通信情報保護學會誌
第6卷 第1號, 1996. 3

전자투표

Electronic Vote

박 춘 식*

요 약

전자투표는 현행 투표방식의 많은 문제점들을 해결할 수가 있으며, 초고속 정보 통신의 보급을 위한 가장 좋은 수단으로써 활용될 수 있다. 본 논문에서는 전자투표에 대한 추진과 연구 현황을 소개하고, 암호를 이용한 전자투표 방식인 다자간 프로토콜을 이용한 방식과 익명 통신로를 이용한 전자투표 방식을 주로 분석하고자 한다. 또한 전자투표에 주로 많이 사용되는 암호학적인 도구들도 간략히 검토하고 다자간 프로토콜과 익명 통신로도 간략히 소개한다.

1. 서 론

현대 사회에 있어서, 여러가지 형태의 선거가 무기명투표로 많이 행하여 지고 있다. 무기명투표는 투표자와 투표내용의 대응이 비밀로 보호되는 투표방식을 말하며 어떤 투표자가 어떤 투표내용을 투표하였는지를 보호할 수 있는 방식이다. 현행의 대부분의 선거는 투표자가 투표소까지 가서 직접 투표하지 않으면 안되는 방식으로 많은 불편이 수반되고 있다. 이는 유권자를 확인할 수 있는 선거인명부가 하나로만 갖추어져 있기 때문이며 이를 복수화할 경우 이중투표를 막을 수 있는 대책이 없기 때문이다. 그러나, 투표소에서 행하는 투표 작업이 자기 집이나 사무실 그리고 역, 공항 등의 공공장소에 있는 전화기나 컴퓨터 또는 공중전화기 등을 이용하는 전자투표로 행하여 질 수 있다면 투표자의 불편은 크게 개선될 것이며 선거 제도 또한 획기적인 전기를 맞이할 것이다.

한편, 인터네트의 급속한 보급이나 초고속 정보통신망의 구축에 따른 정보화 사회의 촉진은 새로운 정보 서비스의 등장이나 생활의 많은 변화를 가져올 것이다. 이러한 차원에서 고려될 수 있는 새로운 정보 서비스 분야중의 하나가 바로 전자투표가 될 수 있다.

전자투표는 신임이나 정책 결정에 대한 의사 표현, 대통령, 국회의원, 지방자치 단체장 등의 선출, 그리고 각종 여론 조사 등 다양한 분야에서 사용될 수 있으며, 초고속 정보 통신의 보급을 위한 가장 좋은 수단으로써 활용될 수 있다.

이미 미국의 일부 지역에서는 투표 용지를 사용하지 않고 기계식이나 전자식으로 선거가

* 한국전자통신연구소 부호기술연구부

이루어지고 있으며, 가까운 일본에서도 전자투표시스템 도입을 위해 각 지방 자치단체가 검토하거나 모의 실험을 실시중에 있다. 최근 우리나라에서도 컴퓨터망을 통한 선거 홍보전을 정당차원에서 수행하고 있으며 선거 사무 자동화나 투.개표 업무의 전산화 추진을 위한 연구[1][2][3] 및 검토가 이루어지고는 있으나, 아직 선거를 전자 투표화하는 단계까지는 이르지 못한 실정이다.

전자투표에 대한 연구는 암호학을 연구하는 그룹들에 의해서도 많이 행하여지고 있다. 이는 안전한 전자투표 그리고 신뢰받을 수 있는 전자투표가 되기 위해서는 암호의 사용이 불가피하기 때문이다. 전자현금으로 유명한 네델란드의 암호학자 D.Chaum이 암호를 이용한 전자투표[4]를 제안한 이래 미국의 J.C.Benaloh[5], 일본의 K.Sako[6], K.Ohta[7]등 세계 여러나라에서 활발히 연구가 진행되고 있으며 이 분야에서의 특허도 다수 출원되고 있는 실정이다.

이 논문에서는 전자투표에 대한 연구 현황을 중심으로 소개하고 암호를 이용한 전자투표방식인 다자간 프로토콜(Multi-party Protocol)을 이용한 방식[5]과 익명 통신로(Anonymous Channel)를 이용한 전자투표 방식[4]을 주로 분석하고자 한다. 또한 전자투표에 주로 많이 사용되는 암호학적인 도구들도 간략히 검토하고 다자간 프로토콜과 익명 통신로도 간략히 소개한다.

이 논문은 모두 8개장으로 구성, 진행된다. 먼저, 전자투표에 대한 설명으로 전자투표의 개념, 전자투표가 최소한 갖추어야 할 요구 사항, 전자투표가 갖는 장점, 전자투표에 대한 사용 현황을 외국의 예와 국내 현황 그리고 전자투표에 대한 연구 현황을 2장에서 소개한다. 3장에서는 전자투표에 사용되는 내용은닉서명(Blind Signature)[8], VSS(Verifiable Secret Sharing)[9][10] 등 각종 암호 관련 Tool들을 소개한다. 전자투표에 사용되는 대표적인 도구들인 다자간 프로토콜과 익명 통신로를 간략히 그리고 알기 쉽게 4장에서 설명한다. 5장에서는 전자투표의 대표적인 방식중의 하나인 다자간 프로토콜을 이용한 전자투표 방식을 소개하고, 6장에서는 익명 통신로를 전제로 하는 효율적인 전자투표 방식을 설명한다. 전자투표의 대표적인 방식들의 비교와 전자투표에 대한 향후 전망을 7장에서 설명한다. 마지막으로 결론부를 8장에 둔다.

2. 전자투표

2.1 전자투표란?

국내의 일반적인 선거 관리 절차는 선거인명부 작성, 명부 열람, 이의 신청, 선거인 명부 확정, 투표통지표 송부 등의 사전 준비 작업과 지정된 투표소에서 신분 확인을 한 후 기표를 하는 투표 절차 그리고 투표함의 도착 완료 후 결과를 집계하는 개표 절차로 이루어진다.

기존의 사전 준비 단계는 전산화 작업으로 선거관리단체에서 안전하게 이루어 질 수 있으므로, 이 논문에서 설명하는 전자투표의 취급 범위는 주로 투표와 개표 단계에서 암호를 이용하여 안전한 전자 투표시스템을 구현하는 것을 말한다. 전자투표 시스템은 선거인 명부를 데이터베이스로 구축한 중앙 시스템과 직접 연결한 단말에 자신이 정당한 투표자임을 증명하면 단말이 있는 전국 어디서나 쉽게 컴퓨터망을 통하여 무기명 투표를 할 수 있는 방식이라고 간략히 정의할 수 있다.(그림 1참조)

전자투표를 간단히 설명하기 위해 정책의 결정이나 신임을 묻는 찬반 투표의 경우를 설명한다. 그림 1에 나타난 바와 같이 센터는 투표 집계소가 되며 컴퓨터 통신망을 통하여 투표가 다음과 같이 이루어지게 된다.

(step 1) 센터는 찬반을 묻고자 하는 사안을 공개하여 투표를 요청한다.

(step 2) 각 유권자는 컴퓨터나 전화기 등을 통하여 자신의 찬반 결과를 센터에게 보낸다.

(step 3) 센터는 각 유권자로부터 받은 찬반 결과를 집계하여 공표한다.

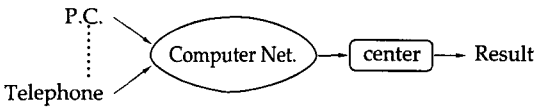


그림 1 전자투표

그러나 위와 같은 방식으로 투표를 실시할 경우에는 많은 문제점을 가지게 된다. 즉, 자신의 투표결과를 제3자가 알게 되어 악용할 소지가 있으며, 센터의 집계나 부정 행위의 가능성 때문에 투표자들이 투표 자체를 신뢰하지 않게 되며, 또한 많은 이의를 제기할 수 있기 때문이다.

결국, 안전하고 신뢰할 만한 전자투표가 되기 위해서는 기본적으로 고려하여야 할 아래의 전자투표 안전기준, 즉 전자투표 시스템에서 제공해야 할 요구 사항이 고려되어야 한다.

- Completeness : 투표 결과의 정확한 집계가 이루어져야 한다.
- Privacy : 투표 결과와 투표자와의 관계는 비밀 유지가 되어야 한다.
- Unresuability : 투표자는 단 1회만 투표 가능(2중 투표 방지)해야 한다.
- Fairness : 투표 도중 집계 결과가 나머지 투표에 영향을 주지 않아야 한다.
- Eligibility : 투표권이 없는 자의 투표 행위는 방지되어야 한다.
- Verifiability : 누구도 투표 결과를 위조할 수 없어야 한다.
- Soundness : 부정 투표자에 의한 선거 방해를 견뎌내어야 한다.

물론 위의 요구 사항은 최소한의 것이며 또한 경우에 따라서는 필요 없는 것이 있을 수도 있으며 시스템의 특성에 따라서는 별도의 요구 사항이 추가될 수도 있다.

전자투표가 위의 요구 사항 중 기본적으로 갖추어야 할 사항은 Completeness, Privacy 그리고 Unresuability이다. Unresuability는 2중 투표자가 검출될 수 있는 방안을, Completeness는 집계센터의 오조작이나 부정이 검사될 수 있는 방안이 확보되면 쉽게 제공할 수 있다. 그러나, Privacy와 Completeness 그리고 Unresuability를 다함께 만족하는 방안을 마련하기가 쉬운일이 아니다. 즉 공개 보드를 이용하여 모든 투표자의 투표 내용과 이름을 공개하면 Completeness와 Unresuability를 만족할 수는 있으나 개인의 투표 내용이 노출되어 Privacy를 만족시키지 못하게 된다. 이러한 문제점을 해결하기 위하여 전자투표에 암호를 이용하는 안전하고 신뢰성 높은 전자투표 연구가 다자간 프로토콜을 이용한 전자투표 방식, 익명 통신로를 이용한 전자투표 방식 등을 중심으로 행하여져 오고 있다. 이들 방식들에 대한 소개는 5장과 6장에서 다루기로 한다.

한편, 최소한의 전자투표 안전기준을 갖추고 실용성을 가진 전자투표는 기존의 투표에 비하여 다음과 같은 장점들을 가질 수 있다.

- 어느 투표소에서도 투표가 가능하다.
- 투표율을 향상시킬 수 있다.
- 투표 관련 투표 요원/집계 요원/개표 요원이 불필요하므로 효율적이고 경제적인 투표가 가능하다.
- 신속하고 정확한 개표 및 집계(투표함 수송 불필요 등)로 투표 종료와 거의 동시에 결과를 공표할 수가 있다.
- 선거 비용을 대폭 삭감할 수 있으며 필

요시 언제라도 투표를 실시할 수 있다.
- 부정 투표 및 무효표를 사전에 방지할 수 있다.

2.2 전자투표 현황

이 절에서는 현재 전자투표를 고려하고 있거나 추진하고 있는 미국, 스위스, 프랑스, 일본 등의 나라들 중에서 미국, 일본 그리고 우리나라의 현황만을 소개한다. 또한 암호를 이용하여 각국에서 연구되고 있는 연구 현황도 발표된 논문들을 중심으로 소개한다.

2.2.1 각국의 전자투표 추진 현황

미국에서는 이미 1892년 뉴욕에서 투표 용지를 사용하지 않는 투표기를 이용한 투표를 시작하였으며, 1964년에는 문맹자들에 대한 투표 기회의 평등을 제공하기 위한 수단으로 레버를 잡아당기는 기계식 투표가 도입되었다. 컴퓨터 시스템의 보급으로 인한 펀치 카드 시스템, Optical Scanner 시스템의 도입을 거쳐, 최근에는 직접기록식 투표인, D.R.E.(Direct Recording Election)라는 보턴식 전자 투표기를 도입하고 있다. D.R.E. 방식은 투표자가 자신의 투표가 정확히 입력되었는지를 확인할 수 없으며 투표기마다 작업원이 필요하게 되어, 아직도 효율적인 전자투표가 실현되고 있는 실정은 아니다. 미국에서 추진되어 온 전자투표 현황은 다음과 같다.

1892 투표용지를 사용하지 않는 투표기 사용
1960 펀치 카드 시스템을 투표에 도입
1970 Mark sheet를 투표 용지로 하고 Optical Scanner를 투표기로 사용한 투표시스템 도입
1980 D.R.E. 버튼식 전자 투표기 설치
1992 대통령 선거시 뉴욕시에서 D.R.E. 시스템 도입
1997 뉴욕시 전투표소에 설치 완료 예정

다음은 일본의 전자투표 추진 현황이다. 투표시에 자서식(우리나라는 기표식), 투표용지에 후보자의 이름을 직접 기입하는 방식을 법적으로 채택하고 있는 일본에서는 투표율의 참여율 향상, 신속한 개표 실현 등의 목적으로 전자투표의 채택을 민간차원에서 적극적으로 검토하고 있다. 정치광보센터, NTT등에 의해 구성된 전자투표 시스템 연구회가 일본의 전자투표 도입에 대한 검토, 의견 수렴, 데모 시스템의 구현 그리고 각종 단체에 대한 전자투표의 홍보 등을 행하고 있다. 일본에서 검토하고 있는 방식은 미국의 off-line식 D.R.E. 방식에 비해 on-line식 D.R.E. 방식으로 효율적이며 네트워크의 암호화에 따른 안전 대책의 수립, 첨단 전자 기술의 활용으로 인한 우수한 시스템의 개발로 인하여 보다 뛰어난 전자투표 시스템이 실현될 것으로 예상된다. 최근에 검토되고 있는 일본의 전자투표 도입의 내용은 다음과 같다.

1989 NTT 중심의 전자투표 시스템 연구회 발족
1990 도시바가 단말기를 제작, NTT는 네트워크 개발로 시스템 개발 착수
1992 연구회가 각 자치성에 시스템 도입 제안
1993 각 자치성이 시스템 도입 검토 및 전자투표 모의 실험 실시

우리나라에서는 전자투표의 도입 차원보다는 선거 관리 업무의 사무 자동화 단계에서 이루어지고 있으며 투.개표 단계의 연구와 검토가 이루어지고 있으나 암호를 이용하여 안전하고 실용적인 전자투표 시스템의 도입 검토는 아직 이루어지지 않고 있는 실정으로 추정된다. 문헌상[1]에서 살펴 본 한국에서의 선거 및 투표관련 현황은 다음과 같다.

1991 중앙선거관리위원회 전산 추진 계획 수립
1994 선거관리 자동화 체제 구축
1995 선거관리 전국 전산망 및 자동화 시스템 구축

2.2.2 전자투표 연구 현황

전자투표의 연구는 전자투표 시스템의 도입과는 별개로 행하여져 왔다. 이는 전자투표의 실현시에 수반되는 security 문제를 해결하기 위한 수단으로써 암호의 사용이 필요하게 되었으며, 암호의 응용 분야의 확대라는 의미에서도 연구가 행하여져 왔다. 전자투표의 연구는 1981년, 전자현금으로 유명해진 네덜란드 Digicash사의 D.Chaum에 의해서 행하여 진 Mix형 익명통신로를 이용한 전자투표가 최초이다[4]. 이후 암호의 발달로 인하여 ZKIP(Zero Knowledge Interactive Protocol)[11]와 다자간 프로토콜[12]이 등장하여 이를 이용한 전자투표가 미국의 J.C.Benaloh에 의해 연구되게 되었다.

다음에 정리한 전자투표 연구현황은 크게 다자간 프로토콜을 이용한 전자투표와 익명 통신로를 이용한 전자투표로 생각할 수 있다. Chaum이 제안한 Mix형 익명 통신로는 RSA 암호[13]를 이용한 방식이므로 공개키 암호[13], [14], [15]를 이용한 전자투표[16], [17] 특히 RSA암호를 이용한 전자투표는 Chaum의 전자투표의 확장이나 개선 방식이라고 볼 수 있기 때문이다.

공개키 암호를 이용한 전자투표는 신뢰할 만한 센터를 이용하는 방식으로 공개키 암호가 제안된 이후 많은 연구가 되었으나 현재는 별로 이루어지지 않고 있다. 다자간 프로토콜을 이용한 전자투표는 투표내용을 비밀로 하는 방식으로 안전성이 우수한 방식이나 계산량이 많고 통신 복잡도가 높기 때문에 찬반투표나 소규모 투표에 적합한 방식이다. 현재는 전자투표권의 매매를 방지하기 위한 연구나 기권자를 고려한 전자투표 그리고 다자간 프로토콜 자체의 연구가 행하여 지고 있는 분야이다. 익명통신로를 이용한 전자투표는 투표자와 투표내용의 대응관계를 비밀로 하는 방식으로 효율성면에서는 우수하나 안전성측면에서 다소 부족하다. 일본에서 활발한 연구가 행하여 지고 있으며, Fairness를 만족하는 방안이나 효율적인 익명통신로의 구현과 실용적인 전자투표의 연구가 이루어지고 있다. 전자투표 연구현황을 요약하면 다음과 같다.

- 공개키 암호를 이용한 전자 투표
  - Akiyama(일본 동경대)[16]
  - Koyama(일본 NTT)[17]
- 다자간 프로토콜(Multi-party Protocol)을 이용한 전자 투표
  - Cohen(Benaloh)(미국)[5][18][19]
  - Iversen(노르웨이)[20]
- 익명 통신로(Anonymous Channel)를 이용한 전자 투표
  - Chaum(네덜란드)[4][40]
  - Ohta / Fujioka(일본 NTT)[7][21]
  - Sako(일본 NEC)[22][23]
  - Boyd(영국)[24]
  - Nurmi(핀란드)[25]
  - Asano(일본 요코하마 국립대)[26]
  - 박춘식(한국)[27]

3. 전자투표 관련 암호 도구들

3.1 내용은닉 서명(Blind Signature)

일반적으로 서명자는 자신들이 서명할 메시지의 내용을 알고서 서명을 하게 된다. 그러나, 경우에 따라서는 메시지의 내용을 보지 않은 채 서명을 받고 싶은 경우가 있다. 내용은닉 서명은 메시지 내용은 상대방에게 알려주

지 않으면서도 메시지에 대한 상대방의 서명을 얻게 되는 것으로 전자현금이나 전자선거 등 프라이버시를 제공해야 하는 곳에 활용될 수 있는 추적불가능 서명이다. 이곳에서 개인의 프라이버시는, 전자현금에서는 개인과 개인의 구매 사항의 관계를 알 수 없게 해주는 기능이며, 전자투표에서는 개인과 개인의 투표 내용과의 관계를 비밀로 해주는 기능을 말한다. 그리고 전자현금인 경우 서명을 해주는 곳은 은행이며, 전자투표인 경우 선거관리위원회가 해당될 수 있다. 내용은닉 서명의 기본적 개념 제안[8]과 실현 방안[28]은 전자현금에 활용하기 위해 D. Chaum에 의해 처음으로 제안되었다.

이러한 내용은닉 서명의 기본적인 요구 조건은 다음과 같다.

- 메시지의 내용은 서명자에게 노출되지 않아야 한다.
- 메시지와 서명문이 노출된 이후라도 메시지와 서명을 받은 사람과의 관계가 추적 불가능해야 한다.

이와 같은 조건을 만족하는 RSA 암호를 이용한 내용은닉 서명은 다음과 같다[32]. 먼저 A가 B에게 메시지 m을 은닉한 채 서명을 받고 싶다고 하고, B의 공개키를(e, n), 비밀키를 d라고 하자.

(step 1) A는 난수 r을 생성하여 B에게 $C = mr^e \bmod n$을 계산하여 보낸다.

(step 2) B는 수신한 C에 대한 서명문 $C^d = (mr^e)^d \bmod n$을 계산하여 A에게 제시한다.

(step 3) A는 $S = C^d / r = m^d r^{ed} / r = m^d \bmod n$을 계산하여 B의 메시지 m에 대한 서명문으로 S를 얻게 된다.

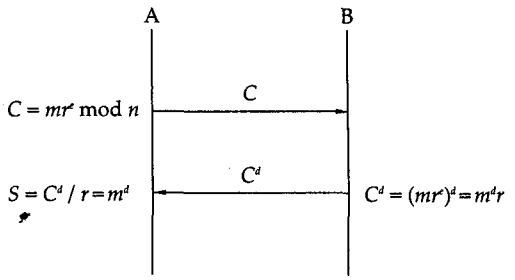


그림 2 RSA를 이용한 내용은닉 서명

이 경우 B는 서명을 해주는 기관으로 위에서 언급한 전자현금의 경우 은행이 역할을 하게 되며 전자투표의 경우 선거 관리 위원회가 된다. 또한, 이 서명이 내용은닉 서명이 되는 이유는 서명자가 메시지를 암호화하여 B에게 전송하므로 B가 서명의 내용을 알지 못한채 서명문을 발생하기 때문이다.

3.2 증명가능 비밀 분배(Verifiable Secret Sharing)

다자간 프로토콜에서는 각 참가자의 비밀 정보를 분할해서 다른 참가자에게 분배하고, 분할된 형태로 계산을 행하거나 필요에 따라서는 원래의 정보를 복원할 필요가 있다. 이와 같은 목적에 사용될 수 있는 Tool이 VSS (Verifiable Secret Sharing)[9],[10]이다.

VSS는 Shamir의 secret sharing(SS)[29]을 영지식증명(Zero-knowledge Proof)과 함께 구성한 것이다. 먼저, SS에 대해서 간략히 소개한다. 분배자가(dealer) 어떤 비밀을 n개의 분할 정보로 분할하고 그것을 n명의 참가자에게 분배한다. 이중 k명이 모이면 원래의 비밀을 복원할 수 있는 방식을 (k, n) threshold secret sharing이라고 한다. 실현 방법은 다음과 같다.

(step 1) 분배자는 자신의 비밀 s를 상수항으로 하는 랜덤한 $(k-1)$ 차의 다항식

$f(x)$을 선택한다.

$$f(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1} \bmod p$$

분배자는 각 참가자 $j(j = 1, \cdots, n)$에게 $f(j)$를 분배한다. 여기서, p는 $s < p$인 소수이다.

(step 2) n개의 분할된 분할 정보 $f(j)$의 가운데서 임의의 $(k-1)$개의 분할 정보로는 s를 복원할 수가 없다. 그러나 k개 이상의 분할 정보를 이용하면 반드시 s가 복원될 수 있다.

이러한 SS를 이용하여 VSS를 구성하는 방법을 지금부터 소개한다. 위에서 언급한 SS에서는 분배자가 정상적으로 그리고 정당하게 분할 정보를 만들지 않으면 k개 이상의 분할 정보를 이용해도 비밀 정보를 복원할 수가 없게 된다. 그래서 VSS에서는 분배자가 정확하게 그리고 정상적으로 분할 정보를 만들었다는 사실을 즉, 임의의 k명 이상의 참가자에 의하여 비밀 정보가 복원되어도 동일한 비밀 정보가 얻어짐을 영지식증명으로 증명하는 것이다. VSS의 실현을 설명하면 다음과 같다.

(step 1) 비밀 정보 s를 가진 분배자는 s를 $c(s)$로 암호화하고, 그 결과를 n명의 참가자에게 전송한다.

(step 2) 분배자는 SS를 이용해서 각 참가자 $j(j = 1, \cdots, n)$에게 $f(j)$를 분배한다.

(step 3) 분배자는 각각의 분할 정보가 위에서 설명한 순서대로 올바르게 만들어졌는지를 각 참가자에게 영지식증명에 의해 증명한다.

3.3 r치 잉여 암호 (Public Key Residue Cryptosystem)

r치 잉여 암호의 파라메터와 암호, 복호화 과정은 다음과 같다.

(비밀키) 2개의 큰 소수 p와 q

(공개키) $N(=pq)$, y

(평 문) $m(0 \le m < r)$

(암호문) $E(m) = y^m x^r \bmod N$, 단 r는 랜덤수이다.

(복 호) mod p와 mod q에 대해서 다음을 각각 계산한다.

$$\{E(m)\}^{(p-1)/e_1} = (y^{(p-1)/e_1})^m \bmod p$$
$$\{E(m)\}^{(q-1)/e_2} = (y^{(q-1)/e_2})^m \bmod q.$$

그리고 $1 \le i < r$가 되는 i에 대해서 위의 계산 결과와 다음의 값을 비교하면 된다.

$$(y^{(p-1)/e_1})^i \bmod p \text{ and } (y^{(q-1)/e_2})^i \bmod q$$

e_1, e_2 그리고 r에 대한 조건 등 r치 잉여 암호에 대한 자세한 내용은 참고문헌 [30]을 참조하기 바란다.

r치 잉여 암호가 갖는 주요 성질은 다음과 같은 준동형사상(Homomorphism)을 만족하는데 있다.

$$E(m+n) = E(m)E(n)x^r \bmod N, \text{ for } \exists x$$

위와 같은 성질이 전자투표 등에 잘 활용될 수 있다.

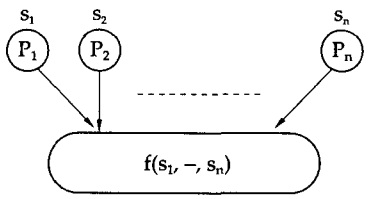


그림 3 다자간 프로토콜

4. 다자간 프로토콜과 익명 통신로

4.1 다자간 프로토콜 (Multi-party Protocol)

n명의 참가자 P_1, ···, P_n가 각각의 비밀 정보 s_i를 가지고 있어서 각 P_i는 s_i를 비밀로 한채 임의의 함수의 값 $f(s_1, \cdots, s_n)$을 알고 싶다고 생각해 보자. 예를 들면, 신임여부를 묻는 신임투표의 경우, $x_i = 0$(반대) 또는 1(찬성)로 $f(s_1, \cdots, s_n) = s_1 + \cdots + s_n$가 된다. 신뢰할 만한 센터 (예를들면, 전자선거관리위원회 등)를 사용하면 다음과 같이 간단하게 실현할 수가 있다. 각 P_i는 s_i를 센터에게 비밀리에 그리고 안전하게 보내면, 센터는 $f(s_1, \cdots, s_n)$의 값을 계산하여 공표하면 된다.

다자간 프로토콜은 위와 같은 신뢰할만한 센터를 사용하지 않고, 그림 3와 같이 $f(s_1, \cdots, s_n)$의 값을 얻기 위해 P_1, ···, P_n 사이의 메시지를 주고 받는 규칙이라고 말할 수 있다. 영지식증명을 이용하면 임의의 f에 대해서, 다자간 프로토콜의 실현 가능함이 알려져 있다[39].

다자간 프로토콜에서 주로 요구되는 사항들로 privacy와 correctness가 있다. privacy는 반수미만의 P_i의 집합 A는 어떠한 부정을 한다 할 지라도 A이외의 P_j의 s_j를 아는 것이 불가능함을 말하며, A가 어떠한 부정을 한다할 지라도 임의의 P_j는 $f(s_1, \cdots, s_n)$의 값을 알 수 있는 것을 correctness라고 말한다.

4.2 익명 통신로 (Anonymous Channel)

익명 통신로는 그림 4에서 보는 바와 같이 참여자가 자신의 정보를 임의의 통신로에 보내었을 경우, 제3자에 의해서 자신과 자신이 보낸 메시지와의 대응 관계가 노출되지 않아 자신의 프라이버시를 지킬 수 있는 통신로를 말한다. 이러한 익명 통신로는 전자투표, 전자현금, 전자우편 등의 프라이버시 기능을 제공해야 하는 분야에 널리 활용되게 되었으며, D. Chaum이 제안한 Mix형 익명 통신로[4]가 가장 최초로, 그 이후에도 많은 익명 통신로들이 제안되어 왔다[27][31][32][33][34][35][36][37].

여기서는 맨 처음 소개된 Mix형 익명 통신로에 대해서 설명한다. Mix는 하나의 컴퓨터나 workstation 등으로 간주할 수 있으며 입력된 내용을 처리하여 출력하는 장치로 생각할 수 있다. k개의 Mix 센터를 사용하는 Chaum의 Mix형 익명 통신로[4]는 다음과 같다. n명의 송신자를 A_1, ···, A_n라 하고, 각각의 송신자 A_i는 A_i와 m_i의 대응 관계를 비밀로 유지한 채, 메시지 m_i를 안전하게 전송하고자 한다. 수신자 B_i의 공개 키를 E_{B_i}라 하고 센터 S_i의 공개키를 E_i이라고 한다. 여기서, 센터 S_i의 역할은 각 송신자의 암호문을 복호화하여, 난수 성분을 제거한 후 그 결과를 알파벳순으로 순서를 바꾸어 출력하는 것이다.

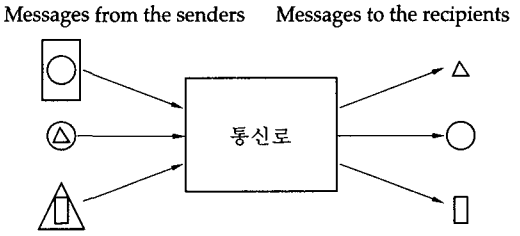


그림 4 익명통신로

[Mix형 익명 통신로]

(step 1) 각 송신자 A_i는 k개의 난수 R_1, ···, R_k를 발생하여, 다음과 같은 암호문을 계산한 후 공개 보드(Public board)에 전송한다.

$$E_1(R_1 \circ E_2(R_2 \cdots E_k(R_k \circ B_i \circ E_{B_i}(m_i))\cdots))$$

(step 1은 A_i가 메세지, $B_i \circ E_{B_i}(m_i)$를

Mix형 익명 통신로에 보낸다고 하는 의미이다.) 여기서 ∘는 연접(concatenation)을 나타낸다.

(step 2) 최초의 Mix S_1는 수신한 암호문들을 복호화하고, 그 내용중에서 난수 R_1을 제거한 후, 남은 내용들을 알파벳 순으로 나열하여 공개 보드에 전송한다.

$$E_2(R_2 \cdots E_k(R_k \circ B_i \circ E_{B_i}(m_i))\cdots)$$

(step 3) 마지막 Mix S_k를 제외한 나머지 Mix들 S_2, …, S_{k-1}는 차례로 step 2와 같은 동작을 반복 수행한다.

(step 4) 마지막으로, S_k는 $\{B_i \circ E_{B_i}(m_i)\}$를 알파벳 순으로 나열하여 공개 보드에 전송한다.

Mix형 익명 통신로에서는 적어도 단 하나의 Mix만이라도 정직하다면, $\{A_i\}$와 $\{m_i\}$의 대응 관계는 나머지 다른 Mix들에게 조차도 비밀로 할 수가 있다. 즉, multi-party sender anonymity의 기능을 실현하게 된다.

5. 다자간 프로토콜을 이용한 전자투표

ZKIP를 최초로 전자투표에 적용한 이는 J.D.Cohen(결혼 후에 J.C.Benaloh로 이름을 바꿈)으로 여기서는 센터를 가정한 Cohen의 전자투표 방식[5]을 소개한다.

(step 1) 센터는 r치 잉여암호(3.3절 참조)를 구성하고 공개키 파라메터(N, y)를 공개한다. 단, 투표자 수 h는 r미만으로 한다.

(step 2) 투표자 i는 자신의 투표 내용 $m_i(=0$ or $1)$를 센터의 공개키로 암호화하여 그 결과인

$$z_i = y^{m_i} x^r_i \bmod N$$

를 공개한다. 여기서 x_i는 랜덤 수이다.

(step 3) 센터는 투표자로 부터 받은 암호문을 각각 복호화하여

$$M = m_1 + m_2 + \cdots + m_h$$

을 투표 집계 결과로써 공표한다.

Completeness를 만족하기 위해서는 먼저 센터의 집계 결과의 점검이 필요하며 Reusability를 위해서는 위 프로토콜에서 행한 투표자의 행위의 정당함을 ZKIP를 이용하여 증명하여야 한다. 즉 위의 기본 프로토콜의 각 스텝마다 확인 절차가 이루어져야 한다. 다음은 기본 프로토콜에 대한 확인 절차이다.

(step 1) 센터는 (N, y)가 r치 잉여 암호의 공개키 파라메터의 조건을 모두 만족하고 있다는 것을 ZKIP를 이용하여 나타낸다.

(step 2) 각 투표자 i는 z_i의 평문이 $m_i(=0$ or $1)$을 만족하고 있음을 ZKIP로써 나타낸다.

(step 3) 센터는

$$z_1 z_2 \cdots z_h = y^M x^r \bmod N$$

가 성립함을 ZKIP로 나타낸다.

Cohen이 제안한 방식은 센터가 신뢰할 만한 경우에는 투표자의 privacy를 만족할 수 있으므로 전자투표의 신뢰성과 안전성이 센터에 크게 의존하게 된다. 이를 보완하여 즉 센터에 대한 의존성을 줄이면서 투표자의 privacy를 향상시켜 주는 방식인, 센터를 복수로 하는 방식[18]을 설명하면 다음과 같다.

(step 1) 센터 j는 r치 잉여 암호를 구성하고 공개키 파라메터(N_i, y_i)를 공개한다. 단, 투표자 수 h는 r미만으로 하며 센터의 수는 n으로 한다.

(step 2) 투표자 i는 자신의 투표 내용 $m_i(=0$

or 1)를

$$m_i = m_{i1} + m_{i2} + \cdots + m_{in} \bmod r$$

를 만족하는 n개 메시지들로 분할한다. 그리고 센터 j의 공개키로 m_{ij}를 암호화 하여 그 결과인

$$z_{ij} = y_j^{mij} x_{ij}^r \bmod N_j$$

를 공개한다. 여기서 x_{ij}는 랜덤 수이다.

(step 3) 각 센터 j는 투표자로부터 받은 암호문을 각각 복호화하여

$$M_j = m_{1j} + m_{2j} + \cdots + m_{hj}$$

을 투표 집계 결과로써 공개한다. 최종 투표 집계결과는

$$M = M_1 + M_2 + \cdots + M_n \bmod r$$

로 계산되게 된다.

각 스탭에 대한 확인 절차는 ZKIP를 이용하여 센터가 하나일 경우와 유사하게 행하게 된다.

센터를 이용하는 방식들은 센터가 전자투표 실시 도중에 고장이나 불의의 사고를 당할 경우에는 전자투표 전체에 영향을 주게되어 결국은 투표 자체가 무효로 되게 된다. 센터의 고장이나 부정 행위를 위한 센터의 결탁 등에 안전하게 대처할 수 있는 방식인, VSS(3.2.절 참조)를 이용한 Fault-tolerent한 전자투표 방식[10]도 제안되어 있다. 그러나 기본적으로 센터가 존재하지 않는 전자투표의 실현은 덧셈의 다자간 프로토콜로 실현될 수 있다. 이는 전자투표 보다는 다자간 프로토콜과 ZIKP로써 많은 연구[38][39]가 되어 오고 있으며, 복잡한 프로토콜 그리고 많은 통신량과 계산량, 특히 찬반 투표가 아닌 여러 후보자자 중 당선자를 확정 짓는 형태의 전자투표시에는 실용성 면에서는 많은 문제점이 있지만 현재까지 제안되어 있는 어떠한 전자투표 방식보다도 안전성 측면에서 우수함이 입증되고 있다.

6. 익명통신로를 이용한 전자투표

효율적인 전자투표 방식으로, 최초로 제안된 것은 Mix형 익명 통신로를 이용한 D. Chaum의 방식[4]이다. 전자투표의 연구 동향에서 공개키를 이용한 전자투표 방식이 소개된 바 있으나 이들은 넓은 의미에서 본다면 Chaum의 방식의 변형 또는 유사한 방식으로 볼 수 있다. 공개키 중에서도 특히 RSA를 이용한 전자 투표 방식들은[16][17], Chaum의 전자투표 방식을 잘 이해하지 못하였거나 또는 Chaum과는 별도로 행한 연구 결과로 생각된다. 일본에서 주로 행하여지고 있는 실용적인 전자투표의 형태는 대개 Chaum류의 방식이 주류를 이루고 있다.

이 장에서는 효율적인 투표를 행하기 위하여 Mix형 익명 통신로를 이용한 Chaum의 투표 방식을 중심으로 설명한다. 먼저 다음과 같은 방법을 생각하여 보자. 단 하나의 Mix와 공개 보드 그리고 각 투표자와 Mix 사이는 비밀통신로가 구축되어 있다고 가정한다.

(step 1) 각 투표자 P_i는 투표 내용 x_i외에 랜덤 수 r_i를 택하여 (x_i, r_i)를 Mix에 보낸다.

(step 2) Mix는 $\{(x_i, r_i)\}$를 알파벳순으로 정리하여 공표한다.

(step 3) P_i는 자신의 (x_i, r_i)가 공표되어 있는지 확인한다.

위의 방식은 공표된 집계결과로 부터 자신이 투표한 내용이 있는지의 여부를 step 3에서 직접 확인할 수 있다. 그러나, 만일 없는 경우 해당 투표자는 자신의 투표 내용이 집계 되지 않았다는 사유로 이의를 제기할 수 있다. 이때, 이 투표자가 부정한 수단으로 (예를들면 투표 결과에 불복하여 투표를 무효화 시키기 위할 경우 등) 이의를 제기하였는지 또는 Mix

가 부정을 저질렀는지를 판단할 수가 없게 된다. 또한, Mix가 단 하나만 존재하므로 Privacy가 Mix의 신뢰성에 크게 의존하게 된다. 이러한 문제점을 다소 보완하기 위하여 Chaum은 Mix의 수를 복수화하고 부정하게 이의를 제기하는 것을 방지하기 위해 2회의 투표 형식을 이용한 전자투표 방식[4]을 제안하였다. Chaum의 Mix형 익명 통신로를 이용한 최초의 전자투표 방식은 등록 단계, 이의 신청 단계 그리고 투표 단계로 구분되어 있다. 다음의 프로토콜에서 사용되는 P_i는 투표자를, V_i는 투표자의 투표 내용을 나타내며 익명 통신로는 k개의 Mix로 이루어진다.

[등록 단계]

(step 1) 각 투표자 P_i는 (K_i, K_i^{-1})를 임의로 선택한다. 여기서, K_i는 공개키이며 K_i^{-1}는 비밀키이다. P_i는 Mix형 익명 통신로에서 설명한 바와 같이 다음 사항을 계산하여

$$E_1(R_1 \circ E_2(R_2 \cdots E_k(R_k \circ K_i)\cdots))$$

디지털 서명과 함께 공개 보드에 기록한다. (다시말하면, P_i가 Mix형 익명 통신로에 K_i를 보내는 것을 말하며, Mix형 익명 통신로의 step 1에서 $B_i \circ E_{B_i}(m_i)$ 대신에 K_i를 대치시키면 된다.)

(step 2) Mix형 익명 통신로는 K_i를 비밀리에 섞는다. (이 과정은 Mix형 익명통신로의 step 2와 step 3의 과정을 수행하면 된다.)

(step 3) 마지막 Mix인 S_k는 K_i를 알파벳순으로 나열하여 공개 보드에 표시한다. 여기서 이러한 공개 list를 $(\hat{K}_1, \hat{K}_2, \cdots)$라고 하자.

[이의 신청 단계]

(step 4) 각 투표자 P_i는 공개 보드상의 list에 자신이 등록한 K_i가 존재하는 지를 확인한다. 만일 존재하지 않는다면, P_i는 이의를 신청하며 전자투표는 중단되게 된다. 만일 일정한 시간동안 아무런 이의 신청이 없다면, 다음 투표단계로 진행한다.

[투표 단계]

(step 5) 각 투표자 P_i는 step 1과 같이 다음 암호문을 만들어 디지털 서명과 함께 공개 보드에 기록한다.

$$E_1(R_1 \circ E_2(R_2 \cdots E_k(R_k \circ (K_i \circ K_i^{-1}(V_i \circ 0^l)))\cdots))$$

(step 6) 투표가 모두 완료된 후 Mix형 익명 통신로는 $K_i \circ K_i^{-1}(V_i \circ 0^l)$을 비밀리에 섞는다.

(step 7) S_k는 $K_i \circ K_i^{-1}(V_i \circ 0^l)$를 알파벳순으로 공개 보드에 나열한다. 이것을 $(u_1 \circ v_1)$, $(u_2 \circ v_2)$, ...라고 하자.

(step 8) 누구든지 $U_i = \hat{K}_i$와 $u_i(v_i) = * \cdots * 0^l$인지를 확인할 수 있다. 만일, 확인결과 틀린 것이 발견될 경우에는 투표는 즉시 중단된다.

(step 9) 에러가 없다면 투표결과인 $V_1, \cdots, V_n$을 투표의 최종 집계 결과로써 얻을 수 있다.

■ 참고사항

step 1과 step 5에서 사용된 디지털 서명은 투표자의 신분을 확인하기 위해서 사용되는 것이다.

Chaum이 제안한 익명 통신로를 이용한 전자투표는 등록 단계시 내용은닉 서명을 이용하는 방식[6],[7],[21],[26],[27],[40]등으로 개선되어가며, 요구 조건중의 하나인 Fairness을 만족하기 위

한 연구도 추진되어 왔다[26],[27]. 익명 통신로를 이용한 전자투표의 연구는 앞에서 설명한 바와 같이 일본을 중심으로 많은 연구가 진행되어 왔다. 그러나 이 방식들은 효율적인 점에서는 다소 뛰어난 점이 있으나 안전성을 고려할 경우에는 다자간 프로토콜을 이용하는 전자투표에 비해서 다소 미흡한 점이 있다. 안전성을 증가시키기 위해서는 결국은 복잡한 전자투표 방식이 되리라 예상된다.

7. 방식별 비교와 향후 전망

앞장에서 설명한 전자투표 방식들을 비교하여 요약하면 표 1과 같다. 이외에도 최근에는 기권자를 고려한 전자투표[41] 그리고 투표 매매 방지를 위한 전자투표[42]등이 연구되고 있다. 보다 실용적이고 보다 안전한 즉 부담없이 모두가 신뢰할 수 있는 전자투표시스템을 만드는 것은 아직도 많은 연구가 행하여 져야 한다.

안전하고 높은 신뢰성과 실용성을 갖춘 전자투표가 본격적으로 활용되기 위해서는, 다음과 같은 해결하여야 할 많은 과제들이 남아 있다.

표 1 선거 방식별 비교

구 분	다자간 프로토콜	익명 통신로
제 안 자	Cohen(Benaloh)	D.Chaum
방 식	r차 잉여암호 + ZKIP	은닉서명 + 익명 통신로
안 전 성	우수	양호
효 율 성	불량	우수
적용선거	찬반(신임)	다목적용
선거규모	소규모	대규모
고려사항	효율성	익명통신로 실현 문제

- 투표 도중 시스템의 고장, 해커 등의 침입에 대한 안전 대책
- 투표 결과에 대한 이의 신청시의 컴퓨터에 의한 증거 능력
- 투표 결과를 교묘히 조작하거나 집계하지 않을 지도 모른다는 불신 등과 기존 투표 방식에 대한 문제점이 심각하지 않은 상황에서의 전자투표에 대한 부정적인 생각에 대한 요인 해소
- 전자투표에 대한 법적. 제도적 측면의 보완과 정치적인 결정
- 초기 투자비의 재원 충당 등.

그러나 이외에도 실용적인 측면에서 고려하여야 할 사항이나 문제점들이 많이 존재하리라 생각되지만, 많은 실용화 연구를 거쳐 상당부분 해결될 것으로 보이며, 인터네트의 급속한 확산과 초고속정보통신망의 구축으로 인한 전자투표의 실현은 예상외로 빨리 이루어질 것으로 예상된다.

8. 결 론

인터네트의 급속한 보급과 초고속정보통신의 기반 구축이 완료되면 전자투표의 이용은 현실로 다가올 것이다. 우리나라에서는 선거의

자동화에는 관심을 기울여오고 있는 실정이나, 암호를 이용한 전자투표에 대해서는 연구나 실용화면에서 관심이 부족한 실정이다. 이 논문에서는 전자투표에 대한 일반적인 내용과 암호를 이용한 전자투표의 연구 내용을 중심으로 살펴보았다. 안전하고 신뢰성을 갖춘 그리고 실용적인 전자투표가 이루어지기 위해서는 많은 연구가 행하여져야 한다. 전자투표 분야에 대한 국내 연구 활성화를 기대해 보며 초보적인 자료로써 활용될 수 있기를 바란다.

참 고 문 헌

[1] 이 문구, "투.개표 자동화에 관한 고찰", 선거 관리, No.38, pp.145-162, 1992.

[2] 류 몽희, "투.개표 의무의 전산화 방안에 대한 연구", 중앙대 국제경영 논총, pp. 49-99, 1993.

[3] 문 의승, "선거종류와 투표방법에 관한 고찰", 제주전문대논문집, No.14, pp. 293-317, 1993.

[4] D.L. Chaum, "Untraceble Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, Vol.24, No.2, pp.84-88, 1981.

[5] J.D.Cohen and M.H.Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme", Proceedings of the 26th Annual IEEE Symposium on the Foundations of Computer Science, pp. 372-382, 1985.

[6] K.Sako, "Electronic Voting System with Objection to the Center", The Proceedings of the 1992 Symposium on Cryptography and Information Security, SCIS 92-13C, 1992.

[7] K. Ohta, "An Electrical Voting Scheme Using a Single Administrator", 1988 Spring National Convention Record, IEICE, A-294, 1988.

[8] D.Chaum, "Security without Identification : Transaction Systems to Make Big Brother Obsolete", *Communications of the ACM*, Vol.28, No.10, pp.1030-1044, 1985.

[9] B.Chor, S.Goldwasser, S.Micali and B.A werbuch, "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults", Proceedings of the 23rd Annual IEEE Symposium on the Foundations of Computer Science, pp.383-395, 1985.

[10] J.C.Benaloh, "Secret Sharing Homomorphisms : Keeping Shares of a Secret", Advances in Cryptology, Proceedings of Crypto' 86, pp.251-260, 1986.

[11] S.Goldwasser, S.Micali and C.Rackoff, "The Knowledge Complexity of Interactive Proof Systems", Proceedings of the 17th ACM Symposium on Theory of Computing, pp.291-304, 1985.

[12] A.C.Yao, "How to Generate and Exchange Secrets", Proceedings of the 27th Annual IEEE Symposium on the Foundations of Computer Science, pp. 162-167, 1986.

[13] R.L.Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the Association for Computing Machinery*, Vol.21, No.2,

pp.120-126, 1978.

[14] W.Diffie and M.E.Hellman, "New directions in cryptography", IEEE Transaction on Information Theory, Vol.22, No.6, pp.644-654, 1976.

[15] T.ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms", *IEEE Trans.Inform. Theory*, Vol.31, No.4,p p.469-472, 1985.

[16] M.Akiyama, Y.Tanaka, T.Kikuchi and H.Uji, "Secret Ballot Systems Using Cryptography", IEICE Trans., Vol.J67-A, No.12, pp. 1278-1285, 1984.

[17] K.Koyama, "Secure Secret Voting System Using the RSA Public-Key Cryptosystem", IEICE Trans., Vol.J68-D, No.11, pp.1956-1965, 1985.

[18] J.C.Benaloh and M. Yung, "Distributing the Power of a Government to Enhance the Privacy of Voters", Proceedings of the 5th ACM Symposium on the Principles in Distributed Computing, pp.53-62, 1986.

[19] J.C.Benaloh and D.Tuinstra, "Receipt Free Secret Ballot Elections", Proceedings of the 26th ACM Symposium on the Theory of Computing, pp.544-553, 1994.

[20] K.R.Iversen, "A Cryptographic Scheme for Computerized General Elections", Advances in Cryptology, Proceedings of Crypto' 91, pp.405-419, 1992.

[21] A.Fujioka, T. Okamoto and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology, Proceedings of AUSCRYPT' 92, pp.244-251, 1993.

[22] K.Sako and J.Kilian, "Secure Voting Using Partially Compatible Homomorphisms", Advances in Cryptology, Proceedings of Crypto' 94, pp.411-424, 1994

[23] K.Sako and J.Kilian, "Receipt Free Mix Type Voting Scheme-A Practical Solution to the Implementation of a Voting Booth", Advances in Cryptology, Proceedings of EUROCRYPT' 95, pp.393-403, 1995.

[24] C.Boyd, "A New Multiple Key Cipher and an Improved Voting Scheme", Advances in Cryptology, Proceedings of EUROCRYPT' 89, pp.617-625, 1990.

[25] H.Nurmi, A.Salomaa and L.Santean, "Secret ballot elections in computer networks", Computer & Security, Vol. 10, No.6, pp.553-560, 1991.

[26] T.Asano, T.Matsumoto and H.Imai, "A Scheme for Fair Electronic Secret Voting", Technical Report, IEICE Japan, ISEC 90-35, pp.21-31, 1990.

[27] C.S. Park, K.Itoh and K.Kurosawa, "Efficient Anonymous Channel and All / Nothing Election Scheme", *Advances in Cryptology, Proceedings of EUROCRYPT'93*, pp.248-259, 1993.

[28] D. Chaum, "Blind Signatures for Untraceable Payments" , *Proc. of Crypto' 82*, Plenum Press, pp.199-203,1983.

[29] A.Shamir, "How to share a Secret", *Communications of the ACM*, Vol.22, No.11, pp.612-613, 1979.

[30] K.Kurosawa, Y.Katayama, Y.Ogata and S.Tsujii, "General Public Key Residue Cryptosystems and Mental Poker Protocols", Advances in Cryptology, Proceedings of EUROCRYPT'90, pp.374-388, 1990.

[31] A.Pfitzmann and M. Waidner, "Networks without user observability design options", *Advances in Cryptology, Proceedings of EUROCRYPT'85*, pp.245-253, 1986.

[32] D.L. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", *Journal of Cryptology*, Vol.1, No.1, pp.65-75, 1988.

[33] B.Pfitzmann and A.Pfitzmann, "How to break the direct RSA implementation of MIXes", *Advances in Cryptology, Proceedings of EUROCRYPT'89*, pp.373-381, 1989.

[34] C.Rackoff and D.R.Simon, "Cryptographic Defense Against Traffic Analysis", *Proceedings of 25th ACM Symposium on Theory of Computing*, pp.672-681, 1993.

[35] M.Waidner and B.Pfitzmann, "The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability", *Advances in Cryptology, Proceedings of EUROCRYPT'89*, pp.690, 1990.

[36] M.Waidner, "Unconditional Sender and Receipient Untraceability in spite of Active Attacks", Advances in Cryptology, Proceedings of EUROCRYPT'89,pp.302-319, 1990.

[37] J. Bos and B. den Boer, "Detection of Disrupters in the DC Protocol", *Advances in Cryptology, Proceedings of EUROCRYPT'89*, pp.320-327, 1990.

[38] D.Beaver and D.Goldwasser, "Multiparty Computations with Faulty Majority", Proceedings of the 30th Annual IEEE Symposium on the Foundations of Computer Science, pp.468-473, 1989.

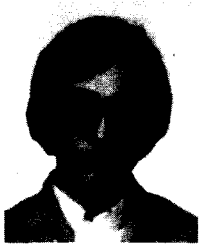
[39] O.Godreich, S.Micali and A.Wigderson, "How to Play Any Mental Game", Proceedings of the 19th ACM Symposium on the Theory of Computing, pp.218-229, 1987.

[40] D.L. Chaum, "Elections with Unconditionally Secret Ballots and Disruptions Equivalent to Breaking RSA", Advances in Cryptology, Proceedings of EUROCRYPT'88, pp.177-181, 1988.

[41] L.Chen and M.Burminster, "A Practical Secret Voting Scheme which Allows Voters to Abstain", Proceedings of Chinacrypt'94, pp.100-107, 1994.

[42] V.Niemi and A. Renvall, "How to Prevent Buying of Voters in Computer Elections", Advances in Cryptology, Proceedings of ASIACRYPT'94, pp. 164-170, 1995.

□ 著者紹介



박 춘 식(정회원)

광운대학교 전자통신과 졸업(학사)
한양대학교 대학원 전자통신과 졸업(석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원 연구원
1982년 ~ 현재 한국전자통신연구소 책임연구원

※ 주관심 분야 : 암호이론, 정보이론, 통신이론