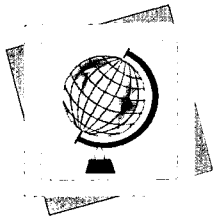
| 특집 02 |



인터넷 기반 전자선거시스템의 요구사항과 특징

김 상 진
(한국기술교육대학교)

목 차

1. 서 론

선거는 민주주의 사회를 실현하는데 가장 중요한 요소 중 하나다. 그러나 현행 선거방식은 그 낙후성으로 인해 자원낭비가 심하고, 다양하고 복잡해진 현대사회에서 국민의 의견을 정확하고 신속하게 반영하기에는 부족한 면이 많다. 또한 오늘날 선거는 저조한 참여율 때문에 그 역할을 제대로 하지 못하고 있다. 이것은 선거 쟁점에 대한 관심 부족, 선거 참여 의식 부족 등 사회, 정치적 문제 때문에 발생하는 요인도 크지만 현재 선거 방식의 시간과 공간 상의 제약도 선거 참여에 큰 영향을 주고 있다. 현재는 정부에서 마련한 선거소에 지정된 시간 내에 직접 가서 투표를 해야만 선거에 참여할 수 있다. 선거를 전자적으로 구현하여 인터넷으로 선거에 참여할 수 있으면 장애인, 노약자의 참여 문제뿐만 아니라 일반 참여자의 참여율도 높아질 것이라는 것은 의심할 여지가 없다. 또한 사람의 오류를 줄여 무효표를 완전히 없앨 수 있고, 투표와 개표하는 시간이 짧아지며, 집계에 드는 시간과 비용도 절감된다. 이런 전자선거 기술은 다양한 규모의 의견수렴 수단, 여론수렴 수단으로 널리 활용될 수도 있다.

통신과 컴퓨팅 기술이 놀랍게 발전한 지금까지 아직 전자선거를 실현하지 못하고 있는 것은 제도적 문제 등 여러 다른 문제도 있지만 안전성 측면에서도 전자적으로 네트워크를 통해 선거를 치르기에는 아직 해결해야 하는 기술적 문제도 많이 남아 있다. 그 가운데 공간상 제약이 없기 때문에 도청불가능한 안전한 채널을 확보하는 문제, 표를 사고파는 매표행위를 방지하는 문제, 유권자의 표가 제대로 집계에 반영되었는지 검증할 수 있는 수단을 제공하는 문제가 가장 어렵다. 암호기술을 사용하여 선거가 갖추어야 할 여러 요구사항을 충족하도록 만든 기존 전자선거 기법들은 매표방지와 전체검증을 제공하기 위해 거의 대부분 통신 채널에 대한 도

청불가능이란 물리적 가정이 필요하거나 요구되는 계산과 통신비용이 많아 현실성이 부족하였다. 하지만 최근에는 이런 문제점들도 어느 정도 극복되고 있다.

이 논문에서는 암호기술을 사용하여 선거가 갖추어야 하는 요구사항들을 충족하고자 시도했던 전자선거시스템에 대해서 살펴본다. 현행 선거 방식을 개선하기 위해 선거의 일부 단계에서 전자적인 하드웨어를 사용하는 시스템들이 존재하지만 이들에 대해서는 이 논문에서 고려하지 않는다. 이 논문에서 고려하는 전자선거시스템은 선거의 모든 요소가 컴퓨터 소프트웨어를 통해 이루어져야 하며, 통신 상에서 특히, 인터넷을 통해 공간과 시간에 대한 제약 없이 선거에 참여할 수 있어야 한다. 인터넷으로 공간과 시간에 구애받지 않고 할 수 있어야 진정으로 유권자의 편리성과 만족도를 높일 수 있으며, 전자선거를 도입하고자 목적을 달성할 수 있을 것이다. 이런 전자선거시스템은 암호기술을 사용하지 않고는 선거가 갖추어야 하는 요구사항들을 충족하기가 매우 어렵다. 이 논문에서 이런 시스템의 요구사항과 특징을 분석하고, 현재 기술 수준이 어디까지 도달해있는지 살펴본다.

이 논문의 구성은 다음과 같다. 2장에서는 전자선거시스템이 갖추어야 하는 요구사항과 요구사항을 충족하기 위해 사용되는 암호기술을 설명하고, 3장에서는 전자선거시스템에 참여하는 참여자의 특성을 설명한다. 4장에서는 전자선거시스템의 각 단계의 특성을 살펴보고, 5장에서는 전자선거시스템을 다양한 기준에 따라 분류한다. 6장에서는 전자선거시스템에서 사용하는 통신 모델을 살펴보고, 7장에서 결론을 맺는다.

2. 전자선거시스템의 요구사항

Fujioka 등[1]은 전자선거 기법이 갖추어야 할 다음과 같은 요구사항을 제안하였다.

■ 요구사항 1. 완전성(completeness)

유효한 모든 표는 집계에 정확하게 반영되어야 한다.

■ 요구사항 2. 건전성(soundness)

정직하지 않은 유권자는 선거를 방해할 수 없어야 한다.

■ 요구사항 3. 비밀성(privacy)

유권자가 투표한 내용을 알 수 없어야 한다.

■ 요구사항 4. 선거권(eligibility)

인가된 유권자만이 선거에 참여할 수 있어야 한다.

■ 요구사항 5. 이중투표 방지(unreusability)

모든 유권자는 한 표만 투표할 수 있어야 한다.

■ 요구사항 6. 공정성(fairness)

선거에 영향을 주는 것이 없어야 한다. 특히, 선거의 중간 결과를 알 수 없어야 한다.

■ 요구사항 7. 검증성(verifiability)

선거가 제대로 이루어졌는지 확인할 수 있어야 한다.

투표의 비밀성은 다른 유권자가 투표한 내용을 알 수 없어야 한다는 것을 말하지만 무조건적으로 이것을 보장할 수 있는 것은 아니다. 예를 들어 찬반 투표에서 모든 유권자가 찬성 표를 행사했을 경우에는 투표의 비밀성을 보장할 수 없다. 따라서 투표의 비밀성을 보다 정확하게 정의하면 어떤 표가 주어졌을 때 선거의 결과로부터 예측할 수 있는 것 이상으로 이 표의 내용을 알 수 없어야 한다는 것을 의미한다.

투표의 비밀성을 보장하기 위해서는 기본적으로 투표한 내용을 암호화해야 한다. 그러나 결정적 암호방식으로 암호화하면 암호문을 통해 투표 내용을 알 수 있거나 추측할 수 있게 된다. 따라서 투표를 암호화할 때 사용하는 암호기법은 확률적 암호방식이어야 한다. 이 때 암호문을 결정하기 위해 사용되는 랜덤값을 이 암호의 랜덤요소(randomness)라 한다. 투표의 내

용을 암호화하는 이유는 다른 유권자나 제3자로부터 유권자의 비밀성을 보장하기 위한 것이다. 하지만 집계를 하기 위해서는 암호화된 값을 복호화해야 하므로 유권자의 비밀성을 집계자에게 보장하기가 어렵다. 초기 전자선거시스템은 집계하는 관리자에게는 투표의 비밀성을 제공하지 못하였다[2]. 최근에는 이런 문제를 극복하기 위해 개별 표의 복호화 없이 집계를 할 수 있도록 고안하고 있다. 이를 위해 보통 준동형(homomorphic) 특성을 만족하는 암호시스템을 사용한다. 그런데 한 명의 선거관리자가 집계하는 방식에서는 이런 장치가 있다 하더라도 유권자의 비밀성을 보장하기가 어렵다. 이에 현재는 여러 명의 집계자를 두어 일정 수 이상의 집계자가 협력해야 개별 표의 복호화가 가능하도록 고안하고 있다. 이것은 뒤에 설명하고 있는 선거의 강건성 요구사항과도 밀접한 관계가 있다.

선거권과 이중투표 방지는 제시된 여러 특성 중 충족하기가 가장 쉽다. 보통 전자서명이나 기타 인증절차를 통과한 유권자만이 선거에 참여할 수 있도록 제한하여 선거권 요구사항을 충족시킨다. 선거권과 이중투표 방지 특성을 합쳐 민주주의(**democracy**) 특성이라고도 한다.

Sako와 Kilian[3]은 검증성을 다음과 같이 개별검증(**individual verifiability**)과 전체검증(**universal verifiability**)으로 세분화하였다.

■ 요구사항 7-1. 개별검증

선거에 참여한 유권자는 자신의 표가 집계에 올바르게 포함되었는지를 확인할 수 있어야 한다.

■ 요구사항 7-2. 전체검증

선거의 참여 여부와 상관없이 누구나 개별 투표지의 유효성과 집계 결과의 유효성을 확인할 수 있어야 한다.

검증성은 완전성 요구사항과 밀접한 관계가 있다. 한편으로 이런 기능이 유권자들의 이의제기를 증폭시켜 선거의 진행을 저해할 수 있다고 주장하는 이도 있다.

Chaum[4]은 검증성과 유사한 무조건적 무결성(unconditional integrity) 요구사항을 제시하였다. 이 요구사항은 무한한 컴퓨터 자원이 있더라도 집계 결과를 바꿀 수 없어야 한다는 것을 말한다. 완전성과 관련된 요구사항이지만 이 요구사항에서 추가적으로 주장하고 있는 것은 무결성이 비밀성보다 우선해야 한다는 것이다. 즉, 집계의 정확성은 무한한 컴퓨터 자원이 있더라도 집계 결과를 조작할 수 없어야 하며, 이를 위해 비밀성이 희생되어야 하면 비밀성에 대해서는 계산적 안전성만 제공해도 된다는 것을 말한다.

Benaloh와 Tuinstra[5]는 선거를 전자적으로 구성하면 유권자는 자신이 누구에게 투표하였는지에 대한 증거를 남길 수 있다는 문제점을 발견하였다. 현행 선거 방식에서는 밀폐된 투표소를 사용하고, 결과표를 투표함에 비밀스럽게 넣어 선거하므로 누구도 유권자가 투표한 내용을 확인할 수 없다. 따라서 현행 선거 방식에서는 표를 사고파는 것이 어렵다. 그러나 전자선거에서 유권자가 증거를 남길 수 있으면 이 증거를 구매자에게 제시하고 표를 팔 수 있으며, 구매자는 증거를 확인한 후에 표를 살 수 있다. 따라서 이런 증거를 남길 수 없도록 하거나 남길 수 있어도 구매자가 이 증거를 통해 확신을 가질 수 없도록 해야 한다. 이런 요구사항을 매표방지(**receipt-freeness**)라 한다.

■ 요구사항 8. 매표방지

유권자는 선거 과정에서 얻은 정보를 이용하여 다른 사람에게 자신이 투표한 내용을 증명할 수 없어야 한다.

암호프로토콜을 이용하여 구성하는 전자선거 시스템의 경우에는 증거를 전혀 남길 수 없도록 만드는 것은 어렵다. 특히, 공개된 통신 채널로

선거 과정이 진행되면 보통 이 채널로 교환된 메시지들은 증거가 되기 충분하다.

Michels와 Horster[6]는 매표자가 유권자를 어느 정도 제어할 수 있는지에 따라, 매표자가 누구와 공모가 가능한지에 따라 시스템의 매표방지 수준을 정의하였다. 유권자에 대한 제어 수준은 매표자가 접근할 수 있는 정보에 의해 다음과 같이 결정된다.

■ 제어 수준 1.
매표자가 공개된 정보만 볼 수 있다.

■ 제어 수준 2.
매표자는 공개된 정보뿐만 아니라 유권자가 전송한 표의 형태를 볼 수 있다. 그러나 선거 과정에서 유권자는 비밀로 선거관리자에게 정보를 전달할 수 있다.

■ 제어 수준 3.
매표자는 공개된 정보뿐만 아니라 유권자가 전송한 표의 형태를 볼 수 있다. 그러나 선거 과정에서 선거관리자는 비밀로 유권자에게 정보를 전달할 수 있다.

■ 제어 수준 4.
매표자는 공개된 정보뿐만 아니라 모든 통신 채널을 제어할 수 있다. 단 유권자는 시스템 초기에 선거관리자와 비밀통신을 할 수 있다.

■ 제어 수준 5.
매표자는 공개된 정보뿐만 아니라 모든 통신 채널을 제어할 수 있다.

이것은 시스템에서 가정하는 통신 모델과 매우 밀접한 관련이 있다. 통신 모델에서는 제어 수준 2와 3을 유권자에서 선거관리자로 일방향 비밀 채널, 선거관리자에서 유권자로 일방향 비밀 채널, 유권자와 선거관리자간에 양방향 비밀 채널, 세 가지로 세분화한다.

매표자가 누구와 공모가 가능한지에 따른 Michels와 Horster의 분류는 다음과 같다.

■ 공모 수준 1.
다른 유권자와 공모가 가능하다.

■ 공모 수준 2.
최소한 한 명의 선거관리자와 공모가 가능하다.

■ 공모 수준 3.
모든 선거관리자와 공모가 가능하다.

매표자의 목적은 유권자가 자신이 원하는 후보자에게 투표하도록 하는 것이다. 매표방지가 제공되어 매표자가 유권자가 제시한 증거를 통해서는 어떤 후보자에게 투표하였는지 확신할 수 없다고 하더라도 임의 투표 공격(random voting attack)이 가능할 수도 있다. 김상진과 오희국[7]이 제안한 시스템은 매표 방지가 제공되지만 임의 투표 공격을 방지하지는 못한다.

매표방지의 상위 개념으로 **강요불가능성(uncoercibility)**이 있다. 하지만 전자선거시스템에서는 강요자가 유권자가 투표하는 것을 지켜보면서 특정한 표를 행세하도록 강요하는 것은 고려하지 않는다. 또한 유권자가 자신을 인증하는데 사용되는 개인키를 매표자에게 주어 매표자가 유권자를 대신하여 투표하도록 하는 공격도 방지하기가 어렵다. 이런 것의 방지는 암호기술만을 사용하여 충족시킬 수 없다. 매표방지를 위해서는 증거를 가질 수 없어야 하지만 전체검증을 위해서는 증거를 남겨야 한다. 즉, 두 요구사항이 그 목적에 있어 상충하므로 두 요구사항을 동시에 충족하는 것은 어렵다.

최근에는 종이 영수증을 유권자에게 제공해야 한다는 주장도 있다. 종이 영수증 자체만 생각하면 이것은 매표방지와 상충되는 것이라고 생각할 수 있다. 하지만 이런 종이 영수증은 유권자의 만족도를 높일 수 있는 좋은 수단이 된다. 그러나 종이 영수증을 제공하더라도 매표방지를 여전히 제공해야 되므로 안전한 시스템 설계가 더욱 어려워진다. 물론 종이 영수증 개념은 인터넷 기반 전자선거 환경에서는 제공되기

어려운 기능이다. 참고로 Chaum은 이런 종이 영수증은 다음과 같은 요구사항을 충족해야 한다고 주장하고 있다[4].

■ 종이 영수증의 요구사항 1

영수증이 제대로 게시되면 해당 유권자의 표가 집계에 포함되었다는 것을 유권자는 확신할 수 있어야 한다.

■ 종이 영수증의 요구사항 2

영수증이 제대로 게시되지 않았으면 유권자는 자신이 가지고 있는 영수증을 이용하여 이 사실을 증명할 수 있어야 한다.

■ 종이 영수증의 요구사항 3

제대로 게시된 영수증의 내용을 들키지 않고 변경할 수 있는 확률은 매우 낮아야 한다.

■ 종이 영수증의 요구사항 4

일정한 수 이상의 신뢰기관이 올바른 키를 이용하여 복호화하지 않는 이상 누구도 영수증을 복호화하여 유권자가 투표한 내용을 알 수 없어야 한다.

요구사항 1은 검증성과 연관이 있고, 요구사항 4는 매표방지와 연관이 있다. 이런 종이 영수증은 영상 암호학(visual cryptography) 기술을 이용하여 만들 수 있다.

비밀성 요구사항을 설명할 때 언급하였듯이 전자선거에서는 확률적 암호기법을 이용하여 표를 암호화하여야 한다. 이 때 사용되는 랜덤요소를 누가 생성하느냐에 따라 매표방지에 다른 영향을 주게 된다. 보통 표는 유권자와 선거관리자 또는 제3의 신뢰기관과 프로토콜을 수행하여 구성한다. 따라서 가능한 랜덤요소의 선택 시나리오는 다음과 같다.

■ 시나리오 1. 유권자만 선택

유권자만 선택하면 유권자는 선택한 랜덤 값을 구매자에게 제시하여 표의 구성을 증명할 수 있다. 이것을 극복하기 위해 Okamoto[8]는 트랩도어 비트위임 기법을 이용하여 나중에 거짓 랜덤 값을 제시할 수 있도록 하여 매표방지를 제공하고 있다. 그러나 매표자가 대신 랜덤 값을 선택해주면 매표방지를 제공할 수 없거나 임의투표 공격에 취약하다.

■ 시나리오 2. 신뢰기관만 선택

Hirt와 Sako[9]처럼 신뢰기관만 선택할 수 있다. 신뢰기관은 유권자가 어떤 후보를 선택할지 모르기 때문에 모든 후보에 대한 표를 암호화하여 유권자에게 전달해주어야 한다. 유권자가 신뢰기관이 만들어 준 표들 중 하나를 선택하여 투표하면 여전히 비밀성을 만족할 수 없기 때문에 여러 기관이 믹스넷을 통해 계속 재암호화해야 한다. 따라서 유권자는 각 믹스넷의 진행과정을 관찰 수 있어야 하며, 각 과정의 유효성을 확인할 수 있어야 한다. 이런 관찰은 도청불가능한 채널로 이루어져야만 매표방지를 제공할 수 있다.

■ 시나리오 3. 둘다 선택하지만 유권자가 먼저 선택

이병천과 김광조[10]는 유권자가 표를 암호화하여 그것의 유효성을 증명한 다음 신뢰기관으로부터 새 랜덤값이 포함된 값을 받아 표를 다시 암호화하여 최종표를 구성한다. 이처럼 둘다 선택하면 유권자나 신뢰기관은 서로가 선택한 랜덤요소를 알 수 없어 매표자가 신뢰기관과 공모하지 않는 이상 매표방지를 제공할 수 있다. 그러나 전체검증을 제공하기 위해 유권자는 신뢰기관에 초기 표의 유효성을 증명해야 하고, 신뢰기관은 반대로 유권자에게 새 랜덤값이 포함된 값의 유효성을 증명해야 한다. 이들 증명은 증거로 사용될 수 있어 도청불가능한 채널로 전달되어야 하며, 거짓 증명이 가능하도록 일반 영지식 증명 대신에 지정된 확인자 증명을 이용하여 증명해야 한다. Hirt[11]는 이병천과 김광조와 달리 유권자가 표를 암호화하여 신뢰기관에 전달하면 신뢰기관은 이것을 재암호화하여

최종표를 구성하고, 이를 유권자를 대신하여 게시판에 게시한다. 이 방법 역시 매표방지는 제공할 수 있으나 전체검증을 제공하기가 어렵다. 그 이유는 유권자가 전달한 표를 제시하지 않고는 최종표의 유효성을 증명할 수 없기 때문이다. 그러나 유권자의 초기표가 공개되면 시나리오 1과 마찬가지로 매표방지를 제공할 수 없다.

■ 시나리오 4. 둘다 선택하지만 신뢰기관이 먼저 선택

신뢰기관은 유권자가 어떤 후보에게 투표할지 모르므로 신뢰기관이 먼저 선택한다는 것은 Hirt와 Sako[5]의 기법처럼 각 후보의 표를 각각 암호화하여 유권자에게 전달해야 한다. 김상진과 오희국[7]은 이 방법을 사용하였다. 그러나 이들은 Hirt와 Sako[5]의 기법과 달리 믹스넷을 사용하지 않고 유권자가 새 랜덤요소를 선택하여 투표하고자 하는 후보의 표를 재암호화하여 최종표를 구성한다. 따라서 이 방법에서는 섞은 순서를 전달하기 위해 오직 신뢰기관에서 유권자로의 일방향 도청불가능한 채널만 필요하다. 신뢰기관이 공개한 표 묶음의 유효성 증명과 이 중 하나를 재암호화하였다는 증명을 이용하면 전체검증도 쉽게 제공할 수 있다. 그러나 이 방식은 임의 투표 공격 가능하다는 단점이 있다.

Cranor[12]는 이 외에 다음 요구사항을 제안하였다.

■ 요구사항 9. 이동성(mobility)

유권자는 지리적 위치에 제한받지 않고 투표를 할 수 있어야 한다.

■ 요구사항 10. 유연성(flexibility)

다수후보 투표와 같이 다양한 형태의 선거를 지원하면 시스템은 유연하다고 말한다.

또한 Cramer 등[13]은 다음 요구사항을 추가로 제안하였다.

■ 요구사항 11. 표의 복사 가능성(vote duplication)

다른 유권자가 투표한 것을 복사하여 투표할 수 없어야 한다. 이것은 다른 유권자가 어떻게 투표하였는지 모르는 채 그 유권자가 공개한 내용을 이용하여 동일하게 투표하는 것을 말한다.

■ 요구사항 12. 강건성(robustness)

어떤 수 이하의 참여자의 부정은 허용할 수 있어야 한다.

강건성은 유권자들 간에 공모, 유권자와 관리자 간에 공모, 관리자들 간에 공모로 나누어 생각해볼 수 있다. 이 중에 선거관리자들 간에 공모에 대한 강건성을 충족시키기 위해 보통 여러 명의 선거관리자를 두며, 이들은 threshold 암호 시스템을 이용하여 일정한 수 이상이 협력하여야 개별 표를 복호화할 수 있도록 고안한다. 집계 또한 일정한 수 이상의 선거관리자가 협력하여야 할 수 있도록 만든다.

3. 전자선거시스템의 참여자

전자선거시스템에 참여하는 참여자는 크게 다음과 같이 분류할 수 있다.

■ 유권자

■ 선거관리자

선거관리자는 선거가 정상적으로 이루어지기 위해 권한을 부여받은 참여자를 말한다. 초기 전자선거시스템에서는 한 명의 선거관리자가 유권자의 인증, 표의 유효성 확인, 집계 등 모든 과정을 책임졌다. 그러나 현재는 선거관리자의 권한 집중을 분산하기 위해 여러 명의 선거관리자를 두는 형태를 대부분 사용한다.

■ 집계자

집계자는 최종 집계를 계산하고 발표하는 참여자를 말한다.

■ 후보자

후보자가 직접 선거 프로토콜에 참여하는 경우는 드물다. 하지만 Iverson[14]이 제안한 시스템과 같이 유권자가 각 후보자와 상호작용하여 표를 구성하는 시스템도 제안된 바 있다.

이들 참여자 중 유권자는 다음과 같은 부정행위를 할 수 있다.

■ 부정행위 1.
선거권이 없는데 등록을 시도할 수 있다.

■ 부정행위 2.
다중 이름으로 등록을 시도할 수 있다.

■ 부정행위 3.
다른 사람의 표를 복사하여 투표할 수 있다.

■ 부정행위 4.
매표 행위를 시도할 수 있다.

선거관리자는 다음과 같은 부정행위를 할 수 있다.

■ 부정행위 1.
선거권이 없는 참여자를 등록시켜 줄 수 있다.

■ 부정행위 2.
선거권이 있는 참여자가 둘 이상의 표를 투표하도록 허용할 수 있다.

■ 부정행위 3.
투표하지 않은 유권자를 대신하여 투표할 수 있다.

■ 부정행위 4.
유효한 표를 집계에서 누락할 수 있다.

■ 부정행위 5.
유효한 표 자체를 파괴할 수 있다.

■ 부정행위 6.
집계 결과를 허위로 발표할 수 있다.

이와 같은 부정행위는 게시판이란 통신 모델과 전체검증성을 제공하여 대부분 방지하고 있다.

4. 전자선거시스템의 단계

전자선거시스템에는 보통 다음과 같은 과정이 존재한다.

■ 등록과정

선거에 참여할 수 있는 선거권이 있는 유권자는 이 과정을 통해 선거에 필요한 암호키, 토큰 등을 선거관리자로부터 발급받는다. 선거관리자는 유권자의 명부를 이 단계에서 작성한다.

■ 선거과정

이 과정은 다시 크게 다음 두 단계로 나뉘어질 수 있다.

- 표를 구성하는 단계 : 보통 선거관리자와 암호 프로토콜을 수행하여 표를 구성하게 된다.
- 투표하는 단계 : 보통 공개 게시판에 지정된 자신의 공간에 표와 이 표의 유효성을 검증할 수 있는 정보를 게시하여 투표한다. 이 과정에서 반드시 유권자를 인증하여 전자선거의 민주주의 특성을 충족해야 한다.

■ 집계과정

믹스넷을 사용하지 않는 시스템에서는 각 유권자의 비밀성을 보장하기 위해 개별 표를 복호화하여 집계를 할 수 없다. 준동형 암호시스템을 사용하는 시스템은 이것을 극복하기 위해 모든 표를 결합하여 한번에 복호화하는 방식을 사용한다. 보통 시스템들은 그러나 집계의 정확한 결과를 알기 위해 이산대수를 문제를 해결해야 하는 문제점이 있어, 대규모 선거에는 아직 사용하기에는 적합하지 않다. 믹스넷 기반 선거시스템들은 이와 달리 믹스넷을 통해 비밀성을 보장하므로 개별 표를 복호화하여 집계를 할 수 있다.

5. 전자선거시스템의 분류

전자선거시스템은 기준에 따라 다음과 같이 다양하게 분류할 수 있다.

■ 분류 1. 투표 방식에 따른 분류

찬반 투표, 다수후보 투표, t개 중 1개 선택 투표, 서면기입(write-in) 투표

■ 분류 2. 선거 규모에 따른 분류

소규모, 대규모

■ 분류 3. 가정하는 통신 모델에 따른 분류

일방향 도청불가능한 채널, 양방향 도청불가능한 채널, 공개 채널

■ 분류 4. 사용하는 암호기술에 따른 분

- 믹스넷 기반[3,15,16]
- 은닉서명 기반[1,8,14,17]
- 준동형 암호 기반[5,7,9-11,13,18-21]

분류 1의 경우 가장 많은 표를 받은 여부만 판별할 수 있는 경우와 각 후보가 정확하게 몇 개의 표를 받았는지 결정할 수 있는 기법으로 다시 세분화할 수 있다. 다수후보 투표가 가능하면 선거시스템이 유연하다고 말한다. 분류 2에 대해서는 다음 장에서 자세히 분석한다. 분류 4에서 아직까지 매표방지와 전체검증을 동시에 제공하는 은닉서명 기반 전자선거시스템은 제안되지 못하고 있다. 믹스넷 기반 선거시스템들은 앞서 언급한 바와 같이 개별 표를 복호화하여 집계를 할 수 있는 장점이 있지만 믹스넷을 이용한 선거시스템은 다음과 같은 문제점이 있을 수 있다.

■ 첫 믹서에게 전달되는 메시지의 크기

초기 믹스넷 기반 시스템의 경우에는 메시지의 크기가 사용하는 믹서 수에 비례하였다[15].

■ 표들을 여러 번 섞을수록 비밀성은 향상되지만 여러 번 섞을수록 비용이 많이 소요된다. 특히 전체 검증성을 제공하기 위해서는 섞는 과정의 올바름까지 증명해야 하므로 그 비용은 매우 크다고 할 수 있다. 최근에는 섞는 과정에 소요되는 비용을 향상시킬 수 있는 새로운 기술[22]과 섞는 과정의 올바름을 효율적으로 증명하는 방법[23]들이 등장하고 있지만 여전히 비용이 많이 소요된다고 할 수 있다.

■ 최종 믹서에 의한 허위 표 게시

■ 게시된 최종 결과에 오류가 있을 경우

초기 믹스넷 기반 시스템의 경우에는 재투표를 하여야 하는데 이 경우에 기존 투표의 부분결과를 유권자들이 알게 되며, 이것이 재투표에 영향을 줄 수 있다. 따라서 공정성에 위배될 수 있다. 이 문제는 모든 표가 유효한 표임을 확신할 수 있는 경우에만 실제 표를 개방하도록 하여 해결할 수 있다.

준동형 암호 기반 시스템은 대부분 ElGamal 암호기법을 사용하지만 최근에는 Paillier가 제안한 다차잉여 문제의 어려움에 의존하는 암호시스템와 같이 새롭게 제안된 준동형 암호기법을 이용하는 시스템들이 제안되고 있다[20,21].

6. 전자선거시스템의 통신모델

대부분의 전자선거 기법에서 유권자는 선거관리자와 프로토콜을 수행하여 투표할 표를 구성한다. 표를 구성한 후에 유권자는 이 표를 집계에 반영되도록 공개 게시판(bulletin board)의 자신의 특정 영역에 게시한다. 선거관리자는 선거가 끝나면 게시판에 게시된 모든 표를 이용하여 최종 집계를 계산한다. 이런 게시판은 일반적으로 다음과 같은 특성을 만족한다.

■ 게시판 요구사항 1.

게시판에 게시된 내용은 누구나 읽을 수 있다.

■ 게시판 요구사항 2.

게시판에 게시된 내용은 누구도 변경 또는 삭제할 수 없다. 즉, 데이터를 추가할 수만 있다.

■ 게시판 요구사항 3.

각 유권자는 게시판에 자신의 영역을 가지며, 각 영역에는 그 영역을 할당받은 유권자만 쓸

수 있다.

유권자는 자신의 영역에 표를 게시하여 선거에 참여하므로 게시판에 표를 게시할 때 유권자를 인증하여야 한다. 이를 통해 선거의 요구사항 중 선거권을 제공한다. 보통 사용자 인증을 위해 전자 서명 기술을 이용한다고 가정한다. 또한 유권자는 자신의 영역에만 쓸 수 있으므로 이중투표 방지도 게시판을 통해 제공한다. 따라서 게시판의 역할은 다음과 같다.

■ 게시판의 역할 1. 선거권 : 유권자의 인증
■ 게시판의 역할 2. 이중 투표 방지
■ 게시판의 역할 3. 전체검증을 위한 자료 공개장 역할

따라서 게시판을 사용하는 경우에는 보통 준동형 암호시스템을 사용하여 개별 표를 복호화하지 않고, 모든 표를 결합한 후에 복호화하여 집계 결과를 알아낸다. 그러나 Acquisti[20]는 게시된 표들을 다시 믹스넷을 통해 섞은 다음에 개별 표를 복호화하여 집계를 하는 방식을 제안하였다.

공개 게시판을 사용할 경우에 한 가지 문제점은 공격자는 유권자가 기권하도록 강요할 수 있다는 것이다[21]. 공개 게시판이므로 누구나 누가 투표를 하였고, 누가 투표를 하지 않았는지 알 수 있다. 따라서 유권자는 공격자가 나중에 게시판을 통해 투표 참여 여부를 확인할 수 있다는 것을 알기 때문에 협박을 당할 경우 기권할 확률이 높다. 다른 한편으로 기권한 사실이 공개되므로 사생활이 침해될 수 있는 소지도 있다.

매표방지성에 대한 요구로 인해 선거 과정에서 유권자와 선거 관리자 간에 통신 내용을 제3자가 볼 수 없도록 하여야 한다. 단순하게 생각하면 교환되는 메시지를 암호화하여 이 요구사항을 충족할 수 있다고 생각할 수 있다. 그러나 키를 유권자가 구매자에게 줄 수 있으므로 단순 암호화를 통해 채널의 안전성을 확보할 수 없다. 따라서 매표방지를 제공하는 선거 기법은 보통 통신 채널에 대한 다음과 같은 물리적 가정을 한다.

■ 일방향 도청불가능한 채널
(uni-directional untappable channel)

이 채널은 다음을 물리적으로 보장하는 안전한 채널이다.

- 전송자만 수신자에게 이 채널로 메시지를 보낼 수 있다.
- 수신자는 이 채널로 어떤 메시지를 수신하였는지 제3자에게 증명할 수 없다.
- 제3자는 이 채널을 도청할 수 없다.

■ 양방향 도청불가능한 채널
(bi-directional untappable channel)

이 채널은 양방향으로 메시지를 교환할 수 있다는 것을 제외하고는 일방향 도청불가능한 채널과 특성이 같다. 이 채널을 다른 말로 선거부스(voting booth)라 한다.

이런 종류의 통신 채널을 실제 구현하여 전자적으로 선거를 한다는 것은 비용측면에서도 현실성이 없으며, 현재의 종이 선거의 공간적과 시간적 제약이 그대로 전자 선거에도 유지되는 형태가 되어 전자 선거의 장점이 크게 퇴색한다. 하지만 Hirt와 Sako[9]는 매표방지를 위해서는 최소한 선거관리자에서 유권자로의 일방향 도청불가능한 채널을 가정해야 한다고 주장하고 있다. 최근까지는 이런 물리적 가정은 스마트카드와 같은 보안 하드웨어를 사용하지 않고는 제거하는 것이 어렵다고 간주되었다. 즉, 유권자와 선거관리자 간에 통신 대신에 유권자와 스마트카드 간에 통신을 통해 표를 구성하는 방법을 사용하면 이와 같은 물리적인 가정을 제거할 수 있으며, 실제로 이병천과 김광조[19]는 스

마트 카드를 사용하여 물리적 가정이 필요 없는 시스템을 제안한 바 있다. 그러나 최근 Acquisti [20]나 Juels와 Jakobsson[21]이 제안한 시스템은 하드웨어나 물리적인 가정 없이 매표방지와 전체 검증성을 동시에 제공할 수 있음을 보이고 있다.

7. 결 론

이 논문에서는 암호기술을 사용하여 선거가 갖추어야 하는 요구사항을 충족하고자 노력했던 전자선거시스템들에 대해 분석하였다. 이 시스템들은 기존 현행 선거 방식이 만족해야 하는 요구사항뿐만 아니라 전자적으로 공개된 통신 채널을 통해 공간과 시간 제약 없이 선거를 할 수 있어야 하므로 기존에는 없던 새로운 요구사항들도 충족해야 한다. 이들 요구사항을 모두 만족하면서 모든 과정이 효율적인 시스템을 개발하는 것은 어려울 것으로 생각되었다. 특히 통신 채널에 대한 물리적인 가정 없이 전체검증과 매표방지를 동시에 제공하면서 공개채널로 선거를 할 수 있고 집계가 효율적이며 유연한 시스템을 개발하는 것은 가능하지 않을 것으로 생각되었다. 그러나 최근에 서면기입 투표까지 제공하면서 물리적인 가정이나 보안 하드웨어를 사용하지 않고 전체검증과 매표방지가 동시에 제공될 수 있는 시스템들이 제안되고 있다 [20,21]. 따라서 이런 추세라면 멀지 않아 유권자들이 인터넷을 통해 암호기술을 사용한 순수 소프트웨어로 구현된 전자선거시스템을 사용할 수 있게 될 것으로 생각된다. 물론 전자선거 소프트웨어 자체가 안전하다는 것은 전체 시스템의 안전성의 일부분 밖에 되지 않는다. 실제 인터넷을 이용한 전자선거가 도입되기 위해서는 투표에 사용되는 각 컴퓨터의 안전성 문제, 서버에 대한 DOS 공격 차단 문제 등 이 논문에서 살펴본 내용 외에 다양하게 고려하고 해결해야 하는 기술적인 문제들이 여전히 많다.

참고문헌

[1] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology, Auscrypt 1992, LNCS~718, pp.244-251, Springer, 1993.

[2] J.D. Cohen and M.J. Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme", Proc. of the 26th IEEE Symp. on Foundations of Computer Science, pp.383-395, IEEE Press, 1985.

[3] 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 1995, LNCS 921, pp.393-403, Springer, 1995.

[4] D. Chaum, "Secret-Ballot Receipts True Voter-Verifiable Elections", IEEE Security & Privacy, Vol. 2, No. 1, pp.38-47, 2004.

[5] J. Benaloh and D. Tuinstra, "Receipt-free Secret-ballot Elections", Proc. of the 26th ACM Symp. on Theory of Computing, pp. 544-553, ACM Press, 1994.

[6] M. Michels and P. Horster, "Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme", Advances in Cryptology, Asiacrypt 1996, LNCS 1163, pp.125-132, Springer 1996.

[7] S. Kim and H. Oh, "A New Universally Verifiable and Receipt-Free Electronic Voting Scheme Using One-way Untappable Channels", Proc. of the AWCC 2004, LNCS 3309, pp.335-345, Springer, 2004.

[8] T. Okamoto, "Receipt-Free Electronic Voting Schemes for Large Scale Elections", Proc. of Workshop on Security Protocols 1997, LNCS~1361, pp.25-35, Springer, 1998.

[9] M. Hirt and K. Sako, "Efficient Receipt-

Free Voting Based on Homomorphic Encryption", Advances in Cryptology, Eurocrypt 2000, LNCS 1807, pp.539-556, Springer, 2000.

[10] B. Lee and K. Kim, "Receipt-free Electronic Voting through Collaboration of Voter and Honest Verifier", Proc. of the JWISC 2000, pp.101-108, 2000

[11] M. Hirt, "Receipt-free Voting with Randomizers", Presentated at the Workshop on Trustworthy Elections, Aug. 2001. http://www.vote.caltech.edu/wote01/

[12] L.F. Cranor, "Electronic Voting: Computerized Polls May Save Money, Protect Privacy", ACM Crossroads, Vol.2, No.4, pp. 12-16, 1996.

[13] R. Cramer, R. Gennaro, and B. Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology, Eurocrypt 1997, LNCS 1233, pp.103-118, Springer, 1997.

[14] K.R. Iversen, "A Cryptographic Scheme for Computerized General Election", Advances in Cryptology, Crypto 1991, LNCS~576, pp.405-419, Springer, 1992.

[15] D.L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Comm. of ACM, Vol.24, No.2, pp.84-88, 1981.

[16] C. Park, K. Itoh, and K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology, Eurocrypt 1993, LNCS 765, pp.248-259, Springer, 1994.

[17] C. Boyd, "A New Multiple Key Cipher and an Improved Voting Scheme," Advances in Cryptology, Eurocrypt 1989, LNCS 434, pp. 617-625, Springer, 1990.

[18] R. Cramer, M.K. Franklin, B. Schoenmakers, and M. Yung, "Multi-Authority Secret-Ballot Elections with Linear Work", Advances in Cryptology, Eurocrypt 1996, LNCS 1070, pp.72-83, Springer, 1996.

[19] B. Lee and K. Kim, "Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer", Proc. of the ICISC 2002, LNCS 2587, pp.389-406, Springer, 2003.

[20] A. Acquisti, "Receipt-Free Homomorphic Elections and Write-in Ballots". IACR Cryptology ePrint Archive, No.105, 2004.

[21] A. Juels, D. Catanalo, and M. Jakobsson, "Coercion-resistant electonic election", in submission.

[22] J. Furukawa and K. Sako, "An Efficient Scheme for Proving a Shuffle", Advances in Cryptology, CRYPTO 2001, LNCS 2139, pp.368-387, Springer, 2001.

[23] M. Jakobsson, A. Juel, and R.L. Rivest, "Making Mix Nets Robust for Electronic Voting By Randomized Partial Checking", Proc. of USENIX Security 2002, pp.339-353. 2002.

저자약력

김 상 진

1995년 한양대학교 전자계산학과(학사)
1997년 한양대학교 전자계산학과(석사)
2002년 한양대학교 전자계산학과(박사)
2003년~현재 한국기술교육대학교 정보미디어공학부 조교수
관심분야 : 암호기술응용(전자선거, 신원기반 시스템, 센서 네트워크 보안 등)