| 특집 03 |

전자선거 도입을 위한 이슈 분석

이 병 천
(중부대학교)

목 차

1. 서 론

초고속 정보통신기술의 발전과 함께 전자선거가 빠르게 우리 앞에 다가오고 있다. 전자선거란 컴퓨터, 인터넷 등 전자적인 방식을 선거행위에 적용함으로써 효율성, 편의성, 정확성, 비용절감 등을 추구하는 것을 말한다. 때때로 두 가지 용어를 구분하여 사용하기도 하는데 전자선거란 선거행위 전반을 전자화 하는 것을 말하며 전자투표란 투표행위를 전자화 하는 것을 말한다. 전자적인 방식을 도입함으로써 투표의 편의성을 높일 수 있고 그 결과 유권자의 투표참여를 높일 수 있어서 영국, 스위스, 네덜란드, 독일, 미국, 일본, 호주, 인도 등 세계 각국은 전자선거의 도입을 위해 연구, 개발, 시범투표사업 등의 노력을 아끼지 않고 있다. 국내에서도 중앙선거관리위원회에서 전자투표사업 추진 로드맵을 마련하여 학계, 산업계, 정치권 등의 의견수렴을 거쳐 체계적인 도입을 준비하고 있다. 전자투표의 도입은 정치를 선진화하고 국민들의 투표참여를 유도하여 직접민주주의 사회를 발전시켜 나가는 중요한 계기가 될 것으로 생각된다.

전자투표를 도입하면 다음과 같은 장점이 있다.

- **편의성(Convenience)** : 투표자는 발전된 IT 기술을 이용하여 터치스크린 방식 등 편리한 방법으로 투표에 참여할 수 있다. 인터넷 원격투표가 사용되면 지정된 투표소에 나가지 않고도 인터넷이 연결된 어느 곳에서나 투표에 참여 가능하다.
- **효율성(Efficiency)** : 투표과정이 간단해지고 개표과정이 신속하게 처리되어 투표 결과를 빠르게 얻을 수 있다.
- **정확성(Accuracy)** : 인간에 의한 에러를 방지하여 정확한 결과를 얻을 수 있다.
- **비용절감(Cost)** : 투표소를 더 많은 곳에 값싸게 준비할 수 있다. 종이투표지를 준비할 필요가 없고 투표함의 물리적 이송이 필요 없다. 대규모 개표인력이 불필요하다.
- **보안성(Security)** : 종이투표 방식에 비해 여러 가지 추가적인 보안기능을 제공한다.

전자투표에 대해서는 많은 기술적 연구들이 이루어져 왔고 도입의 준비도 해 왔지만 정작 이의 도입에 대해서는 아직도 찬반 의견이 엇갈리고 있는 것이 사실이다. IT 기술과 결합된 전자투표가 제공하는 여러 가지 편의성, 효율성, 정확성, 투표 참여도 증가 등의 장점을 강조하는 사람들은 전자투표의 도입을 지지하고 있으나 전자적인 방식의 투표에 대한 낯설음과 거부감, 투표조작에 대한 우려, 보안성에 대해 걱정하는 사람들은 도입에 유보적인 태도를 보이고 있다. 이것은 전자투표에 대한 자세한 이해와 전자투표 도입에 대한 사회적 토의가 아직 부족하기 때문이라고 생각된다.

이 논문에서는 전자투표 기술에 대한 전반적인 소개와 함께 전자투표의 구현방식에 따른 특징 및 차이점을 분석한다. 전자투표의 실용화를 위해 고려해야 할 기술적, 사회적 이슈들에 대하여 토의해 본다. 아울러 주요 핵심 이슈중의 하나인 인터넷 전자투표, 모바일 전자투표의 도입 가능성에 대해 검토해 보고자 한다.

2. 전자투표 기술의 개요

전자투표란 컴퓨터, 인터넷 등의 IT 기술을 전통적인 투표행위에 적용함으로써 전자적인 방식으로 투표를 할 수 있도록 하는 것을 말하는데 이를 통해 선거과정의 효율성, 편의성, 정확성, 비용절감 등을 추구할 수 있다.

투표란 민주주의 사회에서 구성원들의 의견을 수렴하는 가장 기본적인 수단이다. 그런데 부적격자에 의한 투표, 이중 투표, 선거관리자의 부정행위, 투표값의 노출 등 여러 가지 부정행위가 발생할 소지가 있으므로 선거과정은 이런 부정행위가 발생하지 않도록 엄격히 관리되어야 한다. 더구나 전자적인 방식으로 투표를 수행하는 전자투표에서는 이러한 불법행위가 가능하지는 않은지 세심한 설계와 운영이 요구된다. 왜냐하면 모든 기술적인 사항이 표준화되고 공개되어 있는 컴퓨터와 인터넷 통신망을 이용하는 경우 정보의 노출, 위조, 해킹 등의 위험성이 상존하고 있기 때문이다.

따라서 전자투표시스템에서 요구되는 보안요구사항을 만족시키기 위해서는 암호기술을 사용하는 것이 필수불가결하며 암호학계에서는 오래 전부터 전자투표를 안전하게 수행하기 위한 이론적인 연구를 수행해 왔다. 또한 전자투표시스템을 실제로 구현하여 시범서비스를 통해 도입 가능성을 검토해왔다[3].

2.1 전자투표 연구의 발전과정

전자투표의 가능성이 처음 제시된 것은 1982년 D. Chaum[7]이 은닉서명(blind signature) 기법을 제안하면서 이를 투표과정에 적용하려고 했던 시도가 처음이라고 할 수 있다. 은닉서명이란 메시지 소유자가 서명자에게 메시지의 내용은 감추고서 서명자의 유효한 서명을 받기 위해 사용하는 상호작용형(interactive) 특수서명 기법이다. 메시지 소유자는 비밀정보를 이용하여 메시지를 은닉시켜 서명자에게 보내고 서명자가 은닉된 메시지에 대해 서명하면 메시지 소유자가 자신만이 알고 있는 은닉정보를 이용하여 원래의 메시지에 대한 서명을 복구할 수 있다. 이 방법을 이용하면 메시지의 내용이 서명자에게 알려지지 않고도 유효한 서명을 얻을 수 있기 때문에 은행에서의 전자화폐 발행과정, 선거관리자에 의한 투표용지 발급 등의 과정에서 프라이버시 보호를 위해 적용될 수 있다는 것이 제안되었다. 이후 은닉서명을 이용한 전자투표 기법들이 발표되었다[8,11]. 그런데 은닉서명을 이용한 전자투표 기법들은 프라이버시 서비스를 제공하기 위해 익명채널(anonymous channel)의 존재를 가정하고 있다. 즉 통신채널에서 복수의 서버가 메시지를 섞어주는 서비스를 제공하여 투표자가 자신의 투표값을 선거관리자에게 익명으로 전달할 수 있다는 것이다. 이것이 존재하지 않는다면 개표 시 각 투표자의 투표값을 개별적으로 복호화하기 때문에 투표자의 프라이버시가 보호되지 못

한다.

익명채널을 암호학적으로 구현하기 위해 믹스넷(mixnet)[1] 기법이 제안되었다. 믹스넷이란 전통적인 투표함의 역할을 암호학적으로 구현한 것으로 복수의 입력값들을 믹스서버가 복호화(decryption) 또는 재암호화(re-encryption) 기법 등을 이용해서 메시지 내용은 변화시키지 않으면서도 달라보이도록 암호학적으로 처리하고 뒤섞어서(shuffling) 출력함으로써 입력과 출력 간의 상호관계를 감추는 방법이다. 이러한 믹스넷 기법을 적용한 전자투표 기법이 다수 제안되었는데[2, 13, 17, 20, 22, 24] 투표자는 개표자의 공개키로 암호화된 투표값을 자신이 서명하여 제출하고, 믹스서버가 이들을 섞은 후, 암호화된 투표값이 개표자에 의해 개별적으로 복호화된다. 투표값들은 개표되기 전에 믹스서버에 의해 섞여지기 때문에 투표자와 투표값과의 관계가 드러나지 않는다. 그런데 이러한 믹스넷 기법이 사용된다면 선거관리자가 투표용지를 따로 발급할 필요가 없기 때문에 더 이상 은닉서명을 사용할 필요가 없게 된다.

암호기법을 사용하여 투표값의 비밀성을 보장하는 또다른 방법은 준동형암호(homomorphic encryption)를 이용하는 방법이다[4, 5, 6, 9, 10, 15, 16, 18, 23]. 즉 각각의 투표값을 개별적으로 복호화하지 않고 암호알고리즘의 준동형 성질을 이용하여 전체 투표값들을 결합시켜 한번에 복호화하여 전체 투표결과를 얻는 방법이다. 이 방법은 각각의 개별 투표값을 복호화하지 않기 때문에 투표값의 비밀성을 지킬 수 있다.

매표방지(receipt-freeness)라는 기능은 전자투표에서만 요구되는 매우 특이한 보안요구사항이라고 볼 수 있다. 일반적인 전자거래에서는 거래 내용에 대한 증거물을 갖게 되는 것이 일반적인 상거래 방식인데 투표라는 행위에서는 투표자가 자신이 어떤 투표를 했는지에 대한 증거를 가질 수 없어야 한다. 만일 자신의 투표값에 대한 증거물이 공식적으로 발급된다면 돈을 받고 원하는 투표를 해주는 매표행위나 특정 투표를 하도록 강요하는 강압투표가 공식적으로 가능해지기 때문에 이를 방지해야 한다. 전자적인 도구를 이용한 거래에서 증거물을 만드는 것은 쉽지만 증거물을 만들지 못하도록 하면서도 정확성을 검증할 수 있도록 설계하는 것은 쉽지 않은 일이다. 이런 기능을 제공하기 위해 영지식증명, 믹스넷, 검증자지정영지식증명, 비밀통신로 등 복잡한 암호기술을 사용하는 매표방지형 전자투표 기법들이 제시되었다[5, 6, 12, 15, 16, 17, 18, 19, 21, 24].

위에서 제시된 방법들은 인터넷을 통해 원격지에서 투표하는 일반적인 모델을 고려하고 있으나 안전한 투표부스(voting booth)를 이용하는 방법도 많이 연구되고 있다. 특정의 투표부스에서만 투표를 하도록 함으로써 투표자의 신원확인이 쉽고 투표자와 선거관리자 사이의 데이터 전송에 있어서의 보안을 고려할 필요가 없어서 전자투표 모델이 매우 간단해진다. 선거관리자는 투표자의 신원을 투표소에서 직접 확인하고 투표용 토큰을 제공하고 투표자는 이 토큰을 사용하여 투표하도록 하는 방법이다. 기존의 투표시스템 운영방식을 그대로 전자화 한 방법으로 실용적인 측면에서 설계, 구현되어 시범투표사업에 많이 적용되고 있다. 투표부스를 이용한다면 불법적인 행위가 일어나지 않도록 선거관리자가 투표부스를 안전하게 관리할 수 있으므로 매표방지 등의 기능을 근본적으로 제공할 수 있다. 반면 투표자가 반드시 투표부스에 와서 투표해야 한다는 제약이 있다.

한편 이러한 이론적 연구와 함께 실제 전자투표 시스템을 구현하고 전자투표 시범서비스를 실시하는 시도가 이루어지고 있다[3]. 세계적으로 영국, 스위스, 네덜란드, 독일 등의 유럽국가들과 미국, 일본, 호주, 인도 등에서의 시범서비스 사례를 찾아볼 수 있다. 우리나라에서는 아직 정부 차원의 시범서비스는 없었지만 각 정당별로는 정당내부 선거에 투표부스 방식과 인터넷 투표방식 등 전자투표를 활발히 이용하고 있다. 학계에서는 2002년

한일월드컵 행사를 맞아 한일의 연구팀들이 월드컵 MVP를 뽑는 인터넷 전자투표 시범서비스를 실시한 사례가 있다[14].

2.2 전자투표의 일반적인 시나리오

전자투표가 실제 이루어지는 경우의 대표적인 시나리오를 살펴보자. 전자투표의 참여자로서는 투표자와 선거관리자로 구분해 볼 수 있으며 선거관리자는 세부적인 역할에 따라 관리자와 개표자 등으로 구분할 수 있다.

1) 투표시스템 준비 단계 : 선거관리자는 투표시스템을 준비하고 여기에 사용되는 암호 파라메터들을 준비한다. 후보자 등록을 받아 후보자리스트를 공지한다.
2) 유권자 등록단계 : 투표에 참여하고자 하는 사람은 등록기관에 등록을 하며 등록기관은 자격여부를 심사하여 유권자로 등록한다. 등록단계가 끝나면 유권자 목록이 공개된다. 인터넷투표가 실시될 경우 등록된 유권자에게 인증서를 발급할 수 있다.
3) 투표단계 : 등록된 유권자는 선거관리자에게 자신의 신분을 확인한 후 투표용 토큰을 받은 후 투표부스에서 투표에 참여한다. 인터넷투표를 사용할 경우 자신이 편리한 장소에서 인터넷을 통해 투표용 웹서버에 접속하여 공인인증서로 자신을 확인하고 투표한다. 투표값은 개표기관의 공개키로 암호화되고 자신의 서명을 포함하여야 한다.
4) 개표단계 : 개표자는 투표값의 유효성을 검사하여 유효한 투표값을 모은다. 사전에 마련된 절차와 방법에 따라 개표를 하여 결과를 공표한다.

2.3 전자투표의 보안 요구사항

이와 같이 전자적인 방식으로 투표가 이루어지는 경우 부적격자에 의한 투표, 이중 투표, 선거관리자의 부정행위, 투표값의 노출 등 다양한 위협이 존재할 수 있다. 그러므로 안전한 전자투표시스템으로 사용되기 위한 보안요구사항에 대해서는 지금까지 많은 논의가 있었으며 일반적으로 다음과 같은 보안요구사항들이 제시되고 있다.

- **비밀성**(privacy) : 투표자와 투표값과의 연관성이 드러나지 않아야 한다. 비밀성이 제공되어야 투표자는 강압없이 자신의 자유의사에 따라 투표를 할 수 있다. 이를 위해서는 개표자의 공개키로 암호화하고 믹스넷을 이용해 섞어주는 등의 방법을 사용한다.
- **정확성**(accuracy, correctness) : 모든 투표값은 투표결과에 정확히 반영되어야 하며 유효한 투표만이 포함되어야 한다.
- **공정성**(fairness) : 전자선거는 투표단계에서 일부 후보, 또는 일부 투표자에게 불법적인 영향을 미치지 않도록 공정하게 운영되어야 한다. 만일 일부 결과가 마감시간 이전에 공표되거나 하면 투표자들의 판단에 영향을 줄 수 있다.
- **적임성**(eligibility) : 투표권이 부여된 유권자만이 투표에 참여할 수 있다. 이를 위해서는 사전에 유권자 등록을 받아 유권자 리스트를 공개하고 데이터베이스를 관리하여야 한다. 투표단계에서는 투표자의 신분을 직접 인증하거나 공인인증된 전자서명을 사용하도록 해야 한다.
- **중복투표방지**(prevention of double voting) : 1인 1표의 원칙이 지켜져서 한 사람이 두 번 이상 투표할 수 없어야 한다. 이를 위해서는 투표 사실 여부에 대한 데이터베이스가 안전하게 운용되어야 한다.
- **매표방지**(receipt-freeness) : 투표자는 자신이 어떤 투표를 했는지를 제3자에게 증명할 수 없어야 한다. 만일 투표자가 자신의 투표내용을 제3자에게 증명할 수 있다면 돈을 받고 투표를 해주는 매표행위나 강압에 의한 투표

행위가 일어날 수 있다. 투표시스템은 매표행위가 체계적이고 효율적으로 가능하지 못하도록 설계, 운영되어야 한다.

- 검증성(verifiability) : 투표과정이 바르게 운영되고 정확하게 개표되는지 전반에 대해 검증할 수 있는 기능이 필요하다. 검증성이 제공되지 않는다면 선거관리자들을 무조건 신뢰할 수밖에 없지만 검증성이 제공되면 투표시스템 전체에 대한 신뢰성을 크게 향상시킬 수 있다. 검증성을 상황에 따라 좀 더 구분해보면 누구나 정확성을 검증할 수 있는 전체검증성(universal verifiability)과 투표자가 자신의 투표에 대해서만 검증할 수 있는 투표자검증성(voter verifiability)으로 나눌 수 있다. 또한 투표소에서만 검증할 수 있는 경우와, 투표소 이외의 외부에서도 검증할 수 있는 경우로 나눌 수 있다.
- 강인성(robustness) : 일부 시스템 및 관리자들의 에러에 의해 전체 투표시스템의 운영이 영향을 받지 않아야 한다.

이러한 모든 보안요구사항을 만족시킬 수 있는 투표시스템을 설계하는 것은 쉽지 않다. 특히 검증성과 매표방지 기능을 함께 제공하는 것은 쉽지 않으며 가능하더라도 많은 암호학적 계산량과 통신량을 요구한다.

2.4 전자투표에 사용되는 암호기술

이러한 보안요구사항을 만족시키는 전자투표 프로토콜을 설계하기 위해서는 다음과 같은 암호기반기술이 복합적으로 사용된다.

- 전자서명(digital signature) : 본인확인, 메시지 인증 등에 사용.
- 암호화(encryption) : 투표값을 개표자만이 복호화할 수 있도록 함.
- 준동형암호(homomorphic encryption) : 준동형 암호 기반의 투표프로토콜에서 복수의 투표값을 결합하여 한번에 복호화함으로써 결과를 직접 얻을 수 있도록 함.
- 은닉서명(blind signature) : 유효한 투표용지 발급에 사용.
- 재암호화(re-encryption) : 하나의 암호문을 메시지는 변화시키지 않으면서 다른 암호문으로 바꾸는 방법으로 믹스넷의 구현을 위해 사용.
- 비밀분산(secret sharing) : 개표자의 비밀키를 복수의 개표자에게 분산하기 위해 사용.
- 문턱암호(threshold cryptography) : 복수의 개표자들이 상호 협력하여 투표값을 복호화하는데 사용.
- 영지식증명(zero knowledge proof) : 투표값의 유효성 증명, 믹스서버의 믹스작업의 유효성 증명, 복호화의 유효성 증명 등에 사용하며 투표시스템의 검증성을 제공하기 위해 사용.
- 믹스넷(mixnet) : 투표값들을 섞어서 투표자와 투표값과의 연결정보를 감추기 위해 사용.
- 공개키기반구조(public key infrastructure) : 투표자의 전자서명용 키, 개표자의 공개키를 인증하기 위해 사용.

2.5 전자선거 방식

세계 각국은 역사적 전통 및 사회 환경에 따라 여러 가지 복잡한 선거시스템(Electoral system, counting system)을 사용하고 있으며 선거시스템이 바뀌기도 한다. 이를 당선자 결정 방식에 따라 구분해 보면 다음과 같다.

- 다수득표시스템(plurality system) : 후보자 중에서 가장 많은 득표를 한 후보자가 당선된다. 과반 이상을 득표하는지 여부와는 상관없다.
- 과반득표시스템(majority system) : 후보자 중에서 과반 이상의 득표를 하는 후보자가 당선된다. 1차 투표에서 당선자가 없을 경우 결선투표를 다시 해서 당선자를 결정하기도 한다. 영국, 호

주 등의 경우에는 선호투표(preferential election)라는 방식을 사용하는데 후보들에 대한 선호도에 따라 순위를 매겨 투표한다. 1순위 선호자들에 대한 개표에서 과반득표자가 없을 경우 1순위 선호도가 가장 낮은 후보에 대한 투표 중에서 2순위 선호자의 득표를 추가하여 계산하며 이 과정을 과반득표자가 나타날 때까지 순서대로 계속한다. 즉 결선투표를 별도로 하지 않고도 한 번의 투표로 과반득표자를 가려낼 수 있는 투표방법이다.

- 비례대표시스템(proportional representation system) : 정당별 전체 투표값을 합산하여 정당의 득표율에 비례하여 당선자 수를 배정하는 방법이다.

한편 1인 1표 방식뿐만 아니라 1인 다표 방식의 복잡한 투표방식도 사용될 수 있다. 여러 종류의 투표를 한꺼번에 수행하는 경우에는 투표용지가 복잡해지고 설문지와 같은 투표방식을 사용할 수도 있다. 이러한 다양한 종류의 투표방식에 전자투표를 사용하기 위해서는 투표시스템이 이러한 복잡한 투표용지의 사용을 허용할 수 있어야 한다.

3. 전자투표의 구현 방식

전자투표를 구현하는 방식들에 대해 구분해보고 특징과 차이점을 분석해본다. 사용하는 암호기법에 따른 분류와 투표부스 사용여부에 따른 분류를 고려한다. 아울러 주요 핵심 이슈중의 하나인 인터넷 전자투표, 모바일 전자투표의 도입 가능성에 대해 검토해 본다.

3.1 사용하는 암호기법에 따른 분류

투표의 비밀성을 제공하기 위해서는 투표자의 ID 정보를 감추는 방법과 투표값을 감추는 방법을 사용할 수 있다. 믹스넷을 이용하는 방식은 각각의 투표값을 개별적으로 개표하여 투표값은 최종적으로 드러나게 되지만 믹스서버에 의한 섞는 과정을 통해 투표자의 ID 정보를 감추는 방법이다. 반면 준동형암호를 이용하는 방식은 투표자의 ID는 드러나지만 암호화된 투표값들을 모아서 한꺼번에 개표함으로써 개별적인 투표값은 드러내지 않는 방법이다. 이 두 가지 방식에 대해 간단히 알아보자. 자세한 내용은 관련된 참고문헌을 참조하기 바란다.

- 믹스넷(Mixnet) 방식 [2, 13, 17, 20, 22, 24]

전통적인 종이투표에서는 투표자가 투표지를 투표함에 넣는 순간 투표자와 투표지의 상관관계가 없어지게 된다. 믹스넷 방식은 전통적인 투표함의 기능을 암호학적으로 구현한 것이다. 이것을 암호학적으로 구현하기 위해서는 복수의 믹스서버를 이용하여 순차적으로 섞어주는 서비스를 한다. 믹스서버는 입력된 투표값들에 대해서 복호화 또는 재암호화와 함께 순서를 섞어서 출력을 하게 된다. 이러한 믹스넷 방식의 투표시스템은 일반적으로 다음과 같은 순서로 진행된다.

1) 투표 : 투표자는 후보자를 선택한 후 개표자의 공개키로 암호화하고 자신의 서명을 덧붙여 선거관리자에게 제출한다.
2) 믹스 : 복수의 믹스서버는 순차적으로 입력을 받아들여 믹스 서비스를 하여 출력한다. 최종 믹스서버는 결과를 개표자에게 출력한다.
3) 개표 : 복수의 개표자는 비밀분산 기법으로 비밀키를 공유하고 있다. 개표자들은 협력하여 문턱암호기법을 이용하여 투표값들을 복호화하여 평문 투표값을 얻는다. 이들을 합산하여 최종 투표결과를 얻고 공표한다.

- 준동형암호(homomorphic encryption) 방식 [4, 5, 6, 9, 10, 15, 16, 18, 23]

이 방식은 복수의 투표값을 결합하여 한번에 복호화할 수 있도록 준동형암호 기법을 이용하는

것으로 다음과 같이 진행된다.

1) 투표 : 투표자는 투표값을 개표자의 공개키로 암호화하고 자신의 투표값이 유효하게 구성되었음(후보자 중에서 하나를 선택하였으며 1표만을 가지고 있음)을 영지식증명을 이용하여 증명한다. 투표값과 증명값을 서명하여 선거관리자에게 제출한다. 여기에서 영지식증명을 사용하여 유효성을 확인하는 것이 필요한 이유는 투표자가 1표 이상의 투표값을 제출하거나 유효하지 않은 투표값을 제출할 수 있으며 이런 경우 결합된 투표값이 유효한 결과를 내지 못할 수 있기 때문이다.
2) 투표값의 유효성 확인 : 개표자는 서명을 확인하여 누가 투표했는지 체크한다. 영지식증명을 검증하여 유효한 투표인지 확인한다.
3) 개표 : 복수의 개표자는 유효한 투표값들을 결합하여 하나의 암호문을 만든다. 이것을 문턱암호기법을 이용하여 복호화하고 최종 결과를 계산하여 공표한다.

여기에서 준동형암호를 이용하는 방식은 투표값들이 준동형암호 방식으로 결합될 수 있도록 간단하게 인코딩될 수 있는 경우에만 사용될 수 있기 때문에 복잡한 방식의 투표지가 사용되는 경우 적용되기 어렵다는 단점이 있다. 또한 투표 시 영지식증명 값은 투표자가 계산하여야 하는데 이것의 계산량은 후보자의 수에 비례하여 증가하므로 후보자 수가 많은 경우에는 비효율적일 수 있다. 반면 개표과정은 결합된 암호문을 한번만 복호화하면 결과를 얻을 수 있으므로 매우 효율적이다. 한편 믹스넷을 이용하는 방식은 복잡한 형태의 투표형태에도 사용될 수 있어서 유연성이 높은 투표방식이다. 투표자의 계산량은 매우 적어서 효율적이지만 믹스서버 및 개표자의 계산량은 많다. 이러한 장단점이 있으므로 적용하고자 하는 투표형태에 맞는 전자투표방식을 선택하여 사용해야 할 것이다. 투표지 형태의 유연성과 투표자의 계산량이 적은 측면에서는 믹스넷 방식을 사용하는 것이 더 유리하다.

3.2 투표부스 방식 vs. 인터넷 투표

전자투표의 구현방식을 투표부스(voting booth)를 이용하는지 여부에 따라 구분할 수 있다. 투표부스를 이용하는 방식은 선거관리자에 의해 안전하게 관리되는 투표부스에서만 투표를 할 수 있도록 허용하는 방식이며 이와 반대되는 개념으로는 네트워크 통신기술을 이용하여 인터넷이 연결된 곳이면 아무 곳에서나 투표할 수 있도록 허용하는 인터넷 투표방식이 있다.

■ **투표부스 방식**

이것은 선거관리자에 의해 안전하게 운영되는 투표부스에서만 투표할 수 있도록 허용하는 방식이다. 투표자가 투표소에 도착하면 선거관리자에게 본인확인 절차를 거치고 스마트카드 등 투표용 토큰을 받는다. 투표부스 안에 설치된 터치스크린 방식 등으로 동작하는 투표기에 스마트카드를 넣고 화면의 지시에 따라 투표를 하게 된다. 투표가 제대로 되는지 확인하기 위하여 투표내용을 종이에 프린트하여 투표자가 확인 후 투표함에 저장하는 방식을 사용하기도 한다.

■ **인터넷투표 방식**

인터넷을 통해 투표용 웹사이트에 접속해 투표할 수 있도록 허용하는 방식이다. 투표자는 자신의 서명 및 인증서를 통해 자신의 신분을 인증하게 되며 투표값에는 자신의 서명이 포함되어야 한다.

위 두가지 투표 방식에는 믹스넷방식과 준동형암호방식의 투표방식 모두 사용될 수 있다. 투표부스 방식은 선거관리자가 투표부스를 안전하게 관리할 수 있으므로 강압투표나 매표행

위를 방지할 수 있으나 투표자가 반드시 투표소에 출석해야 한다는 단점이 있다. 인터넷투표 방식은 투표자가 편리한 장소에서 투표에 참여할 수 있다는 장점이 있지만 강압투표나 매표행위가 가능할 수 있다.

우리나라에서도 각 정당의 내부투표에서는 이 두가지 방식이 모두 사용된 사례가 있으나 투표부스 방식은 도입에 거부감이 적은 반면 인터넷투표 방식은 강압투표 등의 가능성으로 인해 아직 도입에 거부감이 있고 인터넷을 통한 인기투표 등의 부수적인 수단으로만 인식되기도 한다.

3.3 인터넷 전자투표의 도입 가능성 분석

인터넷 전자투표는 투표자가 투표소에 가지 않고도 자신의 집이나 회사 등 인터넷이 연결된 어느 곳에서나 편리하게 투표에 참여할 수 있도록 하는 것이다. 특히 외국에 여행하고 있거나 잠시 체류 중인 유권자들도 쉽게 참여할 수 있어서 매우 매력적인 방법이다. 이것은 전통적으로 사용되어왔던 우편투표 방식을 인터넷 기술을 사용하여 대체하는 것으로 볼 수 있다. 우편투표 제도는 국가마다 전통에 따라 인식이 다르기 때문에 허용하는 국가도 있고 허용하지 않는 국가도 있다. 투표소 이외의 곳에서 투표가 가능하게 된다면 대리투표, 가족투표, 공동투표 등의 가능성이 있을 수 있어서 허용해서는 안된다고 하는 주장도 있지만 유럽 국가들에서는 투표자의 참여를 높이기 위해 우편투표를 허용해왔다. 심지어는 대리투표를 공식적으로 허용하기도 한다. 이러한 전통 때문인지 유럽 각국에서는 특히 인터넷투표의 도입에 관심이 많다. 그러므로 우편투표를 허용할 수 있다는 사회적 공감대가 이루어져 있다면 인터넷 전자투표는 얼마든지 가능한 투표수단이 될 수 있다. 또한 최근 발전하고 있는 휴대폰 등 모바일 통신기기를 이용한 모바일 투표로 쉽게 발전시켜 나갈 수 있다.

투표소 이외의 곳에서의 투표를 허용한다면 매표행위나 강압투표가 일어날 수 있다. 그러므로 인터넷전자투표를 도입하고자 한다면 체계적이고 자동화된 효율적인 매표행위가 일어날 수 없도록 최소한의 기술적인 대책을 마련해야 한다. 예를 들면 투표자가 투표화면을 디지털카메라로 촬영하여 투표내용에 대한 증거물로 삼는 등의 방법이 이용될 수 없도록 설계하여야 한다. 한편 투표매수자 또는 강압자가 투표자를 직접 감시하는 억압적인 상황에서 투표가 이루어질 수도 있다. 이것을 방지하는 것은 기술적으로는 해결이 불가능한 문제이며 법제도, 처벌대책, 사회적 환경, 교육, 정부정책 등의 비기술적 대책을 충분히 세워서 매표행위나 강압투표가 실질적으로 매우 어렵고 비효율적이 되도록 만들어야 한다.

인터넷 전자투표를 도입하는데 있어서 가장 중요한 이슈 중의 하나는 투표자의 신분을 어떻게 인증할 것인가 하는 문제다. 우리나라의 경우 공인인증서를 이용한 인증기반구조가 잘 구축되어 있어서 이 문제를 쉽게 해결할 수 있다. 현재 은행, 증권회사, 정부기관 등에서 공인인증서를 발급하고 있는데 엄격한 신분확인을 거쳐 공인인증서를 발급하고 있으므로 이러한 공인인증서를 투표시스템에 연동하여 사용할 수 있도록 함으로써 투표자의 신분을 쉽게 확인할 수 있다. 투표자가 자신의 공인인증된 비밀키로 서명하여 투표값을 제출하도록 하면 전자서명의 안전성에 기반하여 이를 제3자가 위조하는 것은 불가능하며 1인 1투표의 원칙을 지킬 수 있다.

이러한 인증체계에서 투표용 인증서를 따로 발급하여 사용하는 것은 투표라는 행위가 자주 발생하는 것이 아니고 투표자가 인증서를 안전하게 보관해야 할 책임을 느끼지 않을 수 있기 때문에 인증서와 비밀키의 안전한 보관이 어렵

고 투표자가 인증서와 비밀키를 타인에게 제공하여 타인이 대리투표하게 할 수도 있어서 큰 위협이 된다. 이러한 행위를 방지하기 위해서는 투표자의 경제활동에 지속적으로 사용되고 있는 공인인증서를 투표에 사용하게 하고 불법행위가 발생한 경우 경제활동에 제약을 가하거나 처벌하는 등의 법적인 대비책을 마련할 수 있다. 자신의 경제활동에 사용되는 비밀키를 타인에게 불법적으로 대여하거나 하는 것은 어렵다.

인터넷 투표에 있어서의 강압투표 등 불법적인 행위들에 대해서는 투표자들의 신고를 받고(포상금제 실시) 엄격한 수사를 통해 처벌을 하는 등 법적인 대책이 필요하다. 원격 통신을 통해 투표를 진행하게 되면 많은 통신 기록이 남게 되며 투표관리자들은 이러한 정보를 바탕으로 투표자의 프라이버시가 침해되지 않는 범위에서 불법행위가 발생하는지를 엄격히 감시해야 한다. 인터넷 투표에서 강압투표 등 체계적인 불법행위가 대규모로 발생할 경우 이것이 노출되지 않고 은밀히 진행되기는 매우 어렵다.

인터넷 투표방식은 매우 매력적인 새로운 투표제도이며 투표참여도를 크게 끌어올리는 계기가 될 것으로 예상된다. 새로운 투표제도의 도입 시에는 항상 찬반 논쟁이 있어 왔지만 강압투표의 가능성 문제는 인터넷투표의 도입 자체를 막을 만한 문제제기는 아니며 이런 위협을 최소화하는 방법으로 도입해야 한다. 투표소 방식의 투표뿐만 아니라 인터넷 투표가 부작용 없이 잘 시행되는 환경을 만든다면 정치의 선진화에 큰 기여를 하게 되고 국민들의 참여를 유도하여 직접민주주의 사회를 발전시키는 초석이 될 것이다. 우리나라의 국민들은 세계 최고의 IT 강국으로서 전자상거래, 인터넷뱅킹, 전자정부 등 정보화 사회에 잘 적응되어 있으며 인터넷 전자투표에서도 건전한 직접민주주의의 참여자로서 빠르게 적응해 나갈 것으로 예상된다.

4. 전자선거 도입을 위한 이슈 분석

이번 장에서는 전자선거의 성공적인 도입을 위해서 고려해야 할 여러 가지 이슈들을 분석해본다. 전자투표에 있어서의 위협요인을 분석하고 이를 방지하기 위한 기술적, 비기술적 대책들을 제시한다.

4.1 전자투표의 위협요인 분석

- **개발사, 벤더에 의한 위협** : 소프트웨어 개발자들이 개발과정에서 설계와 다르게 코딩하거나 투표자의 눈에 보이는 결과와는 다른 결과를 내도록 제작하거나 백도어(backdoor)를 불법적으로 설치하는 등의 적극적인 속임수를 사용하려는 시도가 있을 수 있다. 또한 소프트웨어의 사용 중 업데이트 시 원래의 설계와는 다르게 불법적인 코드를 삽입하거나 할 수 있다. 이를 방지하기 위해서는 표준화된 소프트웨어 개발 방법론을 따르도록 강제하고, 독립적인 전문가그룹에 의한 소스분석, 소프트웨어 테스트 등을 거쳐 인증기관에게 인증을 받도록 하며 인증된 소프트웨어만 사용되도록 해야 한다. 투표시스템에 대한 신뢰도를 높이기 위해서는 공개소스 정책을 사용할 수 있다.
- **투표관리자에 의한 위협** : 등록기관, 투표관리자, 개표자, 운영 보안요원 등에 의한 불법행위가 가능할 수 있다. 투표시스템에서 관리자에 대한 신뢰의존도가 높을수록 관리자는 더 심각한 불법행위를 할 수 있다. 이를 방지하기 위해서는 명성이 높은 신뢰할 수 있는 관리자를 선택해야 하며 투표시스템의 운영규정, 불법행위에 대한 처벌규정 등이 준비되어야 한다. 모든 관리자의 행위에 대해서는 기록이 남고 추후 제3자가 검증해 볼 수 있도록 운영되어야 한다. 하나의 역할에 대해 키

분배 기술 등을 통해 복수의 관리자를 배정함으로써 서로 협력해야만 역할을 수행할 수 있도록 할 수 있다.

- **투표자에 의한 위협** : 부자격자에 의한 투표, 이중투표 등의 위험성은 투표시스템을 안전하게 설계하고 엄격하게 운영함으로써 방지할 수 있다. 매표행위, 강압투표 등의 불법행위를 방지할 수 있는 대책을 세우는 것도 중요하다.
- **제3의 공격자에 의한 위협** : 공격자가 투표소를 물리적으로 봉쇄하거나 투표자를 투표하지 못하도록 봉쇄할 수 있다. 투표기, 개표기 등을 해킹하거나 서비스거부 공격 등으로 정상적인 투표서비스를 방해할 수 있다. 네트워크를 통해 투표값을 전송할 때는 정보가 노출되지 않도록 암호기술, 통신보안기술을 적용하여 암호화된 상태로 전송하며 안전한 사설 네트워크를 이용해야 한다. 개인의 PC를 이용해 투표할 때는 방화벽 등 보안프로그램을 설치해야만 투표에 참여할 수 있도록 강제할 수 있다.
- **시스템의 장애, 오류, 운영자의 실수에 의한 위협** : 사전에 충분하고 세밀한 테스트를 거쳐 사용해야 하며, 데이터 백업장치, 예비시스템 등을 준비해야 한다. 운영자의 실수를 방지하기 위해서는 운영매뉴얼을 갖추고 사전교육과 모의테스트를 통해 점검해야 한다.

4.2 기술적 대책

안전한 투표시스템을 설계하고 구현하여 적용하기 위해서는 다음과 같은 기술적 이슈에 대해 고려해야 한다.

- **전자투표시스템의 설계** : 투표시스템의 설계에 있어서는 전자투표의 보안요구사항들을 만족시킬 수 있도록 적절한 암호알고리즘과 프로토콜 요소들을 사용하여 안전한 투표시스템을 설계하여야 한다. 단순한 통신보안 기법만으로는 전자투표에서 나타날 수 있는 다양한 위협요소들에 대해 적절히 대처할 수 없다.
- **투표자 신원확인** : 1인 1투표의 원칙이 지켜지기 위해서는 투표자의 신원을 확인할 수 있어야 한다. 인터넷 전자투표가 사용된다면 공인인증서 기반의 신원확인 및 투표값에 대한 전자서명이 사용되어야 한다. 전자서명의 사용으로 투표의 위조를 막을 수 있다.
- **전자투표 기술의 표준화** : 국내외 전문가들의 참여를 바탕으로 전자투표 기술을 표준화하여 사용할 수 있다. 참고로 IEEE에서 전자투표 기술에 대한 표준화를 진행하고 있다(http://grouper.ieee.org/groups/scc38/index.htm 참조).
- **소프트웨어 개발체계** : 전자투표 소프트웨어 개발에 있어서 표준화된 소프트웨어 개발 방법론에 의거하여 개발되어야 하며 버전관리, 버그패치 등의 업무에서도 표준화된 체계를 갖추어야 한다. 소프트웨어의 버그를 줄이고 소스검사를 쉽게 하기 위해 개발과정에 표준화된 코딩기법, 보안관리요소기술 등이 적용되어야 한다. 개발자는 소프트웨어 개발과정에서 시스템 설계자의 컨설팅을 받아야 한다.
- **소프트웨어 인증제도** : 독립된 인증기관이 전자투표 소프트웨어를 엄밀히 검증, 테스트하여 인증을 하고 인증된 소프트웨어만 사용될 수 있도록 하여야 한다.
- **공개소스정책** : 시스템 설계의 상세내용과 소프트웨어의 소스는 관심있는 전문가라면 누구나 검증해 볼 수 있도록 공개되어야 한다. 투표시스템의 안전성은 시스템 구성의 비밀유지가 아닌 사용되는 비밀키의 안전한 보관으로서만 유지될 수 있어야 한다.
- **복수의 운영자 체제** : 어느 한 운영자의 결정으로 관리업무를 수행하기 보다는 키분배 기술을 사용하여 복수의 운영자가 같은 업무를 담당하도록 하고 운영자들이 협력해야만 업무를 수행

하도록 할 수 있다. 일부 운영자의 부재 또는 오류시에도 시스템이 동작할 수 있도록 강인성을 제공할 수 있다.

- **투표시스템의 안전한 운영 대책** : 해킹방지 대책, 공격 발생시 공격자 확인 및 추적 대책, 오류 발생시 데이터 백업 및 오류의 원인 파악 대책, 보안 이벤트에 대한 기록, 관리자 업무의 기록 등 안전한 운영대책이 제공되어야 한다.
- **불법행위 감시체제 구축** : 투표 진행 시 획득되는 정보들을 바탕으로 불법행위가 발생하는지 여부에 대한 감시체제가 운용되어야 한다.
- **투표 사전 준비** : 시스템의 장애, 오류, 운영자의 실수가 나타나지 않도록 리스크 분석, 침투 테스트, 장애 시 대책, 운영자의 교육훈련 등이 준비되어야 한다.
- **키관리의 안전성** : 투표자의 비밀키가 안전하게 사용될 수 있도록 비밀키에 대한 적절한 접근통제 대책이 사용되어야 한다.
- 실제 운영시 투표소에 대한 적절한 물리적 보안대책이 사용되어야 한다.

4.3 비기술적 대책

- 전자투표는 새로운 투표방법으로서 제공되는 것이며 당분간은 기존의 투표 방법들과 함께 병행하여 제공하고 투표자가 투표방법을 선택할 수 있도록 운영하여야 한다. 투표소 이용 방식으로는 기존의 종이투표지 방식과 전자투표기 방식을 병행 사용할 수 있으며 원격 투표방식으로는 우편투표, 인터넷투표, 모바일투표를 함께 사용할 수 있다.
- 전자투표시스템의 장점에 대해 홍보하고 자세한 투표방법에 대해 충분한 사전교육이 필요하다.
- 불법행위에 대한 신고제도, 포상제도, 처벌대책 등이 필요하다.
- 공식적인 선거관리자와는 별도로 정당관계자, 학자, 기술자, 시민단체, NGO 등으로 구성되고 투표감시에 관한 전권을 갖는 독립적인 감시기구를 운영하는 것이 필요하다.

5. 결 론

전자투표는 IT기술의 발전을 투표영역에 접목시킨 매력적인 새로운 투표방법으로서 지금까지 많은 연구개발을 통해 실용화를 준비해왔으며 이제 전자투표를 도입할 수 있는 기술적 환경, 사회적 발전단계에 와 있다고 생각된다. 세계 각국에서는 전자투표의 도입을 위해 연구, 개발, 시범서비스 추진 등 많은 노력을 아끼지 않고 있는데 우리나라에서는 정치적인 이유 등으로 실용화 추진이 많이 늦어지고 있다. 반면 세계 제일의 IT 강국으로서 기술적 측면뿐만 아니라 전자상거래, 인터넷뱅킹, 전자정부 등 사회의 정보화가 크게 진전되어 전자투표를 도입하기 위한 기술적, 사회적 준비가 잘 되어 있다. 특히 인터넷 전자투표가 도입될 경우 유권자의 투표참여율이 크게 높아질 것으로 예상되며 정치를 선진화하고 세계 제일의 직접민주주의 모델로 발전해 나가는 중요한 계기가 될 것으로 예상된다.

투표부스를 이용한 투표방식은 우리나라에서도 각 정당의 내부 투표 등에서 시범 실시해 왔으며 도입에 거부감이 상대적으로 적은 편이다. 반면 인터넷투표 방식은 각 정당에서도 시범 실시한 사례가 있기는 하지만 부수적인 인기투표수단 정도로만 인식되었고 강압투표의 가능성으로 인해 도입에 거부감이 있다. 하지만 강압투표의 위협은 기술적으로 해결할 수 없는 근본적인 문제이며 법적, 사회적 수단에 의해 위협을 줄이는 방향으로 해결해야 한다.

지금까지 우리나라에서 시범 실시해 왔던 전자투표 시스템들은 설계내용이나 소프트웨어 소스코드가 공개되지 않아 검증이 부족하였으며 전자

투표의 보안요구사항들을 만족시키도록 잘 설계되었다고 보기 어렵다. 중앙선관위에서 야심차게 추진하는 전자투표 도입 계획은 산학연의 전문가들이 협력하여 기술을 표준화하고 설계내용 및 소프트웨어 소스를 공개하는 등 확고한 기술대책의 기반위에서 추진되어야 하겠다. 아울러 전자투표가 쉽게 도입될 수 있도록 사회적, 법적 대책을 마련해야 한다.

참고문헌

[1] M. Abe: Universally verifiable mix-net with verification work independent of the number of mix-servers, Advances in Cryptology - Eurocrypt'98, LNCS 1403, pp.437-447, Springer-Verlag, 1998.

[2] R. Aditya, B. Lee, C. Boyd, and E. Dawson: An efficient mixnet-based voting scheme providing receipt-freeness, First International Conference on Trust and Privacy in Digital Business(TrustBus 2004), LNCS 3184, pp. 152-161, Springer-Verlag, 2004.

[3] R. Aditya, B. Lee, C. Boyd, and E. Dawson: Implementation issues in secure e-voting schemes, The 5th Asia-Pacific Industrial Engineering and Management Systems Conference(APIEMS 2004), Ana hotel, Goldcoast, Australia, Dec. 12-15, 2004.

[4] O. Baudron, P.-A. Fouque, D. Pointcheval, G. Poupard and J. Stern: Practical Multi-Candidate Election System, Proc. of the 20th ACM Symposium on Principles of Distributed Computing, N. Shavit, pp.274-283, ACM Press, 2001.

[5] J. Benaloh: Verifiable secret-ballot elections, PhD Thesis, Yale University, Department of Computer Science, New Haven, September 1987.

[6] J. Benaloh and D. Tuinstra: Receipt-free secret-ballot elections, Proc. of 26th Symp. on Theory of Computing(STOC'94), pp.544-553, New York, 1994.

[7] D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto'82, pp.199-203, 1982.

[8] D. Chaum, Elections with unconditionally secret ballots and disruption equivalent to breaking RSA, Advances in Cryptology - Eurocrypt'88, LNCS 330, Springer-Verlag, pp.177-182, 1988.

[9] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung: Multi-authority secret ballot elections with linear work, Advances in Cryptology - Eurocrypt'96, LNCS 1070, pp. 72-83, Springer-Verlag, 1996.

[10] R. Cramer, R. Gennaro, and B. Schoenmakers: A secure and optimally efficient multi-authority election schemes, Advances in Cryptology - Eurocrypt'97, LNCS 1233, pp. 103-118, Springer-Verlag, 1997.

[11] A. Fujioka, T. Okamoto, and K. Ohta: A practical secret voting scheme for large scale election, Advances in Cryptology - Auscrypt '92, LNCS 718, pp.244-260, Springer-Verlag, 1992.

[12] M. Hirt and K. Sako, Efficient receipt-free voting based on homomorphic encryption, Advances in Cryptology - Eurocrypt2000, LNCS 1807, pp.539-556, Springer-Verlag, 2000.

[13] M. Jakobsson, A practical mix, Advances in Cryptology - Eurocrypt'98, LNCS 1403, pp. 449-461, Springer-Verlag, 1998.

[14] K. Kim, J. Kim, B. Lee, and G. Ahn:

Experimental design of worldwide Internet voting system using PKI, SSGRR2001, L'Aquila, Italy, Aug. 6-10, 2001.

[15] B. Lee, and K. Kim, Receipt-free electronic voting through collaboration of voter and honest verifier, Proceeding of JW-ISC2000, pp.101-108, Jan. 25-26, 2000, Okinawa, Japan.

[16] B. Lee and K. Kim, Receipt-free Electronic Voting Scheme with a Tamper-Resistant Randomizer, ICISC2002, LNCS 2587, pp. 389-406, 2002.

[17] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, Providing Receipt-freeness in Mixnet-based Voting Protocols, ICISC 2003, pp.245-258, 2003.

[18] E. Magkos, M. Burmester, V. Chrissikopoulos, Receipt-freeness in large-scale elections without untappable channels, 1st IFIP Con- ference on E-Commerce/E-business/E-Government, Zurich, Octomber 2001, Kluwer Academics Publishers, pp.683-693, 2001.

[19] M. Michels and P. Horster, Some remarks on a receipt-free and universally verifiable mix-type voting scheme, Advances in Cryptology-Asiacrypt'96, LNCS Vol.1163, pp.125-132, Springer-Verlag, 1996.

[20] M. Ohkubo, F. Miura, M. Abe, A. Fujioka and T. Okamoto: An Improvement on a practical secret voting scheme, Information Security'99, LNCS 1729, pp.225-234, Springer-Verlag, 1999.

[21] T. Okamoto, Receipt-free electronic voting schemes for large scale elections, Proc. of Workshop on Security Protocols'97, LNCS Vol. 1361, pp.25-35, Springer-Verlag, 1997.

[22] C. Park, K. Itoh, and K. Kurosawa, Efficient anonymous channel and all/nothing election scheme, Advances in Cryptology - Eurocrypt '93, LNCS Vol. 765, pp.248-259, Springer-Verlag, 1994.

[23] K. Sako and J. Killian, Secure voting using partial compatible homomorphisms, Advances in Cryptology-Crypto'94, LNCS Vol. 839, pp.411-424, Springer-Verlag, 1994.

[24] K. Sako and J. Kilian, Receipt-free mix-type voting scheme-a practical solution to the implementation of a voting booth, Advances in Cryptology-Eurocrypt'95, LNCS Vol.921, pp.393-403, Springer-Verlag, 1995.

저자약력

이 병 천

1986년 서울대학교 물리학과(학사)
1988년 서울대학교 물리학과(석사)
2002년 한국정보통신대학교 공학박사(정보보호전공)
1988년~1994년 LG전선연구소
1994년~1998년 LG전자기술원
2003년~2004년 호주 QUT 방문연구원
2002년~현재 중부대학교 정보보호학과 교수
관심분야 : 정보보호, 암호학, 암호프로토콜, 전자투표, 컴퓨터네트워크보안, 전자상거래 등