Journal of Korea Multimedia Society Vol. 19, No. 12, December 2016(pp. 1981-1991)
https://doi.org/10.9717/kmms.2016.19.12.1981

원격 헬스케어 모니터링 시스템에서 키 격리기법을 이용한 개선된 건강정보 전송 보안 프로토콜

노시완[†], 박영호[††], 이경현[†††]

An Enhanced Secure Health Data Transmission Protocol using Key Insulation in Remote Healthcare Monitoring System

Si-Wan Noh[†], Youngho Park[††], Kyung-Hyune Rhee[†††]

ABSTRACT

In recent, the advancement of wearable devices and wireless body area networking technologies motivate researchers to pay attention to remote healthcare system for monitoring patients health and disease progression effectively. However, in order to implement a practical remote healthcare system, we must consider the security and privacy of patient's personal health information transmitted to healthcare servers through the network. Hence, in this paper, we propose a secure health data transmission protocol in remote healthcare monitoring system to protect patient's health information and prevent privacy from eavesdropping on the network. To achieve our security goals, we design an efficient secure protocol based on the identity-based cryptography with key evolution technique, and then confirm the superiority and the efficiency of the proposed protocol as compared with the existing protocol of Yang et al.

Key words: Secure Healthcare, Anonymous Authentication, Non-interactive Key Sharing, Key Evolution

1. 서 론

세계적으로 인구가 고령화 사회로 변함에 따라 고령 인구를 위한 헬스케어(Healthcare) 산업이 활기를 띄고 있다. 특히 고령 인구뿐만 아니라 병원을 방문할 시간적 여유가 없거나 의료 기반 시설이 취약한 지역에 거주하는 등의 이유로 인해 직접 병원을 찾아 의료서비스를 제공 받기 어려운 환자들을 위한 원격 건강정보 모니터링 시스템이 주목을 받고 있다[1]. 원격 건강정보 시스템에서 환자 또는 사용자는 여러 의료용 센서나 웨어러블 장비(Wearable device)들을 기반으로 IEEE802.15.6과 같은 WBAN(Wireless Body Area Network)을 통해 수집된 자신의 건강정보를 인터넷을 통해 원격지의 병원에 위치한 의사에게 전송하여 의료 서비스를 제공받을 수 있다[2]. 수집된 정보는 원격지의 의사에게 전송되고 의사는 이를 이용하여 환자에게 필요한 진단이나 관련 의료정보를 제공할 수 있다.

그러나 실용적인 원격 헬스케어 시스템을 도입하기 위해서는 반드시 네트워크를 통해 전송되는 환자

※ Corresponding Author : Kyung-Hyune Rhee, Address: (48513) Room 1305, Uung-Bi Bldg., 45 Yongso-Ro, Nam-Gu, Busan, Republic of Korea, TEL : +82-51-629-6247, FAX : +82-51-626-4887, E-mail : khrhee@pknu.ac.kr
Receipt date : Oct. 10, 2016, Revision date : Nov. 17, 2016
Approval date : Dec. 1, 2016
[†] Interdisciplinary Program of Information Security, Graduate School Pukyong National University
(E-mail : nosiwan@pukyong.ac.kr)
[††] Department of IT Convergence and Application Engineering, Pukyong National University
(E-mail : pyhoya@pknu.ac.kr)
[†††] Department of IT Convergence and Application Engineering, Pukyong National University
※ This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government MSIP (No. NRF-2014R1A2A1A11052981)

개인의 건강정보에 대한 보호뿐만 아니라 건강정보에 대한 환자의 익명성도 반드시 고려되어야 한다. 개인의 건강정보는 매우 민감한 정보로서 누구든지 자신의 건강정보가 타인에게 부당하게 공개되는 것을 원하는 사람은 없을 것이다. 네트워크를 통한 정보의 전송에서 사용자의 건강정보가 담당 의사가 아닌 제 3자에게 공개되거나 사용자의 실제 신원정보가 노출된다면 이는 시스템에 대한 사용자의 신뢰문제로 발전할 수 있다.

원격 헬스케어 시스템의 보안과 관련하여, 비대면 통신 환경의 특성상 주로 원격지에 위치한 사용자의 인증에 대한 연구가 활발하게 이루어졌다[3-5]. 이들 연구는 스마트카드와 패스워드를 이용하여 원격지에 위치한 사용자의 신원을 확인하는 사용자 인증에 초점을 맞추고, 스마트카드 분실이나 패스워드 추측 공격에 대한 취약점 개선 방안들이 제안되었다. 하지만 이들은 이전에 제안된 패스워드 기반 사용자 인증 기법의 단순한 개선만을 시도하였으며, 원격지 헬스케어 시스템으로 전송되는 건강정보에 대한 보안은 다루지 않았다.

안전한 건강정보 전송을 위해, Lin 등은 [6]에서 신원기반 암호기법을 사용하여 원격 건강정보 모니터링 시스템으로 전송되는 환자의 건강정보의 보호와 익명성을 보장할 수 있는 모델을 제시하였다. 그리고 Yang 등은 [7]에서 Lin의 모델에서 비밀키를 저장한 디바이스를 분실하였을 경우 환자의 비밀키의 노출문제를 해결하기 위해 키 격리(Key insulation or key evolution) 기법[8]을 적용하는 방안을 제안하였다. 하지만 Yang 등의 기법은 저자들의 주장과 달리 잘못된 키 격리 기법의 적용으로 인해 여전히 환자가 단말을 분실하였을 때 이를 습득한 다른 환자가 단말을 분실한 환자의 의사와의 공유 비밀키를 계산할 수 있다는 문제점이 있다. 또한 전송되는 메시지에서 환자가 선택한 의사의 신원정보의 노출에 대한 보안문제를 고려하지 않았다. 의사의 신원정보가 노출되는 경우 비록 환자의 익명성은 보장되더라도 의사의 신원정보로부터 해당 의사의 전문 진료과목을 유추하여 환자의 병력과 같은 프라이버시 침해요인이 발생할 수 있으므로, 전송되는 건강정보로부터 의사를 식별할 수 있는 정보도 노출되지 말아야 할 필요가 있다.

이에 본 논문에서는 신원기반 암호기법과 키 격리 기법을 이용한 개선된 건강정보 전송 보안 프로토콜을 제안한다. 제안기법은 Yang 등의 기법에서 잘못 설계된 키 격리 기법 문제를 해결하였으며, Yang의 기법과 달리 환자가 보안 프로토콜 수행에 필요한 암호키들을 발급받는 등록과정에서 오프라인 등록과 같은 별도의 안전한 채널을 가정하지 않는다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 본 연구의 배경으로 Yang이 제안한 기법에서 발생 가능한 보안 문제점에 대해 서술하고, 3장에서 제안기법을 위한 시스템 모델과 안전한 건강정보 전송 프로토콜을 설계한다. 그리고 4장에서는 제안기법에 대한 분석과 성능비교 결과를 제시하고, 5장에서 결론을 맺는다.

2. 연구배경

[6]에서 Lin은 웨어러블 센서 등으로부터 수집된 자신의 건강정보를 스마트폰과 같은 모바일 기기를 이용하여 원격 헬스케어 시스템을 통해 의사에게 전송하여 진료를 받는 eHealth 시스템 모델을 제시하였다. 그리고 신원기반 암호기법을 사용한 비대화식 키 설정(Non-interactive key establishment) 기법을 통해 환자와 의사 사이에 공개키 교환 같은 추가적인 정보의 전송 없이 암호화에 필요한 동일한 비밀키를 공유할 수 있도록 하였다. 하지만 Lin 등이 제시한 모델에서 환자의 개인키를 스마트폰과 같은 환자가 보유한 모바일 단말기에 저장하는데 환자가 이를 분실하거나 도난당하였을 경우 이는 곧 개인키의 노출이라는 문제가 발생한다.

Yang은 [7]에서 Lin이 [6]에서 제안한 모델에 대한 개선안을 제안하였다. 개인키를 저장한 단말기의 분실로 인한 개인키의 노출 문제를 해결하기 위해 단말기에는 짧은 주기의 임시 개인키를 저장하고 임시 개인키의 생성에 필요한 헬퍼키(Helper key)를 개인용 데스크톱과 같이 분실의 위험이 적은 기기에 저장하는 키 격리 기법을 적용하였다. 이를 통해 임시 개인키가 저장된 단말을 분실하더라도 이전의 임시 개인키는 무효화되고 헬퍼키로 새로운 개인키를 생성할 수 있으므로 개인키의 분실로 인한 위협을 감소시킬 수 있다.

본 논문에서 제안되는 기법은 Yang 등이 제안한 모델을 기반으로 하므로, 본 장에서는 먼저 Yang 등

의 모델을 간략하게 살펴보도록 한다. Yang이 제안한 모델의 구성은 다음과 같다.

• HMS (Healthcare Monitoring Server)

환자의 건강정보(Personal Health Information, PHI)를 환자가 선택한 의사에게 전달하는 중개인 역할을 수행하며 시스템에서 사용할 보안 파라미터를 생성하고 환자에게 가명을 발급한다.

• 환자 (Patient)

자신의 건강정보를 의사에게 전송하여 이를 이용해 의료서비스를 제공받는다.

• 의사 (Doctor)

환자로부터 전달받은 건강정보를 이용하여 환자에게 의료서비스를 제공한다.

• BH (Body Hub)

무선 센서 노드를 이용하여 측정된 환자의 건강정보를 수집하고 이를 의사에게 전송하는 역할을 수행한다. 제안 기법에서는 스마트폰을 가정하였다.

• HKU (Helper of Key Update)

HKU는 새로운 주기의 임시 개인키의 생성에 필요한 헬퍼키를 생성하여 BH에 전달한다. 제안 기법에서는 가정의 데스크톱 PC와 같이 분실의 위험이 없는 장치를 가정하였다

Yang은 HKU를 이용하여 임시 개인키를 생성하여 이를 단말에 저장하여 단말을 분실하더라도 새로운 키를 생성하여 분실로 인한 위험을 줄이는 키 격리 기법을 제안하였다. 하지만 이들의 기법에서 다음과 같은 보안 문제가 발생할 수 있다.

2.1 단일 헬퍼 비밀키 문제

Yang은 [7]에서 환자가 HMS에 등록을 하는 과정과 HKU를 사용하여 디바이스에 저장하는 개인키를 갱신하는 과정을 다음과 같이 설명하고 있다.

a. HMS는 환자 PT의 신원정보 ID_{PT}의 유효성을 검사한다.

b. 환자 PT의 초기 개인키$(t=0)$ $SK_{PT}^{0}=sH_1(ID_{PT})+s_1H_1(ID_{PT}\|0)$를 계산한다.($s\in Z_q^*$: HMS의 마스터키, $s_1\in Z_q^*$: HKU의 헬퍼 비밀키)

c. SK_{PT}^{0}를 안전한 채널을 사용하여 환자 PT에게 전송한다. 동시에 s_1를 환자의 HKU에 헬퍼 비밀키로 저장한다.

d. 환자는 HKU에 저장된 헬퍼 비밀키 s_1을 이용하여 새로운 주기 t에서의 헬퍼키 $H_{PT}^{t}=s_1(H_1(ID_{PT}\|t)-H_1(ID_{PT}\|t-1))$를 계산한 뒤 $SK_{PT}^{t}=SK_{PT}^{t-1}+H_{PT}^{t}$를 계산하여 주기 t에서의 새로운 개인키를 얻는다.

여기서 만약 어떤 환자 Bob이 다른 환자 $Alice$의 주기 t에서의 개인키 SK_{Alice}^{t}가 저장된 단말을 습득했다고 가정할 때, Bob은 다음과 같이 $Alice$의 $t+1$에서의 개인키 SK_{Alice}^{t+1}을 생성할 수 있다. $Alice$의 주기 $t+1$에서의 헬퍼키 $H_{Alice}^{t+1}=s_1(H_1(ID_{Alice}\|t+1)-H_1(ID_{Alice}\|t))$를 Bob의 HKU에 저장된 마스터키 s_1을 이용하여 계산한다. 습득한 $Alice$ 개인키 SK_{Alice}^{t}를 이용하여 주기 $t+1$에서의 개인키 $SK_{Alcie}^{t+1}=SK_{Alice}^{t}+H_{Alice}^{t+1}$를 계산한다. 이 문제는 HMS가 모든 환자의 HKU에 같은 마스터키 s_1을 발급함으로서 발생한다.

1) 서비스제공자에 대한 환자의 익명성 문제

Yang의 기법에서 환자에 대한 가명의 발급은 HMS가 수행한다. HMS는 환자의 가명 발급의 주체로서 가명으로부터 환자의 실제 신원정보의 추적이 가능하고 결국 시스템 내에 가명으로 전송되는 PHI에 대한 환자 식별정보에 접근이 가능해진다. 즉, HMS는 환자가 익명으로 전송하는 PHI에서 환자의 실제 신원정보를 추적하여 PHI를 생성한 환자의 식별이 가능해진다.

2.2 의사의 식별정보의 노출 문제

Yang은 제안 기법에서 개체 간에 비대화식으로 공유하는 키의 생성과 키 격리 기법에 중점을 두었다. 제안 기법의 목적이 환자의 익명성 보장과 전송되는 PHI의 보호이기 때문에 PHI는 암호화되어 의사에게 전달되겠지만 의사의 식별정보가 암호화 되지 않을 경우 의사의 식별정보가 노출되어 발생할 수 있는 환자의 프라이버시 침해 가능성의 문제도 고려해야한다.

2.3 안전한 채널을 가정한 환자의 비밀키 전달

Yang의 제안기법에서 HMS는 환자가 PHI의 전

송에 사용할 환자의 초기 개인키 PSK_i^0, 헬퍼 비밀키 hk_i와 헬퍼 공개키 HP_i를 오프라인과 같은 안전한 채널을 사용하여 환자에게 전달한다고 가정하였다. 반면 본 논문에서는 오프라인 등록을 가정하지 않고 온라인 등록 환경에서의 환자의 인증과 키의 안전한 전달을 고려한다.

3. 제안 기법

3.1 시스템 모델

본 장에서는 제안 기법에 대해 설명한다. Yang의 기법의 문제를 해결하기 위해 제안기법에서는 모든 사용자에게 키 격리기법을 위한 서로 다른 헬퍼 비밀키 hk_i를 부여한다. 그리고 환자와 HMS 사이에서 PHI와 환자가 선택한 의사의 정보가 외부에 노출되는 것을 막기 위해 환자는 HMS와 비대화식으로 공유하는 키 K_{PID_i-H}를 사용하여 메시지를 암호화한다. Table 1은 제안하는 시스템에서 사용하는 표기법이며 Fig. 1은 제안하는 시스템의 구성을 간략하게 표현한 것이다.

시스템을 구성하는 각 개체의 역할은 다음과 같이 기본적으로 Yang과 같으며 본 논문에서는 신뢰기관인 TA(Trusted Authority)를 가정하며, TA는 환자의 가명과 시스템 보안 파라미터를 관리한다.

• TA

신뢰기관으로서 프로토콜의 수행에 필요한 공개 시스템 파라미터의 생성 및 배포와 사용자의 신원정보를 등록하고 서비스에서 사용할 환자의 가명을 발급한다.

• 의사(Doctor)

기본적인 역할은 Yang의 모델과 같고 HMS에 소속되어 있으며 HMS와 의사 사이에는 신뢰할 수 있는 네트워크가 존재하고 이 네트워크를 통해 통신을 주고받는다고 가정한다.

이러한 시스템 모델에 대해 본 논문에서는 다음과 같은 보안 요구사항들을 고려한다.

• 환자의 익명성 : 환자의 익명과 실제 신원정보의 관계는 TA를 제외한 다른 개체에 알려져서는 안된다.

• 전송 PHI의 보호 : 전송되는 환자의 PHI는 외부의 도청으로부터 보호되어야하고 환자가 선택한

Table 1. Notations

Notation	Description
G, G_T	bilinear groups of a prime order q, respectively
$P \in G$	generator of group G
$\hat{e}: G \times G \rightarrow G_T$	bilinear pairing
$H_1 : \{0,1\}^* \rightarrow G$	one-way hash function
$H_2 : \{0,1\}^* \times G \rightarrow G$	one-way hash function
PT_i, PID_i	identity and pseudonym of patient i, respectively
SK_X	private key of an entity X
hk_i , HP_i	helper private key and public key pair of patient i, respectively
PHI_i	personal health information of patient i
PSK_i^t	service private key of patient i at period t
ts	time stamp
K_{X-Y}	shared secret key between X and Y
s_0	master secret of TA
s_1	master secret of HMS
$IBEnc(id_X, m)$	id-based encryption for the message m under the identity id_X
$IBDec(SK_X, c)$	id-based decryption for the ciphertext c under the private key SK_X corresponding to id_X
$IBSig(SK_X, m)$	id-based signature for the message m under the private key SK_X corresponding to id_X
$IBVrf(id_X, m, \sigma)$	id-based signature verification for the given message m and signature σ under the id_X

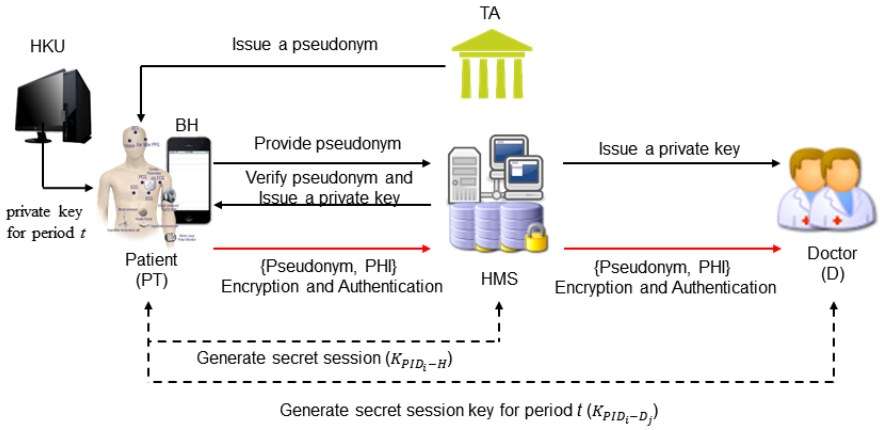

Fig. 1. System model for the proposed scheme.

의사를 제외한 제 3자는 해당 PHI에 접근할 수 없어야한다.

• 의사 식별정보의 기밀성 : 환자가 선택한 의사의 정보는 PHI 전송에 참여하는 개체를 제외한 제3자에게 노출되지 않아야한다.

3.2 초기화 (Initialization)

TA는 다음과 같이 자신의 마스터키를 선택하고 공개 시스템 파라미터를 생성한 뒤 이를 배포한다. 그리고 환자에게 시스템에서 사용할 가명을 발급한다.

1) TA는 시스템에서 사용할 겹선형 함수 파라미터 $(q, P, G, G_T, \hat{e})$를 생성한다.

2) 마스터키로 사용할 $s_0 \in Z_p^*$를 랜덤하게 선택하고 공개키 $P_{TA} = s_0 P$를 계산한다.

3) 일방향 해시함수 $H_1 : \{0,1\}^* \rightarrow G$, $H_2 : \{0,1\}^* \times G \rightarrow G$를 선택하고 공개 시스템 파라미터 $< q, P, G, G_T, \hat{e}, P_{TA}, H_1, H_2 >$를 구성하여 배포한다.

4) 환자의 신원정보 PT_i의 유효성을 검사한 뒤 환자의 가명 PID_i와 가명에 대한 신원기반 개인키 $SK_{PT_i} = s_0 H_1(PID_i)$를 발급하고, $\langle PT_i, PID_i \rangle$를 자신의 데이터베이스에 저장한다.

HMS는 공개 시스템 파라미터를 사용하여 자신의 마스터키를 생성하고 소속된 의사들에게 신원기반 개인키를 안전한 채널을 통해 전달한다.

1) HMS는 마스터키로 사용할 $s_1 \in Z_q^*$를 랜덤하게 선택하고, 공개키 $P_{HMS} = s_1 P$를 계산한다.

2) 소속된 각 의사의 개인키 $SK_{D_j} = s_1 H_1(D_j)$를 생성하여 전달한다.

3.3 등록(Registration)

서비스를 원하는 환자는 TA로부터 발급받은 가명을 HMS에 등록하고 인증과 건강정보 전송 보안에 필요한 서비스 개인키를 발급받는다.

1) 환자는 자신의 가명을 사용하여 서비스 등록요청 메시지 $\{req, PID_i, \sigma = IBSig(SK_{PT_i}, req)\}$를 HMS에게 전송한다. 이때 $IBSig(SK_{PT_i}, req)$는 PID_i에 대응되는 신원기반 개인키 SK_{PT_i}를 이용한 등록 요청메시지의 신원기반 전자서명(ID-based signature)이다[10].

2) HMS는 요청 환자의 가명 PID_i를 이용한 서명검증 $IBVrf(PID_i, req, \sigma)$이 유효한 경우, 다음과 같이 서비스 개인키를 발급한다.

3) HMS는 환자를 위한 헬퍼 비밀키 $hk_i \in Z_q^*$를 랜덤하게 선택하고 헬퍼 공개키 $HP_i = hk_i P$를 계산한다. 이후 환자의 초기$(t=0)$ 개인키 PSK_i^0를 다음과 같이 계산한다.

$$PSK_i^0 = s_1 H_1(PID_i) + hk_i H_1(PID_i, HP_i, 0) \quad (1)$$

4) HMS는 키 전달을 위한 메시지 $m = \{PSK_i^0, hk_i, HP_i\}$에 대한 암호문 $c = IBEnc(PID_i, m)$를 등록요청 환자에게 전송하고, $< PID_i, PSK_i^0, hk_i, HP_i >$를 자신의 데이터베이스에

저장한다. 이때 $c = IBEnc(PID_i, m)$는 신원기반 암호를 의미한다[9].

5) 환자는 신원기반 개인키 SK_{PT_i}를 이용하여 c로부터 $m = \{PSK_i^0, hk_i, HP_i\} = IBDec(SK_{PT_i}, c)$와 같이 복호화하고, 초기 서비스 개인키 PSK_i^0를 자신의 BH에 저장하고 헬퍼 비밀키 hk_i를 자신의 HKU에 저장한다.

3.4 키 갱신(Key Evolving)

주기 t에서 키를 저장한 BH를 분실하였을 경우 환자는 새로운 주기 $t+1$의 서비스 개인키를 생성하여 키 분실로 인한 위협을 최소화한다.

1) 환자의 HKU는 주기 $t+1$에서의 헬퍼키 TK_i^{t+1}를 다음과 같이 생성하고 이를 BH에 전달한다.

$$TK_i^{t+1} = hk_i(H_1(PID_i, HP_i, t+1) - H_1(PID_i, HP_i, t)) \quad (2)$$

2) BH는 $t+1$번째 주기의 서비스 개인키를 다음과 같이 계산한 뒤 t 주기의 개인키 PSK_i^t와 새로운 서비스 개인키 계산에 사용한 헬퍼키 TK_i^t를 삭제한다.

$$PSK_i^{t+1} = PSK_i^t + TK_i^{t+1} \quad (3)$$

기존에 분실한 BH에 저장되어있던 t주기의 서비스 개인키 PSK_i^t는 $t+1$주기에서는 더 이상 사용이 불가능 하므로 위협을 분실시점과 새로운 주기사이로 최소화할 수 있다.

3.5 건강 기록 전송(Sending Patient Health Information)

환자 PT_i는 HMS가 온라인으로 공개하는 소속 의사들의 정보를 통해 진단을 받고자 하는 의사 D_j를 선택한다. 그리고 HMS를 통해 선택한 의사와 건강기록의 전송을 통해 진단을 받는다.

1) 환자는 HMS에 소속된 의사 D_j를 선택한 후, 해당 의사의 신원정보를 사용하여 HKU에서 $DP_i^j = hk_i H_1(D_j)$를 계산하고 이를 BH에 저장한다. 이 과정은 의사를 선택하는 초기에 한번만 수행되어진다.

2) 현재 주기가 t라고 할 때 의사와 비대화식으로 공유할 비밀키 $K_{PID_i - D_j}$를 다음과 같이 생성한다. 여기서 KDF는 키 유도 함수(Key Derivation Function)을 의미한다.

$$K_{PID_i - D_j} = \hat{e}(PSK_i^t, H_1(D_j)) \quad (4)$$

$$k_{PD,0} = KDF(K_{PID_i - D_j} | 0),\ k_{PD,1} = KDF(K_{PID_i - D_j} | 1) \quad (5)$$

3) 환자는 계산된 비밀키를 이용하여 다음과 같이 암호문을 생성하고 메시지 $m = \{PID_i, ts, C_3\}$를 생성하여 HMS에 전송한다.

$$C_1 = Enc_{k_{PD0}}(PHI, ts)$$
$$C_2 = MAC_{k_{PD1}}(PID_i, HP_i, DP_i^j, ts, D_j, C_1)$$
$$C_3 = Enc_{K_{PID_i - H}}(HP_i, DP_i^j, D_j, C_1, C_2)$$

4) C_3의 암호화에 사용한 환자와 HMS 사이의 공유 비밀키 $K_{PID_i - H}$는 다음과 같이 계산한다.

$$K_{PID - H} = KDF(\hat{e}(PSK_i^t, H_1(HMS))) \quad (6)$$

HMS는 등록 단계에서 데이터베이스에 저장해둔 $< PID_i, PSK_i^0, hk_i, HP_i >$를 이용하여 환자와 HMS 사이에서 비대화식으로 공유하는 키 $K_{PID_i - H}$를 계산할 수 있다. HMS는 이렇게 계산한 키를 이용하여 C_3를 복호화하여 메시지 $m = (PID_i, HP_i, DP_i^j, D_j, ts, C_1, C_2)$를 얻을 수 있다. HMS는 이를 해당하는 의사 D_j에게 전송한다.

1) 의사는 주기 t에서의 비대화식으로 공유하는 비밀키를 다음과 같이 계산한다.

$$K'_{PID_i - D_j} = \hat{e}(H_1(PID_i, SK_{D_j}))\hat{e}(H_1(PID_i, HP_i, t), DP_i^j) \quad (8)$$

$$k'_{PD,0} = KDF(K'_{PID_i - D_j} | 0),\ k'_{PD,1} = KDF(K'_{PID_i - D_j} | 1) \quad (9)$$

2) 의사는 $C_2 = MAC_{k'_{PD1}}(PID_i, HP_i, DP_i^j, ts, D_j, C_1)$를 식 (9)에서 계산한 비밀키를 이용하여 검증한 뒤 $Dec_{k'_{PD0}}(C_1)$ 복호화를 통해 환자의 건강정보 PHI_i를 획득한다.

다음의 계산식을 통해서 의사와 환자가 각각 계산한 키 $K_{PID_i - D_j}$와 $K'_{PID_i - D_j}$가 일치함을 확인할 수 있다.

$$\begin{aligned} K_{PID_i - D_j} &= \hat{e}(PSK_i^t, H_1(D_j)) \\ &= \hat{e}(s_1 H_1(PID_i) + hk_i H_1(PID_i, HP_i, t), H_1(D_j)) \\ &= \hat{e}(s_1 H_1(PID_i), H_1(D_j))\hat{e}(hk_i H_1(PID_i, HP_i, t), H_1(D_j)) \\ &= \hat{e}(H_1(PID_i), s_1 H_1(D_j))\hat{e}(H_1(PID_i, HP_i, t), hk_i H_1(D_j)) \\ &= \hat{e}(H_1(PID_i) SK_{D_j})\hat{e}(H_1(PID \end{aligned} \quad (10)$$

4. 안전성 및 성능 분석

4.1 안전성분석

이 절에서는 앞서 기술한 보안요구사항을 제안기

Table 2. Security comparisons

	Lin et al. [6]	Yang et al. [7]	Proposed
Key-evolution			√
Patient's anonymity to HMS	√		√
Patient's anonymity to doctor	√	√	√
Protecting doctor's identity			√

법이 어떻게 만족하는지를 설명하고 Lin의 기법과 Yang의 기법 그리고 제안기법을 비교 분석한다. Table 2는 [6]에서 Lin이 제안한 기법과 [7]에서 Yang이 제안한 기법, 그리고 본 논문에서 제안한 기법의 보안기능을 비교하여 나타내고 있다. Lin은 스마트폰과 같은 모바일 기기를 이용한 건강기록 전송 환경에서 가명과 신원기반 비대화식 키 설정기법을 이용한 익명인증 기법을 제안하였고, 이에 대해 Yang은 사용자 모바일 기기의 분실로 인한 개인키 노출문제를 해결하기 위해 키 격리 기법을 추가적으로 적용한 익명인증 기법을 제안하였다. 그러나 Yang은 제안한 기법에서 개인키를 저장한 단말의 분실을 가정하여 주기적으로 새로운 개인키를 생성하는 키 격리 기법을 사용하였으나 모든 환자의 HKU에 같은 마스터 비밀키를 부여함으로서 안전한 키 격리 기법을 제공하지 못하였다. 또한 HMS가 환자의 익명 발급을 수행함과 동시에 서비스 제공자로서 환자의 개인건강정보를 의사에게 전달하는 역할을 동시에 수행하기 때문에 서비스 제공자인 HMS에 대한 환자의 익명성을 보장할 수 없다. 본 논문의 핵심 기여는 Yang이 제안한 기법을 개선한 것이므로 Yang의 기법과 비교하여 제안기법의 보안성을 분석하도록 한다.

• 단일 헬퍼키 문제 해결

Yang의 기법에서는 시스템에 존재하는 모든 환자들에게 동일한 헬퍼 비밀키($s_1 \in Z_q^*$)를 부여하였다. 하지만 2장에서 논의한 바와 같이, 이 때문에 어떤 사용자(Alice)의 BH를 다른 사용자(Bob)가 습득하였을 경우 자신이 보유한 동일한 헬퍼 비밀키 s_1을 사용하여 Alice의 BH에 저장된 주기 t의 서비스 개인키 SK_{Alcie}^{t}를 사용하여 주기 $t+1$의 서비스 개인키 SK_{Alcie}^{t+1}를 다음과 같이 생성할 수 있는 문제가 있었다.

$$H_{Alice}^{t+1} = s_1(H_1(ID_{Alice} \| t+1) - H_1(ID_{Alice} \| t))$$

$$SK_{Alcie}^{t+1} = SK_{Alice}^{t} + H_{Alice}^{t+1}$$

이를 해결하기 위해, 제안기법은 시스템의 모든 환자들에게 고유한 헬퍼 비밀키 $hk_i \in Z_q^*$(즉, $hk_{Alice} \neq hk_{Bob}$)를 부여함으로써 시스템의 다른 환자 Bob이 Alice의 서비스 개인키 PSK_i^t를 습득하더라도 Alice의 헬퍼 비밀키 hk_{Alice}를 모르고서는 $TK_i^{t+1} = hk_{Alice}(H_1(PID_i, HP_i, t+1) - H_1(PID_i, HP_i, t))$를 계산하는 것이 어려우며 따라서 $t+1$ 주기의 서비스 개인키 $PSK_i^{t+1} = PSK_i^t + TK_i^{t+1}$를 계산할 수도 없다. 헬퍼 비밀키의 저장은 제안 기법에서는 분실의 위험이 없는 개인용 컴퓨터를 가정하였으므로 이를 통해 의사와의 세션 비밀키의 생성에 필요한 서비스 개인키의 갱신은 HKU를 소유한 사용자만이 가능함을 확인할 수 있다.

• 환자 신원정보의 익명성

환자는 신뢰기관 TA로부터 시스템에서 사용할 익명을 발급받아 사용한다. 환자는 발급받은 익명을 등록과정과 PHI 전송과정에서 실제 식별정보 대신 사용한다. 시스템의 다른 참여자인 HMS와 의사는 TA가 신뢰기관이고 환자 신원정보 PT_i에 대응하는 익명 PID_i가 안전한 채널을 통해 환자에게 발급되었다고 가정할 때 익명 PID_i을 통해 실제 환자의 신원정보 PT_i를 추적할 수 없다.

하지만 의사는 진단과정에서 큰 문제가 발견되거나 추가적인 정밀 검사가 필요할 경우 환자의 신원정보를 필요로 할 수도 있다. 즉 필요할 경우 환자의 익명 PID_i를 통해 환자의 신원정보 PT_i의 추적이 가능한 조건부 프라이버시(Conditional Privacy)를 만족하여야한다. 의사는 HMS를 통해 TA에 환자의 익명 PID_i의 추적을 요청하게 되고 TA는 요청의 타당성을 검증한 후 환자의 신원정보를 제공하게 된다. Yang의 제안기법에서도 마찬가지로 필요할 경우

HMS는 환자의 익명을 통해 실제신원을 확인할 수 있지만 익명의 발급기관과 서비스 제공자가 동일하기 때문에 서비스 제공자인 HMS에 대해서는 환자의 익명성을 보장할 수 없게 된다. 하지만 본 논문의 제안프로토콜에서는 환자의 익명의 발급과 서비스 제공자는 다른 개체로서 서비스제공자인 HMS는 전달하는 메시지에서 환자의 실제 신원정보를 추적할 수 없고 필요할 경우 TA에 요청하여 실제 신원정보의 추적이 가능하므로 환자의 신원정보에 대한 조건부 프라이버시를 보장할 수 있다.

• 환자가 선택한 의사의 신원정보의 기밀성

Yang이 제안한 기법은 네트워크를 통한 건강기록 전송 시 의사의 신원정보 노출을 보안의 대상으로 고려하지 않는 문제가 있었다. 의사의 신원정보가 노출되는 경우 비록 환자의 익명성은 보장되더라도 의사의 신원정보로부터 해당 의사의 전문 진료과목을 유추하여 환자의 병력과 같은 프라이버시 침해요인이 발생할 수 있으므로, 전송되는 건강정보로부터 의사를 식별할 수 있는 정보도 노출되지 말아야 할 필요가 있다. 이를 위해 제안 기법에서는 환자와 HMS ($PID_i - H$) 그리고 HMS와 의사($H - D_j$) 사이의 전송에서 암호화를 통해 정당한 수신자만 정보를 확인할 수 있도록 하였다. 3.5절에서 설명한 제안기법의 건강 기록 전송단계에서, 네트워크를 통한 전송과정에서 시스템 외부에서 메시지를 가로챌 경우 공격자는 메시지 $m = \{PID_i, ts, C_3\}$ 만을 획득할 수 있다. 이때 건강 기록 수신을 위한 의사 신원정보는 오직 HMS만 내용을 확인할 수 있도록 의사의 신원정보 D_j를 포함한 전체를 환자와 HMS사이에 공유하는 세션 비밀키 $K_{P-H} = \hat{e}(PSK_i^t, H_1(HMS))$를 사용하여 C_3 형태로 암호화되어 전송된다. HMS는 환자의 등록과정에서 $< PID_i, PSK_i^0, HK_i, HP_i >$를 저장해둠으로써 환자와 동일한 세션키를 생성하여 C_3를 복호화 한다. HMS는 메시지의 복호화를 통해 환자가 선택한 의사의 신원정보 D_j의 확인이 가능하고 앞서 가정한 신뢰할 수 있는 네트워크를 이용해 소속된 의사에게 전달한다. 외부 공격자는 메시지에서 오직 전송하는 환자의 익명과 타임스탬프만을 획득할 수 있다.

• 전송 PHI의 보호

환자는 선택한 의사 D_j와 비대화식 키 공유를 통해 생성한 키를 이용해 PHI를 암호화한다. 키는 $K = \hat{e}(PSK_i^t, H_1(D_j)) = \hat{e}(H_2(PID_i, SK_{D_j}))\hat{e}(H_2(PID_i HP_i, t), DP_i^j)$와 같이 계산되므로 오직 환자가 선택한 의사와 환자만이 계산 가능하므로 외부의 제 3자는 PHI에 접근할 수 없다. 이는 [11]에서 기술한 비대화식 키 분배 기법의 안전성 증명에 의해 해당 기법을 사용한 PHI의 전송에서의 기밀성을 보장할 수 있다.

• 안전한 채널을 가정하지 않은 환자의 비밀키 전달

Yang의 제안 기법에서는 HMS가 생성한 환자가 시스템에서 사용할 키 $< PSK_i^0, hk_i, HP_i >$를 안전한 채널을 사용하여 환자에게 전달한다고 가정한다. 본 논문에서는 신원기반의 암호화와 인증 기법을 사용하여 안전한 채널이 아닌 공개된 네트워크 환경에서도 환자의 키를 안전하게 전달하는 방법을 제안하였다. 환자는 TA로부터 익명과 함께 익명을 사용한 신원기반의 개인키 $SK_{PT_i} = s_0 H_1(PID_i)$를 발급받는다. 환자는 HMS에 등록과정에서 TA로부터 발급받는 SK_{PT_i}를 사용한 서명 $\sigma = IBSig(SK_{PT_i}, req)$를 생성하여 등록요청 메시지에 포함하여 전달한다. 신뢰기관 TA가 정당한 사용자에게만 익명과 함께 개인키를 발급했다고 가정할 때, HMS는 환자의 익명 PID_i를 사용한 서명의 검증을 통해 등록요청 메시지의 발신자가 정당한 사용자인지 확인할 수 있다. HMS는 환자를 위한 키 $m = \{PSK_i^0, hk_i, HP_i\}$를 환자의 익명 PID_i을 사용한 신원기반 암호화를 통해 $c = IBEnc(PID_i, m)$를 생성하여 환자에게 전달한다. 환자는 TA로부터 발급받은 SK_{PT_i}를 사용하여 복호화한 결과 $m = \{PSK_i^0, hk_i, HP_i\} = IBDec(SK_{PT_i}, c)$를 획득한다. 이를 통해 안전한 채널을 가정하지 않고도 등록과정에서 HMS에 대한 인증과 암호화를 통한 키의 안전한 전달이 가능하다.

4.2 성능분석

본 절에서는 제안된 건강정보 전송 보안 프로토콜의 효율성에 대해 분석한다. 3장에서 제안된 건강정보 전송 보안 프로토콜의 성능 분석을 위해 시스템에 참여하는 개체인 환자의 모바일 단말BH와 원격지 서버 HMS 그리고 의사의 단말로 구분하여 프로토콜 수행에 따른 암호기법의 연산량을 Yang 등의 기

Table 3. Computational costs for the proposed secure PHI transmission protocol

Proposed	Patient (BH)	HMS	Doctor
Registration	$1T_{pair}+2T_{mul}$	$3T_{pair}+4T_{mul}+1T_{exp}$	-
PHI transmission	$2T_{pair}+2T_{enc}+1T_{mac}$	$1T_{pair}+1T_{mul}+1T_{dec}$	$2T_{pair}+1T_{mul}+1T_{mac}$
Yang et al	Patient (BH)	HMS	Doctor
Registration	off-line		
PHI transmission	$2T_{pair}+2T_{enc}+1T_{dec}$	$3T_{pair}+2T_{enc}+1T_{dec}$	$2T_{pair}+2T_{dec}$

법과 비교하여 Table 3에 각각 나타내고 있다. 연산량 분석을 위한 주요 지표로서 신원기반 암호기법의 겹선형 페어링(T_{pair})과 스칼라 곱셈(T_{mul}), 대칭키 암호화(T_{enc})와 복호화(T_{dec}) 그리고 메시지 인증코드(T_{mac}) 연산을 고려하였다. 이때, 제안기법의 등록단계에서 연산량은 3.3절에서 사용되는 신원기반 암호(*IBEnc*)와 전자서명 기법(*IBSig*)으로 [9]와 [10]을 각각 가정하였을 때 소요되는 연산량으로 분석하였고, Yang 등은 등록과정을 오프라인과 같은 별도의 보안채널을 가정하였으므로 비교 대상에서 제외하였다. 건강기록 전송 메시지의 보안은 신원기반 암호기법의 비대화식 키 설정기법을 통해 생성된 비밀키를 기반으로 하므로 Table 3의 제안기법의 분석내용은 3장의 식 (6)과 식 (8)로부터 도출된 비밀키를 이용한 암호화와 메시지 인증코드 연산의 결과이다.

그리고 건강기록(PHI) 전송 메시지의 보안처리 수행시간을 평가하기 위해 공개 암호 라이브러리 PBC[14]와 jPBC[13]에서 제공하는 512비트 소수 p의 F_p에서 160비트 소수 q를 위수(Subgroup order)로 하는 타원곡선상에서 정의된 겹선형 페어링 연산을 이용하여 측정된 결과를 이용하여 Yang 등의 기법과 비교하였다. 이때, 환자의 BH의 성능은 사용자 스마트폰 단말 환경을 고려하여 갤럭시 S4 기기에서 측정된 수행시간을 고려하였고, 이에 반해 HMS 서버와 의사의 단말은 비교적 고성능을 가정하여 인텔 I7 2.4GHz PC에서 측정된 지표를 고려하였다.

환자의 건강정보 PHI는 HMS를 통해 담당 의사에게 분배되므로, 여러 환자로부터 수신된 PHI들을 효율적으로 처리하고 분배하기 위해서는 HMS 연산부담을 우선적으로 고려할 필요가 있다. Yang 등의 기법과 비교해서 제안기법은 환자와 의사에게 부담되는 연산량은 큰 차이가 없으나 HMS에 부가되는 연산은 Yang 등의 기법보다 더 효율적으로 처리될 수 있으며, Fig. 2는 HMS가 처리해야 하는 PHI의 개수에 따른 전체 처리 시간을 비교하여 나타내고 있다.

또한 여러 환자들로부터 HMS가 수신하는 PHI의 수신율에 따른 HMS에서의 메시지 처리시간을 측정하기 위해 M/D/1 대기모델을 이용하여 제안 프로토콜의 성능을 분석하였다[6]. 이러한 결과로 Fig. 3은 PHI 수신율의 변화에 따른 HMS에서의 예상 처리시간과 시뮬레이션을 통해 측정된 평균 처리시간을 나타내고 있고, Fig. 4는 10 msg/second의 비율로 HMS가 50개의 PHI를 수신하는 경우에 대해 메시지 보안처리에 따른 각 PHI의 대기 지연시간을 추적한 결과를 보여주고 있다. 이러한 결과로부터 짐작할 수 있듯이 제안 프로토콜은 HMS의 빠른 PHI 처리를 가능하게 하며 Yang 등의 기법에 비해 실시간성을 요구하는 원격 건강정보 전송서비스의 경우에 보다 효율적으로 적용될 수 있다.

5. 결 론

본 논문에서는 기존 Yang이 제안한 기법의 문제

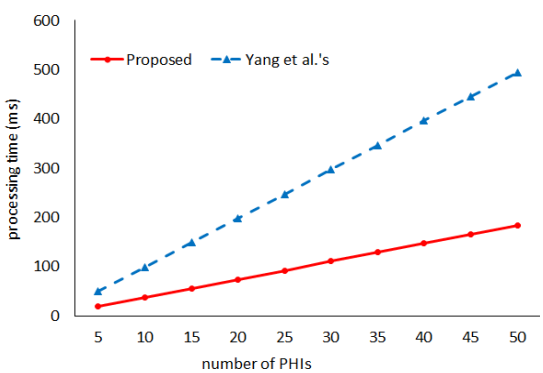

Fig. 2. Processing time of HMS according to the number of PHIs received.

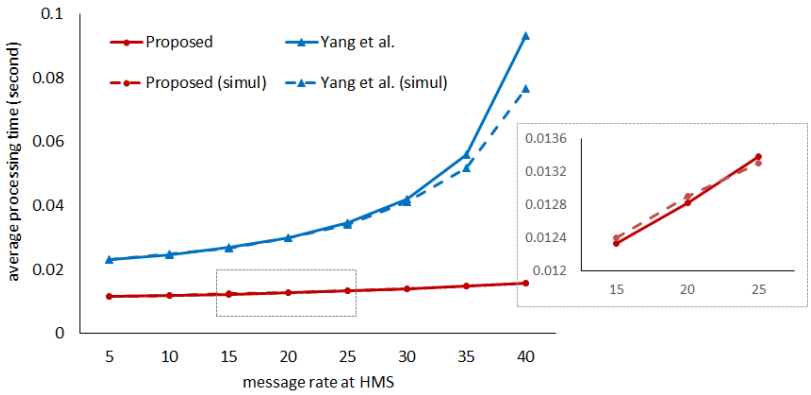

Fig. 3. Average processing delay depending on the PHI receiving rate at the HMS.

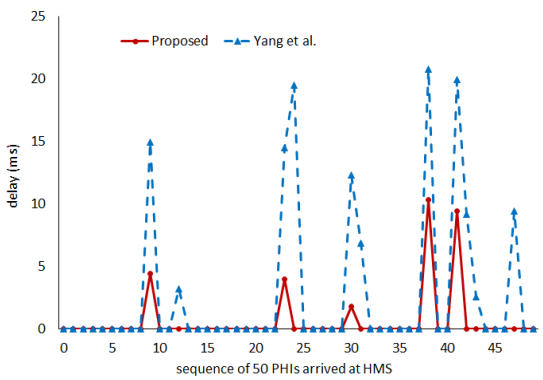

Fig. 4. Trace of queueing delay on the HMS for 50 PHIs sequentially received with 10msg/second rate.

점인 단일 헬퍼키의 문제를 모든 환자에게 고유한 헬퍼키를 부여함으로서 안전한 키 격리 기법을 적용하였고 이와 함께 PHI의 전송 간에 메시지에서 의사의 신원정보가 노출되는 것을 막기 위해 환자와 HMS간에 비대화식 공유 비밀키를 사용한 암호화를 이용해 제 3자의 전역적 도청으로 인한 의사의 신원정보의 노출을 해결하였다. 또한 Yang의 제안기법에서 안전한 채널 가정을 통해 HMS가 PHI 암호화 전송을 위해 사용하는 비밀키 전달을 가정하였으나, 본 논문에서는 이를 개선하여 TA로부터 발급받은 환자의 익명과 신원기반 암호기법을 사용하여 안전한 건강정보 전송 프로토콜을 설계하였다. 또한 안전성과 성능분석을 통해 제안방안이 기존 방안보다 우수함을 인증하였으며 제안 방안은 향후 고령화 사회에 따른 헬스케어 산업의 안정적인 정착과 구현에 도움이 될 것으로 기대한다.

REFERENCE

[1] G. Kim, and M. Park, "A Study on the Methods of Fault Analysis to Improve Safety in U-Healthcare System for Managing Emergency Rescue for Seniors," *Journal of Korea Multimedia Society*, Vol. 17, No. 2, pp. 170-179, 2014.

[2] K.S. Kwak, S. Ullah, and N. Ullah, "An Overview of IEEE 802.15.6 Standard," *Proceeding of IEEE International Symposium on Applied Sciences in Biomedical and Communication Technologies*, pp. 1-6, 2010.

[3] H.M. Chen, J.W. Lo, and C.K. Yeh, "An Efficient and Secure Dynamic ID-Based Authentication Scheme for Telecare Medical Information Systems," *Journal of Medical Systems*, Vol. 36, No. 6, pp. 3907-3915, 2012.

[4] T. Cao, and J. Zhai, "Improved Dynamic ID-Based Authentication Scheme for Telecare Medical Information Systems," *Journal of Medical Systems*, Vol. 37, No. 2, pp. 1-7, 2013.

[5] Q. Jiang, J. Ma, Z. Ma, and G. Li, "A Privacy Enhanced Authentication Scheme for Telecare Medical Information Systems," *Journal of Medical Systems*, Vol. 37, No. 1, pp. 1-8, 2013.

[6] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems," *IEEE Journal on Selected*

Areas in Communications, Vol. 27, No. 4, pp. 365-378, 2009.

[7] H. Yang, H. Kim, and K. Mtonga, "An Efficient Privacy-Preserving Authentication Scheme with Adaptive Key Evolution in Remote Health Monitoring System," *Peer-to-Peer Networking and Applications*, Vol. 8, No. 6, pp. 1059-1069, 2014.

[8] P. Gopal, and P.V. Reddy, "Efficient ID-Based Key-Insulated Signature Scheme with Batch Verifications using Bilinear Pairings over Elliptic Curve," *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 18, No. 4, pp. 385-402, 2015.

[9] D. Boneh, and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Proceeding of Advances in Cryptology-CRYPTO 2001*, pp. 213-229, 2001.

[10] J.C. Choon and J.H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," *Proceeding of Public Key Cryptography-PKC 2003*, pp. 18-30, 2003.

[11] R. Dupont and A. Enge, "Provably Secure Non-Interactive Key Distribution Based on Pairings," *Discrete Applied Mathematics*, Vol. 154, No. 2, pp. 270-276, 2006.

[12] J. Weng, S. Liu, K. Chen, and X. Li, "Identity-Based Key-Insulated Signature with Secure Key-Updates," *Proceeding of Information Security and Cryptology-Inscrypt 2006*, pp. 13-26, 2006.

[13] A. De Caro, and V. Iovino, "jPBC: Java Pairing Based Cryptography," *Proceedings of the 16th IEEE Symposium on Computers and Communications*, pp. 850-855, 2011.

[14] The Pairing-Based Cryptography Library, https://crypto.stanford.edu/pbc/ (accessed Dec., 26, 2016).

노 시 완

2016년 2월 부경대학교 IT융합응용공학과 졸업
2016년 3월~현재 부경대학교 대학원 정보보호학(협) 석사과정
관심분야 : 정보보호, 차량통신보안, 헬스케어 보안

박 영 호

2000년 2월 부경대학교 전자계산학과 졸업
2002년 2월 부경대학교 대학원 전자계산학과 석사
2006년 8월 부경대학교 대학원 정보보호학(협) 박사
2014년 7월~현재 부경대학교 전자정보통신연구소 전임연구원
관심분야 : 정보보호, 암호기술 응용, 통신보안, 인증, 키관리

이 경 현

1982년 2월 경북대학교 수학교육과 졸업
1985년 2월 한국과학기술원 응용수학과 석사
1992년 8월 한국과학기술원 수학과 박사
1985년 2월~1993년 2월: 한국전자통신연구원 연구원, 선임연구원
1993년 3월~현재: 부경대학 IT융합응용공학과 교수
관심분야 : 정보보호, 암호이론, 암호 프로토콜, 통신보안