논문 2010-47TC-4-8

# RSA 기반의 익명 전자처방전에 관한 연구

## ( A Study on Anonymous Electronic Prescription based on RSA Cryptosystem )

정 찬 주*, 윤 정 미**, 원 동 호***

( Chanjoo Chung, Jungmee Yun, and Dongho Won )

요 약

본 논문은 대학병원, 개인병원 등에서 의사의 진료에 따라 전자처방전을 발급·이용하는 RSA 기반의 익명 전자처방전을 제안한다. 전자처방전은 최근 디지털 의료정보의 통합 및 의료기관간 네트워크 구축 등을 통해 환자의 진료 데이터 및 영상 공유가 보편화되고 있는 국내 의료기관에서 실제 사용되고 있다. 제안된 RSA 기반의 익명 전자처방전은 기존 PKI 환경을 활용하여 전자처방전을 발급한 의사의 익명성을 보장하고, 전자처방전을 발급 받은 환자의 프라이버시를 보호한다. 기존 방식에서는 위임 서명자 또는 건강보험기관이 전자처방전의 내용을 알 수 있지만, 제안하는 방식에서는 전자처방전으로 조제되어 판매된 이후에 건강보험기관이 전자처방전의 내용을 알 수 있다. 제안된 방식은 국내에 전자주민증이 도입되고 국민건강보험공단이 처방전달시스템을 운영한다면 건강보험의 투명성을 높이는데 기여 할 것이다.

Abstract

This paper proposes RSA cryptosystem based anonymous electronic prescription which is issued from university and local hospitals by authorized medical professionals. Electronic prescription is now being used in domestic hospitals where sharing medical records and images are prevailing, facilitated by digitalizing medical information and building network infrastructure between the institutes. Proposed RSA based anonymous electronic prescription makes use of PKI protects the identity exposure of doctors and privacy of patients. While traditional prescription fails to protect identities to mandates party or to health insurance, the proposed RSA based prescription opens the contents of the prescription to health insurance authority only after its prescribing function is finished. The proposed approach along with soon to be deployed electronic ID card will help national health insurance corporation to increase the transparency of national prescription system.

**Keywords :** 익명성, 프라이버시, 전자처방전, 처방전달시스템, 네트워크보안

## I. 서 론

최근 IT, BT와 NT의 발달에 따라 병원은 원격진료 및 전자의무기록(EMR : Electronic Medical Records), 처방전달시스템(OCS : Order Communication System), 의료영상저장전송시스템(PACS : Picture Archiving and Communication System) 등의 의료정보시스템(HIS : Hospital Information System)을 도입하고 있다. 의료정보시스템은 국가 차원의 디지털 의료정보의 통합 및 유·무선 의료 통신망의 개방, 환자의 진료 데이터 및 영상 공유할 수 있는 체계로 구축되고 있다.

* 정회원, 성균관대학교 전기전자컴퓨터공학과 (SUNGKYUNKWAN UNIVERSITY)
** 정회원-교신저자, 전자부품연구원 (KOREA ELECTRONICS TECHNOLOGY INSTITUTE)
*** 정회원, 성균관대학교 정보통신공학부 (School of Information & Communication Engineering, SUNGKYUNKWAN UNIVERSITY)
※ 본 연구는 지식경제 프론티어기술개발사업의 일환으로 추진되고 있는 지식경제부의 유비쿼터스컴퓨팅 및 네트워크 원천기반기술개발사업의 10C2-C2-40S과제로 지원된 것임.
접수일자: 2009년6월2일, 수정완료일: 2010년4월13일

특히, 처방전달시스템은 의료정보시스템의 통합적 구축을 위한 필수적 기능을 수행하는 체계로 인식되고 있으며, 의사가 환자 진료 후 환자에 대하여 내리는 적절한 치료 및 추가적인 검사의 처방전을 발행하는 과정을 정보화한 시스템이다. 처방전달시스템은 의사가 단말기에서 처방전을 작성하여 보내면 접수 창구 및 치료 부서에서 바로 알 수 있어 전체적인 업무의 흐름을 빠르게 할 수 있고, 진료의 내용이 기록되어 국민건강보험 등의 의료보험료 청구 등에 쉽게 활용할 수 있다. 또한 의도되지 않은 약제간의 상호작용으로 생길 수 있는 부작용 및 의료사고를 사전에 제거할 수 있어 진료의 질과 안전성을 높이는 데에도 기여하고 있다[1].

본 논문에서는 대학병원, 개인병원 등에서 의사의 진료에 따라 전자처방전을 발급·이용하는 RSA[2] 기반의 익명 전자처방전을 제안한다. 제안된 RSA 기반의 익명 전자처방전은 기존 PKI[3] 환경을 활용하여 전자처방전을 발급한 의사의 익명성을 보장하고, 전자처방전을 발급 받은 환자의 프라이버시를 보호한다. 또한 전자처방전을 건강보험기관이 온라인으로 관리함으로서 전자처방전의 이중사용 및 건강보험료의 이중 청구 등을 원천적으로 막을 수 있는 장점이 있다. 제안된 시스템은 국내에 전자주민증이 도입되고 국민건강보험공단이 처방전달시스템을 운영한다면 건강보험의 투명성을 높이는 데 기여 할 것이다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 의료정보시스템 중에서 필수적인 처방전달시스템에 대해서 알아보고, Ⅲ장에서는 익명 전자처방전이 가져야할 보안 요구사항과 본 논문에서 사용할 용어에 대해 알아본다. Ⅳ장에서는 B. Lee 등이 제안한 위임 서명방식[4]과 Y. Yang 등이 제안한 서명자 위조 방지 전자처방전을 기술하고[5], RSA 기반의 익명 전자처방전을 Ⅴ장에서 제안한다. Ⅵ장에서는 제안된 방식의 안전성 분석과 B. Lee 및 Y. Yang의 방식과 비교한다. 끝으로 Ⅶ장에서는 결론을 내리고자 한다.

## Ⅱ. 처방전달시스템

처방전달시스템은 의사가 환자 진료 후 환자에 대하여 내리는 적절한 치료와 추가적인 검사의 처방전을 발행하는 과정을 정보화한 시스템이다. 처방전을 발행하는 업무는 병원 고유의 특성을 갖고 있는 업무로 기존에는 검사 처방전, 투약 처방전 등의 각종 처방전 용지에 환자에 대하여 후속적으로 요구되는 작업을 작성하여 환자 및 해당 부서로 전달하는 방법을 사용하였다.

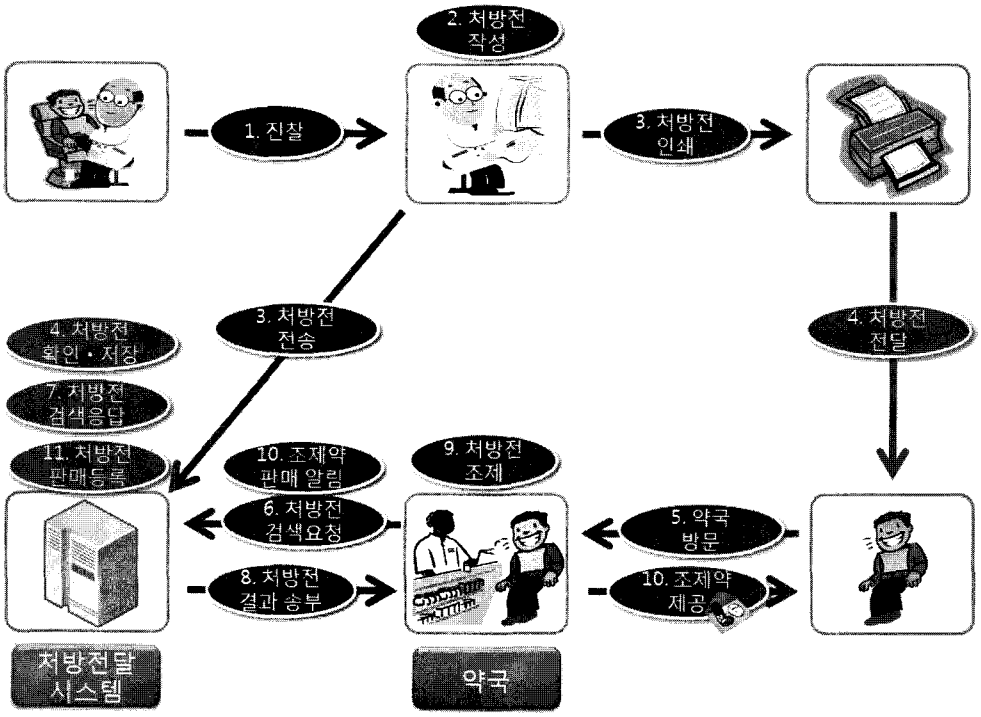



그림 1. 처방전달시스템의 흐름도
Fig. 1. Flow of Order Communication System.

종이 처방전은 모든 절차가 수작업으로 진행되어 능률이 떨어지고 인력을 효율적으로 활용할 수 없는 문제점이 있다. 병원은 이를 개선하기 위하여 환자 및 경영관련 정보를 전산화하여 자동으로 전달되고 처리됨으로서 직원의 능률 및 업무의 효율성을 높이는 방향으로 처방전달시스템을 도입하고 있다. 처방전달시스템의 업무절차는 그림 1과 같이 진행된다.

환자는 병원을 방문하여 의사로부터 진찰을 받는다. 의사는 환자의 진찰 결과에 따라 처방전을 작성한다. 작성된 처방전은 처방전달시스템으로 전달되며, 인쇄되어 환자에게 제공된다. 인쇄된 처방전에는 처방전에 대한 전자서명을 2차원 바코드로 인쇄한다. 환자는 제공받은 처방전을 가지고 약국을 방문하게 된다. 환자는 약사에게 처방전을 제출하면 2차원 바코드를 바코드 인식기로 전자서명 값을 읽고, 해당 정보를 처방전달시스템으로 송부한다. 이는 환자가 제공한 처방전이 정당한 처방전인지 여부를 확인하기 위함이다. 처방전달시스템은 해당 처방전이 등록된 처방전인지 여부를 확인하여 약사에게 결과를 알려준다. 약사는 처방전달시스템으로부터 전달받은 결과 등록된 처방전인 경우에 종이 처방전에 따라 처방약을 조제하고 조제약을 환자에게 제공하게 된다. 이때 약국은 처방전에 따라 조제약을 판매하였음을 처방전달시스템에 알린다. 처방전달시스템 도입에 따른 효과는 환자, 의사, 병원측면으로 나누어보면 표 1과 같다.

표 1. 처방전달시스템 도입에 따른 효과
Table 1. Effect of Applied Order Communication System.

| 구분 | 효과 | 내용 |
|---|---|---|
| 환자 | 진료절차 간소화 | o 외래접수, 수납, 진료, 검사, 원외처방전 발행, 다음 진료예약 등 전 분야에 걸쳐 처리과정의 단순, 보편화 |
| | 진료대기 시간 감소 | o 처방내역이 관련 부서로 전달되어 진료대기시간 절감 및 진료 예약기능 등을 통한 환자 집중 시간의 분산이 가능 |
| 의사 | 진료의 간편 | o 의사 처방 내역이 각 관련 부서별 처방전 전달 방식에서 일괄 전달되는 방식으로 변경을 통해 진료가 간편 |
| | 검사 등의 정확한 처리 | o 의사가 요청한 검사를 해당 부서에서 정확하게 처리할 수 있고 이에 따른 검사결과의 신속하고 정확한 처리가 가능 |
| | 진료 정보 교류 | o 진료 정보의 공유 및 의학적 통계 추출을 용이하게 하며, 진료의 신뢰성을 확보하고 타 의료기관과의 정보 교류를 통한 의료의 임상학적 발전을 지원 |
| 병원 | 생산·효율성 향상 | o 단순 반복 수작업의 전산화로 업무의 생산성을 극대화하고, 효율성이 높아지며 업무수행의 만족도가 향상 |
| | 가용성 향상 | o 인적자원의 효율적인 배치로 경영효율을 높이고 제한된 자원의 가동률을 향상 |
| | 병원 운영의 효율성 제고 | o 각종 양질의 통계자료와 정보를 실시간 활용하여 병원의 효율성 제고에 기여 |

국내의 처방전달시스템은 건강보험심사평가원에서 마련한 의약품처방·조제지원시스템[6]과 연동을 통해 의약품 처방·조제 시 병용금기 약품 사용을 점검함으로써 부적절한 약물사용을 사전에 예방하는 등의 효과를 보고 있다 .

## Ⅲ. 전자처방전 보안 요구사항 및 용어

본 장에서는 처방전달시스템 내에서 전자처방전이 갖추어야 할 보안 요구사항을 설명하고, Ⅳ장 이후에서 사용할 용어에 대하여 정의한다.

### 1. 보안 요구사항

본 소절에서는 익명 전자처방전이 가져야할 보안 요구사항에 대하여 정의한다. 먼저 전자처방전이 갖추어야 할 일반적인 보안 요구사항[7]과 B. Lee 등이 제안한 위임 서명기반의 전자처방전의 요구사항[4]을 정리하면 표 2와 같다.

제안하는 익명 전자처방전은 기존의 처방전달시스템을 2개 이상의 시스템으로 분리하여 하나는 전자처방전을 작성한 의사의 익명성을 보장하고, 만약 의사와 약사 또는 제약사간의 불법적인 거래에 따른 특정 제약사의 약품만을 처방 또는 조제하는 경우의 문제점을 해결하고자 한다. 다른 하나는 의사가 발행한 전자처방전의 정당성을 보장하는 방식이다. 현재 처방전달시스템을 통해 환자에게 배포되는 종이 처방전의 경우에 처방전을 작성한 의사의 실명이 포함되어 있어, 특정 의사가

표 2. 전자처방전의 보안 요구사항
Table 2. Security Requirements of Electronic Prescription.

| 보안 요구사항 | 설 명 |
|---|---|
| 위조불가 | o 전자처방전 생성자 이외의 어떤 누구도 정당한 전자처방전을 생성할 수 없어야 함 |
| 검증가능 | o 전자처방전은 공개적으로 이용할 수 있는 정보를 이용하여 누구든지 검증할 수 있어야 함 |
| 식별가능 | o 전자처방전 생성자가 생성한 전자처방전으로부터 서명자의 신원을 확인할 수 있어야 함 |
| 부인불가 | o 전자처방전 생성자는 자신이 생성한 전자처방전을 부인할 수 없어야 함 |
| 남용방지 | o 전자처방전을 위한 키쌍은 전자처방전을 생성하는 이외의 용도로 사용되지 않아야 함 |
| 기밀성 | o 전자처방전은 전송 중에 허가 받지 않은 자가 처방 내용을 볼 수 없어야 함 |
| 조제자 선택권 | o 환자 또는 보호자에 의해 선택된 조제자만이 전자처방전의 내용을 확인할 수 있어야 함 |

표 3. 전자처방전의 추가 보안 요구사항
Table 3. Added Security Requirements.

| 추가 보안 요구사항 | 설 명 |
|---|---|
| 담합 방지 | o 전자처방전을 생성하는 의사 또는 처방전에 따라 약을 조제하는 약사와 처방전에 있는 제약사간의 담합을 방지 할 수 있어야 함 |
| 추적성 | o 전자처방전에 따른 처방에 따른 의료 분쟁 시 과실여부를 판별하기 위해 환자 또는 의사를 추적할 수 있어야 함 |
| 의사의 불연결성 | o 같은 의사에 의한 전자처방전은 약사에 의해 가명성과 불연결성을 제공해야 함 |
| 재사용 방지 | o 조제에 사용된 전자처방전은 약물 남용 방지를 위해 재사용될 수 없어야 함 |
| 가명성 | o 환자와 의사의 실제 신원을 숨길 수 있는 가명성을 제공해야 하고, 신뢰기관에 의해서 가명성은 취소될 수 있어야 함 |
| 데이터 최소 노출 | o 절대적으로 필요하지 않은 경우에 전자처방전은 기밀로 유지 되어야 함 |

어떤 제약사의 제약품을 처방하는지를 쉽게 알 수 있다. 따라서 특정 제약사는 약국을 통해 특정 의사가 작성한 처방전의 내용만 취합하면 담합한 의사가 자사의 제약품을 얼마나 처방하였는지 쉽게 알 수 있는 구조이며, 이와 같은 일이 사회문제화 되고 있다[8].

의사의 전자처방전이 익명성을 보장받게 됨에 따라 처방전에 따른 사고가 발생하고 이에 따른 분쟁이 발생한 경우에 누구의 과실인지 여부를 확인하기 위하여 전자처방전을 추적할 수 있어야 한다. 또한, 조제에 사용된 전자처방전은 약물 남용을 방지하기 재사용될 수 없어야 한다. Y. Yang 등이 제안한 서명자 위조 방지 전자처방전의 보안 요구사항을 추가하면 표 3과 같다.

## 2. 용어 및 표기

본 논문에서 사용되는 개체는 표 4와 같이 정의하고, 표기는 표 5와 같이 정의한다.

표 4. 개체
Table 4. Entities.

| 개체 | 설 명 |
|---|---|
| $P$ | o 환자(Patient)를 정의함 |
| $CA$ | o 인증서를 발급하는 인증기관(Certification Authority)을 정의함 |
| $GP$ | o 일반의사(General Practitioner)를 정의함 |
| $HA$ | o 건강보험기관(Healthcare Authority) 또는 위임 서명자를 정의함 |
| $HC$ | o 건강보험 중앙기관(Healthcare authority for the Center)을 정의함 |
| $HL$ | o 건강보험 지방기관(Healthcare authority for the Local)을 정의함 |
| $PH$ | o 약사(PHarmacist) 또는 전자처방전을 검증하는 자를 정의함 |

표 5. 표기
Table 5. Notations.

| 표기 | 설 명 |
|---|---|
| $Sig_X(Y)$ | o 메시지 $Y$에 대해 개인키 $X$를 이용한 RSA 방식의 전자서명을 정의함 |
| $\sigma_X(Y)$ | o 메시지 $Y$에 대해 개인키 $X$를 이용한 이산대수 기반의 전자서명을 정의함 |
| $veri(\cdot)$ | o 전자서명의 검증 알고리즘을 정의함 |
| $w_d$ | o 전자처방전에 대한 위임 보증을 정의함 |
| $E_X(Y)$ | o 메시지 $Y$를 키 $X$로 암호화를 정의함 |
| $D_X(Y)$ | o 메시지 $Y$를 키 $X$로 복호화를 정의함 |
| $H(X)$ | o 메시지 $X$를 안전한 일방향 해쉬하는 함수로 정의함 |
| $h$ | o 안전한 일방향 해쉬함수에 의한 결과 값을 정의함 |
| $\leftarrow_R$ | o 값의 범위 $R$로부터 난수를 선택하는 것을 정의함 |
| $A \parallel B$ | o 메시지 $A$와 $B$를 연접한 것을 정의함 |
| $\phi(X)$ | o $X$를 오일러(Euler) 함수에 입력한 결과 값을 정의함 |
| $y_A$ | o $A$의 이산대수 공개키를 정의함 |
| $x_A$ | o $A$의 이산대수 개인키를 정의함 |
| $pk_A$ | o $A$의 공개키를 정의함 |
| $sk_A$ | o $A$의 개인키를 정의함 |
| $p_A$, $q_A$ | o $A$의 큰 소수 $p$와 $q$를 정의함 |
| $RegNo$ | o 등록대행기관 또는 인증기관으로부터 인증서 신청을 위해 발급 받은 등록번호를 정의함 |
| $e_{HA}$ | o 건강보험기관의 RSA 공개키 지수를 정의함 ($e_{HA} \cdot d_{HA} = 1 \bmod \phi(N_{HA})$) |
| $N_{HA}$ | o 건강보험기관의 RSA 공개키 및 개인키의 모듈러를 정의함 ($N_{HA} = p_{HA} \cdot q_{HA}$) |
| $d_{HA}$ | o 건강보험기관의 RSA 개인키 지수를 정의함 ($d_{HA} = d_C \cdot d_L \bmod \phi(N_{HA})$) |
| $d_C$ | o 건강보험 중앙기관의 RSA 개인키 지수를 정의함 |
| $d_L$ | o 건강보험 지방기관의 RSA 개인키 지수를 정의함 |
| $g$ | o $Z_p^*$ 상의 원시원소를 정의함 |
| $M$ | o 전자처방전의 처방 내용을 정의함 |
| $WN$ | o 전자처방전의 작성자(Writer Name)를 정의함 |
| $SN$ | o 전자처방전의 일련번호(Serial Number)를 정의함 |
| $Cert_A$ | o $A$의 인증서(Certificate)를 정의함 |
| $AP_A$ | o $A$의 익명 전자처방전(Anonymous Prescription)을 정의함 |
| $TM_i$ | o $i$번째 전송(Transmission) 또는 중간(Temp) 메시지를 정의함 |
| $k$ | o 1024 또는 2048 비트의 보안 파라미터를 정의함 |

# Ⅳ. 기존의 전자처방전

본 장에서는 먼저 B. Lee 등이 제안한 위임 서명을 활용한 전자처방전과 Y. Yang 등이 제안한 서명자 위조 방지 전자처방전[5]에 대하여 알아본다.

### 1. 위임서명 기반 전자처방전

Y. Yang 등은 서명자 위조 방지 전자처방전을 제안하기 위하여 기존의 B. Lee 등이 제안한 위임 서명방식을 전자처방전에 응용한 프로토콜을 먼저 소개하였다.

#### 가. 시스템 설정

B. Lee 등은 이산대수 기반의 위임 서명을 위해 다음과 같이 시스템을 설정하였다. $p$와 $q$는 $q|(p-1)$을 만족하는 큰 소수이고, $g$는 $Z_p^*$ 상에서 위수 $q$를 갖는 원시원소이다.

#### 나. 위임 단계

위임 단계에서 일반의사 $GP$는 $k_{GP} \in_R Z_q^*$을 만족하는 $k_{GP}$ 를 선택하고, $r_{GP} = g^{k_{GP}} \bmod p$를 계산하고, 위임을 위한 이산대수 기반의 전자서명 $\sigma_{GP} = x_{GP} \cdot h(w_d, r_{GP}) + k_{GP} \bmod q$를 계산한 후 $(w_d, r_{GP}, \sigma_{GP})$을 안전하게 $HA$에게 전송한다. 여기서 $w_d$는 전자처방전에 대한 위임 보증이다. $HA$는 $(w_d, r_{GP}, \sigma_{GP})$가 $g^{\sigma_{GP}} \stackrel{?}{=} y_{GP}^{h(w_d, r_{GP})} \cdot r_{GP} \bmod p$를 만족한다면 정당한 위임으로 받아들인다. 여기서 $(x_{GP}, y_{GP} = g^{x_{GP}} \bmod p)$는 일반의사 $GP$의 키 쌍이다.

#### 다. 서명과 검증 단계

위임 서명자인 $HA$는 자신의 위임서명 키쌍 $(x_\rho, y_\rho)$을 $x_\rho = \sigma_{GP} + x_{HA} \bmod q$와 $y_\rho = g^{x_\rho} = y_{GP}^{h(w_d, r_{GP})} \cdot r_{GP} \cdot y_{HA} \bmod p$와 같이 계산한다. 여기서 $(x_{HA}, y_{HA} = g^{x_{HA}} \bmod p)$는 건강보험기관 $HA$의 키 쌍이다. 위임 서명자인 $HA$는 위임 서명 개인키 $x_\rho$으로 위임 보증 $w_d$에 따른 전자처방전 $M$에 대한 위임 전자서명 $\sigma_{x_\rho}(M)$을 생성한다. $(M, \sigma_{x_\rho}(M), w_d, r_{GP}, y_{GP}, y_{HA})$을 검증자 $PH$에게 전송한다.

검증자 $PH$는 수신된 $(M, \sigma_{x_\rho}(M), w_d, r_{GP}, y_{GP}, y_{HA})$로부터 $M \in w_d$임을 확인하며, $y_\rho = y_{GP}^{h(w_d, r_{GP})} \cdot r_{GP} \cdot y_{HA} \bmod p$를 계산하고, $veri(M, \sigma_{x_\rho}(M), y_\rho) \stackrel{?}{=} true$를 검사한다. 이상의 과정은 표 6과 같다.

#### 라. 위임 서명기반 전자처방전의 문제점

위임 서명기반 전자처방전 방식의 경우 일반의사 $GP$가 위조하는 경우에 위임 서명을 위조할 수 있는 문제점이 있다. 부정직한 일반의사 $GP$는 $r'_{GP} = y_{HA}^{-1} \bmod p$를 계산할 수 있다. 따라서 $x'_\rho = x_{GP} \cdot h(w_d, r'_{GP}) \bmod q$는 정당한 위임 서명을 생성하는 키이고, $(M, \sigma_{x_\rho}(M), w_d, r'_{GP}, y_{GP}, y_{HA})$는 정당한 위임 서명 키이다. 왜냐하면, $y_\rho = y_{GP}^{h(w_d, r'_{GP})} \cdot r'_{GP} \cdot y_{HA} \bmod p = g^{x_{GP} \cdot h(w_d, r'_{GP})} \cdot y_{HA}^{-1} \cdot y_{HA} \bmod p = g^{x_{GP} \cdot h(w_d, r'_{GP})} \bmod p = g^{x'_\rho} \bmod p$ 이기 때문이다. 또한 위임 서명기반의 전자처방전의 경우 환자의 프라이버시를 고려하지 않은

표 6. 위임 서명기반 전자처방전
Table 6. Electronic Prescription based on Proxy Signature.

| 단계 | 송신자 → 수신자 | 전송 정보 |
|---|---|---|
| 위임단계 | $GP \rightarrow HA$ | $(w_d, r_{GP}, \sigma_{GP})$, where $r_{GP} = g^{k_{GP}} \bmod p$ with $k_{GP} \in_R Z_q^*$,<br>$\sigma_{GP} = x_{GP} \cdot h(w_d, r_{GP}) + k_{GP} \bmod q$,<br>그리고, $w_d$는 전자처방전에 대한 위임 보증<br>$HA$는 위임서명 키쌍 $(x_\rho, y_\rho)$을 계산,<br>where $x_\rho = \sigma_{GP} + x_{HA} \bmod q$, and<br>$y_\rho = g^{x_\rho} = y_{GP}^{h(w_d, r_{GP})} \cdot r_{GP} \cdot y_{HA} \bmod p$<br>with $(x_{HA}, y_{HA} = g^{x_{HA}} \bmod p)$ |
| 서명단계 | $HA \rightarrow V$ | $(M, \sigma_{x_\rho}(M), w_d, r_{GP}, y_{GP}, y_{HA})$ |
| 검증단계 | $PH$ | 수신된 $(M, \sigma_{x_\rho}(M), w_d, r_{GP}, y_{GP}, y_{HA})$로부터 $M \in w_d$임을 확인<br>$y_\rho = y_{GP}^{h(w_d, r_{GP})} \cdot r_{GP} \cdot y_{HA}$를 계산<br>$veri(M, \sigma_{x_\rho}(M), y_\rho) \stackrel{?}{=} true$인지 확인 |

프로토콜이기 때문에 환자 개인정보를 보호하지 못하고 있다.

## 2. 서명자 위조를 방지하는 전자처방전

Y. Yang 등은 B. Lee 등이 제안한 위임 서명 방식에서 $r'_{GP} = y_{HA}^{-1} \bmod p$을 위조할 수 없게 하기 위하여 $r_{GP} \| y_{GP}$에 대해 위임 서명자 $HA$가 전자서명을 하는 것으로 서명자 위조를 방지한다.

### 가. 시스템 설정

시스템 설정은 B. Lee 등이 사용한 것과 동일하게 $p$와 $q$는 $q|(p-1)$을 만족하는 큰 소수이고, $g$는 $Z_p^*$ 상에서 위수 $q$를 갖는 원시원소이다.

### 나. 위임 단계

일반의사 $GP$는 $k_{GP} \in_R Z_q^*$을 만족하는 $k_{GP}$ 를 선택하고, $r_{GP} = g^{k_{GP}} \bmod p$를 계산하고, $r_{GP}$와 자신의 공개키 $y_{GP}$를 위임 서명자 $HA$에게 전달한다. $HA$는 $k_{HA} \in_R Z_q^*$을 만족하는 $k_{HA}$를 선택하고, $r_{HA} = g^{k_{HA}} \bmod p$와 $r = x_{HA} \cdot h(y_{GP} \| r_{GP}, r_{HA}) + k_{HA} \bmod q$를 계산하고, $(r_{HA}, r)$쌍을 일반의사 $GP$에게 전달한다. 일반의사 $GP$는 위임 서명자가 보내온 $(r_{HA}, r)$쌍을 이용하여 위임 서명자의 공개키 $y_{HA}$를 이용하여 $g^r \stackrel{?}{=} y_{HA}^{h(y_{GP} \| r_{GP}, r_{HA})} \cdot r_{HA} \bmod p$인지를 확인한다. 일반의사 $GP$는 $\sigma_{GP} = x_{GP} \cdot h(w_d, r) + k_{GP} \bmod q$를 계산하고, 위임 보증 $w_d$과 함께 위임 서명자 $HA$에게 전달한다. 위임 서명자 $HA$는 $g^{\sigma_{GP}} \stackrel{?}{=} y_{GP}^{h(w_d, r)} \cdot r_{GP} \bmod p$를 만족하기만 한다면 정당한 위임으로 받아들인다. 위임 서명자 $HA$는 위임 서명용 개인키 $x_\rho = \sigma_{GP} + x_{HA} \bmod q$를 계산한다. 여기서 위임 서명용 키쌍은 $(x_\rho, y_\rho = g^{x_\rho} \bmod p)$이다.

### 다. 서명과 검증 단계

위임 서명자인 $HA$는 자신의 위임서명 키쌍 $(x_\rho, y_\rho)$을 $x_\rho = \sigma_{GP} + x_{HA} \bmod q$와 $y_\rho = g^{x_\rho} = y_{GP}^{h(w_d, r)} \cdot r_{GP} \cdot y_{HA} \bmod p$와 같이 계산한다. 여기서 $(x_{HA}, y_{HA} = g^{x_{HA}} \bmod p)$는 건강보험기관 $HA$의 키 쌍이다. 위임 서명자인 $HA$는 위임 서명 개인키 $x_\rho$으로 위임 보증 $w_d$에 따른 전자처방전 $M$에 대한 위임 전자서명 $\sigma_{x_\rho}(M)$을 생성한다. $(M, \sigma_{x_\rho}(M), w_d, r_{GP}, y_{GP}, r, r_{HA}, y_{HA}, y_\rho)$을 검증자 $PH$에게 전송한다.

검증자 $PH$는 수신된 $(M, \sigma_{x_\rho}(M), w_d, r_{GP}, y_{GP}, r, r_{HA}, y_{HA}, y_\rho)$로부터 $M \in w_d$임을 검사하고, $g^r \stackrel{?}{=} y_{HA}^{h(y_{GP} \| r_{GP}, r_{HA})} \cdot r_{HA}$와 $veri(y_{GP}^{h(w_d, r_{GP})} \cdot r_{GP} \cdot y_{HA}, M, \sigma_{x_\rho}(M)) \stackrel{?}{=} true$인지를 검증한다. 이상의 과정은 표 7과 같다.

표 7. 서명자 위조 방지 전자처방전
Table 7. Electronic Prescription to protect signer forgery attack.

| 단계 | 송신자 → 수신자 | 전송 정보 |
|---|---|---|
| 위임단계 | $GP \rightarrow HA$ | $r_{GP} = g^{k_{GP}} \bmod p$, where $k_{GP} \in_R Z_q^*$ |
| | $HA \rightarrow GP$ | $(r_{HA}, r)$, where $r_{HA} = g^{k_{HA}} \bmod p$ with $k_{HA} \in_R Z_q^*$,<br>$r = x_{HA} \cdot h(y_{GP} \| r_{GP}, r_{HA}) + k_{HA} \bmod q$;<br>$GP$는 $g^r = y_{HA}^{h(y_{GP} \| r_{GP}, r_{HA})} \cdot r_{HA}$인지 확인 |
| | $GP \rightarrow HA$ | $(w_d, \sigma_{GP})$, where $\sigma_{GP} = x_{GP} \cdot h(w_d, r) + k_{GP} \bmod q$<br>$HA$는 $g^{\sigma_{GP}} = y_{GP}^{h(w_d, r)} \cdot r_{GP} \bmod p$인지 확인<br>$HA$는 위임 서명용 개인키 $x_\rho = \sigma_{GP} + x_{HA} \bmod q$를 계산<br>위임서명키 쌍$(x_\rho, y_\rho = g^{x_\rho} \bmod p)$ 보유 |
| 서명단계 | $HA \rightarrow V$ | $(M, \sigma_{x_\rho}(M), w_d, r_{GP}, y_{GP}, r, r_{HA}, y_{HA})$ |
| 검증단계 | $V$ | $g^r \stackrel{?}{=} y_{HA}^{h(y_{GP} \| r_{GP}, r_{HA})} \cdot r_{HA}$ 및<br>$veri(y_{GP}^{h(w_d, r_{GP})} \cdot r_{GP} \cdot y_{HA}, M, \sigma_{x_\rho}(M)) \stackrel{?}{=} true$ 확인 |

### 라. 서명자 위조를 방지하는 전자처방전의 문제점

Y. Yang 등이 제안한 서명자 위조 방지 전자처방전은 이산대수 기반의 전자서명을 활용하고 있어 실제 환경에 적용하기 위해서는 현재 소인수 분해 문제 기반의 PKI가 이산대수 기반의 PKI로 변경되어야 하는 문제점이 있다. 단적으로 인터넷 익스플로러에 탑재된 국내·외 인증서만 보더라도 대부분의 PKI는 소인수 분해 문제 기반임을 알 수 있다. 또한 서명자 위조 방지를 위한 위임 단계에서 계산량이 B. Lee가 제안한 방식보다 많은 문제점 등이 있다.

## V. 제안하는 RSA 기반의 익명 전자처방전

본 장에서는 국내·외 대부분의 PKI(Public Key Infrastructure) 구축 시 사용되고 있는 RSA 기반의 익명 전자처방전을 제안한다.

### 1. 시스템 설정

환자 $P$는 국가 또는 건강보험기관으로부터 자신의 공개키 $(e_P, n_P)$을 포함하는 인증서 $Cert_P$와 개인키 $(d_P, n_P)$를 포함하는 스마트카드를 발급 받고, 스마트카드의 내용은 PIN(Personal Identification Number) 인증을 통해 접근 통제가 가능하다고 가정한다. 여기서 $e_P \cdot d_P = 1 \bmod \phi(N_P)$이다.

일반의사 $GP$는 인증기관 $CA$ 또는 등록대행기관 $RA$을 방문하여 대면확인 후에 인증서 발급을 위한 등록번호 $RegNo$를 받는다[9]. $GP$는 발급 받은 등록번호를 가지고 자신이 생성한 공개키쌍 $(pk_{GP}, sk_{GP})$을 이용하여 전자서명 $Sig_{sk_{GP}}(RegNo \| pk_{GP})$ 및 $RegNo$와 $pk_{GP}$를 $CA$로 보안채널을 통해 전달하여 인증서를 신청한다. 여기서 $pk_{GP} = (e_{GP}, N_{GP})$, $sk_{GP} = (d_{GP}, N_{GP})$이고, $e_{GP} \cdot d_{GP} = 1 \bmod \phi(N_{GP})$이다. $CA$는 $GP$로부터 전달받은 전자서명 $Sig_{sk_{GP}}(RegNo \| pk_{GP})$을 $pk_{GP}$로 검증하고, $RegNo$로부터 신청자를 확인한 후 일반의사 $GP$를 위한 인증서 $Cert_{GP}$를 발급한다. $GP$는 발급 받은 $Cert_{GP}$를 이용하여 건강보험기관 $HA$에 등록하고, 이후 전자처방전 등록 시 $Cert_{GP}$의 개인키로 전자서명하여 로그인 한다.

건강보험기관 $HA$는 중앙기관 $HC$와 지방기관 $HL$로 구성되고, $GP$가 인증서를 발급 받는 절차와 동일하게 $CA$로부터 $Cert_{HA}$를 발급 받는다. 이때 건강보험기관 $HA$의 개인키는 $d_{HA} = d_{HC} \cdot d_{HL} \bmod \phi(N_{HA})$을 만족하는 $d_{HC}$와 $d_{HL}$로 나눈다[2, 10~11]. 나누어진 $d_{HC}$와 $d_{HL}$은 익명 전자처방전을 부분 서명하기 위한 건강보험 중앙기관 $HC$와 지방기관 $HL$의 각각의 개인키이다. $HL$은 전송 정보 암호화를 위한 공개키쌍 $(pk_{HL}, sk_{HL})$을 갖고 있으며, $pk_{HL}$은 $HC$에게 사전에 제공한다.

환자 $P$는 자신의 스마트카드를 가지고 진료를 받기 위해 병원을 방문하여 일반의사 $GP$에게 스마트카드를 전달한다. $GP$는 $P$를 진찰하고 익명 전자처방전을 작성하기 위해 자신의 $Cert_{GP}$로 $HA$에 로그인 한다. 이때 $GP$와 $HA$간에는 SSL(Secure Socket Layer) 또는 TLS (Transport Layer Security) 보안채널이 설정된다[12~13].

### 2. 익명 전자처방전 위임 및 부분 서명 단계

$GP$는 익명 전자처방전의 작성자 $WN$을 익명으로 설정하고, 전자처방전 $M$을 ($WN$, $SN$, 처방정보)로 구성하고, $M$을 안전한 일방향 해쉬함수에 입력하여 $h = H(M)$을 계산한다. $GP$는 전자처방전의 익명성을 보장하기 위한 은닉요소(blind factor) $b \leftarrow_R \{0, 1\}^k$를 선택하고[10], $TM_1 = h \cdot b^{e_{HA}} \bmod N_{HA}$를 계산하고, $TM_1$을 $HC$에게 전송한다.

$HC$는 $GP$로부터 전달받은 $TM_1$에 자신의 개인키로 $TM_2 = TM_1^{d_{HC}} \bmod N_{HA}$을 계산하고, 안전한 데이터베이스에 $(TM_1, Cert_{GP})$를 보관한다. 부분 서명에 대한 $GP$의 변조를 방지하기 위하여 $HL$의 공개키로 $TM_3 = E_{pk_{HL}}(TM_2)$와 같이 암호화하여 $GP$에게 전달한다.

$GP$는 $HC$로부터 전달받은 $TM_3$와 앞에서 계산한 $h$와 은닉요소 $b$을 포함하는 $TM_4 = (h, b, TM_3)$를 $HL$에게 전달한다.

$HL$은 $GP$로부터 전달받은 $TM_4$의 내용 중 $TM_3$를 자신의 복호화키 $sk_{HL}$로 복호화하여 $TM_2 = D_{sk_{HL}}(TM_3)$를 얻는다. $TM_2$에 대하여 자신의 부분 서명 개인키 $d_{HL}$로 서명하여 $TM_5 = TM_2^{d_{HL}} \bmod N_{HA}$를 계산한다. $HL$은 $TM_5$에 은닉요소의 역수를 곱한 후 $HA$의 공개키 $e_{HA}$로 검증한 값이 $TM_4$의 내용 중 $h$와 같은지 $h \stackrel{?}{=} (TM_5 \cdot b^{-1})^{e_{HA}} \bmod N_{HA}$를 비교한다. $HL$은 비교 결과가 같다면 안전한 데이터베이스에 $(TM_5, h)$를 보관하고, $h^{d_{HA}} = TM_5 \cdot b^{-1} \bmod N_{HA}$를 계산하여

$HA$에게 제공한다. $HA$는 $HL$로부터 전달 받은 $h^{d_{HA}}$를 정당한 전자처방전으로 데이터베이스에 $(h^{d_{HA}}, valid)$로 저장한다. $HL$은 $TM_5$를 $GP$에게 전달한다.

$GP$는 $HL$로부터 전달 받은 $TM_5$에 대하여 $TM_5 \cdot b^{-1} \bmod N_{HA}$를 계산하여 $h^{d_{HA}}$을 복구한다. 복구된 $h^{d_{HA}}$을 $HA$의 공개키 $e_{HA}$로 검증한 값이 자신이 생성한 $h$와 같은지 비교하여 같다면 환자 $P$에 대한 익명 전자처방전에 대한 전자서명 $AP_P = h^{d_{HA}} \bmod N_{HA}$을 얻게 된다. $GP$는 전자처방전 $M$과 전자처방전에 대한 전자서명 $AP_P$를 환자의 스마트카드에 넣어 $P$에게 전달한다.

### 3. 익명 전자처방전 검증 단계

환자 $P$는 $GP$로부터 전달 받은 스마트카드를 가지고 약국을 방문하여 약사 $PH$에게 스마트카드를 제출하고 전자처방전에 따른 조제를 요청한다.

$PH$는 스마트카드에서 $M$과 $AP_P$를 꺼내서 익명 전자처방전의 내용을 확인하고, 익명 전자처방전 전자서명 $AP_P$의 정당성을 $HA$의 공개키 $e_{HA}$로 검증한 값이 전자처방전 $M$의 해쉬값 $h = H(M)$과 $AP_P^{e_{HA}} \bmod N_{HA} \stackrel{?}{=} h$가 같은지를 확인한다. 같은 값을 갖는다면 $PH$는 $AP_P$를 $HA$에게 전송하여 전자처방전의 상태를 요청한다.

$HA$는 $PH$로부터 전달받은 $AP_P$를 검색어로 데이터베이스로부터 상태정보를 가져와 $PH$에게 전달한다. $PH$는 전달받은 상태정보가 $valid$이면 익명 전자처방전에 따라 약을 조제하여 $P$에게 제공하고, $HA$에게 $AP_P$가 조제·판매되었음을 $used$로 전달한다. $HA$는 데이터베이스의 $AP_P$의 상태정보를 $used$로 갱신한다. 이상의 과정은 표 8과 같다.

표 8. 익명 전자처방전
Table 8. Anonymous Electronic Prescription based on RSA Cryptosystem.

| 단계 | 송신자 → 수신자 | 전송 정보 |
|---|---|---|
| 위임 및 서명 단계 | $GP \rightarrow HC$ | $TM_1$, where $TM_1 = h \cdot b^{e_{HA}} \bmod N_{HA}$ with $h = H(M)$,<br>$b \leftarrow_R \{0, 1\}^k$<br>$HC$는 $(TM_1, Cert_{GP})$를 데이터베이스에 보관 |
| | $HC \rightarrow GP$ | $TM_3$, where $TM_3 = E_{pk_{HL}}(TM_2)$<br>with $TM_2 = TM_1^{d_{HC}} \bmod N_{HA}$, $HL$의 공개키 $pk_{HL}$ |
| | $GP \rightarrow HL$ | $TM_4$, where $TM_4 = (h, b, TM_3)$<br>$HL$은 자신의 개인키 $sk_{HL}$로 $TM_2 = D_{sk_{HL}}(TM_3)$를 계산<br>$TM_5 = TM_2^{d_{HL}} \bmod N_{HA}$ with $d_{HL}$ 계산하고<br>$h \stackrel{?}{=} (TM_5 \cdot b^{-1})^{e_{HA}} \bmod N_{HA}$ 비교하여 동일하다면<br>$(TM_5, h)$를 데이터베이스에 보관 |
| | $HL \rightarrow GP$ | $TM_5$, where $TM_5 = TM_2^{d_{HL}} \bmod N_{HA}$<br>$GP$는 자신의 은닉요소 $b$의 역수를 $TM_5$에 곱하여<br>$h^{d_{HA}} = TM_5 \cdot b^{-1} \bmod N_{HA}$를 계산<br>$h \stackrel{?}{=} (h^{d_{HA}})^{e_{HA}} \bmod N_{HA}$ 비교하여 동일하다면<br>전자처방전 $M$과 $AP_P = h^{d_{HA}} \bmod N_{HA}$를 $P$의 스마트카드에 저장 |
| 검증단계 | $P \rightarrow PH$ | $(M, AP_P)$, where $AP_P = h^{d_{HA}} \bmod N_{HA}$<br>$PH$는 전자처방전 $M$에 대한 해쉬값 $h = H(M)$를 계산<br>$AP_P$에 대해 $HA$의 공개키 $e_{HA}$로 검증한 값과 $h$가 같은지 비교<br>$h \stackrel{?}{=} (AP_p)^{e_{HA}} \bmod N_{HA}$ 비교하여 동일하다면 $AP_P$의 상태정보를<br>$HA$에게 요청하여 결과에 따라 전자처방전을 조제 |

## VI. 제안하는 방식의 안전성 분석 및 비교

본 장에서는 제안하는 방식이 Ⅲ장에서 정의한 전자처방전의 보안 요구사항을 만족하는지 알아보고, B. Lee가 제안한 방식과 Y. Yang이 제안한 방식과 비교한다.

### 1. 안전성 분석

(1) 위조불가

일반의사 *GP*가 진료 후에 처방하는 익명 전자처방전은 건강보험기관 *HA*의 개인키 $d_{HA}$에 의한 RSA 전자서명에 의해 발행되기 때문에 *GP*, *HA*와 약사 *PH* 등 모든 개체에 의해 검증될 수 있다. 따라서 합법적인 *HA*에 의해서만 익명 전자처방전이 생성되기 때문에 위조불가하다. 처방전을 작성하는 *GP*는 자신의 인증서 $Cert_{GP}$의 개인키를 이용한 전자서명을 통해 *HA*에게 사용자 인증 절차를 거쳐 로그인하기 때문에 등록되지 않은 *GP*는 처방전을 생성할 수 없다.

(2) 검증가능

익명 전자처방전에 대한 전자서명 $AP_P$는 건강보험기관 *HA*의 인증서 $Cert_{HA}$의 공개키 $e_{HA}$로 검증할 수 있다. *HA*의 인증서 $Cert_{HA}$는 인증기관 *CA*의 디렉토리(Directory)[14]에 게시되어 있기 때문에 $AP_P$와 처방전 *M*을 수신한 누구든지 익명 전자처방전의 내용을 검증할 수 있다.

(3) 식별가능

제안하는 방식은 전자처방전 내에 *GP*의 신원을 확인할 수 있는 어떤 정보도 포함하고 있지 않기 때문에 처방전을 작성한 *GP*를 식별할 수 없지만, 익명 전자처방전에 전자서명을 수행한 서명자 *HA*는 식별할 수 있다. *HA*는 자신의 인증서 $Cert_{HA}$를 발급 받기 위하여 *CA* 또는 등록대행기관 *RA*에 대면확인을 통한 신원확인을 수행하기 때문이다.

(4) 부인불가

익명 전자처방전에 전자서명을 수행한 *HA*의 개인키 $d_{HA}$는 *HC*와 *HL*이 협력해야 만이 생성할 수 있기 때문에 *HA* 이외에는 익명 전자처방전을 생성할 수 없다. 따라서 익명 전자처방전에 대한 정당성을 익명 전자처방전에 대한 *HA*의 전자서명이 수행된 이후에는 부인할 수 없게 된다.

(5) 남용방지

익명 전자처방전을 생성하는데 사용되는 *HA*의 개인키 $d_{HA}$는 $d_{HA} = d_{HC} \cdot d_{HL} \bmod \phi(N_{HA})$을 만족하는 $d_{HC}$와 $d_{HL}$ 분리되어 보관된다. 익명 전자처방전에 대한 구문 형식이 맞지 않는 경우에 *HL*은 전자서명을 수행하지 않기 때문에 익명 전자처방전을 생성하는 이외의 용도로 사용되지 않는다.

(6) 기밀성

익명 전자처방전은 환자 *P*가 처방전에 따른 조제를 위해 약국을 방문하여 약사 *PH*에게만 전달되기 때문에 허가 받은 *PH*와 처방전을 작성한 *GP* 이외에는 아무도 알 수 없다. 또한, 익명 전자처방전에 대해 전자서명을 수행하는 *HA*, *HC*와 *HL* 조차도 전자처방전의 내용을 알 수 없다. *HA*는 *PH*가 전자처방전에 따라 약을 조제하여 환자에게 제공한 이후에 약사가 의료보험료를 청구하기 위해서 처방전을 *HA*에게 제공하기 전까지는 처방전의 내용을 알 수 없다.

(7) 조제자 선택가능성

익명 전자처방전은 환자 *P*가 어느 약국의 약사 *PH*에게 익명 전자처방전을 제공했느냐에 따라 처방전에 따른 조제가 가능하다. 따라서 환자 *P*가 선택한 조제자만이 처방전에 따라 조제할 수 있는 방식이다.

(8) 담합방지

익명 전자처방전 내에는 처방한 자가 누구인지 알 수 있는 어떠한 정보도 포함하고 있지 않다. 만약 의사가 약사 또는 제약사 간에 담합을 하더라도 약사, 제약사 입장에서는 처방전으로부터 처방전을 작성한 의사가 누구인지 알 수 없기 때문에 담합에 따른 이익이 증가 되었는지 확인할 수 있는 방법이 없다.

(9) 추적성

익명 전자처방전에 따른 의료 분쟁이 환자 *P*와 의사 *GP* 또는 환자 *P*와 약사 *PH*간에 발생한 경우에는 누구의 실수 인지를 확인할 수 있다. 이때 익명 전자처방전에 전자서명을 수행한 *HC*와 *HL*의 도움이 필요하다. 먼저 *HL*은 $AP_P$에 *HA*의 공개키 $e_{HA}$ 지수 연산을 하

여 $h = (AP_P)^{e_{HA}} \bmod N_{HA}$를 계산하고, $HL$의 데이터베이스를 검색 키 $h$로 검색하여 $TM_5$를 찾는다. $HL$은 찾은 $TM_5$를 $HC$에게 전달한다. $HC$는 $TM_5$에 대해 $HA$의 공개키 $e_{HA}$ 지수 연산을 하여 $TM_1 = (TM_5)^{e_{HA}} \bmod N_{HA} = (TM_2^{d_{HL}})^{e_{HA}} \bmod N_{HA} = ((TM_1^{d_{HC}})^{d_{HL}})^{e_{HA}} \bmod N_{HA} = (TM_1^{d_{HA}})^{e_{HA}} \bmod N_{HA}$을 계산한다. $HC$는 자신의 데이터베이스에서 검색 키 $TM_1$로 검색하여 $Cert_{GP}$를 찾는다. $Cert_{GP}$는 전자처방전을 작성한 일반의사 $GP$의 인증서이므로 전자처방전을 작성한 $GP$를 추적할 수 있다.

(10) 의사의 불연결성

익명 전자처방전 자체는 $GP$에 관한 어떠한 정보도 포함하고 있지 않다. 전자처방전에 대해서 전자서명을 수행하는 $HA$ 이외에는 동일한 의사에 의해 작성된 전자처방전의 작성자의 가명성과 연결할 수 있는 방법이 없다. 따라서 약사는 전자처방전으로부터 처방전을 작성한 의사를 연결할 수 있는 방법이 없다.

(11) 재사용 방지

익명 전자처방전의 상태정보가 건강보험기관 $HA$에 의하여 관리되기 때문에 전자처방전의 이중 사용으로 인한 약물 남용의 피해를 막을 수 있다. 처방전 조제에 사용된 익명 전자처방전은 $PH$에 의해 $HA$에게 보고되기 때문에 2번 이상 사용될 수 없다. 처방전의 상태 정보를 제공하는 $HA$는 PKI에서 인증서 상태 정보를 제공하는 OCSP(Online Certificate Status Protocol)[15] 서버와 동일한 역할을 한다. 따라서 환자 $P$는 한번 사용된 익명 전자처방전으로 1번 이상 약을 조제 받을 수 없다.

(12) 가명성

제안된 익명 전자처방전에서 환자의 가명성은 보장되지 않는다. 하지만, 익명 전자처방전을 발급하는 과정과 동일한 방식으로 익명 인증서를 환자에게 발급하는 방식으로 변경하여 적용한다면 환자의 가명성 또한 보장될 수 있다. 일반의사의 가명성은 익명 전자처방전 내에 어떠한 $GP$의 개인정보도 포함하고 있지 않기 때문에 가명성이 제공된다.

(13) 데이터 최소 노출

제안된 익명 전자처방전의 내용은 처방전의 작성자 $GP$와 검증자 $PH$ 이외에는 알 수 없다. $PH$가 처방전 조제가 완료된 이후에 의료보험료 요청을 위해 $HA$에게 처방전을 제공하기 전까지 전자처방전의 내용은 노출되지 않는다. 또한, 전자처방전은 환자 $P$의 스마트카드 내에 저장되어 있기 때문에 스마트카드의 기본 속성에 의해 PIN 인증을 통해 보호된다[16].

## 2. 기존 방식과 비교

본 소절에서는 B. Lee 등이 제안한 위임 서명기반 전

표 9. 계산 복잡도 비교를 위한 용어
Table 9. Notations to compare computation complexity.

| 용어 | 설 명 |
|---|---|
| $T_h$ | o 안전한 일방향 해쉬함수의 결과 값을 얻는데 걸리는 시간 |
| $T_{EXP}$ | o 모듈러 지수 연산을 하는데 걸리는 시간 |
| $T_{MUL}$ | o 모듈러 곱하기 연산을 하는데 걸리는 시간 |
| $T_{INV}$ | o 모듈러 역 연산을 하는데 걸리는 시간 |
| $\|k\|$ | o 정수 $k$의 비트 길이 |

표 10. 계산 복잡도 비교
Table 10. Comparison of computation complexity.

| 단계 | 개체 | 위임 서명기반 전자처방전 | 서명자 위조방지 전자처방전 | 제안한 익명 전자처방전* |
|---|---|---|---|---|
| 위임 | $GP$ | $T_{EXP}+T_{MUL}+T_h$ | $3 \cdot T_{EXP}+2 \cdot T_{MUL}+2 \cdot T_h$ | $T_{EXP}+T_{MUL}+T_h$ |
| | $HA$ | $2 \cdot T_{EXP}+T_{MUL}+T_h$ | $T_{EXP}+T_{MUL}+T_h$ | $2 \cdot T_{EXP}$ |
| 서명** | $GP$ | - | - | $T_{EXP}+T_{MUL}+T_{INV}$ |
| | $HA$ | $T_{EXP}+2 \cdot T_{MUL}+T_h$ | $3 \cdot T_{EXP}+3 \cdot T_{MUL}+2 \cdot T_h$ | $3 \cdot T_{EXP}+T_{MUL}+T_{INV}$ |
| 검증 | $PH$ | $3 \cdot T_{EXP}+3 \cdot T_{MUL}+2 \cdot T_h$ | $4 \cdot T_{EXP}+2 \cdot T_{MUL}+2 \cdot T_h$ | $T_{EXP}+T_h$ |
| 합계 | - | $7 \cdot T_{EXP}+7 \cdot T_{MUL}+5 \cdot T_h$ | $11 \cdot T_{EXP}+8 \cdot T_{MUL}+7 \cdot T_h$ | $8 \cdot T_{EXP}+3 \cdot T_{MUL}+2 \cdot T_h+2 \cdot T_{INV}$ |

* 제안하는 방식은 위임과 서명을 동시에 처리하지만 과정을 2개로 나누어 비교표에 적용함
** 위임 및 서명자 위조 방식의 이산대수 기반 전자서명은 Schnorr 전자서명 방식을 적용하여 비교함

자처방전, Y. Yang 등이 제안한 서명자 위조 방지 전자처방전과 제안하는 익명 전자처방전 방식을 계산 복잡도와 통신 비용을 비교한다. 먼저 계산 복잡도 비교를 위해 표 9의 표기를 사용한다.

모듈러 지수, 곱하기, 역 연산을 수행하기 위한 각각의 시간 복잡도는 $O(\log^3(p))$, $O(\log^2(p))$ 및 $O(\log^2(p))$이다[17]. 하지만 안전한 일방향 해쉬함수 계산하기 위한 시간 복잡도는 사용되는 암호학적 원시함수에 따라 달라진다. 본 논문에서는 $|p|$, $|q|$, $|h|$, $|b|$ 및 $|M|$의 크기를 각각 1024bit, 160bit, 160bit, 1024bit 및 1024bit로 정의한다[18].

표 10에서 보는 것과 같이 제안하는 방식이 위임 및 서명 단계의 전체 계산량을 비교해보면 상당히 효율적임을 알 수 있다. 제안된 방식은 서명자 위조 방지 전자처방전 보다는 최소한 효율적임을 알 수 있다.

## Ⅶ. 결 론

본 논문에서는 RSA 기반의 익명 전자처방전을 제안하였다. 제안된 방식은 현재 대부분의 국가에서 적용하고 있는 RSA 기반의 PKI 환경에 바로 적용할 수 있는 실용적인 방식이다. 제안된 방식은 전자처방전의 익명성을 보장하며 전자처방전에 대한 분쟁이 발생한 경우 건강보험기관과 협력하여 익명성을 추적할 수 있다. 또한 기존 방식에서 지적하고 있는 서명자 위조 방지를 건강보험기관의 부분 전자서명에 대한 권한을 분리하여 제공한다. *HC*는 전자처방전을 생성하기 위한 권한을 확인한 후 부분 전자서명을 생성하고, *HL*은 전자처방전의 내용 변경을 방지하기 위해 내용에 대한 검증 후에 부분 전자서명을 수행하도록 구성하였다. 또한 제안된 방식이 기존의 방식보다 시간 복잡도 및 통신비용 측면에서 효율적임을 보였다. 국내에 전자주민증이 국민에서 보급되고, 국민건강보험관리공단이 제안하는 방식을 도입한다면 전자처방전에 사용에 따른 분쟁을 쉽게 해결할 수 있고 약물 남용및 제약사와 약사간의 담합을 방지하는 등 국민의료건강보험에 투명성을 높이는데 기여할 것이다.

## 참 고 문 헌


[1] 박광석, "디지털 병원의 발전 동향", *전자공학회지*, 제33권 제11호, pp. 17-22, 2006.

[2] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems", *Communications of the ACM*, Vol.21, No.2, pp.120-126, 1984.

[3] ISO, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", *ISO/IEC 9594-8*, 2005.

[4] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its applications", *in Proc. SCIS*, pp.603-608, 2001.

[5] Y. Yang, X. Han, F. Bao and R.H. Deng, "A Smart-Card-Enabled Privacy Preserving E-Prrescription System", *IEEE Transactions on Information Technology in Biomedicine*, Vol.8, No.1, pp.47-58, 2004.

[6] 건강보험심사평가원, "의약품처방·조제지원시스템", http://www.hira.or.kr/rfl_dur_freeboard_intro_01.do 참조

[7] D Chadwick, D Mundy, "The secure electronic transfer of prescriptions", *Healthcare Computing 2004*, BCS HIC, pp.11-25. 2004.

[8] 한겨레신문, "제약사 리베이트 받은 의사·약사 처벌키로", http://www.hani.co.kr/arti/society/health/266182.html 기사 참조

[9] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", *IETF Request for Comment 5280*, 2008.

[10] D. Chaum, "Blind signature system", *CRYPTO '83*, Plenum Press, p.153, 1984.

[11] V. Shoup, "Practical threshold signatures", EUROCRYPT 2000, *Lecture Note in Computer Science, Vol.1087*, Springer-Verleg, pp.207-220, 2000.

[12] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., 1996.

[13] T. Dierks and C. Allen, "The TLS Protocol version 1.0", *IETF Request for Comment 2246*, 1999.

[14] J. Sermersheim, "Lightweight Directory Access Protocol (LDAP) : The Protocol", *IETF Request for Comment 4511*, 2006.

[15] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", *IETF Request for Comment 2560*, 1999.

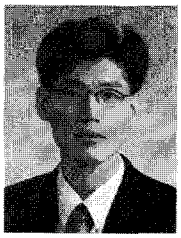
[16] M. Abadi , M. Burrows , C. Kaufman , B.

Lampson, "Authentication and Delegation with Smart-cards", *Proceedings of the International Conference on Theoretical Aspects of Computer Software*, p.326-345, 1991.

[17] J. Camenisch, "Group signature schems and payment systems based on the discrete logarithm problem", In: Maurer, U. (Ed.), *ETH Series in Information Security andCryptography*, vol. 2, Hartung-Gorre Verlag Konstanz, pp.11-12, 1998.

[18] A. Lenstra. E. Verheul, "Selective Cryptographic Key Sizes", Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography : Public Key Cryptography, *Lecture Notes in Computer Science, Vol.1751*, Springer-Verleg, pp.446-465, 2000.

## 저 자 소 개

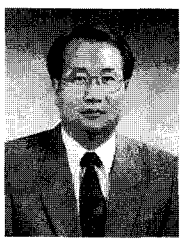


**정 찬 주**(정회원)

1999년 강남대학교 전자계산학과 학사 졸업.
2001년 성균관대학교 전기전자 컴퓨터공학과 석사 졸업.
2005년 성균관대학교 컴퓨터 공학과 박사수료.
2000년~현재 한국인터넷진흥원 책임연구원
2005년~현재 TTA 정보보호기술위원회(TC5) 개인정보보호 및 ID관리 프로젝트 그룹(PG502) 위원
<주관심분야 : 암호이론, PKI, 개인정보보호>

**윤 정 미**(정회원)-교신저자

1996년 성균관대학교 정보공학과 학사졸업.
2001년 성균관대학교 전기전자 컴퓨터공학과 석사졸업.
2007년 성균관대학교 컴퓨터 공학과 박사수료.
2000년~현재 전자부품연구원 선임연구원
<주관심분야 : 무선통신, RFID>



**원 동 호**(정회원)

1976년 성균관대학교 전자공학과 학사 졸업
1978년 성균관대학교 전자공학과 석사 졸업
1988년 성균관대학교 전자공학과 박사 졸업
1978년~1980년 한국전자통신연구원 전임연구원
1992년~1994년 성균관대학교 전자계산소 소장
1995년~1997년 성균관대학교 교학처장
1997년~1998년 정보화추진위원회 자문위원(발령 정보화추진위원회 위원장 국무총리)
1999년~2001년 성균관대학교 정보통신대학원 원장
2002년~2003년 한국정보보호학회 회장
2002년~2004년 대검찰청 컴퓨터 범죄 수사 자문위원
2002년~2004년 성균관대학교 연구처장
2002년~2003년 감사원 IT 감사 자문위원
2002년~2004년 산학연 정보보안협의회 회장
2005년~현재 정보보호인증기술연구소 소장
2005년~2008년 한국정보보호진흥원 이사
2009년~현재 성균관대학교 BK21 사업단장
<주관심분야 : 암호이론, 정보이론, 정보보호>