http://dx.doi.org/10.14400/JDPM.2013.11.11.389

양자 암호를 이용한 유헬스케어 환경의 키 분배 모델 설계

정윤수*, 한군희**
목원대학교 정보통신공학과*, 백석대학교 정보통신공학과**

Quantum cryptography-used Key Distribution Model Design of U-healthcare environment

Yoon-Su Jeong*, Kun-Hee Han**
Dept. of Information Communication & Engineeringe, Mokwon University*
Dept. of Information Communication & Engineeringe, Baekseok University**

요 약 IT 기술과 의료기술이 융합되면서 환자의 체내에 의료장비를 부착한 환자의 수가 증가하고 있다. 그러나 환자의 생체정보를 제 3자가 악의적으로 도청 및 변경하는 문제점이 발생하고 있다. 본 논문에서는 환자와 병원관계자 사이에서 환자의 생체정보를 제3자가 도청하거나 변조없이 키를 공유하도록 양자 암호 기반의 키 분배 모델을 제안한다. 제안 모델의 양자 정보는 메시지 직접전달보다는 임의의 비트들을 전달하여 키를 공유하는 one-time pad 키를 사용한다. 또한, 제안 모델은 체내삽입장치의 생체정보가 제3자에게 불필요하게 노출되지 않아 환자의 익명성을 보장받는다.

주제어 : 유헬스케어, 양자 암호, 인증

Abstract As fusing IT and medical technique, the number of patients who adhere medical equipment inside of them is increasing. However there is a problem of for the third person to tap or modulate the patient's biometric data viciously. This paper suggests quantum encryption-based key distribution model to share key for the third person not to tap or modulate the patient's biometric data between patient and hospital staff. The proposed model uses one-time pad key that shares key sending random bits not direct sending message of quantum data. Also, it guarantees patient's anonymity because the biometric data of injected-device in the body doesn't be exposed unnecessarily.

Key Words : u-Healthcare, Quantum Cryptography, Authentication

1. 서론

최근 유헬스케어 서비스를 위해 사용되는 체내삽입장치는 다양한 종류의 소형, 휴대 가능한 장치로 사용되기 때문에 병원관계자(의사, 간호사, 약사 등)가 환자의 건강상태를 모니터링하고 개인화된 건강관리 서비스가 수행되고 있다.[1,2]

환자의 체내에 삽입되는 체내삽입장치는 심장질환이

Received 30 September 2013, Revised 20 October 2013
Accepted 20 November 2013
Corresponding Author: Kun-Hee Han(Baekseok University)
Email: hankh@bu.ac.kr

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.otg/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

나 당뇨병과 같은 만성질환을 가지고 있는 환자에게 사용되며 무선 통신 수행능력을 가지는 기능이 있다. 체내삽입장치는 무선 구간에서 환자의 생체정보가 송·수신되기 때문에 환자의 정보유출 사고 발생시 국가적인 혼란과 사회적 이슈가 야기될 수 있는 문제점이 있다.[3,4,5,6].

제3자는 체내삽입장치를 부착한 환자의 생체 정보를 환자에게 근접하지 않고 의료장비의 기능을 모니터링하고 변경함으로써 쉽게 체내삽입 장치의 도청 공격할 뿐만 아니라 체내삽입장치의 리더 기능을 가지는 이동전화를 통하여 환자의 개인 정보를 손쉽게 얻을 수 있다[7,8].

현재까지 연구된 전통적인 체내삽입장치에 대한 보안 기법은 다음과 같은 문제점이 있다. 첫째, 체내삽입 장치의 여러 자원 제약(에너지 공급, 프로세싱, 저장)에 의해서 체내삽입장치에 직접적으로 적용할 수 없다. 둘째, 체내삽입 장치의 배터리를 수시로 교체할 수 없어 체내삽입 장치의 자원을 효율적으로 관리할 수 없다. 셋째, 생체정보 신호를 보호하기 위해 사용되는 키가 게이트웨이 역할을 하는 중재자가 공유하기 때문에 제3자에 의한 도청이 가능하다.

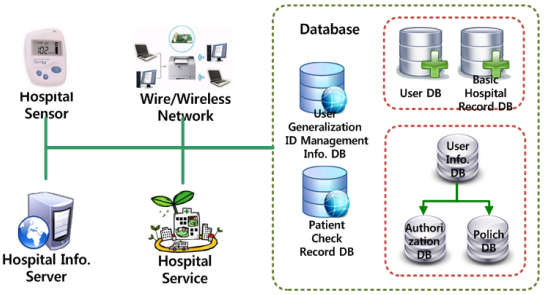
본 논문에서는 유헬스케어 서비스를 제공받는 환자와 서비스를 제공하는 병원관계자 사이에 어떤 비밀 정보도 갖고 있지 않도록 함으로써 제3자의 도청이나 변조가 없이 키를 공유하는 키 분배 모델을 제안한다. 제안한 모델은 양자암호체계의 불확정성의 원리와 편광 등의 특성을 통하여 체내삽입장치의 생체 신호가 제3자에 의해 도청되거나 변조되었는지를 확인함으로써 기존 암호체계보다 안전성을 높이면서 키를 분배한다. 특히, 제안 모델은 충분한 임의의 비트를 전달하여 키를 공유하는데 양자정보를 사용함으로써 one-time pad의 공유키를 사용한다. 또한, 체내삽입장치의 생체정보가 제3자에게 불필요하게 노출되지 않도록 양자 상태를 사용하여 병원관계자에게 안전하게 생체정보를 전달할 수 있어 환자의 익명성을 보장받도록 하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 체내삽입장치를 가지는 유헬스케어 시스템과 양자 역학 기반의 키 분배 프로토콜에 대해서 알아본다. 3장에서는 양자 암호를 이용한 키 분배 모델을 제안하고, 4장에서는 제안 모델의 보안평가와 성능평가를 분석하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 유헬스케어 시스템과 체내삽입장치

유헬스케어 시스템은 IT 기술에 의료서비스를 접목함으로써 환자의 건강 관련 정보를 병원관계자(의사, 약사, 간호사 등)이 언제, 어디서나 수집, 처리, 전달, 관리할 수 있게 함으로써 환자가 질병을 예방하고 관리하는 새로운 형태의 건강관리 및 의료 서비스이다[1].



[Fig. 1] Service Concept of U-healthcare with Implantable Device

유헬스케어 시스템에서는 다양한 종류의 소형, 휴대가능한 장치들이 인체내부에 삽입되어 유헬스케어 시스템과 연동되면서 환자의 건강상태를 모니터링하고 환자의 건강관리 서비스를 제공하고 있다[2]. 체내삽입장치는 환자의 생체정보를 수집하기 위해서 환자 몸에 부착함으로써, 심장질환이나 당뇨병과 같은 만성질환에 폭넓게 사용된다. 그리고 많은 체내삽입장치들이 무선 통신 수행능력을 가지고 있기 때문에 외부 프로그래머/리더와 무선 통신이 가능하다[3].

그림 1은 환자 신체에 체내삽입장치를 삽입하여 병원관계자로부터 의료서비스를 제공받는 개념도를 보여주고 있다. 그림 1처럼 유헬스케어 시스템에서 사용되는 체내삽입장치는 환자의 생체정보를 병원관계자가 수집·처리할 수 있도록 전송하면 병원관계자는 데이터베이스에 저장된 환자 진료기록을 이용하여 환자 상태를 진단한다. 병원관계자는 환자 정보를 전달받은 후 판독 및 진찰하는 역할을 수행한다. 체내삽입장치를 부착한 환자는 응급상황이 발생할 경우 타병원으로 진찰을 요청하거나 외부 장치를 통해 환자의 상태를 본인의 상태를 확인할 수 있다.

2.2 양자 역학 기반의 키 분배 프로토콜

양자 역학에서 파동과 입자 개념은 물체를 나타내는데 사용되며, 동일한 물체라 할지라도 상황에 따라 파동의 측면을 드러낼 수 도 있고 입자의 측면을 드러낼 수 있다.

양자컴퓨터에서는 정보의 최소 단위인 양자 비트 또는 큐빗을 사용한다. 큐빗은 불연속적인 두 양자 역학계를 |0>, |1>로 나타내어 직교기저(orthogonal basis), 인지 아니면 정규직교기저(orthonormal basis)로 하는 2차원 Hilbert 공간에서의 임의 상태를 표현한다.

큐빗의 일반적인 상태는 a|0> + b|1>로 표현한다. 여기서 a와 b는 $|a|^2+|b|^2=1$인 복소수의 관계를 의미하며 $|a|^2$와 $|b|^2$의 값이 각각 0과 1로 측정될 확률로 나타낸다. 양자 역학을 이용한 양자 키 분배 프로토콜은 1984년 Bennet와 Brassard에 의해서 처음 제시된 프로토콜(BS84 프로토콜)로써 불확정성 원리를 기반으로 하고 있다. 이 프로토콜은 키를 분배하는 프로토콜이다.

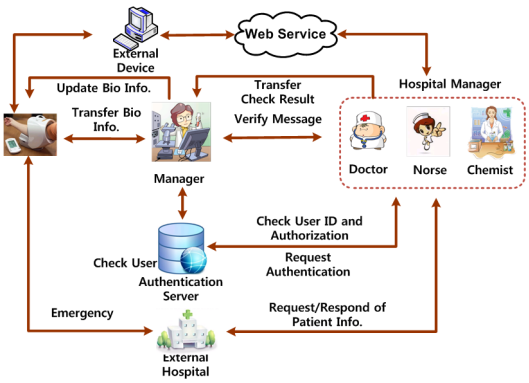
D. Bruss는 BS84 프로토콜을 six-state 프로토콜로 일반화하였고, A. Ekert는 양자역학의 양자 얽힘을 기반으로 한 E91 프로토콜을 개발하였다[9]. 이 프로토콜은 양자 얽힘이 비국소성을 가지는 것이 특징이다. C. Bennett. et. al 등은 양자 얽힘 기반의 프로토콜로 전환될 수 있음을 증명하였다. 양자 키 분배 프로토콜과 고전의 키 분배 프로토콜의 차이점은 상태 분배 과정에서 양자 상태에 0과 1의 값을 대응시키는 점이다.

3. 양자 암호를 이용한 키 분배 모델 설계

유헬스케어 환경에서는 환자의 생체정보를 악의적으로 수집하여 환자의 동의 없이 사용하는 보안 문제점이 있다. 이 장에서는 환자와 병원관계자간 사전에 어떤 정보도 갖고 있지 않은 상태에서 제3자의 도청이나 변조가 없이 키를 공유하여 환자의 개인 정보를 보호하는 모델을 제안한다.

3.1 개요

병원관계자은 환자의 체내삽입장치 안에 생체정보를 수집 및 검사하기 위해서는 환자의 생체신호를 무선구간에서 시그널 신호로 전달받아야 한다. 이때, 무선구간에서 발생되는 환자의 생체정보 신호를 제3자가 불법적으로 도청하거나 변조할 수 있다. 제안 모델에서는 이 구간에서 발생되는 환자의 생체정보를 도청하거나 변조 없이 병원관계자에게 전달하기 위해서 양자 암호를 이용하고 있다. 제안 모델에서 양자 암호를 이용하는 이유는 양자 역학 측정이 양자 상태의 붕괴를 수반하여 원래 정보의 상태를 변형시키기 때문에 도청 시도의 여부를 거의 완벽하게 판단할 수 있기 때문이다.



[Fig. 2] Proposed Model for Privacy Security of Patient

그림 2은 환자의 개인 정보를 보장하기 위한 제안 모델을 보여주고 있으며, 그림 2은 체내삽입장치, 게이트웨이 역할을 수행하는 관리자 또는 위장자(Cloaker), 병원관계자, 인증서버 등으로 구성된다.

체내삽입장치는 태그와 같은 센서로 구성되고 신뢰성이 있다거나 악의적으로 사용할 수 있다는 가정을 만들지 않으며 서비스 전에 공유키를 부여 받아 환자의 생체정보를 수집한다. 관리자는 체내삽입장치와 병원관계자 사이에서 중재자와 같은 게이트웨이 역할을 수행한다. 병원 관계자는 환자의 생체정보를 관리자로부터 전달받아 데이터를 판독 및 진료하는 역할을 수행한다. 인증서버는 환자의 체내삽입장치나 의료관계자 정보(권한 및 레벨 등)을 저장 및 관리하는 역할을 수행한다.

3.2 용어

[표 1]은 제안 모델에서 사용되는 용어를 정의하고 있다.

〈Table 1〉 Definition of Notation

Notaion	Definition
p	Patient
m	Manager
h	Hospital
BI_X	Bio. information of X
GHZ	Greenberger-Home-Zeilinger
$\|\psi>$	GHZ State Value

3.3 GHZ 상태 정보를 이용한 키 분배

이 절에서는 양자 암호의 GHZ (Greenberger-Home-Zeilinger)를 이용하여 환자의 생체정보 신호를 제3자가 불법적으로 도청하거나 변조하는 것을 예방하기 위한 모델을 제안한다. 제안 모델에서 관리자는 키 분배에 관여하지만 분배된 키에 대해서는 어떠한 정보도 알 수 없도록 한다.

3.3.1 초기화 과정

초기화 과정은 환자와 병원관계자의 신원을 보증하기 위한 단계로써, 신원보증은 관리자가 GHZ (Greenberger-Home-Zeilinger) 입자를 키 분배 이전에 환자와 병원관계자에게 전달한다. 초기화 과정은 두 단계로 이루어진다.

· 1단계 :

병원관계자가 환자의 생체정보를 수집하기 위해서 관리자에게 환자의 생체정보 수집 요청 메시지를 전달하면, 관리자는 병원관계자의 요청 메시지를 해당 환자에게 전달한다.

· 2단계 :

환자는 임의의 비트 수열(0과 1로 구성된 수열)을 식 (1)처럼 N개 생성하여 관리자에게 전달한다. 전달된 임의의 비트 수열을 식 (2)처럼 GHZ 상태 $|\psi>$로 생성한다. 이때, 관리자는 생성된 GHZ 상태 $|\psi>$를 편광시킬 편광판(십자형 혹은 대각형)을 무작위로 선택한다.

$$Generate \quad s \cong \{0,1\}^{*} \rightarrow \{0,1\}^{N} \tag{1}$$

$$|\psi>=\frac{1}{\sqrt{2}}(|s>_{pmh}+|\bar{s}>_{pmh}) \tag{2}$$

여기서, p은 환자, m은 관리자, h는 병원관계자를 의미한다. ($\bar{s}$은 무슨 의미인지?)

3.3.2 키 분배 과정

키 분배 과정은 관리자가 각각의 비트를 편광판으로 편광시켜 $|\psi>$의 첨자가 p인 것은 환자에게 h는 병원관계자에게 m인 것은 관리자가 보관하도록 평광된 $|\psi>$ 정보를 환자와 병원관계자에게 전달한다.

· 1단계 :

환자의 생체정보에 해당하는 편광정보 $|\psi>$를 관리자가 환자와 병원관계자에게 각각 전달하면, 환자와 병원관계자는 각각의 비트를 편광판으로 편광시킬 때, 비트가 0인 경우 십자형 편광판에서는 식 (3)처럼 $|\psi>$을 －로 편광시키고, 대각형 편광판에서는 식 (4)처럼 $|\psi>$을 ／로 편광시킨다.

$$|0^{o}> = \frac{1}{\sqrt{2}}(|45^{o}>_{pmh} - |135^{o}>_{pmh}) \tag{3}$$

$$|45^{o}> = \frac{1}{\sqrt{2}}(-|0^{o}>_{pmh} + |90^{o}>_{pmh}) \tag{4}$$

만약 비트가 1인 경우 십자형 평광판에서는 식 (5)처럼 $|\psi>$을 |로 편광시키고, 대각형 편광판에서는 식 (6)처럼 $|\psi>$을 ＼로 편광시킨다.

$$|90^{o}> = \frac{1}{\sqrt{2}}(|45^{o}>_{pmh} + |135^{o}>_{pmh}) \tag{5}$$

$$|135^{o}> = \frac{1}{\sqrt{2}}(-|0^{o}>_{pmh} - |90^{o}>_{pmh}) \tag{6}$$

· 2단계 :

환자와 병원관계자는 관리자가 전송한 환자의 생체정보를 이용하여 GHZ 상태 $|\psi>$을 생성한다. 관리자는 무작위로 생성한 GHZ 상태 $|\psi>$의 각 비트를 환자와 병원

관계자에게 전송한다. 환자와 병원관계자는 GHZ 상태 $|\psi>$의 각 비트들을 측정하기 위해서 십자형 편광판과 대각형 편광판을 임의로 바꿔가며 측정한다.

· 3단계 :

환자와 병원관계자는 같은 비트를 공유하기 위해서 그렇지 못한 비트들을 제거하는 작업을 수행한다. 병원관계자는 측정에 사용된 편광판의 순서를 환자에게 알려준다. 동일한 방법으로 환자 또한 편광판 중에서 환자가 사용한 편광판만을 병원관계자에게 알려준다.

· 4단계 :

환자와 병원관계자는 동일한 편광판으로 사용한 정보만을 수집하여 비트의 수열을 생성한다. 이 때, 생성된 수열은 환자와 병원관계자의 공유키로 사용한다.

3.3.3 검증 과정

이 단계는 환자와 병원관계자가 같은 비트의 수열을 공유하는 것을 검증하는 단계이다. 환자와 병원관계자가 동일한 편광판을 사용하여 정보를 수집하는 과정 중에 도청이 없었다면 비트 수열을 그대로 키로 사용해도 무방하다. 제안 모델에서는 도청이 발생할 수 있는 상황을 대비하기 위해서 다음과 같은 과정을 수행한다.

· 1단계 :

병원관계자는 병원관계자가 편광판을 통해 생성한 비트 정보가 정상적인 정보인지를 검증하기 위해서 수집된 비트 수열 중에서 일부를 환자에게 공개한다.

· 2단계 :

환자는 병원관계자가 공개한 비트 수열 정보를 확인한다.

· 3단계 :

환자는 병원관계자가 공개한 비트 수열 값이 이전에 병원관계자에게 전송한 비트 수열과 일치하는지 검증한다. 만약 정보가 일치하지 않는다면 도청이 있었던 것이므로 교환된 비트 수열을 전부 버리고 그렇지 않다면 도청이 없었다는 것을 의미하므로 비트 수열을 공유키로 사용한다.

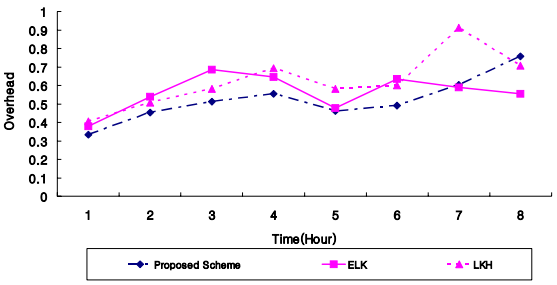
4. 평가

4.1 보안평가

제안 모델은 환자와 병원관계자 사이에서 교환되는 생체정보를 암호화하기 위해서 GHZ 상태 정보를 이용한 키를 이용하여 기밀성을 제공하고 있다. 특히, 제안 모델에서 제3자가 도청한다고 가정할 때, 환자의 큐빗에 대한 측정치를 알 수 없기 때문에 분배되는 키가 무엇인지 알 수 없다. 환자가 병원관계자에게 송신하는 생체신호의 무결성을 보장하기 위해서 제안 모델에서는 큐빗의 GHZ 상태 정보를 전달할 때 제3자는 병원관계자의 큐빗 측정치를 알지 못하기 때문에 환자의 생체신호의 무결성을 보장받는다. 모든 체내삽입장치들은 GHZ 상태를 이용하여 인증을 수행하기 때문에 환자와 병원관리자 사이에 공유된 키는 관리자에게 노출되지 않으면서 안전하게 사용되어 안전성과 신뢰성이 보장받는다.

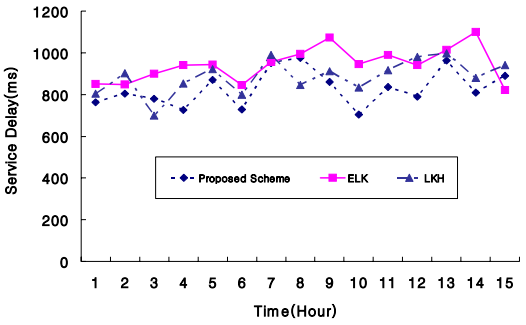
4.2 성능평가

제안 기법에서는 유헬스케어 환경에서 환자와 병원관계자 사이의 통신 오버헤드를 평가하기 위해서 OPNET 시뮬레이터를 이용하여 GKMP[10], LKH[11]과 비교 평가하였다. 그림 3처럼 제안 기법은 기존 기법과 달리 양자 키 분배를 이용하기 때문에 추가적인 정보 없이 환자의 생체정보를 전달하기 때문에 환자와 병원관계자 사이의 무선구간에서 발생하는 통신 오버헤드가 다른 기법에 비해 6.8% 낮게 나타났다. 이 같은 결과는 환자가 부착한 체내삽입장치의 센서들의 수에 따라 2.7% 차이가 났지만 전체 처리량에 비해 큰 차이를 보이지 않았다.



[Fig. 3] Communication Overhead between Patient and Hospital Manager

그림 4는 환자와 병원관계자 사이의 서비스 지연을 GKMP, LKH, SGKMP기법과 비교한 결과이다. 비교 평가 결과 시간대별 서비스 지연은 200ms 차이를 보이고 있지만 평균 서비스 지연 시간은 평균 40ms로 큰 차이가 나지 않는 결과를 보였다.



[Fig. 4] Service Delay between Patient and Hospital Manager

5. 결론

유헬스케어 환경에서 체내삽입장치를 사용하는 환자가 증가하고 있지만 환자의 생체정보를 악의적으로 이용하는 보안 문제도 증가하고 있는 추세이다. 본 논문에서는 GHZ 상태 정보를 이용하여 환자와 병원관계자 사이에서 환자의 생체 정보를 병원관계자에게 전달하는 관리자는 환자와 병원관계자 사이의 키 분배 내용을 알지 못하게 함으로써 제3자의 도청 및 신호 변경을 예방하여 환자와 병원관계자간 쌍방 인증을 안전하게 수행하기 때문에 신뢰도도 높게 나타났다. 향후 연구에서는 병원관계자(의사, 약사, 직원)와 체내삽입장치 사이에 안전한 ID를 통합관리하기 위한 모델을 설계 할 예정이다.

REFERENCES

[1] D. W. Kim, J. W. Han, and K. I. Chung, "Trend of Home Device Authentication/Authorization Technology", Weekly IT BRIEF, No. 1329, pp. 1-11, 2008.

[2] S.Y. Lee, K.B. Yim, K.J. Bae, Taeyoung Jeong, and Jong-Wook Han, "Counterplan of Ubiquitous Home Network Privacy based on Device Authentication and Authorization," Korea Institute of Information Security & Cryptology, Review of KIISC, 18(5), pp.125-131, 2008.

[3] T. Denning, Y. Matsuoka, and T. Kohno, "Neurosecurity: Security and Privacy for Neural Devices", Neurosurgical Focus, Vol. 27, Jul. 2009.

[4] D. Panescu, "Emergingg technologies: wireless communication systems for implantable medical devices", Engineering in Medicine and Biology Magazine, vol. 27, pp. 96-101, Mar.-Apr. 2008.

[5] D. Halperin, T. S. Heydt-Benjamin, B. Ransford et al., "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses", in Proc. of SP'08, pp. 129-142, May. 2008.

[6] P. Inchingolo, S. Bergamasco, and M. Bon, "Medical data protection with a new generation of hardware authentication tokens", in Proc. of Mediterranean Conf. on Medical and Biological Engineering and Computing, pp. 12-15, Jun. 2001.

[7] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proxymity-based Access Control for Implantable Medical Devices", 16th ACM conference on Computer and communications security, pp. 411-419, Nov. 2009.

[8] Z. Omary, f. Mtenzi, B. Wu, C. O'Driscoll, "Accessing sensitive patient information in ubiquitous healthcare systems", 2010 International conference for internet Technology and Secured Transactions(ICITST), pp. 1-3, Nov. 2010.

[9] H. Y. Lee, G. H. Cho, and H. J. Yang, "quantum key distribution protocol",Korea Institute of Information Security & Cryptology, Vol. 12, No. 5, pp.1-7. Oct. 2002.

[10] H. Harney, C. Muckenhirn, "Group Key Management Protocol(GKMP) Specification", RFC 2093, July 1997..

[11] Z. H. Liu, Y. X. Lai, X. B.. Ren, S. P. Bu ,"An Efficient LKH Tree Balancing Algorithm for Group

Key Management", ICCECT 2012, pp. 1003-1005, Dec. 2012

정 윤 수(Jeong, Yoon Su)

- 2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월 : 충북대학교 대학원 전자계산학 박사
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
- 관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail: bukmunro@gmail.com

한 군 희(Han, Kun Hee)

- 2000년 2월 : 충북대학교 컴퓨터공학과(공학박사)
- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 멀티미디어, 정보보호
- E-Mail : hankh@bu.ac.kr