Journal of the Korea Convergence Society
Vol. 7. No. 1, pp. 49-55, 2016
http://dx.doi.org/10.15207/JKCS.2016.7.1.049

바이오메트릭 인증 기반의 동적 그룹 서명 기법

윤성현*
백석대학교 정보통신학부

The Biometric Authentication based Dynamic Group Signature Scheme

Sunghyun Yun*
Division of Information and Communication, Baekseok University

요 약 대리 인증은 제 3자에게 자신의 인증 정보를 제공하여 본인 대신 인증을 받도록 하는 것으로, 패스워드와 같이 내가 기억하는 것에 기반을 둔 인증 방법은 이러한 공격에 취약하다. 바이오메트릭 인증은 사람마다 고유한 바이오메트릭 데이터를 이용하기 때문에 대리 인증의 위험을 최소화할 수 있다. 그룹 인증은 그룹 멤버들이 해당 그룹에 속해 있음을 증명하는 것이다. 전자투표, 모바일 회의와 같이 멤버의 수가 동적으로 변하는 응용에서는 그룹 상태의 변화를 실시간으로 반영하는 새로운 인증 기법이 필요하다. 본 논문에서는 바이오메트릭 인증 기반의 동적 그룹 서명 기법을 제안한다. 제안한 기법은 바이오메트릭 키 생성, 그룹 공통키 생성, 그룹 서명 생성, 그룹 서명 검증 그리고 멤버 업데이트 프로토콜로 구성된다. 제안한 멤버 업데이트 프로토콜은 기존 멤버의 공모 공격으로부터 안전하고 그룹 상태를 실시간으로 반영한다.

• Key Words : 서명 위임, 바이오메트릭 인증, 그룹 인증, 모바일 회의, 전자 투표

Abstract In a delegate authentication, a user can lend his/her own authentication data to the third parties to let them be authenticated instead of himself/herself. The user authentication schemes based on the memory of unique data such as password, are vulnerable to this type of attack. Biometric authentication could minimize the risk of delegate authentication since it uses the biometric data unique by each person. Group authentication scheme is used to prove that each group member belongs to the corresponding group. For applications such as an electronic voting or a mobile meeting where the number of group members is changing dynamically, a new group authentication method is needed to reflect the status of group in real time. In this paper, we propose biometric authentication based dynamic group signature scheme. The proposed scheme is composed of biometric key generation, group public key creation, group signature generation, group signature verification and member update protocols. The proposed member update protocol is secure against colluding attacks of existing members and could reflect group status in real time.

• Key Words : Signature Delegation, Biometric Authentication, Group Authentication, Mobile Business Meeting, Electronic Voting

*Corresponding Author : Sunghyun Yun(shyoon@bu.ac.kr)
Received October 29, 2015 Revised January 8, 2016
Accepted February 20, 2016 Published February 29, 2016

1. 서론

사용자 인증은 제 3자에게 나 임을 입증하는 것으로 일반적으로 나 만이 알고 있는 또는 나 만이 가지고 있는 고유정보에 기반을 둔다. 아이디와 패스워드를 이용하여 인터넷 계정에 접근하는 것은 나 만이 기억하는 것에 기반을 둔 방법이고, 주민등록번호, 공인인증서, 신용카드는 나 만이 가지고 있는 것을 이용하는 방법이다[1,16].

이러한 인증 방법의 단점은 사용자가 제 3자에게 본인의 고유 정보를 알려주어서 제 3자가 본인을 대신하여 인증하는 대리 인증이 가능하다는 것이다. 전자투표, 원격회의 등과 같이 본인이 직접 인증에 참여해야 하는 응용에서는 적합하지 않다[2,3].

지문, 홍채, 얼굴모양과 같은 바이오메트릭 데이터는 사용자마다 고유하고 자기 몸의 한 부분이기 때문에 제 3자에게 위임할 수 없다. 따라서, 대리 인증의 위험을 최소화 하기 위해서는 바이오메트릭 데이터 기반의 사용자 인증 기법을 사용해야 한다.

바이오메트릭 데이터는 사람마다 그 개수가 한정적이기 때문에 제 3자에게 노출될 경우에 다시 사용할 수 없다. 따라서 바이오메트릭 인증을 위해서는 원본을 이용하면 안되고 취소 및 재등록이 가능한 템플릿(Cancellable Biometric Template)으로 변형해야 한다[4,5,6].

최근의 스마트폰은 카메라 및 지문인식 센서가 기본 사양으로 포함되어 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[7,8,9].

그룹 인증은 그룹의 멤버들이 해당 그룹에 속해 있음을 입증하는 것으로 주로 디지털 다중 서명 기법을 사용하여 구현한다. 디지털 다중 서명 기법은 그룹을 구성하는 멤버의 수가 미리 정해져 있는 경우에 그룹의 공증이 필요한 도큐멘트를 서명하기 위한 용도로 많이 이용된다[10,11,17,20].

그룹의 구성원 수가 시간에 따라 변하는 대표적인 사례로는 전자투표 또는 모바일 비즈니스 회의 등을 들 수 있다. 전자투표에서 유권자들은 투표에 참여할 수도 있고 그렇지 않을 수도 있다. 또한 투표 후에 마음이 바뀌어 이전 투표를 취소하고 새로운 후보자에게 투표할 수도 있다. 마찬가지로 모바일 비즈니스 회의에서도 회의 구성원은 회의에 늦게 참석할 수도 있고 회의 중에 여러 가지 사정으로 회의장을 떠나게 될 수도 있다. 이 경우에 그룹 멤버들이 추가되거나 이탈되는 경우가 발생하여 그룹 상태가 변하게 된다.

본 논문에서는 실시간으로 그룹 상태를 반영할 수 있는 바이오메트릭 인증 기반의 그룹 서명 기법을 제안한다. 제안한 기법은 바이오메트릭 키 생성, 그룹 공통키 생성, 그룹 서명 생성 및 검증, 그리고 멤버 업데이트 프로토콜로 구성된다. 2 장에서는 바이오메트릭 인증 방법과 그룹 서명 기법에 대해서 살펴본다. 3 장에서는 바이오메트릭 인증 기반의 동적 그룹 서명 기법을 제안한다. 4 장에서는 제안한 멤버 업데이트 프로토콜의 안전성을 분석하고 5장에서 결론을 제시한다.

2. 기존 연구

2.1 바이오메트릭 기반 인증

바이오메트릭 템플릿은 사람마다 고유한 정보이기 때문에 한 번 도용되면 다시 사용할 수 없다. 따라서, 바이오메트릭 템플릿은 원본을 직접 사용되면 안되고, 사용자 만이 기억하는 패스코드를 이용하여 원본을 변형해야 한다. 사용자 바이오메트릭 템플릿이 노출되더라도, 패스코드만 변경하면 다시 사용할 수 있는 변형된 템플릿을 생성할 수 있다[5,6].

바이오메트릭 키는 사용자의 바이오메트릭 템플릿을 이용하여 만들어진다. 사용자가 직접 자신의 바이오메트릭 템플릿을 제시해야만 키 생성 및 검증이 가능하도록 ITU-T X.1088에서 표준화된 바이오메트릭 키 생성 절차를 제공한다[6].

2.2 그룹 서명 기법

그룹 서명 기법은 그룹을 구성하는 멤버들이 그룹에 속해 있음을 인증하고, 서명한 문서에 대해서 멤버들이 부인할 수 없도록 한다. 기존의 일반 그룹 서명 기법은[10,11] 그룹을 구성하는 멤버의 수가 한정적이며 대리 인증이 가능한 특성을 갖는다. 바이오메트릭 그룹 서명 기법은[3] 대리 인증의 위험을 최소화할 수 있지만, 일반 그룹 서명 기법과 마찬가지로 그룹 멤버의 수가 미리 정해져 있어야 한다.

2.3 고려사항

그룹 멤버 모두가 그룹에 속해 있음을 인증하고 서명한 문서에 대해 부인할 수 없도록 하려면 그룹 서명 기법이 필요하다. 멤버들 간의 공모 또는 대리 인증의 피해를 최소화하기 위해서는 바이오메트릭 데이터와 법적 구속력이 있는 PKI 인증서의 사용이 고려되어야 한다. 더불어 그룹 단위의 전자투표 또는 모바일 회의와 같이 그룹 멤버가 직접 참여해야 하고, 실시간으로 멤버의 추가 및 이탈이 발생하는 경우에는 그룹 상태를 어떻게 정의하고 업데이트 할 것인지를 추가적으로 고려해야 한다.

3. 제안한 기법

제안한 기법은 다음과 같은 요구사항을 만족한다.

가. 제 3자가 임의의 멤버인 것처럼 가장하여 대리 서명을 할 수 없어야 한다.
나. 그룹 리스트는 새로운 멤버의 참여 또는 기존 멤버의 탈퇴를 실시간으로 반영할 수 있어야 한다.
다. 그룹의 각 멤버는 해당 그룹에 속해 있음을 증명할 수 있어야 하며, 그룹 서명을 부인할 수 없어야 한다.

본 논문에서 사용된 용어는 다음과 같다.

- $UList = [U_1 \| U_2 \| ... \| U_n]$: 그룹 멤버 리스트
- U_i : i 번째 그룹 멤버 (i=[1..n])
- ID_i : 멤버 ID
- BT_i : 바이오메트릭 템플릿
- CBT_i : 취소가능한 바이오메트릭 템플릿
- $Cert_i$: PKI 공인인증서
- bk_i : 바이오메트릭 개인키
- pk_i : 공개키
- $pcode_i$: 패스코드
- $h()$: 해쉬 함수(MD5 또는 SHA-1)

3.1 바이오메트릭 키 생성

가정 1. 그룹의 멤버 수는 n 명이고 신뢰할 수 있는 센터가 존재한다. 센터는 멤버들의 바이오메트릭 템플릿을 등록 및 관리하기 위하여 데이터베이스를 운영하고, 더불어 바이오메트릭 인증 업무를 담당한다. 센터의 개인키 및 공개키는 다음과 같다.

센터의 개인키 : $bk_C < p$

센터의 공개키 : $pk_C \equiv g^{bk_C} \bmod p$

가정 2. $GF(p)$는 암호학적으로 안전한 유한체이고 g는 $GF(p)$ 상에서 정의된 생성자로 위수 $p-1$을 갖는다. p는 소수이고 $p > 2^{1024}$ 이라고 가정한다[12,13].

단계 1: 그룹 멤버들은 다음과 같이 취소가능한 바이오메트릭 템플릿, 개인키, 공개키를 생성한다.

$CBT_i = h(pcode_i \| BT_i) \in Z_{p-1}, \quad i = [1..n]$

$bk_i = h(Cert_i \| CBT_i \| pcode_i) \in Z_{p-1}$

$pk_i \equiv g^{bk_i} \bmod p$

단계 2: 그룹 멤버들은 센터로 멤버 ID, 인증서, 취소가능한 바이오메트릭 템플릿, 공개키를 전송한다.

$(ID_i, Cert_i, CBT_i, pk_i)$

단계 3: 센터는 멤버 ID와 PKI 인증서를 검증한다. 검증에 성공하면, $(ID_i, Cert_i, CBT_i, pk_i)$ 를 데이터베이스에 등록한다.

3.2 그룹 리스트 구성

단계 1: U_i는 바이오메트릭 인증을 요청하기 위해서 자신의 바이오메트릭 데이터를 스캔하여 템플릿을 생성한다. U_i는 패스코드를 이용하여 원본 템플릿을 취소가능한 템플릿으로 변환한다. U_i는 센터의 공개키로 취소가능한 바이오메트릭 템플릿을 암호화하고 자신의 ID와 함께 센터로 인증 요청을 한다.

$(ID_i, E_{pk_C}(CBT_i')), i = [1..n]$

단계 2: 센터는 자신의 개인키 bk_C로 $E_{pk_C}(CBT_i')$를 복원한다. 센터는 CBT_i'과, U_i가 과거 세션에서 제출했던 모든 템플릿들을 비교하여 CBT_i'이 재사용되었는 지를 검증한다. 검증

에 성공하면 ID_i와 CBT_i'를 데이터베이스에 저장하고 단계 3으로 진행한다.

단계 3: 센터는 단계 2의 CBT_i'과 데이터베이스에 등록된 U_i의 템플릿 CBT_i를 비교하여 U_i를 인증한다. U_i 인증에 성공하면 단계 4로 진행한다.

단계 4: 센터는 다음과 같이 그룹 리스트에 U_i를 추가한다.

$$UList = [U_1 \| U_2 \| \cdots \| U_i]$$

3.3 그룹 키 생성

멤버들은 그룹 리스트에 등록된 순서대로 순차적으로 그룹 공통키를 생성한다.

단계 1: U_1의 그룹 공통키 생성

단계 1.1: U_1은 그룹 리스트의 첫 번째 멤버로 그룹 인증 메시지 msg를 해쉬하고, $p-1$과 서로소인 임의의 난수 k_1을 선택한다. U_1은 해쉬값 $hmsg$와 k_1으로 R_1을 생성하고, 자신의 공개키를 Y_1으로 설정한다.

$$hmsg = h(msg),\ R_1 \equiv hmsg^{k_1} \bmod p$$

$$Y_1 \equiv pk_1 \equiv g^{bk_1} \bmod p$$

단계 1.2: U_1은 $(hmsg, msg, R_1, Y_1)$ 을 U_2에게 전송한다.

단계 2: U_i의 그룹 공통키 생성$(i = [2..n])$

단계 2.1: U_i는 $(hmsg,\ msg,\ R_{i-1},\ Y_{i-1})$을 U_{i-1}로부터 수신한다. 먼저 msg를 해쉬하여 $hmsg$와 같은지 비교한다. 검증에 성공하면 단계 2.2로 진행한다.

단계 2.2: U_i는 $p-1$과 서로소인 임의의 난수 k_i를 구하여 (R_i, Y_i) 를 다음과 같이 생성한다. U_i는 U_{i+1}에게 $(hmsg,\ msg,\ R_i,\ Y_i)$를 전송한다.

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

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

단계 2.3: U_i가 그룹 리스트의 마지막 멤버일 때 까지 단계 2.1과 2.2를 반복한다. U_i가 그룹 리스트의 마지막멤버이면 그룹 공통키 $(R,\ Y)$를 다음과 같이 생성하여 센터 및 모든 멤버에게 전송한다.

$$R \equiv R_n \equiv R_{n-1}^{k_n} \equiv hmsg^{\prod_{j=1}^{n} k_j} \bmod p$$

$$Y \equiv Y_n \equiv Y_{n-1}^{bk_n} \equiv g^{\prod_{j=1}^{n} bk_j} \bmod p$$

3.4 그룹 서명 생성

단계 1: $U_i(i = [1..n])$ 는 msg_t에 대한 서명 sig_i를 생성하여 센터로 전송한다. k_i와 $p-1$은 서로소이기 때문에 다음 식을 만족하는 sig_i가 존재한다[14].

$$k_i \cdot sig_i \equiv bk_i \cdot R - k_i \cdot hmsg \bmod p-1$$

단계 2: 센터는 다음과 같이 msg_t에 대한 그룹 서명 sig_G를 생성한다. 센터는 sig_G를 데이터베이스에 저장하고 모든 멤버들에게 전송한다.

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

3.5 그룹 서명 검증

그룹 서명 검증은 D. Chaum의 도전-응답 프로토콜[15] 방식에 기반을 둔다.

단계 1: U_1의 응답 생성

단계 1.1: 센터는 임의의 두 난수 (a, b) 를 선택하여 도전 값 ch를 다음과 같이 생성한다. 센터는 U_1에게 ch를 전송한다.

$$ch \equiv R^{sig_G \cdot a} \cdot Y^{R^n \cdot b} \bmod p$$

단계 1.2: U_1은 자신의 개인키 bk_1으로 응답 rp_1을 다음과 같이 생성한다. U_1은 rp_1을 U_2에게 전송한다.

$$rp_1 \equiv ch^{bk_1^{-1}} \bmod p$$

단계 2: U_i의 응답 생성$(i = [2..n])$

단계 2.1: U_i는 U_{i-1}로부터 rp_{i-1}을 수신한다. U_i는 자신의 개인키 bk_i로 응답 rp_i를 다음과 같이 생성한다. U_i는 rp_i를 U_{i+1}에게 전송한다.

$$rp_i \equiv rp_{i-1}^{bk_i^{-1}} \bmod p$$

단계 2.2: U_i가 그룹 리스트의 마지막 멤버일 때 까지

단계 2.1을 반복한다. U_i가 그룹 리스트의 마지막 멤버이면 전체 멤버의 응답 rp를 다음과 같이 생성하여 센터로 전송한다.

$$rp \equiv rp_n \equiv rp_{n-1}^{bk_n^{-1}} \bmod p$$

단계 3: 센터는 다음과 같이 응답 rp를 검증한다. 검증에 성공하면 단계 4로 진행한다.

$$rp \equiv hmsg^{R^n \cdot a} \cdot g^{R^n \cdot b} \bmod p$$

단계 4: 센터는 ($UList$, msg_t, R, Y, sig_G)를 데이터베이스에 등록한다.

3.6 멤버 조인 프로토콜

단계 1: U_{n+1}은 그룹에 새로 조인하기 위하여 센터에 바이오메트릭 인증을 요청한다.

단계 2: 센터는 U_{n+1}의 바이오메트릭 인증이 성공하면 다음과 같이 그룹 리스트를 갱신한다.

$$UList = [U_1 \| U_2 \| \cdots \| U_n \| U_{n+1}]$$

단계 3: 센터는 ($hmsg$, msg, R, Y)를 U_{n+1}에게 전송한다.

단계 4: U_{n+1}은 먼저 그룹 인증 메시지 msg를 해쉬하여 $hmsg$와 같은지 비교한다. 검증에 성공하면 단계 5로 진행한다.

단계 5: U_{n+1}은 다음과 같이 그룹 공통키 (R, Y)를 업데이트한다. U_{n+1}은 (R, Y)를 센터로 전송한다.

$$R \equiv R_n^{k_{n+1}} \equiv hmsg^{\prod_{j=1}^{n+1} k_j} \bmod p$$

$$Y \equiv Y_n^{bk_{n+1}} \equiv g^{\prod_{j=1}^{n+1} bk_j} \bmod p$$

단계 6: 센터는 업데이트된 그룹 공통키 (R, Y)를 모든 멤버에게 전송한다.

3.7 멤버 탈퇴 프로토콜

단계 1: $U_b(b=[1..n])$는 그룹에서 탈퇴하기 위하여 센터에 바이오메트릭 인증을 요청한다.

단계 2: 센터는 U_b의 바이오메트릭 인증이 성공하면 다음과 같이 그룹 리스트를 갱신한다.

$$UList = [U_1 \| U_2 \| \cdots \| U_{b-1} \| U_{b+1} \| ... \| U_n]$$

단계 3: U_b는 다음과 같이 그룹 공통키 (R, Y)를 업데이트한다. U_b는 (R, Y)를 센터로 전송한다.

$$R \equiv R_n^{k_b^{-1}} \equiv hmsg^{(\prod_{j=1}^{n} k_j) \cdot k_b^{-1}} \bmod p$$

$$Y \equiv Y_n^{bk_b^{-1}} \equiv g^{(\prod_{j=1}^{n} bk_j) \cdot bk_b^{-1}} \bmod p$$

단계 4: 센터는 업데이트된 그룹 공통키 (R, Y)를 모든 멤버에게 전송한다.

4. 안전성 분석

정리 1. 멤버 조인 및 탈퇴 프로토콜로 업데이트 된 그룹 공통키의 안전성은 업데이트 이전과 동일하다.

(증명) 업데이트 이전과 이후의 그룹 공통키 값을 이용하여 비밀 정보를 유추할 수 없음을 증명한다. 먼저 멤버 조인 프로토콜로 업데이트 된 그룹 공통키 값을 (R', Y')으로 하고 업데이트 이전 값을 (R, Y)로 설정한다.

$$R' \equiv hmsg^{\prod_{j=1}^{n+1} k_j} \bmod p \quad , \quad Y' \equiv g^{\prod_{j=1}^{n+1} bk_j} \bmod p$$

$$R \equiv hmsg^{\prod_{j=1}^{n} k_j} \bmod p \quad , \quad Y \equiv g^{\prod_{j=1}^{n} bk_j} \bmod p$$

R'과 R을 이용하여 U_{n+1}이 보유한 k_{n+1} 값을, 그리고 Y'과 Y를 이용하여 U_{n+1}의 개인키 bk_{n+1}을 구하는 것은 다음과 같이 $GF(p)$ 상에서의 이산 대수 문제가 된다. 가정 2로부터 $GF(p)$는 암호학적으로 안전한 유한체이기 때문에, $GF(p)$ 상에서의 이산 대수 문제는 계산상 불가능하다[12,13].

$$\prod_{j=1}^{n+1} k_j \equiv \log_{hmsg} R' \bmod p, \quad \prod_{j=1}^{n} k_j \equiv \log_{hmsg} R \bmod p$$

$$\prod_{j=1}^{n+1} bk_j \equiv \log_g Y' \bmod p, \quad \prod_{j=1}^{n} bk_j \equiv \log_g Y \bmod p$$

U_{n+1}을 제외한 모든 멤버들이 공모하여 R' 값에서 k_i 값을, 그리고 Y'에서 bk_i 값을 제거하여도, 새로 가입한 U_{n+1}의 k_{n+1}과 bk_{n+1}을 유추하려면 다음 식 4.1과 4.2를 풀어야 한다.

$$R'' \equiv R'^{\prod_{j=1}^{n} k_j^{-1}} \equiv hmsg^{k_{n+1}} \bmod p$$

$$k_{n+1} \equiv \log_{hmsg} R'' \bmod p \qquad (4.1)$$

$$Y' \equiv Y'^{\prod_{j=1}^{n} bk_j^{-1}} \equiv g^{bk_{n+1}} \bmod p$$
$$bk_{n+1} \equiv \log_g Y' \bmod p \quad (4.2)$$

식 4.1과 4.2는 $GF(p)$ 상에서의 이산 대수 문제가 된다. 따라서 업데이트 이후의 그룹 공통키 값의 안전성은 업데이트 이전과 동일하다.

멤버 탈퇴 프로토콜에서의 그룹 공통키의 안전성은 멤버 조인 프로토콜의 안전성 분석과 동일한 방식으로 증명이 가능하다. Q.E.D.

정리 2. 그룹의 모든 멤버는 그룹 서명을 부인할 수 없다.

(증명) 그룹 멤버들은 바이오메트릭 데이터를 이용하여 서명키를 생성한다. 바이오메트릭 데이터는 사용자 고유 정보이기 때문에 자신의 서명키에 대해서 부인할 수 없다. 센터는 각 멤버의 부인봉쇄 서명을 취합하여 그룹 서명을 생성한다. 그룹 서명 검증은 모든 멤버들이 순차적으로 참여하여 서명이 올바른지 인증한다. 따라서 제안한 다음 검증식을 만족하면 모든 멤버들은 그룹 서명에 대해서 부인할 수 없다.

$$rp \equiv ch^{\prod_{j=1}^{n} bk_i^{-1}} \equiv (R^{sig_G \cdot a} \cdot Y^{R^n \cdot b})^{\prod_{j=1}^{n} bk_j^{-1}} \bmod p$$

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

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

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

5. 결론

본 논문에서는 바이오메트릭 인증 기반의 동적 그룹 서명 기법을 제안하였다. 제안한 기법은 바이오메트릭 키 생성, 그룹 공통키 생성, 그룹 서명 생성, 그룹 서명 검증 그리고 멤버 업데이트 프로토콜로 구성된다. 멤버 업데이트 프로토콜에서 생성된 그룹 공통키의 안전성은 업데이트 이전과 동일하고, 멤버의 공모 공격에 대해서 안전함을 증명하였다. 전자투표 또는 원격 회의와 같은 응용에서는 제 3자에 의한 대리 인증이 불가능해야 한다. 더불어 투표나 회의에 참여하는 그룹 멤버는 시간에 따라서 가입과 탈퇴가 가능하기 때문에 그룹 멤버의 수는 가변적이다. 제안한 기법은 이러한 동적 그룹을 인증하는데 적합하다.

ACKNOWLEDGMENTS

이 논문은 2015년도 백석대학교 대학연구비에 의하여 수행된 것임

REFERENCES

[1] M. Stamp, Information Security: Principles and Practice 2nd Edition, Wiley-Inerscience, 2011.

[2] Tepandi, "Wireless PKI Security and Mobile Voting", IEEE Computer, Vol. 43, No. 6, pp. 54-60, 2010.

[3] S. H. Yun, "The Biometric based Mobile ID and Its Application to Electronic Voting", KSII Transactions on Internet and Information Systems, Vol. 7, No. 1, pp. 166-183, 2013.

[4] P. Janbandhu, M. Siyal, "Novel biometric digital signatures for Internet-based applications", Information Management & Computer Security, Vol. 9, No. 5, pp. 205-212, 2001.

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

[6] ITU-T X.1088, A Framework for biometric digital key generation, ITU-T, 2008.

[7] Apple Support, Ues Touch ID on iPhone and iPad, http://support.apple.com/kb/HT5883.

[8] 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.

[9] H. Li, K. Toh, L. Li, Advanced Topics in Biometrics, World Scientific, 2011.

[10] L. Harn, "(t,n) Threshold Signature and Digital Multisignature", Workshop on Cryptography &

Data Security, pp. 61-73, 1993.
[11] S. H. Yun, "The USIM based Biometric Multi-Signature for Mobile Content Authentication", ICONI, pp. 137-141, 2011.
[12] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, No. 6, pp. 644-654, 1976.
[13] D. M. Burton, Elementary Number Theory, McGraw - Hill, 2010.
[14] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985.
[15] D. Chaum, "Undeniable Signatures", Advances in Cryptology, Proceedings of CRYPTO'89, Springer-Verlag, pp. 212-216, 1990.
[16] D. R. Kim, "A Study on the OTP Generation Algorithm for User Authentication", Journal of Digital Convergence, Vol. 13, No. 1, pp. 283-288, 2015.
[17] Y. J. Song, S. M. Gu, Y. C. Kim, "A Study on the Distributed Transcoding System using Secret Sharing Techniques", Journal of Digital Convergence, Vol. 12, No. 11, pp. 233-239, 2014.
[18] S. H. Hong, "Vulnerability of Directory List and Countermeasures", Journal of Digital Convergence, Vol. 12, No. 10, pp. 259-264, 2014.
[19] H. M. Choi, C. B. Jang, J. M. Kim, "Efficient Security Method Using Mobile Virtualization Technology And Trustzone of ARM", Journal of Digital Convergence, Vol. 12, No. 10, pp. 299-308, 2014.
[20] S. Y. Lee, S. S. Yeo, "Efficient Secret Sharing Data Management Scheme for Privacy Protection in Smart Grid Environment", Journal of Digital Convergence, Vol. 11, No. 12, pp. 311-318, 2013.

저자소개

윤 성 현(Sunghyun Yun) [종신회원]

- 1994년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학석사)
- 1997년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
- 1998년 3월 ~ 2002년 2월 : LG전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수

<관심분야> : 모바일 보안, 바이오메트릭 인증, DRM, 전자선거