EC-ELGAMAL 준동형 암호화기반 전자투표

서화정* · 김호원**

EC-ELGAMAL Homomorphic Cryptography based E-voting System

Hwa-jeong Seo* · Ho-won Kim**

본 논문은 지식경제부 산업융합원천기술개발사업으로 지원된 연구결과입니다(No.10043907).

요 약

디지털로 처리되는 전자투표의 실현은 사회전반에 걸쳐 유권자 투표참여의 확대, 신속한 개표작업을 가능하게 하여 정치적, 사회적 그리고 기술적 혁명을 가지고 오게 될 기술이다. 하지만 기술도입에 있어 안전한 보안투표 기술이 제공되지 않고는 실용화에 큰 문제가 있다. 본 논문에서는 EC-ELGAMAL 준동형 암호화기반 전자투표 프로토콜을 통해 중간과정에서 복호화 과정없이 투표정보를 종합하여 중앙 서버에 보내게 되고 이를 중앙 서버에서 개표가 가능한 프로토콜을 제안한다. 사용자는 중앙서버에서 제공해 주는 pseudo 아이디를 통해 익명성을 보장받음과 동시에 자신의 투표권이 반영되었음을 Bloom Filter 기술을 통해 안전하게 확인할 수 있다. 여기에 더불어 속성기반 정보를 투표자 정보와 결부시켜 투표자의 익명성을 보장받음과 동시에 서버에서는 투표자의 정보를 수집할 수 있도록 하였다.

ABSTRACT

Since realization of E-voting system expands participation of voters and efficient count of voting, political and social and technical revolution is possible. However, without secure e-voting system, practical usages are infeasible. In the paper, we propose an e-voting system which is able to open votes in server without decryption during midst process using EC-ELGAMAL homomorphic cryptography. Users ensure anonymity with pseudo id from server and check their voting with Bloom Filter technology. Furthermore, we combine attributes and voters' information, so we can collect information of voter under the condition of anonymity.

키워드

E-voting, Homomorphic Cryptography, EC-ELGAMAL

Key word

전자투표, 준동형 암호, EC-ELGAMAL

* 정회원 : 부산대학교 컴퓨터공학과 박사과정

** 종신회원 : 부산대학교 컴퓨터공학과 교수(교신저자, howonkim@pusan.ac.kr)

접수일자 : 2012. 09. 03

심사완료일자 : 2013. 04. 01

I. 서 론

인터넷의 급속한 보급과 초고속 정보통신망의 구축은 언제 어디서나 서비스를 제공받는 것이 가능한 유비쿼터스 시대를 가능하게 했다. 이러한 추세는 현재 전 세계의 스마트폰 보급률이 21%를 넘어서면서 보다 가속화되고 있다[1]. 유비쿼터스 시대의 도래는 다양한 서비스를 창출하고 있으며 이 중에서도 사회전반에 걸쳐 큰 영향을 미칠 수 있는 전자투표에 대한 연구가 활발히 진행되고 있다. 전자투표란 디지털화된 투표와 개표를 포괄하는 새로운 개념의 서비스로써 투표를 제고와 투표관리 업무의 생산성 증대가 가능하다[2]. 하지만 비밀투표 문제와 보안성 문제로 인해 그 효용가치가 위협받고 있다[3]. 따라서 보안위협으로부터 안전하게 보호되는 전자투표 시스템의 구축은 성공적인 서비스 제공을 위해 무엇보다 중요하다. 하지만 보안을 위해 투표 메시지를 암호화하여 전송하게 될 경우 중간과정에서 메시지를 복호화하기 어려울 뿐 아니라 모든 메시지를 상위 기관으로 전송 시에는 유통되는 메시지의 크기가 선형적으로 증가하여 실용적이지 못한 측면을 가진다. 따라서 암호문에서 필요한 정보만을 추출하여 상위 기관에 안전하게 전달하는 것이 가능한 준동형 암호화 기술은 안전한 전자투표를 위해 고려되고 있다[4]. 본 논문에서는 익명성이 보장됨과 동시에 안전한 투표가 가능한 전자투표방법을 제안한다. 이를 통해 언제 어디서나 전자투표에 참여하는 것이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서는 논문의 관련연구에 대하여 설명한다. 3장에서는 제안하는 알고리즘을 나타낸다. 4장에서는 제안된 알고리즘을 평가하며 5장에서는 본 논문의 결론을 맺는다.

II. 관련연구

2.1. 전자투표

전자투표는 전자적 수단에 의한 투표와 개표가 가능한 기술로써 투표관리업무의 생산성 증대, 투표를 제고 그리고 해외 거주자 투표문제 해결과 같은 다양한 문제를 해결할 수 있다.

지금까지 공개키를 사용한 다양한 전자투표가 제안되었다. [5, 6, 7, 8]에서는 EC- ElGamal기법을 [9, 10, 11]에서는 ElGamal기법을 사용하여 준동형 암호화 기법을 활용한 투표기법이 제안되었다. 그림 1에서와 같이 전자투표는 준동형 암호화가 가능한 EC-ElGamal에 대한 연구가 활발히 진행되고 있다.

그림 1. 전자투표 상에서의 암호화 기법의 발달과정
Fig. 1 Development of cryptography for E-voting

안전한 전자투표를 위해서는 다음과 같은 보안 요구사항이 충족해야 한다[12].

- 완전성(Completeness) : 모든 정당한 유효 투표는 정확하게 투표 결과에 집계되어야 한다.
- 건전성(Soundness) : 부정 투표자에 의하여 투표가 방해되어서는 안 되며, 투표 결과에 부정 투표가 집계되어서도 안 된다.
- 기밀성, 익명성(Privacy) : 모든 투표는 비밀리에 이뤄져야 하며, 투표자의 투표내용을 알 수 없어야 한다.
- 이중투표 불가성(Unreusability) : 정당한 투표자는 두 번 이상의 투표를 할 수 없어야 한다.
- 권한성(Eligibility) : 투표권이 없는 사람은 투표에 참여할 수 없어야 한다.
- 공정성(Fairness) : 투표에 영향을 미치는 일이 없어야 한다. 특히, 투표과정 중 일부분의 투표내용이 알려져 투표에 영향을 미쳐서는 안 된다.
- 검증성(Verifiability) : 투표결과를 조작할 수 없도록 누구라도 자신의 투표내용이 투표결과에 반영되었는지 검증할 수 있어야 한다.

2.2. 준동형 암호화를 통한 전자투표

식 1은 준동형 암호화의 성질을 나타낸다. 여기서 $En_{k1}(m)$ 은 평문 m 을 공개키 $k1$ 를 이용한 암호화를 나타내며 $De_{k2}(c)$ 은 암호문을 비밀키 $k2$ 를 이용하여 복호화하는 과정을 나타낸다[8, 13]. 준동형 암호를 통한 전자투표는 다음과 같이 수행된다.

$$f_1(m_1, m_2) = De_{k2}(f_2(En_{k1}(m_1), En_{k1}(m_2))) \quad (1)$$

- 후보선택 : 집합 $\{c_0, c_1, c_2, \dots, c_m\}$ 는 각각의 후보자를 나타내는 정수를 나타낸다. 만약 c_i 후보자를 선택하게 되면 후보자에 대한 메시지는 식 2와 같이 나타난다. 여기서 P 는 기저 값으로 사용되게 된다.

$$M_i = c_i \cdot P \quad (2)$$

- 암호화 : 암호화된 메시지는 식 3과 같이 계산된다. 여기서 Q 는 공개된 키를 의미하며 r_i 는 생성된 난수를 의미한다.

$$e_i = encryption(M_i) = (r_i \cdot P, M_i + r_i \cdot Q) \quad (3)$$

- 투표 봉치 생성 : 투표자들의 표가 투표되고 나면 투표결과를 식 4와 같이 투표봉치 형식으로 통합하게 된다.

$$\begin{aligned} Package_j &= e_0 + e_1 + \dots + e_{n-2} + e_{n-1} \\ &= (r \cdot P, (\dots + M_{n-3} + M_{n-2} + M_{n-1}) + r \cdot Q) \end{aligned} \quad (4)$$

- 투표 결과 섞기 : 투표봉치가 제작되고 나면 해당 투표 봉치를 섞어서 구분이 불가능하도록 한다[14].

- 복호화 : 투표봉치에 대한 복호화가 EC-ELGAMAL을 통해 수행된다.

$$\begin{aligned} D = decryption(Package) &= \\ &\dots + M_{i-1} + M_i + M_{i+1} + \dots \end{aligned} \quad (5)$$

- 개표 : 복호화과정에서 생성되었지만 통합된 메시지에서 정보를 얻기 위해 해석하는 작업을 수행한다. 투표수 $(x_1, x_2, \dots, x_m)$ 를 복호화된 메시지 식 6에서 확인한다.

$$D = (x_1 \cdot c_1 + x_2 \cdot c_2 + \dots + x_m \cdot c_m)P \quad (6)$$

- 결과확인 : 개표 작업을 통해 합산된 투표 결과를 확인한다.

2.3. Bloom-Filter

블룸 필터는 1970년 Burton H. Bloom에 의해 제안된 확률적인 특성을 가지는 자료구조이다[15]. 해당 자료구조는 주어진 집합에 찾고자 하는 원소가 포함되어 있는지 판단하기 위해 포함되는 원소의 비트를 해시 함수로 계산한 후 자료구조에 포함시키는 형식으로 동작한다.

2.4. 속성기반 암호화 기법

Sahai와 Waters에 의해 제안된 퍼지 아이디 기반 암호화(Fuzzy Identity-Based Encryption) 기법[16]은 신원(Identity)기반 암호화 기법[11]을 확장한 것으로 송신자가 선택한 속성 값을 암호 인자로 암호화하여 해당 속성값을 가지고 있는 수신자가 복호화 할 수 있도록 제안된 시스템이다. 해당 기법은 암호화 과정이 기존의 신원 기반 암호화 기법에서와 같이 1대1관계가 아닌 1대N관계이므로 분산 환경 시스템에서의 다양한 응용에 적용가능하다. 이는 익명성을 보장하기 위해 신원을 숨기게 됨으로써 기존에 제공하지 못했던 특성에 따른 서비스제공이 가능하다는 장점을 가진다. 예를 들어 기존 방법은 기업과 단체에서의 인증시스템에서 요구하는 서비스의 다양성을 제공하지 못한다. 전자투표에서도 상대방에 대한 정확한 정보는 얻을 수 없지만 그 사람이 가지고 있는 속성을 통해 맞춤형 서비스 제공이 가능하다는 장점을 가진다. 인증의 다양성은 사용자의 프라이버시가 보호되면서 동시에 사용자가 가지는 속성을 통해 다양한 서비스 제공이 가능한 시스템을 의미한다.

III. 제안하는 프로토콜 및 기법

본 장에서는 제안하는 EC-ElGamal 준동형 암호화 기반 전자투표 프로토콜의 동작도를 제시한다.

3.1. 프로토콜 정의

본 장에서는 EC-ElGamal 준동형 암호화 기반 전자투표 프로토콜을 제안한다. 표 1에서는 제안된 프로토콜에서 사용된 용어와 그 의미에 대해 살펴본다.

표 1. 제안된 프로토콜에 사용되는 용어
Table. 1 Description of Notation for Proposed Method

기호	설명
ID	아이디
PW	사용자의 패스워드
r	스마트카드와 서버에서 생성되는 랜덤 값
Pri	비밀키 값
Pub	공개키 값
C	카운터 값
$Cert()$	EC-ElGamal 전자서명
$E()$	EC-ElGamal 암호화
$EH()$	EC-ElGamal을 이용한 준동형 암호화
S	지방 정부의 비밀키 값
M	투표정보
$B()$	블룸필터에 값 적용
$Package$	중간 암호화값을 이용해 작성한 패키지
A_i	사용되는 속성값
U_i	사용자 i 를 나타내는 기호
$h()$	$\{0,1\}^* \rightarrow \{0,1\}^l$ 일방향 해쉬 함수
$T, \Delta T$	타임스탬프, 타임스탬프 허용제한시간
$\oplus$	bitwise exclusive-or 연산
$\Rightarrow$	안전한 회선을 통한 전송
$\rightarrow$	일반 회선을 통한 전송
LA	지방 서버
CA	중앙 서버
$[A:B]$	A로 B를 검색할 수 있는 데이터베이스 레코드

제안된 프로토콜의 사용자 인증과정은 사용자의 비밀번호와 아이디 그리고 속성에 해당하는 값을 생성하

여 중앙 서버에 전달한다. 중앙 서버에서는 사용자에게 해당하는 Y_i 값과 공개키, 비밀키를 생성하고 $h(Y_i \oplus PW)$ 값을 키값으로 하여 $PW_i, ID_i, Y_i, A_i, Pub_i, Pri_i$ 를 저장하게 된다. 중앙 서버는 Y_i, Pub_i, Pri_i 를 사용자에게 전달하고 사용자는 $h(Y_i \oplus PW_i)$ 를 생성한다. 중앙 서버는 이와 동시에 $h(Y_i \oplus PW_i), A_i, H(C \oplus S), Pub_i$ 를 지방 서버에 전달하게 된다. 지방 서버는 $H(C \oplus S)$ 를 확인하고 $h(Y_i \oplus PW_i)$ 값을 키값으로 A_i, Pub_i 를 저장하게 된다.

표 2. 제안된 프로토콜의 사용자인증
Table. 2 User Authentication for Proposed Protocol

1. $U_i : PW_i, ID_i, A_i$ 을 CA 에게 전달한다.
2. $CA : Y_i, Pub_i, Pri_i$ 를 생성하고 $h(Y_i \oplus PW)$ 값을 키값으로 하여 $PW_i, ID_i, Y_i, A_i, Pub_i, Pri_i$ 를 저장한다.
3. $CA : Y_i, Pub_i, Pri_i$ 를 U_i 에게 전달한다.
4. $U_i : h(Y_i \oplus PW_i)$ 를 생성한다.
5. $CA : h(Y_i \oplus PW_i), A_i, H(C \oplus S), Pub_i$ 를 LA 에게 전달한다.
6. $LA : H(C \oplus S)$ 를 확인하고 $h(Y_i \oplus PW)$ 값을 키값으로 A_i, Pub_i 를 저장한다.

사용자는 자신의 투표정보가 담긴 암호문을 준동형 암호화 기법을 통해 암호화하게 되고 이에 대한 서명값과 $h(Y_i \oplus PW)$ 값을 첨부하여 지방 서버에 전송하게 된다. 지방 서버는 $h(Y_i \oplus PW)$ 를 통해 공개키와 속성값을 확인하게 된다. 속성값은 해당 투표자를 나타내는 정보가 아닌 속성을 나타내는 정보로써 추후 빅데이터 처리를 통해 의미있는 정보를 재생산하는 것이 가능하다. 공개키는 전송된 데이터의 서명값을 확인한다. 지방 서버는 카운터값을 증가시킨 후 $h(C \oplus S \oplus T) \oplus h(Y_i \oplus PW_i)$ 값을 생성하게 된다.

해당 정보는 지방 서버의 아이디와 타임스탬프를 동반하여 중앙 서버에 전달되게 된다. 중앙 서버는 타임스탬프를 확인하고 메시지를 검증하게 된다. 그리고 $h(Y_i \oplus PW_i)$ 값을 통해 해당 투표자가 이전에 투표가 되었는지를 확인한다. 확인이 되면 카운터값을 증가시키고 $h(C \oplus S \oplus T) \oplus h(Y_i \oplus PW_i)$ 를 지방 서버에게 전달하게 된다. 지방 서버에서는 난수와 타임스탬프 그리고 암호화된 메시지를 통해 블룸필터 값을 생성하게 된다.

표 3. 제안된 프로토콜의 투표단계
Table. 3 Proposed Protocol for Voting

1. $U_i : eh_L, Cert_i$ 를 생성한다.
2. $U_i : h(Y_i \oplus PW), e_i, Cert_i$ 를 LA 에게 전달한다.
3. $LA : h(Y_i \oplus PW)$ 를 통해 정보를 검색한다.
4. LA : 전송된 메시지를 검증한다.
5. LA : C 를 업데이트 한다.
6. $LA : h(C \oplus S \oplus T) \oplus h(Y_i \oplus PW)$ 를 생성한다.
7. $LA : ID_L, h(C \oplus S \oplus T) \oplus h(Y_i \oplus PW), T$ 를 CA 에게 전달한다.
8. CA : 타임스탬프를 확인하고 메시지를 검증한다.
9. $CA : h(Y_i \oplus PW)$ 를 확인하여 투표가 진행되었는지 확인한다.
10. CA : C 를 업데이트 한다.
11. $CA : h(C \oplus S \oplus T) \oplus h(Y_i \oplus PW)$ 를 LA 에게 전달한다.
12. $LA : r, T, B_i$ 를 생성한다.
13. LA : 암호화 메시지를 패키지에 포함시킨다.
14. LA : 난수와 타임스탬프를 암호화하고 eh_L 을 서명한다.
15. $LA : pi, e_i, Cert_L$ 을 U_i 에게 전송한다.
16. LA : 블룸필터와 투표 봉치를 암호화 및 서명하여 CA 에게 전송한다.
17. U_i : 암호화된 메시지를 복호화하고 블룸필터 정보를 생성한다.
18. CA : 전송된 정보를 검증하고 투표 봉치화된 정보를 개표하여 표를 반영한다.

준동형 암호화로 암호화된 메시지는 투표 봉치에 포함되게 된다. 지방 서버에서는 난수와 타임스탬프를 암호화하고 eh_L 값을 포함하여 서명하게 된다. 지방 서버는 암호문과 서명 그리고 패키지 정보를 사용자에게 전달하게 되고 사용자는 메시지를 검증하고 블룸필터값을 생성하게 된다. 지방서버는 이와 동시에 블룸필터와 투표 봉치를 암호화 및 서명하여 중앙 서버에 전송하게 되고 중앙 서버는 해당 정보를 검증하고 복호화 그리고 개표하여 전체 투표 결과에 반영하게 된다.

유저는 자신의 투표정보가 첨부된 투표 봉치의 아이디에 해당하는 정보를 중앙 서버에 전달한다. 중앙서버는 투표 봉치 아이디를 통해 해당 블룸필터 정보를 확인해서 블룸필터의 서명값과 함께 유저에게 보내주게 된다. 유저는 블룸필터에 자신의 정보가 반영되었는지를 확인함으로써 투표의 정당성을 확인하게 된다.

표 4. 제안된 프로토콜의 투표반영 확인단계
Table. 4 Proposed Protocol for Voting Confirmation

1. $U_i : pi$ 를 CA 에게 전달한다.
2. $CA : pi$ 를 통해 B 를 검색한다.
3. $CA : B$ 를 서명값과 함께 U_i 에게 보낸다.
4. $U_i : B$ 를 확인한다.

그림 2은 제안된 프로토콜의 사용자 인증, 그림 3에서는 투표단계 그리고 투표반영 확인단계에 설명하고 있다.

그림 2. 제안된 프로토콜의 사용자 인증단계
Fig. 2 User Authentication Process for Proposed protocol

그림 3. 제안된 프로토콜의 투표 단계 및 투표반영 확인단계
Fig. 3 Process of voting and confirmation process

IV. 평 가

제안하는 프로토콜은 모든 보안 요구사항을 만족한다.

- 완전성 : 개표결과 검증 시 투표자는 자신이 투표했던 정보를 토대로 작성된 bloom필터 정보를 통해 자신의 투표 내용의 개표 사실을 확인할 수 있다. 따라서 중앙 서버가 악의적인 공격자에 의해 조정당하지 않는 한 정당한 투표는 최종 결과에 반영된다.
- 건전성 : 모든 전송되는 구간에서는 서버의 비밀키와 투표자의 비밀키값만으로 확인이 가능한 메시지를 생성 및 전송함으로 이러한 정보를 생성한다는 것은 EC-ElGamal의 안전성에 기반함으로 전송되는 메시지는 건전하다고 할 수 있다.
- 이중투표 불가능성 : 투표자는 중앙 서버에 의해 운영되는 리스트를 확인하여 이미 투표를 수행했는지 혹은 투표자의 서명값을 확인하여 메시지값이 건전하게 생성되었는지를 확인하는 과정을 가진다. 따라서 부정적인 투표가 반영될 확률은 없다.

- 기밀성/ 익명성 : 전송되는 메시지는 사용자의 아이디가 아닌 패스워드와 Y_i 값을 통해 생성된 해시값으로 지정되므로 이를 통해 사용자의 정보를 확인하는 것은 불가능하다. 만약 오랫동안 정보를 사용하여 해시값을 통해 추측공격이 가능하다면 패스워드를 증가시키는 방안으로 가짜 아이디 정보를 갱신하면 추측공격이 불가능하다. 또한 모든 메시지는 암호화되어 전송되므로 비밀키값을 알지 못할 경우 전송되는 암호문의 평문 정보를 얻는 것은 불가능하다.
- 책임성 : 서버는 투표를 하는 투표자의 정보를 데이터 베이스에서 유지하며 사전에 사용자 등록이 되어 있는 경우에 한해서만 올바른 투표가 가능하도록 설계되어 있다. 따라서 부정한 사용자가 투표를 하는 것은 본 시스템에서는 불가능하다.
- 공정성 : 전송되는 투표 결과값은 EC-ElGamal 암호를 통해 암호화되어 전송된다. 따라서 중간에 공격자가 해당 정보를 도청하더라도 서버의 비밀키값을 확인하지 않고서는 전송되는 정보를 확인하는 것이 불가능하다.
- 전체 검증성 : 투표문치마다 일정수의 투표가 포함되

고 이를 전부 인덱스화하여 저장 및 관리한다. 해당 인덱스 정보는 사용자와 서버가 공유하게 되므로 모든 인덱스값을 전체적으로 확인해 보게 되면 전체 투표결과가 포함되었는지를 확인할 수 있다.

- 개별 검증성 : 투표자는 자신의 투표권이 정당하게 포함되어있는지를 확인하기 위해 패키지의 블룸필터값을 확인하게 되고 해당 값을 중앙서버에서 제공받은 값과 비교하여 정당한 값을 나타낼 때 자신의 투표가 반영되었음을 확인할 수 있는 구조를 제공하고 있다. 따라서 투표자는 개별적으로 자신의 투표권을 확인하는 것이 가능하다.
- 매표 불가성 : 블룸필터의 정보를 통해 자신의 정보가 반영되었음을 확인하는 것은 가능하지만 난수값과 타임스탬프값이 추가되어 해당 블룸필터가 정확히 어떤 후보자를 가리키는 지에 대해서는 확인이 불가능하다. 따라서 이를 통해 자신의 투표권을 매매하는 것은 불가능하다.

제안하는 프로토콜은 표 5에서와 같이 EC-ElGamal을 통해 보다 준동형을 만족함과 동시에 낮은 복잡도로 동작이 가능하다.

표 5. 전자서명 프로토콜들 상에서 사용한 암호화 기술
Table. 5 Cryptography for E-voting

전자서명 프로토콜	사용한 암호화 기술
Lee[18]	공개키
Li[9]	ElGamal
Kim[19]	공개키
Bo[10]	ElGamal
Tohari[17]	ECC
Kim[7]	EC-ElGamal
Sodiya[6]	EC-ElGamal
Yi[5]	공개키
Carrera[8]	EC-ElGamal
제안하는 알고리즘	EC-ElGamal

V. 결 론

본 논문에서는 EC-ELGAMAL 준동형 암호화 기반 전자 투표 프로토콜을 제안하였다. 해당 프로토콜은 EC-ElGamal을 통한 암호화를 통해 중간에서 암호화된 메시지를 전부 복호화하지 않고 상위 서버에서 복호화가 가능한 투표가 가능하며 투표결과 확인이 블룸필터를 통해 가능하다. 또한 속성값을 통해 투표자의 정보를 익명성을 제공한다. 따라서 본 논문에서 제안된 기법은 기존의 준동형 암호화 기법에 사용자 익명성과 투표확인 기능이 추가된 새로운 기법이다.

참고문헌

- [1] V. Manolopoulos, "Security and privacy in smartphone based intelligent transportation systems," Thesis of Royal institute of technology, 2012.
- [2] Electronic voting, http://en.wikipedia.org/wiki/Electronic_voting, last access at 2012.
- [3] 정진우, "전자투표의 효과와 문제점에 관한 탐색적 연구," 행정논총 pp. 107-126. 2003.
- [4] R. Rivest, "Lecture Notes 15: Voting, Homomorphic Encryption," 2002.
- [5] Y. Xun, O. Eiji, "Practical Mobile Electronic Election," SII International, pp. 1119-1124, 2011.
- [6] A. S. Sodiya, S. A. Onashoga and D. I. Adelani, "A Secure E-voting Architecture," 2011 Eighth International Conference on Information Technology, pp. 342-347, 2011.
- [7] C. J. Kim, "A Lightweight ECC Algorithm for Mobile RFID Service," Ubiquitous Information Technologies and Applications (CUTE), 2010 Proceedings of the 5th International Conference on, pp. 1-6, 2010.
- [8] C. F. Treball, "An electronic voting platform with elliptic curve cryptography," Enginyeria Tecnica en Informatica de Sistemes Escola Politecnica Superior Universitat de Lleida, pp. 1-46, 2011.
- [9] L. Xiangdong, C. Michael, K. C. Andis, L. Lin, E. Amara, A. Michael, "An Elementary Electronic Voting

- Protocol Using RFID,” Proceedings of the 2007 IEEE Workshop on Information Assurance, pp. 234-238, 2007.
- [10] M. Bo, “An Internet Voting Protocol With Receipt-free and Coercion-resistant”, Seventh International Conference on Computer and Information Technology, pp. 721-726, 2007.
- [11] D. Boneh, M. Franklin, “Identity-based encryption from the weil pairing,” CRYPTO, pp. 213-229, 2001.
- [12] 허원근, 김희선, 김광조, “전자선거 프로토콜의 요구사항 연구,” 한국정보보호학회, 정보보호학회지, Vol. 10, No. 1, pp. 63-69, 2000.
- [13] Z. Erkin, A. Piva, S. Katzenbeisser R.L. Lagendijk, J. Shokrollahi, G. Neven, M. Barni, “Protection and retrieval of encrypted multimedia content: when cryptography meets signal processing,” EURASIP Journal on Information Security, pp. 1-10, 2007.
- [14] O. Carro, “Random Group Full Checking sobre corbes elliptiques,” Thesis of Carrera. Universitat de Lleida, 2011.
- [15] B. Bloom. “Space/Time Trade-offs in Hash Coding with Allowable Errors,” Communications of ACM, vol. 13, no.7, pp. 422-426, Jul. 1970.
- [16] A. Sahai, B. Waters, “Fuzzy identity-based encryption,” Proc. of EUROCRYPT’05, LNCS3494, pp. 457-473, 2005.
- [17] T. Ahmad, J. Hu, S. Han, “An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography,” IEEE 2009 Third International Conference on Network and System Security, pp. 474-479, 2009.
- [18] 이래, 이동훈, “서비스 현실화에 중점을 둔 인터넷 전자 투표 시스템”, 한국정보보호학회, 정보보호학회지, vol. 14, no. 5, pp. 8-18, 2004.
- [19] 김지웅, 강동민, 이성우, 정현우, “공개키 기반 구조 (PKI)를 이용한 실용적인 인터넷 전자 투표 시스템”, Kaist, 2007.

저자소개

서화정(Hwa-jeong Seo)

2004.3~2010.2 : 부산대학교
정보컴퓨터공학과 학사
2010.3~2012.2 : 부산대학교
컴퓨터공학부 석사

2012.3~현재 : 부산대학교 컴퓨터공학부 박사
※관심분야: 정보보안, RFID/USN, 암호 이론, VLSI 설계

김호원(Ho-won Kim)

1989. 3~1993. 2 : 경북대학교
전자공학과 학사
1993. 3~1995. 2 : 포항공과대학교
전자전기공학과 공학석사

1995. 2~1999. 2 : 포항공과대학교 전자전기공학과
공학박사
1998. 12~2008. 2 : 한국전자통신연구원(ETRI)
정보보호연구단 선임연구원 / 팀장
2008. 3~현재 : 부산대학교 정보컴퓨터공학부 부교수
※관심분야: 스마트그리드 보안, RFID/USN 정보보호
기술, PKC 암호, VLSI 설계, embedded system 보안