ECC 알고리즘을 이용한 의료정보 교환 프로토콜 설계

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

Design of Health Information Exchange Protocol Using ECC Algorithm

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

요 약

본 논문에서는 병원과 외부서비스 간의 의료정보 교환 프로토콜을 설계하고, 설계한 프로토콜에 ECC 알고리즘을 적용하였다. 이를 위하여 관련연구로 CCR, ECC 알고리즘에 대해 분석하고, 의료정보 교환 프로토콜을 정의하였으며, 병원과 외부 서비스 간의 정보를 구분하고, ECC 알고리즘을 적용한 의료정보 교환 프로토콜을 설계하였다.

1. 서론

최근 연구되고 있는 병원 정보를 이용한 각종 서비스는 병원을 직접 다니지 않으면서 개인이 고품질의 의료 서비스 혜택을 받기 위한 것을 의미한다. 이는 개별적으로 서비스 될 뿐만 아니라 병원과의 연계를 통해 더욱 신뢰성 있는 정보를 받을 수 있는 개념으로 확대되고 있다.

그러나 이런 개인정보 및 의료정보의 경우 보안의 이슈가 끊임없이 대두되지만 국내나 국외에 실제로 서비스 될 때에 시장 도입기에 해당되기 때문에 서비스 구현에만 초점이 맞춰져 연구되고 있다.

본 논문에서는 이런 의료정보를 이용한 각종 서비스를 구현하는데 있어서 필요한 병원과 서비스와의 연동 시스템에서의 의료정보 교환 프로토콜을 설계한다. 또한 이렇게 설계된 프로토콜에 보안 알고리즘을 적용하여 안전한 의료정보 전송 시스템을 설계하였다.

2. 관련연구

2.1 CCR(Continuity of Care Record)

CCR은 환자의 건강상태와 진료에 관한 현재와 과거의 관련 정보로 구성된다. 즉, 환자의 건강관리에 대하여 관련된 가장 중요하고, 핵심적 자료의 집합이다. CCR은 환자의 건강상태와 진료에 관한 현재와 과거의 관련 정보로 구성된다[1].

이 표준에는 환자정보와 의료서비스제공자 정보, 보험정보, 환자의 건강상태정보(예를 들면 알레르기, 투약, 맥박, 호흡, 체온, 혈압, 진단, 최근의 처치 등)나 사전의료지시, 미래의 진료 계획에 대한 조언, 환자진료의뢰의 이유 등의 정보가 들어있다.

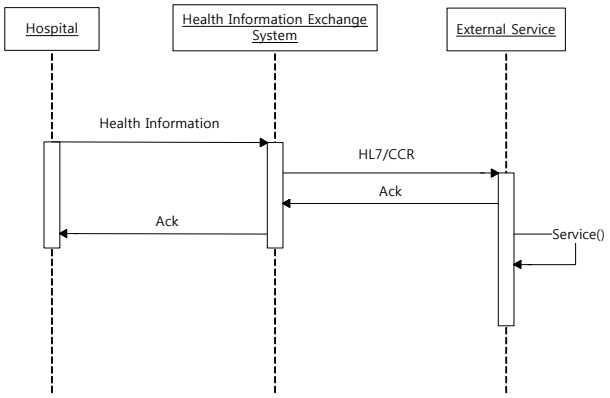
2.2 ECC

유한체(finite fields)위에서 정의된 타원곡선 군에서의 이산대수 문제에 기초한 타원곡선 암호시스템(ECC, Elliptic Curve Crypto-system)은 1985년에 Miller와 Koblitz가 독립적으로 제안한 공개키 암호 알고리즘이다. 이는 최근 150여년전부터 정수론, 대수기하분야에서 집중적으로 연구되어 왔으며, Fermat의 마지막 정리의 증명에서도 타원곡선 이론이 아주 중요하게 이용되었다. 최근에는 타원곡선방법(ECM, Elliptic Curve Method)은 RSA 암호시스템의 근간이 되는 인수분해 문제와 소수판정법 및 공개키 암호 등에 활용되고 있다.

3. 의료정보 교환 프로토콜 설계

개인의 건강관리 서비스는 단말 자체에서 개인 건강 정보를 저장할 수 있지만, 이는 병원과 연동이 되어야 더욱 정확한 의료 서비스를 제공할 수 있다. 기존 개인의 건강정보가 저장되어 있는 병원을 통해 정보를 제공받고, 이를 종합하여 관리함으로써 제공 될 수 있다. 또한 이렇게 전송받고 관리되는 데이터는 HL7 표준을 통해 XML로 교환될 수 있다. 그림 1은 병원과 건강관리 시스템, 그리고 외부 서비스와의 서비스 흐름도를 나타낸다.

* 일반대학원 전자계산학과 박사과정
** IT대학 교수(교신저자)



(그림 1) 병원과 외부 서비스와의 흐름도

일반적으로 개인의 건강을 관리하는 서비스의 경우 단독적으로 사용되어지는 것 보다 병원의 기존 데이터와 연동하여 좀 더 체계적이고 정확하게 관리하게 하는 것이 중요한데, 이를 지원하는 방법으로는 의료정보의 상호운용성이 보장되는 CCR과 같은 표준을 사용하는 것이 있다. 표준을 이용하여 의료정보를 교환하면 다양한 병원들 간의 연동을 지원할 수 있고, 사용자가 이용하는 서비스와도 연동이 가능하다.

의료정보 교환 시스템과 병원간의 정보 교환은 다양한 요청/응답에 의해 동작할 수 있다. 병원과 의료정보 교환 시스템 간의 전송되어 질수 있는 정보의 종류는 표 1과 같이 정의하였다.

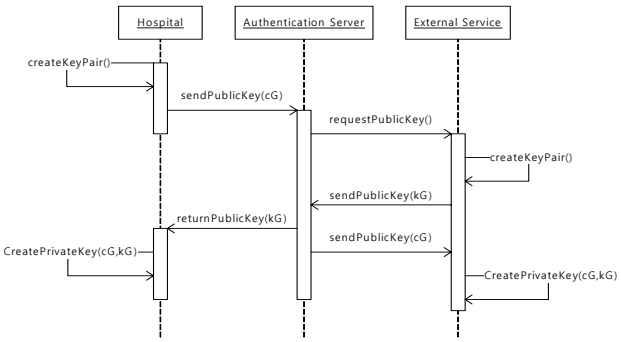
<표 1> 병원과 외부 서비스 간의 정보 종류

전송항목	내용
병력	환자의 병력에 대한 사항
검사결과	환자가 병원에서 받은 검사 내역
수술내역	환자가 병원에서 받은 수술 내역
개인의료정보	환자의 기본 정보
초진기록	환자가 처음 진료 받은 내역
의료기관 내원 기록	환자가 의료기관에 내원한 내역
예방접종	환자가 받은 예방접종에 대한 내역
활력징후	혈압, 혈당 등에 대한 내역
투약	환자가 투약 받은 내역

4. ECC 암호 알고리즘을 적용한 의료정보 교환 프로토콜 설계

ECC 알고리즘의 ECDH 알고리즘을 이용하여 병원과 외부 서비스 간의 키 교환을 통해 서로의 비밀키를 공유하고, 최종적으로는 같은 키를 보유하여 메시지를 송·수신할 때 사용한다. 그림 2는 인증 시스템을 이용한 병원과 외부 서비스 간의 ECC 알고리즘을 적용한 프로토콜 흐름도이다.

ECC 알고리즘을 이용하기 위해서는 서로의 공개키로 메시지를 암호화 하고, 이를 복호화 하여야 하는데 다음의 절차에 의해 이루어진다.



(그림 2) ECC 알고리즘을 적용한 병원과 외부 서비스 간의 의료정보 교환 프로토콜

① 병원은 먼저 c를 비밀키로 하는 KeyPair를 생성한다. 생성한 Key는 공개키화 하여 cG를 인증서버로 송신한다.
② cG를 받은 인증서버는 외부 서비스로 cG를 전송한다.
③ 외부 서비스는 k를 비밀키로 하는 KeyPair를 생성하여 생성한 Key를 공개키화 하여 kG를 인증서버로 송신한다.
④ 양쪽의 공개키를 모두 받은 인증서버는 키를 보관하고, 외부 서비스로부터 받은 kG를 병원으로 전송한다.
⑤ 병원과 외부서비스는 서로 수신받은 공개키를 자신의 비밀키와 조합하여 서로 ckG, kcG를 생성 후 메시지를 암/복호화 하여 통신 할 수 있다.

5. 결론

본 논문에서는 병원과 외부서비스 간의 의료정보 교환 프로토콜을 설계하고, 설계한 프로토콜에 ECC 알고리즘을 적용하여 안전한 의료정보전송 시스템을 설계하였다. 이를 위하여 관련연구로 CCR, ECC 알고리즘에 대해 분석하고, 의료정보 교환 프로토콜을 정의하였으며, 병원과 외부 서비스 간의 정보를 구분하고, ECC 알고리즘을 적용한 의료정보 교환 프로토콜을 설계하였다.

향후에는 본 논문의 연구를 기반으로 하여 더욱 세부적인 프로토콜 구조를 정의하고, 이를 이용하여 실제시스템을 구현할 예정이다.

ACKNOWLEDGMENT

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

참고문헌

[1] 박찬용, 임준호, 박수준, 김승환, "유헬스케어 표준화 기술 동향", 전자통신동향분석 제25권 제4호, 2010. 8.
[2] ANSI X9.62, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 1998.