# 타원곡선암호 알고리즘을 이용한 개인건강기록 암·복호화 시스템 설계

심재성*, 윤성열**, 박석천***
*,**가천대학교 IT대학 전자계산학과
***가천대학교 IT대학 컴퓨터공학과
e-mail : scpark@gachon.ac.kr

# Design of Personal Health Records Encryption and Decryption System Using Elliptic Curve Cryptography Algorithm

Jae-Sung Shim*, Sung-Yeol Yun**, Seok-Cheon Park***
*,**Dept of Computer Science, Gachon University
***Dept of Computer Engineering, Gachon University

요 약

본 논문에서는 사용자에게 PHR(PHR : Personal Health Record) 서비스를 제공 할 때 발생 가능한 개인정보변조 및 유출에 대한 위협에 대응하기 위하여 PHR과 ECC(ECC : Elliptic Curve Cryptosystem)에 대한 연구 및 안전한 개인정보 전송을 위한 XML 형식의 PHR 서비스 메시지 구조설계와 ECC 알고리즘 기법을 이용한 PHR 암·복호화 시스템을 설계하였다.

## 1. 서론

최근 건강관리에 대한 관심이 증가하면서 개인건강기록(이하 PHR)에 대한 관심 또한 증가하고 있다. PHR 서비스는 전자의무기록(EMR : Electronic Medical Record)을 시행중인 병원들 간의 연계를 통한 전자건강기록(EHR : Electronic Health Records)을 병원 중심이 아닌 환자 중심으로 서비스하는 것이다[1,2].

그러나 PHR 정보범위에는 환자의 개인정보가 포함되어 있으며 이는 PHR을 서비스를 제공 할 때 개인정보변조, 유출 등의 위협에 노출되어 있다.

이러한 위협에 대응하기 위하여 본 논문에서는 환자에게 PHR 서비스를 제공 할 때 타원곡선암호화(이하 ECC) 알고리즘을 적용하여 정보를 전송하는 시스템을 제안한다.

본 논문의 구성은 서론에 이어 2장에서는 관련연구로 PHR 서비스와 ECC 알고리즘에 대해 분석하고, 3장에서는 PHR 서비스를 위한 메시지 구조와 ECC 알고리즘을 이용한 PHR 암·복호화 시스템을 설계 하였고, 마지막으로 4장에서 결론을 기술한다.

* 가천대학교 일반대학원 전자계산학과 석사과정
** 가천대학교 일반대학원 전자계산학과 박사과정
*** 가천대학교 IT대학 정교수(교신저자)

## 2. 관련연구

### 2.1 개인건강기록(Personal Health Record)

PHR 서비스는 병원에서 환자의 정보를 관리하기 위해 사용되고 있는 EMR 시스템을 병원중심의 EHR이 아닌 환자 및 사용자 중심으로 서비스하기 위하여, 환자 개인이 자신의 건강에 관한 정보와 접근이 허용된 타인이 정보를 유지하고 관리할 수 있게 서비스하는 것이다.

이는 환자의 중복처치 및 진료과정의 간결화 효과와 함께 진료비용과 진료시간의 절감이 가능할 것으로 기대된다. 또한 환자가 자신의 질병관리에 있어 능동적인 대처가 가능하다[3].

### 2.2 타원곡선암호(Elliptic Curve Cryptosystem)

타원곡선암호 알고리즘은 유한체 위에서 정의된 타원곡선 군(Group)에서의 이산대수 문제의 어려움에 기초한 암호 알고리즘이다. Elliptic Curve는 약 150년 전부터 수학적으로 광범위한 연구가 있어 왔다.

ECC 알고리즘은 약 10년 전부터 1bit(비트)당 안전도가 타 공개키 기반 암호 알고리즘보다 효율적이라고 알려져있다. RSA(Rivest Shamir Adleman) 암호 알고리즘의 근간이 되는 인수분해 문제와 소수성 테스트를 위한 효율적인 알고리즘을 제공하기도 한다[4].

## 3. 타원곡선암호 알고리즘을 이용한 개인건강기록 암·복호화 시스템 설계

### 3.1 PHR 서비스 메시지 구조 설계

본 논문에서 제안하는 ECC 알고리즘을 이용한 PHR 암·복호화 시스템은 XML 형식의 메시지 구조를 사용한다. 그림 1은 사용자가 환자기본정보를 요청할 때 사용되는 메시지 구조를 설계한 것이다.

```
<Request>
 <Type>PatientBasicInformation</Type>
 <HospitalID>병원 아이디</HospitalID>
 <UserID>사용자 아이디</UserID>
 <PatientID>환자 번호</PatientID>
</Request>
```

(그림 1) 환자기본정보 요청 메시지 구조

기본적으로 병원 아이디와 함께 사용자 아이디, 조회하려는 환자번호에 대한 정보가 요구된다. 그림 2는 환자기본정보 요청에 대한 응답 메시지 구조를 설계한 것이다.

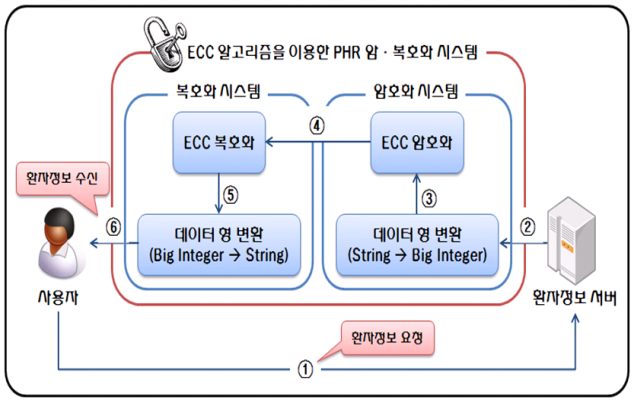
```
<Response statusCode="0">
 <PersonalInformation>개인정보 레코드
  <PatientName>환자명</PatientName>
  <Gender>성별</Gender>
  <Age>나이</Age>
  <ResidentID>주민등록 번호</ResidentID>
  <Address>주소</Address>
  <PhoneNumber>전화 번호
    <CellPhoneNumber>핸드폰 번호<CellPhoneNumber>
  </PhoneNumber>
  <Email>이메일<Email>
  <DetailsOfVisits>내원 경위</DetailsOfVisits>
 </PersonalInformation>
 <PhysicalHistory>건강상태 레코드
  <Physician>진료교수</Physician>
  <MedicalHistory>병력</MedicalHistory>
  <Allergy>알레르기</Allergy>
 </PhysicalHistory>
</Response>
```

(그림 2) 환자기본정보 응답 메시지 구조

그림 1과 그림 2는 환자의 기본정보를 환자 본인 또는 환자가 정보접근을 허가한 의료진 및 가족이 환자의 정보를 조회시 발생되는 메시지 구조로써 병원에서 관리하는 환자에 대한 기본적인 정보가 포함되어 있으며 입력되는 정보는 String 형식이다.

### 3.2 시스템 설계

ECC 알고리즘을 이용한 PHR 암·복호화 시스템은 PHR 서비스 제공시에 사용자의 개인정보 유출을 방지하기 위하여 PHR 정보를 ECC 보안 시스템을 경유해서 데이터를 암호화하여 전송한다. 이를 사용자가 수신 받을 때는 복호화하여 수신 받는다. 그림 3은 ECC 알고리즘을 이용한 PHR 암·복호화 시스템 구조도 이다.




(그림 3) ECC 알고리즘을 이용한 PHR 암·복호화 시스템

ECC 알고리즘을 이용한 PHR 암·복호화 시스템의 동작 절차는 다음과 같이 설계하였다.

① PHR 서비스의 사용자는 환자정보를 조회하기 위하여 서버에 환자정보 요청 메시지를 전송
② 환자정보 서버는 요청받은 환자의 정보를 ECC 알고리즘을 이용한 PHR 암·복호화 시스템의 데이터 형 변환 모듈로 전송
③ 데이터 형 변환 모듈에서는 입력받은 환자정보 String 형식의 데이터를 ECC 암호화를 위하여 Big Integer 형식의 데이터로 변환 ECC 암호화 모듈로 전송
④ ECC 암호화 모듈은 입력받은 Big Integer 형식의 데이터를 암호화 하여 수신자 측의 ECC 복호화 모듈로 전송
⑤ ECC 복호화 모듈은 입력받은 ECC 암호화 데이터를 다시 복호화 하여 복호화된 값을 데이터 형 변환 모듈로 전송
⑥ 데이터 형 변환 모듈에서는 복호화된 Big Integer 형식의 환자정보를 사용자가 조회 가능한 String 형식의 데이터로 변환하여 사용자에 전송

제안하는 시스템은 서비스되는 PHR 정보를 암호화 하여 사용자에게 서비스함으로써 서비스 도중 발생 가능한 정보변조 및 유출 등의 위협에서 환자의 개인정보를 안전하게 서비스 할 수 있다.

## 4. 결론

본 논문에서는 정보를 전송하는 과정에서 개인정보를 보호하기 위해 XML 메시지 구조를 설계하고, 이를 기반으로 하는 ECC 알고리즘을 이용한 PHR 암·복호화 시스템을 설계하였다.

제안하는 시스템은 암호화 및 복호화 시스템으로 분류하였고, 암호화 시스템은 암호화를 위한 데이터 형 변환(String->Big Integer) 모듈과 ECC 암호화 모듈로 구성하였으며, 복호화 시스템은 ECC 복호화 모듈과 사용자가 조회 가능한 형태의 데이터로 변환 시켜주는 데이터 형 변환(Big Integer->String) 모듈로 설계하였다. 제안하는 시스템은 서비스되는 환자의 정보를 암호화 하여 사용자에게 전송함으로써 환자의 개인정보를 보호하는 기능을 한다.

향후에는 제안하는 메시지 구조를 기반으로 하는 프로토콜을 설계하고 구현할 예정이다.

## ACKNOWLEDGMENT

"본 연구는 지식경제부 및 정보통신산업진흥원의 'IT융합 고급인력과정 지원사업'의 연구결과로 수행되었음" (NIPA-2012-H0401-12-1001)

## 참고문헌

[1] kim Yoo-jun, Kwon Hoon, Kwak Ho-young., "A integration system of medical information using Web service", Dept. of Computer Engineeringm Cheju National University, KOSTI 2007.

[2] The National Alliance for Health Information Technology. Defining Key Health Information Technology Terms. 2008.

[3] Johnston, D. et al., "A Framework and Approach for Assessing the Value of Personal Health Records(PHRs)", AMIA 2007 Symposium, 2007.

[4] 염헌영, 강수용, 김현주, 최순호, "대칭키/공개키 암호 알고리즘의 키 길이 따른 안전도 비교 분석 및 관련 S/W 개발", 정보통신연구진흥원 학술기사, 2001