점을 해결할 수 있다[2].

스마트폰 메신저를 이용한 회의에서 회의 참석자는 온라인 상에 있기 때문에 로그인한 참석자가 실제 본인이 맞는지 확인할 수 없다. 비대면 공간에서는 자신의 정보를 남에게 빌려주어 대리 인증하는 것이 가능하다. 중요한 업무 회의에서 제 3자에게 회의 내용 및 결과가 노출될 수 있고, 제 3자가 회의에 개입하여 회의 내용과 결과를 본인의 의도대로 만들어 나갈 수 있다. 따라서 제 3자에 의한 대리 인증의 위험을 최소화하기 위해서는 바이오메트릭 기반의 인증이 필수적이다[3].

최근의 스마트폰은 지문, 얼굴모양, 음성 등의 사용자 고유 데이터를 스캔할 수 있는 센서가 내장되어 출시되고 있다[4, 5]. 스마트폰의 광범위한 보급으로 바이오메트릭 인증 기술의 대중화가 가능하며, 이를 이용하여 저렴한 비용으로 모바일 회의 솔루션을 구축할 수 있다.

본 논문에서는 이동성과 프라이버시를 보장하는 모바일 회의 인증 기법을 제안한다. 제안한 기법은 USIM과 바이오메트릭 데이터를 접목한 그룹 공통키 생성, 그룹 서명 생성 및 검증 프로토콜로 구성된다. 그룹 구성원이 반드시 참여해야 하는 소규모의 모바일 회의 또는 모바일 심사 등의 응용에 적합하다.

2 장에서는 기존의 모바일 메신저 인증과 바이오메트릭 기반 그룹 서명 기법에 대해서 살펴본다. 3 장에서는 모바일 회의 인증 기법을 제안하고 4 장에서 이동성과 프라이버시 요구사항을 분석한다. 5 장에서 결론 및 향후 연구과제를 제시한다.

2. 연구 배경

인증 번호를 이용한 모바일 기기 인증의 위험성과 바이오메트릭 기반의 그룹 인증 기법에 대해서 살펴본다.

2.1 모바일 메신저 인증

메신저 사용자는 본인의 스마트폰 번호를 입력하여 메신저 서버로 전송한다. 서버는 인증코드를 생성하고 SMS로 사용자 스마트폰에 이 코드를 전송한다. 사용자는 수신한 인증코드를 입력하고 이를 다시 서버로 전송한다. 사용자가 보낸 인증코드가 서버가 보낸 코드와 일치하면 기기를 서버에 등록하고 인증통보 SMS 메시지를 사용자 스마트폰으로 전송한다.

인증코드 기반의 모바일 기기 인증은 인증코드와 모바일 기기가 독립적인 관계에 있기 때문에 대리 인증이 가능하다. 해커는 본인의 스마트폰에 설치된 메신저 등록 화면에서 도용하려는 전화번호를 입력하고 이를 메신저 서버로

전송한다. 서버는 인증코드를 생성하여 도용된 스마트폰으로 인증코드를 전송한다. 해커는 서버가 보낸 인증코드를 도청하여 본인의 스마트폰에 있는 메신저에 입력하고 이를 다시 서버로 전송한다. 서버는 해커가 보낸 인증코드가 맞으면 올바른 사용자 및 기기로 등록하고 인증통보 메시지를 보낸다[6].

따라서 인증코드를 이용한 가장 공격을 예방하려면 스마트폰 기기 식별이 가능한 USIM 데이터 기반의 인증이 필수적이다. 스마트폰 USIM은 등록 센터를 방문하여 오프라인으로 신분 인증을 한 후에 등록이 가능하다. USIM 카드 없이는 스마트폰을 사용할 수 없도록 법제화 되어 있기 때문에 개인의 신분을 표현하는 수단으로도 활용이 가능하다[7].

2.2 바이오메트릭 기반 그룹 인증 프로토콜

모바일 회의는 온라인으로 이루어지기 때문에 가상의 참석자가 정말 본인이 맞는지에 대한 인증이 중요하다. 오프라인 회의는 본인의 참석 여부를 쉽게 인증할 수 있지만 온라인 회의는 로그인한 참석자가 본인인지 대리인인지 구분할 수 없다.

바이오메트릭 데이터는 사용자 고유 정보로 그 자체 만으로 신분 인증이 가능하다. 온라인 인증을 위해서는 바이오메트릭 스캐너를 이용하여 사용자의 지문, 얼굴 모양, 음성과 같은 바이오메트릭 데이터를 디지털 데이터로 변환해야 한다. 최근의 스마트폰은 카메라, 지문인식 센서 등이 내장되어 출시되고 있으며 이를 활용할 수 있는 다양한 API도 함께 제공되고 있다. 바이오메트릭 인증은 그 동안 물리적 보안이 필요한 영역에 국한되어 사용되어 왔지만, 스마트폰 기술의 발전으로 대중화가 가능한 시점에 있다.

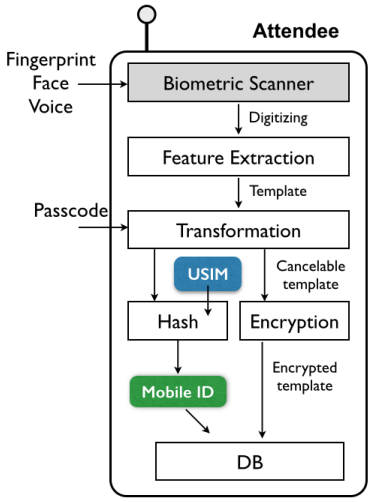
그룹 인증은 회의에 참여한 그룹 구성원들이 회의 결과에 대해서 부인할 수 없도록 법적 증거를 만들어내는 것이다. 디지털 다중서명 기법을 이용하여 여러 사람의 서명을 통합하는 것이 일반적인 방법이며, 이 기법은 구성원들의 공통키 생성, 다중서명 생성, 다중서명 검증 단계로 구성된다[8].

3. 모바일 회의 인증 기법

스마트폰 USIM과 바이오메트릭 데이터를 접목한 회의 그룹 인증 프로토콜을 단계 별로 설명한다.

요구사항 1. 모바일 회의는 이동성과 프라이버시 보장을 위하여 다음과 같은 요구사항을 만족해야 한다.
가. 회의는 여러 사람이 참여하여 안건을 심의하는 것으로 구성원들이 회의 그룹에 속함을 증명할 수 있어야 한다.
나. 회의 내용에 대해서 구성원들이 그 사실을 부인할 수 없어야 한다.
다. 제 3자가 구성원으로 가장하여 회의에 참석할 수 없어야 한다.

3.1 회의 그룹 ID 생성



[Fig. 1] Meeting ID Generation

그림 1은 회의 참석자의 모바일 ID 생성 단계를 보여준다. 사용자 인증을 위해서 지문, 얼굴모양 또는 음성 데이터를 사용하고 기기 인증을 위해서는 스마트폰 USIM을 이용한다. 더불어 패스코드를 추가로 입력하여 바이오메트릭 데이터를 변형한다. 바이오메트릭 데이터는 신체의 일부분으로 도용되면 재사용할 수 없다. 따라서 원본을 저장하면 안되고 취소 가능한 형태로 변환하여야 한다[9].

정의 1. GF(p)는 암호학적으로 안전한 유한체이고 g는 GF(p) 상에서 정의된 생성자로 위수 p-1을 갖는다[10]. p는 2^{512}(512 비트) 보다 큰 값이다.

회의 참석자는 다음과 같이 모바일 ID를 생성하고 회의 서버에 등록한다. M_A는 모바일 ID, H는 암호학적으로 안전한 해쉬 함수인 MD5(Message Digest 5) 또는 SHA-1(Secure Hash Algorithm-1) 함수를 사용한다. $USIM_A$는 참석자 스마트폰의 USIM, BIO_A는 패스코드로 변형된 취소 가능한 바이오메트릭 템플릿이다.

$$M_A = H(USIM_A, BIO_A) \in Z_{p-1}$$

가정 1. 모바일 회의에 참여하는 참석자 수는 n 명이고 신뢰할 수 있는 회의 서버가 존재한다. 회의 서버는 바이오메트릭 템플릿, 모바일 ID, 회의 내용, 그룹 서명을 등록 및 관리하는 데이터베이스와 바이오메트릭 인증 기능으로 구성된다. 회의 서버, 위원장 및 참석자의 인증 정보는 다음과 같다. 회의 참석자의 개인키는 모바일 ID와 사용자 패스워드를 해쉬하여 생성한다.

A_i : 회의 그룹 리스트의 i 번째 (i=[2..n])

A_1 : 위원장 (회의 그룹 리스트의 첫 번째)

$list_A = [A_1||A_2||...||A_n]$: 회의 그룹 리스트

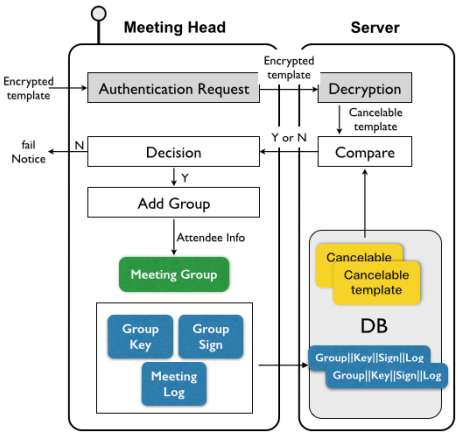
User	Private key	Public key	Biometric template
Server	$sk_S < p$	$pk_S \equiv g^{sk_S} \bmod p$	$E_{pk_S}(BIO_1)$ $E_{pk_S}(BIO_i)$
A_1	$sk_1 < p$	$pk_1 \equiv g^{sk_1} \bmod p$	$E_{pk_1}(BIO_1)$
A_i	$sk_i < p$	$pk_i \equiv g^{sk_i} \bmod p$	$E_{pk_i}(BIO_i)$

3.2 회의 참석자 인증

그림 2는 회의 참석자 인증 프로토콜을 보여준다. 회의 참석자 A_i는 서버의 공개키로 바이오메트릭 템플릿을 암호화하고 위원장 A_1에게 이를 전송한다. A_1은 서버로 A_i에 대한 인증을 요청하고 A_i가 맞으면 회의 그룹 리스트를 갱신한다.

단계 1: A_i는 스마트폰에 바이오메트릭 데이터와 패스코드를 입력하여 취소 가능한 템플릿을 만든다. A_i는 서버의 공개키로 템플릿을 암호화하여 $E_{pk_S}(BIO_i)$를 생성한다. A_i는 자신의 모바일 ID와 $E_{pk_S}(BIO_i)$를 A_1에게 전송한다.

단계 2: A_1은 $E_{pk_S}(BIO_i)$, A_i의 모바일 ID, 인증요청 메시지를 회의 서버로 전송한다.



[Fig .2] Attendee authentication

단계 3: 회의 서버는 자신의 개인키로 $E_{pk_S}(BIO_i)$를 복원하고, 데이터베이스에 저장된 과거 세션의 템플릿들과 비교하여 이중 사용 여부를 검증한다. 검증에 성공하면 데이터베이스에 등록된 A_i의 템플릿과 비교하여 두 값의 유사한 정도를 A_1에게 Y/N으로 알린다. Y는 A_i 임에 틀림이 없다는 것이고, N은 A_i가 아님을 표시한다. 회의 서버는 A_i의 템플릿을 현재 세션 레코드에 저장한다.

단계 4: A_1은 응답이 N일 경우에 A_i에게 인증 실패 메시지를 보내고 Y일 경우에는 다음과 같이 회의 그룹 리스트에 추가한다.

$list_A = [A_1||A_2||...||A_i]$

3.3 그룹 키 생성 및 회의 인증

A_1은 회의가 종료되면 스마트폰 메신저의 로그 기능을 이용하여 회의 내용을 저장한다. 위원장을 포함한 참석자들은 순차적으로 그룹 공통키를 생성한다. 모든 참석자들은 공통키를 이용하여 회의 내용에 대한 부인봉쇄 서명을 생성하여 위원장에게 전송한다. 위원장은 자신의 서명과 참석자들의 서명을 조합하여 그룹 서명을 생성한다.

단계 1: 그룹 공통키 생성

단계 1.1: A_1은 회의 그룹 리스트의 첫 번째 순서이며 위원장이다. A_1은 회의 내용 M_{Log}를 해쉬한다. p-1과 서로소인 임의의 난수 k_1을 구하여 R_1을 생성하고 자신의 공개키로

Y_1을 만든다. A_1은 (h, M_{Log}, R_1, Y_1)을 A_2에게 전송한다.

$$h = H(M_{Log}),\ R_1 \equiv h^{k_1} \bmod p$$

$$Y_1 = pk_1 \equiv g^{sk_1} \bmod p$$

단계 1.2: A_i(i=[2..n])는 A_{i-1}로 부터 (h, M_{Log}, R_{i-1}, Y_{i-1})을 수신한다. M_{Log}를 확인하고 이를 해쉬하여 A_{i-1}이 보낸 해쉬 값 h와 일치하는지 확인한다. M_{Log}가 결함이 없으면 p-1과 서로소인 임의의 난수 k_i로 (R_i, Y_i)를 생성하고 A_{i+1}에게 이를 전송한다.

$$R_i \equiv R_{i-1}^{k_i} \equiv h^{\prod_{j=1}^{i} k_j} \bmod p$$

$$Y_i \equiv Y_{i-1}^{sk_i} \equiv g^{\prod_{j=1}^{i} sk_j} \bmod p$$

만약 A_i가 회의 그룹 리스트의 마지막 순서이면 (R, Y)를 A_1에게 전송한다. 그렇지 않으면 단계 1.2를 반복한다.

$$R = R_n \equiv h^{\prod_{j=1}^{n} k_j} \bmod p \ ,\ Y = Y_n \equiv g^{\prod_{j=1}^{n} sk_j} \bmod p$$

단계 1.3: A_1은 그룹 공통키 (R, Y)를 모든 참석자에게 전송한다.

단계 2: 그룹 서명 생성

단계 2.1: 모든 참석자 A_i(i=[1..n])는 회의 내용에 대한 부인봉쇄 서명을 하고 이를 A_1에게 전송한다. k_i와 p-1은 서로소이기 때문에 다음 서명식을 만족하는 sig_i가 존재한다 [10].

$$k_i \cdot sig_i \equiv sk_i \cdot R - k_i \cdot h \bmod p-1$$

단계 2.2: A_1은 다음과 같이 M_{Log}에 대한 그룹서명 SIG를 생성하여 모든 참석자에게 전송한다.

$$SIG \equiv \prod_{j=1}^{n} (h + sig_j) \bmod p$$

3.4 그룹서명 검증 및 회의 기록 저장

회의 참석자 전원이 회의 내용에 동의하는지 확인하기 위하여 그룹 서명을 검증한다. 검증된 회의 기록은 회의 서버에 전송하여 데이터베이스에 저장한다.

단계 1: 임의로 선택된 검증자 A_i는 임의의 두 난수 (a, b)를 선택하여 도전 값 CH를 생성한다. 자신의 개인키로 응답 RP_i를 계산하여 회의 그룹 리스트의 다음 참석자에게 전송한다. 회의 그룹 리스트는 끝과 처음이 연결된 원형 리스트로 n 명의 참석자가 순차적으로 모두 응답하도록 순환한다.

$$CH \equiv R^{SIG \cdot a} \cdot Y^{R^n \cdot b} \bmod p$$

$$RP_i \equiv CH^{sk_i^{-1}} \bmod p$$

마지막 참석자는 CH에 대한 전체 참석자의 응답 RP를 검증자에게 전송한다.

단계 2: 검증자는 다음과 같이 응답을 검증한다. 검증에 성공하면 모든 참석자에게 RP를 전송한다.

$$RP \equiv h^{R^n \cdot a} \cdot g^{R^n \cdot b} \bmod p$$

단계 3: 위원장은 (회의 그룹 리스트, 회의 내용, 공통키, 그룹서명)을 회의 서버로 전송한다.

$$(list_A,\ M_{Log},\ R,\ Y,\ SIG)$$

단계 4: 회의 서버는 현재 세션 레코드에 ($list_A$, M_{Log}, R, Y, SIG)를 저장한다.

4. 안전성 분석

제안한 회의 인증 프로토콜이 이동성과 프라이버시 요구사항을 만족하는지 분석한다.

정리 1. (프라이버시) 회의 참석자 모두는 회의 내용에 대한 그룹 서명을 부인할 수 없다.

(증명) 회의 참석자들은 바이오메트릭 데이터를 이용하여 서명키를 생성한다. 바이오메트릭 데이터는 사용자 고유 정보이기 때문에 서명키에 대해서 부인할 수 없다. 위원장은 회의 내용에 대한 각 참석자의 부인봉쇄 서명을 취합하여 그룹 서명을 만든다. 서명 검증은 모든 참석자들이 순차적으로 참여해야만 가능하다. 따라서 다음 검증식을 만족하면 회의 참석자는 회의 내용에 대해서 부인할 수 없다.

$$RP \equiv CH^{\prod_{j=1}^{n} sk_j^{-1}} \equiv (R^{SIG \cdot a} \cdot Y^{R^n \cdot b})^{\prod_{j=1}^{n} sk_j^{-1}} \bmod p$$

$$\equiv (h^{\prod_{j=1}^{n} (k_j \cdot (h + sig_j)) \cdot a} \cdot g^{\prod_{j=1}^{n} sk_j \cdot R^n \cdot b})^{\prod_{j=1}^{n} sk_j^{-1}} \bmod p$$

$$\equiv (h^{\prod_{j=1}^{n} (sk_j \cdot R) \cdot a} \cdot g^{\prod_{j=1}^{n} sk_j \cdot R^n \cdot b})^{\prod_{j=1}^{n} sk_j^{-1}} \bmod p$$

$$\equiv h^{R^n \cdot a} \cdot g^{R^n \cdot b} \bmod p \quad \text{Q.E.D.}$$

정리 2. (이동성) 회의 참석자 이외의 제 3자는 모바일 회의에 참석할 수 없다.

(증명) 회의에 참여하려면 스마트폰으로 바이오메트릭 데이터를 입력하여 회의 서버의 인증을 받아야 한다. 본인 인증에 성공한 참석자만 회의 그룹 리스트에 등록될 수 있다. 바이오메트릭 데이터는 사용자 고유 정보이기 때문에 참석자 본인만이 생성할 수 있다. 제 3자가 회의에 참석하려면 회의 참석자의 템플릿을 가로채기 하고 이를 재전송해야 한다. 3.2 절의 단계 3에서 회의 서버는 템플릿의 재사용 여부를 검증한다. 가정 1에서 회의 서버는 신뢰할 수 있음으로 회의 참가자 이외의 제 3자는 회의에 참여할 수 없다. Q.E.D.

5. 결론

본 논문에서는 스마트폰 메신저를 이용하여 업무 회의를 할 수 있는 회의 인증 기법을 제안하였다. 제안한 방법은 모바일 회의 요구사항인 이동성과 프라이버시를 만족한다. 이동성 제공을 위해서 바이오메트릭 기반의 인증을 하고, 기기 변경을 못하도록 USIM 기반의 모바일 ID와 이에 기반을 둔 키를 생성한다. 프라이버시 보장을 위해서 회의 참석자들은 공통키를 생성하여 회의 내용에 대해서 다중서명하고, 검증된 회의 기록은 데이터베이스에 저장한다. 회의 내용 검증은 모든 참석자들이 참여해야만 가능하고 이러한 특성은 이해 관계를 갖는 구성원들 간의 공모 공격을 불가능하게 한다.

스마트폰 인증에 사용된 USIM은 스마트폰 간에 이동이 가능하다. 따라서 USIM을 다른 스마트폰에 삽입하면 기기 대리 인증이 가능하다. 향후 과제는 이러한 USIM의 이동성이 고려된 기기 인증 방법에 대한 연구이다.

REFERENCES

[1] E. J. Choi, KaKaoTalk Mobile App Case Study, http://www.korea-marketing.com/kakaotalk-mobile-app-case-study/

[2] S. H. Yun, The USIM based Biometric Multi-Signature for Mobile Content Authentication, ICONI 2011, pp. 137-141, 2011.

[3] N. K. Ratha, J. H. Connell, R. M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal, Vol. 40, No. 3, pp. 614-634, 2001.

[4] 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.

[5] Apple Support, iPhone 5s: Using Touch ID, http://support.apple.com/kb/HT5883

[6] B. S. Yu, S. H. Yun, The Design and Implementation of Messenger Authentication Protocol to Prevent Smartphone Phishing, Journal of the Korea Convergence Society, Vol. 1, No. 1, pp. 9-14, 2010.

[7] The 3GPP Project, Characteristics of the USIM Application, 3GPP TS 31.02, http://www.3gpp.org/ftp/Specs/html-info/31102.htm.

[8] S. H. Yun, H. S. Lim, Y. S. Jeong, S. Y. Jung, J. K. Chang, The Biometric Based Convertible Undeniable Multi-Signature Scheme to Ensure Multi-Author Copyrights and Profits, Wireless Personal Communications, Springer, Vol. 60, No. 3, pp. 405-418, 2011.

[9] ITU-T X.1088, A Framework for Biometric Digital Key Generation, ITU-T, 2008.

[10] D. M. Burton, Elementary Number Theory, McGraw-Hill Science/Engineering/Math, 2010.

윤 성 현(Yun, Sung Hyun)

- 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