경영정보학연구
제25권 제4호, 2023년 11월 http://dx.doi.org/10.14329/isr.2023.25.4.047

온라인투표의 신뢰 메커니즘에 대한 고찰: 온라인투표 보안기술 및 현황 분석을 중심으로

A Study on the Trust Mechanism of Online Voting: Based on the Security Technologies and Current Status of Online Voting Systems

심 선 영 (Seonyoung Shim) 성신여자대학교 경영학부 교수, 교신저자
동 상 호 (Sangho Dong) 한국전자투표㈜ 연구소장

요 약

본 논문에서는 투표의 본질적 속성인 4대 원칙을 기반으로 온라인투표시스템이 어떻게 신뢰를 구현할 수 있는지 기술적 관점에서 조망해 본다. 이는 오프라인투표가 온라인투표보다 더 안전하고 신뢰할 수 있다는 기존의 믿음을 투표 절차와 기술적 원리를 기반으로 정교하게 평가해 보려는 것이다. 많은 연구들이 온라인투표시스템을 위한 아이디어를 제시해왔지만 투표의 요구조건 관점에서 절차적으로 엄밀히 따져보지 않았고 또 현실적 수용의 측면에서 검증이 미진한 경우가 많았다. 이에 본 연구는 온라인투표시스템이 어떻게 투표라는 과정의 엄격한 요구조건을 충족시키고 있는지 현업에서 검증된 기술을 중심으로 분석해본다. 일반적 데이터 보안에 더하여 온라인투표는 데이터 위·변조 및 부정행위 방지와 검증을 위한 기술이 더 필요하다. 뿐만 아니라 외부자는 물론이고 관리자 및 시스템 자체에게도 투표데이터가 노출되면 안 되는 고도의 기밀성이 요구된다. 이를 위해 은닉서명, 비트위임, 키분할 등을 활용하며 블록체인 기반 투표일 경우 익명성을 보장하기 위해 믹스넷과 영지식증명이 필요하다. 본 연구에서는 이론적으로 설명되고 있는 보안기술들을 실제 서비스하고 있는 현업의 시스템을 기반으로 고찰해봄으로써 온라인투표시스템의 현황을 진단한다. 이러한 시도는 온라인투표 보안기술에 대한 이해를 높이고 온라인투표의 적용 확장성을 조망하여 보다 신뢰 기반 투표 메커니즘을 구축하는데 기여할 것이다.

키워드 : 온라인투표, 보안 기술, 암호화, 부정방지, 데이터 위변조, 블록체인, 데이터 기밀성, 데이터 무결성

† 이 논문은 2022년도 성신여자대학교 학술연구조성비 지원에 의하여 연구되었음.

Ⅰ. 서 론

우리는 끊임없이 '합의'라는 과정을 거쳐 의사결정을 한다. 이 때 가장 대표적으로 사용되는 수단이 바로 투표이다. 투표는 사회적 합의를 이루고 갈등을 해결하는 가장 민주적 수단 중 하나인 것이다(전형준, 김학린, 2013). 본격적으로 포스트코로나 시대에 접어들며 일상의 모든 것이 디지털로 전환되고 있다. 언택트 상황에서도 지속 가능한 참여 및 합의는 절실하게 요구되고 있으며 온라인투표도 그 수단 중 하나이다. 이러한 시점에서 온라인투표, 즉 투표의 디지털 전환은 투표라는 메커니즘이 요구하는 모든 요구 조건을 충족시킬 수 있는 지 그 안전성 및 완성도를 논해 볼 필요가 있다.

온라인투표 이전에 전자투표라는 개념이 먼저 제시되었다. 전자투표란 컴퓨터 운영기술을 투표에 접목한 개념으로 미국에서는 1970년대에 처음 시도된 이래 2004년 대선부터는 일부 주에서 본격 도입되었다. 우리나라의 경우 2002년부터 전자투표 도입을 추진하였고 2006년 터치스크린투표기를 개발하여 정당경선이나 학교선거에 활용해왔다. 이후 전자투표는 인터넷을 기반으로 한 온라인투표로 발전하였다. 온라인투표란 PC와 이동통신단말기 등 디지털 기기를 이용하여 웹이나 모바일 환경에서 진행하는 투표를 의미한다(중앙선거관리위원회, 2018.04.22.).

우리나라는 이미 10년 전에 상법 개정을 통해 주주총회에서 전자투표 제도를 공식적으로 도입하였다. 하지만 그 외의 영역에서는 법적, 제도적 준비의 미흡으로 공직선거뿐만 아니라 민간선거에서도 전자투표 도입이 더딘 편이었다(김용섭, 2020). 보안과 안전에 대한 믿음이 아직 충분치 않았기 때문이다(이루다, 임좌상, 2019). 기술적 측면에서 온라인투표시스템은 지속적으로 발전해왔다. 그러함에도 불구하고 온라인투표는 민간과 공직 선거를 막론하고 어디에나 적용할 수 있을 만큼 수용되지 못했다. 향후에는 과연 가능한 것일까? 이 질문에 대한 답은 온라인투표라는 기술에 대한 정확한 이해로부터 나올 수 있다.

이에 본 논문에서는 투표의 4대 원칙을 기반으로 온라인투표시스템을 어떻게 신뢰할 수 있는지 기술적 관점에서 조망해 보고자 한다. 이는 오프라인 투표가 온라인투표보다 더 안전하고 신뢰할 수 있다는 기존의 믿음을 절차적 과정과 기술적 원리를 기반으로 정교하게 평가해 보려는 시도이다. 많은 연구들이 온라인투표시스템을 구현하기 위한 아이디어를 제시해왔지만(김철진, 2018; 박근덕 등, 2017; 이루다, 임좌상, 2019) 투표의 요건 관점에서 충족여부를 엄밀히 따져보는 시도는 하지 않았고 또 필요한 보안요건의 일부를 제시해왔다. 이에 본 연구는 온라인 투표를 위한 보안기술이 얼마만큼 구현되어 검증되었는지 그 현황을 종합적으로 분석 및 진단해 보고자 한다. 이 과정에서 온라인투표를 위한 보안기술에 대한 이해를 높이고 온라인투표의 적용 확장성을 조망하며 보다 신뢰기반의 투표 메커니즘 구축을 위한 사회적 이해와 수용의 발판을 마련할 수 있을 것이다.

Ⅱ. 배경 이론 및 선행 연구

2.1 선거의 4대 원칙

공정함과 객관성이 보장되어야 한다는 점에서 투표라는 행위에는 4대 원칙이 엄중하게 요구된다(문은영, 2022; 홍재우, 2010). 우리나라 헌법 제1조 22항은 '대한민국의 주권은 국민에게 있고, 모든 권력은 국민으로부터 나온다'라고 명시하며, 헌법 제25조에서는 '대한민국의 모든 국민은 법률이 정하는 바에 의해 선거권을 가진다'라고 명시하여 국민주권주의가 선거를 통해 달성됨을 천명하고 있다. 민주주의의 꽃이라 불리는 선거제도는 국민이 정치에 참여하여 주권을 행사할 수 있게 하는 핵심제도로 보통선거, 평등선거, 직접선거, 비밀선거라는 4대 원칙 또한 헌법에 명시되어 있다(헌법 제41조 제1항 및 제67조 제1항).

첫째, 보통선거란 사회적 신분, 교육, 재산, 인종, 신앙, 성별 등에 의한 자격요건의 제한없이 일정한 연령(우리나라의 경우 만 18세)에 달한 모든 국민에게 원칙적으로 선거권을 인정하는 것이다. 즉 어떠한 상황에 처한 누구라도 선거에 임할 수 있게 한다. 이는 너무나 당연한 것으로 여겨지지만 백인 또는 귀족과 같이 특정 계층에게만 제한적으로 투표권을 부여했던 서구 민주주의 국가에서도 오랜 기간에 걸쳐 점진적으로 보통선거의 원칙을 확립하였고, 일부 이슬람 국가에서는 현재까지도 종교 등을 이유로 제한선거를 하고 있다. 정치나 종교적 제한이 아니더라도 시·공간의 제약을 두는 투표 운영 방식 또한 투표의 보편성을 침해할 수 있다.

둘째, 평등선거란 모든 유권자에게 동등하게 1인 1표의 투표권을 인정하는 것이다. 개인의 사회적 지위나 재산 등 그 영향력에 상관없이 평등하게 부여되는 1인 1표의 원리는 민주주의 선거의 기본 원칙이자 선거관리위원회의 엄격한 관리에 의해 보장될 수 있는 중요한 속성이다. 디지털 작업은 낮은 처리비용으로 인하여 쉽게 중복 또는 반복이 가능하다. 이런 이유로 온라인 투표에서 재투표나 다수투표가 행해진다면 이는 평등선거의 원칙을 위배하는 것이므로 시스템에서 차단해야한다.

셋째, 직접선거란 간접선거에 대응되는 개념으로 선거권자가 중간선거인을 선정하지 않고 본인이 직접 투표에 임함을 의미한다. 미국의 대통령 선거는 국민이 직접 참여하는 한국과 달리 주별 선거인단에 의한 간접선거이다. 그러나 선거인단은 해당 주의 일반 유권자들의 투표로 결정된 후보에게 투표하기 때문에 내용 면에서는 직접선거에 해당한다고 할 수 있다(김병록, 2021). 온라인 투표를 직접민주주의의 수단(심선영, 2019)으로 자주 언급하는 이유는 사용의 편리함으로 인한 직접성이 쉽게 보장되기 때문이다.

넷째, 비밀선거란 투표의 내용이 공개되지 않고 비밀로 보장되어야 함을 뜻한다. 여기서 비밀보장의 대상은 투표 대상인 후보자뿐만 아니라, 투표를 관리하는 선관위 운영자 및 타 유권자를 포함한 '모두'를 의미한다. 그 누구에게도 투표의 내용과 결과가 노출되어서는 안 된다. 우리는 다중의 감시와 견제 시스템을 구현해 가며 유독 비밀선거의 원칙을 고수하는 데 많은 노력과 비용을 지불해 왔다. 그만큼 투표의 비밀보장이 중요함과 동시에 다른 원칙에 비해 쉽게 깨어질 수 있고 또 그때의 파장이 치명적임을 방증하는 것이다. 그렇다면 투표에서 비밀보장이 중요한 이유는 무엇일까? 비밀이 보장되지 않았을 때 치르게 되는 대가로부터 그 답을 쉽게 찾을 수 있다. 투표 결과가 알려진다는 것은 개인의 성향이나 선호가 노출됨을 의미한다. 오늘날 빅테크 플랫폼들이 하고 있는 개인 선호 분석과 이에 대한 타겟 마케팅(Hyun *et al.*, 2020)이 단순히 서비스나 제품 수준이 아니라 사회·정치적 차원에서 가능해지는 것이다. 한두 건의 투표가 아니라 여러 건의 투표 결과가 노출된다면 어떨까? 투표 결과를 통해 소위 빅데이터가 형성되면 우리가 우려하는 '빅브라더' 시스템이 구현되는 것은 시간문제이고, 그 형태 또한 매우 정교하고 치명적일 수 있다. A제품을 사려는 사람을 B제품을 사도록 유인하는 것과는 차원이 다른 것이다. 2018년, 데이터 스캔들로 인해 페이스북 CEO인 마크 저커버그(Mark Zuckerberg)는 미 청문회에 출석하였다(장대익, 2020). 2016년 미국 대선에서 페이스북 이용자 수천만 명의 개인정보가 '케임브리지 애널리티카'라는 데이터 회사에 의해 무단 활용되어 당시 공화당 후보였던 도널드 트럼프를 지원하는 데 사용되었다는 이유에서였다. 케임브리지 애널리티카가 수집한 페이스북 사용자들의 데이터는 각 개인의 성격 특성도(psychographic profiles)를 뽑아낼 수 있을 만큼 충분히 세부적이었다는 것이 데이터 스캔들의 발단이다. 그런데 투표 데이터에서는 이보다 더 직접적으로 개인의 성향이 노출된다.

대선과 같은 공직선거가 아니더라도 투표의 비밀보장이 깨어질 때 개인들이 입을 수 있는 피해는 무수하다. 아파트와 같은 공동주택 주민투표의

경우 일일이 각 세대를 방문하여 투표결과를 수기로 기록하는 일명 기명투표가 공공연하게 이루어지는데 이때 비밀투표의 원칙은 무참히 훼손된다. 문제는 단순히 비밀이 보장되지 않는 수준을 넘어 첨예한 이해관계로 인한 보복의 대상화도 쉽게 가능하다는 것이다. 금전적 이권 다툼의 경우만의 문제는 아니다. 투표 결과가 공개된다는 것은 불이익이라는 부메랑으로 돌아올 수 있기 때문에 자신의 의지와 생각대로 자유롭게 투표할 수 없고 정치적 또는 전략적 선택을 하게 만든다. 이러한 점에서 비밀투표는 중요한 것이다. 그리고 이러한 투표원칙들이 온라인투표를 통해서도 보장된다는 믿음은 온라인투표기술에 대한 정확한 이해로부터 나온다.

2.2 온라인투표 보안기술

2.2.1 공개키 암호화와 디지털서명

온라인투표에서 투표데이터는 암호화되어 저장된다. 암호화 방식은 크게 비밀키(대칭키) 암호화와 공개키(비대칭 키) 암호화로 구분된다(Won, 2006). 비밀키 암호화에서는 송신자와 수신자가 공유하고 있는 동일한 비밀키를 메세지의 암호화 및 복호화에 사용한다. 이를 대칭키라고 하는데 대칭키를 사용하면 암호화 및 복호화 속도는 빨라지지만, 키가 노출될 경우 쉽게 암호를 풀 수 있다. 이러한 단점을 개선한 것이 공개키 암호화이다. 공개키 암호화에서는 공개키와 비밀키라는 서로 다른 두 키를 이용하여 암호화와 복호화를 한다. 만약 수신자의 공개키로 데이터를 암호화했다면 복호화는 개인키를 소유하고 있는 수신자만 할 수 있기 때문에 동일한 비밀키를 공유했던 기존 대칭키 암호화에서의 키 관리 문제를 해결할 수 있다. 그러나 공개키 암호화는 속도가 느리다. 이에 메시지 자체의 암호화보다는 대칭키 암호화를 위한 키 분배나 디지털서명 등에 주로 적용되고 있다(Wong, 1988).

디지털서명이란 수기로 이루어지는 서명을 디지털 데이터에 적용한 것으로 투표데이터가 전송될 때 디지털서명도 함께 전송된다(나장호, 김혜영, 2022). 디지털서명시 암호화와 복호화는 송신자의 키로 이루어진다. 먼저 디지털서명은 투표데이터를 해시함수에 입력하여 생성된다. 해시함수가 만들어낸 해시코드를 송신자의 개인키로 암호화한다. 디지털서명이 준비되면 이를 투표데이터와 함께 수신자인 온라인투표시스템에 전송한다. 온라인투표시스템에는 송신자의 공개키로 디지털서명을 복호화한다. 디지털서명을 복호화하면 다시 투표데이터에 대한 해시코드를 얻게 된다. 한편 원본의 투표데이터를 동일한 해시함수에 넣으면 역시 동일한 해시코드가 생성된다. 이것을 디지털서명으로부터 복호화된 해시코드와 비교해 봄으로써 전송된 데이터가 위조되지 않고 정확함을 확인한다. 따라서 디지털서명은 두 가지 중요한 기능을 한다. 첫째, 메시지의 위조방지이다. 제3자가 투표데이터에 부여된 디지털서명을 위조할 수 없다. 둘째, 부인방지이다. 송신자는 자신이 서명한 투표 데이터를 부인할 수 없다.

2.2.2 은닉 서명

디지털서명시 메시지의 내용이 노출되지 않도록 하기 위해서 은닉서명(Blind Signature) 기술을 적용한다(이재영, 이지영, 2005). 은닉서명은 메시지 송신자가 서명자에게 메시지의 내용을 보여주지 않은 채 메시지에 대한 유효성을 서명받고자 할 때 사용하는 것으로, 투표한 사람의 익명성 및 비밀이 보장된다. 기존 디지털서명에 은닉성을 추가한 은닉서명은 총 3가지 방식이 있다(Brands, 1994; Camenisch *et al.*, 1997; Jeong and Lee, 2000). 서명자가 수신자에게 서명하되 생성되는 메세지와 서명을 알 수 없게 하는 일반적 방식인 보통 은닉서명, 보통 은닉서명에 서명자가 수신자 비밀값의 위탁값을 집어넣는 암시적 수신자 은닉서명, 보통 은닉서명에 서명자가 수신자의 신원을 확인할 수 있는 기능을 추가한 명시적 은닉서명이다. 모든 은닉서명 방식은 위조불가능성과 은닉성이

라는 두 가지 속성을 만족해야 한다. 위조불가능성은 서명자가 발급한 n개의 은닉서명을 가지고 n+1개 이상의 은닉 서명을 만들 수 없어야 하는 것이고, 은닉성은 서명자가 은닉서명을 보고서 어느 시점에 자신이 발급했는지 알 수 없어야 하는 것이다(정익래, 이동훈, 2003).

2.2.3 믹스넷

투표 데이터의 익명화를 위해 사용할 수 있는 또 다른 기술로 David Chaum이 제안한 믹스넷(Mixnet)이 있다(Chaum, 1981). 익명화이란 다른 정보와 결합하여도 특정 개인을 식별할 수 없도록 만드는 기술이다(김종선 등, 2018). 투표에서 누가 누구를 찍었는지 알 수 없도록 하여 비밀을 보장하는 기술이다. 투표과정과 개표과정은 모두 익명화되어야 하는데, 믹스넷은 특히 개표과정에 적용될 수 있다(Jeon *et al.*, 2012). 믹스(mix)란 데이터를 섞는다는 뜻으로 다수의 믹스서버를 구성하고, 각각의 믹스서버는 초기 입력값 또는 이전 믹스서버의 출력값을 받아 섞는 과정을 반복한다(Golle *et al.*, 2004; Neff, 2001). 따라서 믹스넷을 거치고 나면 투표 내용은 무작위로 섞여서 어떤 유권자가 어떤 값에 투표했는지 알 수 없게 된다.

이 때 각 믹스서버는 데이터를 섞더라도 입력값이 출력값으로 동일하게 연결되고 있음을 증명해야 하는 데 이를 위해 사용되는 것이 영지식증명(Zero-Knowledge Proofs)이다(Sako and Kilian, 1995). 영지식증명이란 데이터는 공개하지 않은 채 그 데이터가 특정 조건을 만족함을 수학적으로 증명하는 기술이다. 즉 믹스되어 비밀에 부쳐진 투표데이터가 입력시와 출력시에 동일함을 증명하는 것이다. 결국 믹스넷은 익명화뿐만 아니라, 유권자의 투표가 집계에 정확히 반영되었다는 검증도 함께 제공한다.

2.3 블록체인 기반 온라인투표

온라인투표에 있어 가장 큰 논쟁점은 보안과 신뢰성이다. 오프라인 투표의 경우 막대한 비용이 소요된다. 반면 온라인투표는 편의성, 비용감소, 투표율 향상 등 다수의 장점(심선영, 2019)에도 불구하고 인터넷을 기반으로 원격에서 투표가 일어나기 때문에, 그 과정에서 유권자가 비밀을 지키면서 정확하게 투표권을 행사할 수 있도록 보안과 신뢰성이 보장되는지가 관건이었다(이루다, 임좌상, 2019). 온라인투표시스템의 보안에 대해서 많은 연구들이 시행되어 왔다. 전술한 암호화기술, SHA256 해시함수, 디지털서명 등이 적용되고 있으며 최근에는 블록체인 기술을 활용한 연구들도 부각되고 있다. 블록체인은 데이터의 위변조가 거의 불가능하다는 기술적 장점이 보안면에서 인정되면서 온라인투표에의 적용 연구가 시도되고 있고 일부 국가에서는 대규모로 블록체인 기반 온라인투표가 실행되고 있는 실정이다(Kshetri and Voas, 2018).

박근덕 등(2017)은 분산 원장 기술(DLT, Distributed Ledger Technology)에 기반한 온라인투표를 위한 시스템 모델과 표준화 동향 그리고 보안 위협 및 대응 방안을 제시하였다. 온라인투표에서 발생할 수 있는 보안 위협의 종류를 제시하고 대응 방안으로 분산 원장 기술의 적용을 제시하였다. 이후 이더리움 블록체인을 활용하는 온라인투표 연구들이 등장하였다. 이더리움(Ethereum)은 2015년 비탈릭 부테린(Vitalik Buterin)이 개발한 블록체인으로 2세대 블록체인이라 불리고 있다(Antonopoulos and Wood, 2018). 스마트 컨트랙트(Smart Contract)를 블록체인에서 구현함으로써 다양한 기술을 접목하여 급속도로 발전하고 있으며 관련 연구도 확산되고 있다. 스마트 컨트랙트란 계약 당사자가 사전에 협의한 내용을 미리 프로그래밍해 두고, 계약 조건이 충족되면 자동으로 계약 내용이 이행되도록 하는 시스템이다(Antonopoulos and Wood, 2018). 투표를 스마트 컨트랙트화함으로써 인위적 조작을 차단하는 것이다.

김철진(2018)은 이더리움 블록체인에 기반한 투표 결과의 분산저장 방안을 제시하였다. 솔리디

티 프로그래밍 언어를 이용하여 투표를 위한 스마트 컨트랙트를 구현하였으며 이더리움 클라이언트의 블록 내에 온라인투표에 해당하는 선거 컨트랙트(Election Contract)를 개발·배포하여 노드들 간에 블록의 일관성을 유지시켰다. 그러나 솔리디티 기반의 스마트 컨트랙트를 블록체인 내의 계정으로 배포한 후에는 수정이 불가능하여 유지보수 측면에서 어려움이 있을 것으로 판단된다. 이루다, 임좌상(2019)도 이더리움 환경에서 온라인투표시스템 구축을 제안하였다. 이들은 온라인투표의 기본 요구사항들을 제시하고 블록체인 기반 투표시스템을 제안하여 기존 중앙집중식 시스템과 달리 공격으로 인한 시스템 마비나 중앙서버의 장악으로 인한 거래데이터 위·변조 문제를 해결할 수 있음을 강조하였다. 하지만 전술한 논문들이 제시하고 있는 블록체인 방식 시스템은 투표데이터가 분산 저장되고 추적이 가능하다는 점에서 보안 취약점이 있다. 나아가 대부분의 온라인투표 연구는 투표 절차 구현에 치중할 뿐 보안기술을 구체적으로 다루고 있지 않다. 보안 기술을 다루는 경우에도 데이터 암호화와 같은 투표시의 보안에 치중할 뿐 개표시의 보안 및 검증까지 전반적으로 다루고 있지 않다. 하지만 본 연구에서 소개하는 온라인투표시스템은 투·개표 보안 뿐만 아니라 개표 데이터 검증에 이르기까지 일련의 과정에 요구되는 모든 보안기술을 갖추고 있으며 본 연구에서는 이를 상세하게 분석 및 기술한다. 이에 본 논문에서 제시하는 보안 기술의 범위를 기존 연구들과 비교하여 정리하였다(<표 1> 참조).

Ⅲ. 연구 내용

본 절에는 상기 문헌연구에서 이론적으로 정리한 기술들이 실제로 어떻게 적용되고 있는지 분석해 본다. 이를 위하여 중앙선거관리위원회의 온라인투표서비스를 개발한 한국전자투표(주)의 기술을 심층 분석하였다. 한국전자투표(주)의 온라인투표시스템은 중앙선거관리위원의 온라인투표 표준가이드라인에서 제시하는 각 단계별 요구 기술을 모두 충족하고 있는 국내 유일의 시스템이다. 이에 그 기술력을 인정받아 중앙선거관리위원의 온라인투표시스템을 개발 및 운영하였고, 현재에도 K-Voting(https://pub.kvoting.go.kr) 이라는 서비스명으로 유수 공직선거에 적용되고 있는바, 이러한 공신력을 바탕으로 본 시스템을 분석하게 되었다.

3.1 온라인투표 요구조건 분석

투표의 진행 및 관리에 있어 가장 중요한 것은

〈표 1〉 온라인투표시스템 보안관련 연구

내용 / 저자	투표 절차&이슈	투표 보안	개표 보안	자가 검증
강서일 등(2005)	o	o	o	
이광우 등(2006)				o
전웅렬, 원동호(2020)		o	o	o
Kaliyamurthie *et al.*(2013)	o	o	o	
박근덕 등(2017)	o			
김철진(2018)	o	o		
이루다, 임좌상(2019)	o	o		
박찬형, 김재훈(2020)	o	o		
Jafar *et al.*(2021)	o	o	o	
본 연구	o	o	o	o

크게 두 가지로 볼 수 있다. 첫째, 선거의 4대원칙에도 명시되어 있듯이 투표 내용의 비밀보장이다. 데이터의 관점에서는 이를 기밀성이라고 한다(Kim *et al.*, 2013). 여기서 중요한 점은 유권자 또는 제3자에게만 비밀이 보장되면 되는 것이 아니라, 선거관리위원회와 같은 내부 관리자들 또한 비밀보장의 대상에 포함된다는 것이다. 투표 진행의 주체들도 투표의 각 과정에서 정보 불균형에 의한 권한 행사가 불가하도록 원천적으로 방지되어야 한다.

둘째, 비밀이 보장된 투표 데이터의 무결성을 확보하는 것이다. 이는 투표 데이터의 조작이 불가하고 또 조작되지 않았음을 증명하는 것이다. 원격지에서 수행하는 온라인투표에서는 이러한 비밀성과 무결성을 확인하기가 매우 힘들다. 기술적 원리를 제대로 이해해야 하는 부담에 막연한 의구심이 들어도 누군가 쉽게 문제제기를 하지 못했고, 문제의 핵심이 어디에 있는지 그 맥을 짚어내는 것도 어려웠다.

온라인투표를 제공하는 서비스 제공자의 입장에서도 마찬가지이다. 비밀보장을 위한 보안 수준이 제각각이며 데이터 무결성에 대한 방안도 부실한 경우가 부지기수이다. 이에 중앙선거관리위원회에서는 선거의 4대원칙과 투·개표 과정의 투명성 및 신뢰성 확보를 위한 '온라인투표시스템 표준가이드라인'을 2020년 12월에 발표하였다(중앙선거관리위원회, 2020.12). 주요 내용은 투표의 정확성, 완전성, 기밀성 등 7대 영역에서 충족되어야 할 기본요건을 적시한 것이다.

〈표 2〉 투표의 7대 요건(온라인투표시스템 표준가이드라인 中)

항목	상세내용
정확성	모든 정당한 유효 투표는 투표 결과에 정확히 집계되어야 함
완전성	부정투표자에 의한 방해를 차단하고 부정투표는 미집계 되어야 함
기밀성	투표자와 투표결과의 비밀관계가 보장되어야 함
공정성	투표 중의 집계결과가 남은 투표에 영향을 주지 않아야 함
확인성	투표결과 위조방지를 위한 검증수단이 있어야 함
합법성	투표권이 없는 유권자의 투표참여가 불가해야 함
단일성	정당한 투표자는 오직 1회만 참여 가능해야 함

'비밀선거'의 원칙과 직결되는 '투·개표 보안' 영역을 가장 서두에 기술하며 강조하고 있다. 투표 보안에 있어 '투표의 비밀보장을 위해 절차

〈표 3〉 투·개표 보안 요구사항(온라인투표시스템 표준가이드라인 中)

분 야	항 목	상 세 내 용	선거원칙
투·개표 보안	엑세스 제한	정당한 권한을 가진 관리자만이 시스템에 접근할 수 있으며, 부정한 엑세스를 제한하는 수단을 마련하여 시스템 등이 무단으로 조작·수정·공개·손실되는 것을 방지하여야 한다.	직접선거 비밀선거
	시스템 실행	규정된 방식·조건 등 기능에 대한 전제 조건이 충족되지 않은 경우 시스템 기능이 실행되지 못하도록 제어 논리를 갖추어야 한다.	직접선거 비밀선거
	투표의 **비밀보장**	선거인의 투표 내용은 어느 누구도 알 수 없도록 절차적·보안적·기술적으로 조치해야 하며, 투표 기록을 통하여 **해당 투표를 한 선거인이 특정되지 않도록** 하여야 한다(선거인과 투표값 분리).	비밀선거
	투표값 **암호화 및 키분할**	투표 내용을 **암호화**하여야 하며, '**은닉서명**' 등의 투표 내용의 전자서명 및 암호화에 사용되는 **키는 다수의 투·개표 관리자에 의해 분할**되고 개표 시 복구하여 사용할 수 있도록 구현해야 한다.	비밀선거
	위·변조 여부 **검증**	선거인의 투표 내용은 공개되지 않는 상태에서 개표 완료 후 투표 사실 및 투표 내용이 **위·변조 되지 않았음을 증명**할 수 있는 '**비트위임**' 등의 조치를 마련해야 한다.	직접선거 비밀선거

적 · 보안적 · 기술적으로 조치'해야 하는 것은 물론이며, 투표 기록을 통하여 해당 투표를 한 사람이 누구인지 특정되지 않도록 하는 '투표값의 익명화'도 강조한다. 투표값은 암호화될 뿐만 아니라 암호화에 사용된 키는 다수의 투 · 개표 관리자에 의해 분할 관리되어 특정인의 임의적 접근을 원천 차단토록 요구하고 있다. 투표 사실 및 투표 내용이 '위 · 변조 되지 않았음을 증명할 수 있는 조치'에 대한 요구도 당연히 포함되어 있다. 다시 말해, <표 3>의 모든 요구사항은 오프라인에서 다중의 절차와 집단적 감시를 통해 수행했던 투 · 개표 보안작업을 온라인에서 수행하기 위한 안전 조건인 것이다.

3.2 온라인투표시스템 기술 분석

본 절에는 온라인투표시스템이 어떻게 신뢰할 수 있는 메커니즘이 될 수 있는지 그 기술적 과정을 분석해본다. 전술했듯이 온라인투표에서 가장 중요한 요소는 비밀보장과 무결성이다. 이는 온라인이냐 오프라인이냐의 채널과 상관없는 투표의 본질이다. 그런데 이 두 가지 이슈를 온라인에서 동시에 만족시킨다는 것은 고도의 기술을 요구한다. 마치 블록체인의 보안성과 확장성을 동시에 달성하기 어려운 것처럼(노시완, 이경현, 2019), 비밀을 보장하기 위해 암호화를 하면서도 동시에 조작되지 않고 신뢰할 수 있는 데이터임을 증명할 수 있어야 하기 때문이다. 뿐만 아니라, 이는 투표와 개표라는 두 과정에서 모두 요구된다. 투표시의 신뢰성을 'Cast-as-Intended'라 하여 유권자의 투표가 의도한대로 기록되었음을 신뢰할 수 있어야 하고, 개표시의 신뢰성을 'Counter-as-Cast'라 하여 집계 과정에서 투표값이 모두 정확하게 반영되었음을 확신할 수 있어야 한다(Jeon *et al.*, 2012). 이러한 요구 조건이 어떻게 기술적으로 충족되고 있는지 현존하는 투표 서비스와 보안 기술을 중심으로 분석해 보겠다.

3.2.1 보편적 암호화 기술 – 종단간 암호화

먼저, 데이터의 비밀보장을 위해 가장 기본적으로 필요한 것은 암호화이다. 이는 비단 투표 데이터뿐만 아니라 정보보호와 비밀보장이 필요한 모든 경우에 해당되는 보편적 요구사항이다. 일반적으로 많이 사용되고 있는 기술은 https를 활용한 웹보안 방식이다. 이는 SSL에 기반한 암호화 통신 기술로 데이터 전달 내용을 제 3자가 알 수 없도록 하는 기밀성, 즉 투표 내용의 비밀보장 기술이다. 그런데 여기서 중요한 것은 https 암호화는 투표 데이터 전송의 전 과정을 암호화하지는 못하는 일종의 '통신 구간 암호화'라는 것이다. https가 제공되는 구간에서만 암호화가 적용된다. 오프라인 투표에 비유하자면 투표함을 개표장으로 이송하는 과정에는 엄중한 경호를 하지만, 투표의 시작에서 투표함 투입까지의 구간이나 투표함이 개표장에 도착 후 실제 개표가 시작되기까지는 철저한 엄호가 일어나지 않는 것과 유사하다. 온라인투표에서도 유권자의 기표에서 온라인투표시스템에 데이터가 저장된 후 개표가 일어날 때까지 전 과정이 암호화 되어야 하는데, 이를 위해서는 단순 https 암호화가 아닌 종단간 암호화 기법을 사용해야 한다.

종단간 암호화는 메시지를 보내는 곳에서부터 받는 곳까지 모든 과정에서 암호화된 상태로 메시지를 전달하는 방식이다. 종단간 암호화를 하면 양끝에 있는 사람, 즉 메시지를 발송하는 사람과 수신하는 사람만 내용을 볼 수 있으며 중간에 있는 그 누구도 메시지 내용을 볼 수 없다. 따라서 중간에 한 번도 풀리지 않고 투표 시작에서 개표까지 암호화가 보장된다(박철용 등, 2014). 종단간 암호화가 적용되지 않은 경우 해독 가능한 정보가 중간 서버에 잔류할 수 있다. 이때 공격자가 중간 서버를 공격하거나, 중간 서버를 운영하는 기관 혹은 정부 기관에서 서버 내 정보를 열람할 경우 개인정보 유출 및 사생활 침해가 가능하다. 카카오톡의 서버를 정부가 감청한다는 내용이 공개되자 많이 이들이 종단간 암호화 기반의 텔레그램을 선택했던 사례가 종단간 암호화의 중요성을 보여

준다(박선영 등, 2016). 종단간 암호화를 적용하는 경우 이러한 정보 유출을 막을 수 있다.

하지만 종단간 암호화 기술만으로는 투표의 기밀성과 무결성이 완전하게 보장되지는 않는다. 종단간 암호화를 통해 투표데이터를 암호화했지만 다양한 요소에서 투표데이터는 복호화되거나 노출될 수 있기 때문이다. 종단간 암호화는 투표데이터 보안을 위한 기본적 기술이라 할 수 있고, 추가적으로 온라인투표의 특수성을 보장할 수 있는 보안기술들이 필요하다.

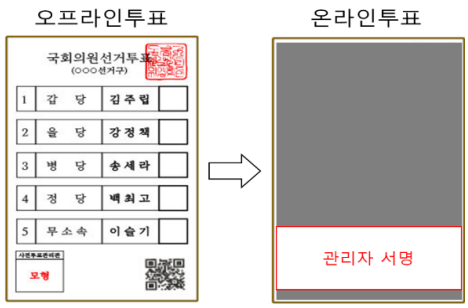
3.2.2 전자투표 보안기술

온라인투표에서 단순 암호화만으로 보안 문제가 해결되지 않는 이유는 투표데이터의 비밀보장 대상에 외부인뿐만 아니라 투표시스템 내지는 관리자까지도 포함되기 때문이다. 쉽게 말해, 세상의 그 누구도 또는 그 어떤 객체도 투표 내용을 알 수 없도록 완벽하게 기밀성을 보장해야 한다. 오프라인 투표를 생각해 보면 이를 위해서 기표소에 혼자만 들어가서 투표를 하고 그 용지를 아무도 열 수 없는 투표함에 넣는다. 그리고 이 투표함을 잘 감시하여 모두가 보는 앞에서 한 번에 개표한다. 따라서 투표 과정 동안 그 내용을 아무도 알 수 없을 뿐만 아니라 개표 시에도 결과만 집계될 뿐 누가 누구를 찍었는지의 기록은 남아있지 않다. 그런데 온라인투표의 경우 그 속성상 누가 어떻게 투표했는지 비밀을 보장하기가 어려울 수 있다. 예를 들면, 디지털서명의 경우 투표데이터 생성 이후에 수행되기 때문이다. 또는 암호화된 데이터를 키만 있으면 복원할 수도 있기 때문이다. 따라서 디지털 프로세스의 특수성에서 오는 위험들을 해결하는 추가적 기술들이 필요하다.

3.2.2.1 투표시의 유효성 및 비밀보장 기술 - 은닉서명

투표의 기밀성과 무결성을 보장하기 위한 첫 번째 이슈는 유효한 용지에 투표하도록 하는 것이다. 유효한 투표용지는 유권자마다 한 장씩만 주어지므로 평등선거의 원칙을 고수한다. 만약 유효하지 않은 투표용지가 발견되면 집계에서 배제함으로써 투표의 유효성을 보장한다. 오프라인 투표의 경우 유효한 투표용지임을 의미하는 '인증도장'이 찍혀있는데 이 인증도장은 사전에 미리 용지에 찍어 배포함으로써 인증 과정에서 투표 내용이 노출되지는 않는다.

온라인투표에서도 유효한 투표임을 인증하기 위해 관리자가 서명을 한다. 바로 디지털서명이다. 그런데 온라인에서는 메시지가 먼저 만들어진 뒤에 디지털서명이 진행된다는 것이 문제이다. 디지털서명시 메시지 즉 투표 내용이 이미 형성되어 있어 디지털서명을 하는 관리자에게 투표의 내용이 노출될 수 있는 것이다. 그렇게 되면 누가 누구에게 투표했는지 알 수 있으므로 비밀보장이 안된다. 이를 해결하는 기술이 바로 은닉서명이다. 서명은 하되 메시지의 내용은 가린채 서명하는 것이다. 오프라인 방식에 비유하자면, 서명하는 문서 위에 먹지를 덮어서 내용을 가린 채 서명을 하는 것과 유사하다. 이렇게 하면 관리자가 투표 내용을 볼 수 없어 비밀이 보장된다. 동시에 먹지 위에 한 서명은 먹지 아래로 스며들어 자연스럽게 투표용지에도 서명이 되므로, 이 투표용지는 유효한 것임이 확인된다. 이러한 과정을 디지털 방식으로 구현한 것이 바로 은닉서명이다. 은닉서명은 투표용지의 유효성을 보장하기 위해 디지털서명을 하면서도 메시지 즉 투표 내용은 노출되지 않도록 은닉하는 기술이다.



〈그림 1〉 은닉서명

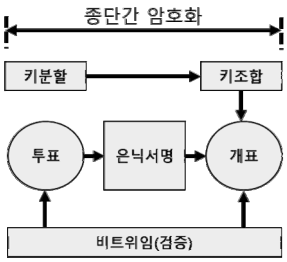
3.2.2.2 관리자 부정 방지 기술-키분할·조합

투표의 기밀성과 무결성을 보장하기 위한 두 번째 이슈는 바로 임의적 복호화 방지이다. 기본적으로 투표데이터는 암호화되지만, 공개키 암호화 기술은 복호화키만 있으면 언제든 암호화된 내용을 풀 수 있다. 복호화키 즉 개인키를 투표 관리자가 함부로 다룰 수 있다면 암호화는 무의미하며 더 이상 투표의 비밀은 보장되지 않는다. 따라서 개인키는 특정인이 독립적으로 접근할 수 없도록 잘 관리할 필요가 있는데 이를 위해 적용하는 방법이 바로 '키분할'이다.

키분할 기술은 개표 시까지 복호화키를 투표시스템에서 제거하고, 투표 참관인, 후보자, 선관위 위원 등 핵심 주체들에게 나누어 보관토록 한다. 개표 시에만 분할 보관된 키를 모두 모아 원래의 키로 복원하여 사용함으로써 절차를 벗어난 임의적 복호화는 불가능하도록 통제하는 것이다.

3.2.2.3 개표시의 검증 기술 - 비트 위임

투표의 기밀성과 무결성을 보장하기 위한 세 번째 이슈는 바로 투표 내용 및 집계에 대한 검증이다. 첫째, 투표 전체의 관점에서 누락없이 모든 투표가 집계되었는지 확인할 수 있어야 한다. 이를 위해 투표시스템은 단순히 투표 데이터만 저장하는 것이 아니라 각 투표에 대응하는 투표용지 및 투표 검증키트를 담은 암호화된 전자봉투를 같이 저장한다. 오프라인 투표에서도 투표자 수와 투표용지 수의 동일여부를 검증하듯 온라인투표에서도 기록된 투표자 수, 투표용지 수, 투표 검증키트 수, 전자봉투 수를 비교하여 모든 투표가 누락없이 집계에 정확하게 반영되었는지 검증한다. 둘째, 개별 투표자 입장에서는 자신이 행사한 투표가 실제로 집계에 정확하게 반영되었는지 검증이 필요하다. 실제 투표수는 100건이고 기록된 투표수도 100건으로 집계에 대한 검증이 되었다 할지라도 투표자의 입장에서는 그 100건의 투표 중 자신의 투표가 반영되었는지 확인이 필요한 것이다. 이때 서로가 유효한 한 쌍임을 확인하기 위해 증표의 조각을 맞추어 보는 개념을 활용한다. 투표 검증키트는 두 조각으로 분할되어 투표시 한 조각은 전자투표용지에 포함되어 서버 시스템에 저장되고, 나머지는 개인의 클라이언트에 저장되었다가 개표시 전자투표용지에서 검증키트를 분리하여 양쪽에 저장된 투표검증키트 조각이 서로 정확하게 부합되는지 확인하여 투표의 실제 반영을 검증한다. 이 기술이 바로 '비트위임'이다(허원근 등, 2000). 이는 투표자가 시스템을 신뢰할 수 있게 만들며 행사한 표가 조작되지 않았음을 증명하는 매우 고도화된 보안 기술이다. 정리하자면, 온라인투표의 전 과정에 걸쳐 전술한 기술들은 <그림 2>와 같이 복합적으로 적용되어 투표 데이터의 기밀성과 무결성을 보장한다. 단계별로 분리해서 보자면 투표시의 위·변조 및 부정행위 방지 기술로 은닉서명과 비트위임을 활용하며 개표시의 위·변조 방지 및 검증 기술로 키분할·조합 및 비트위임을 사용하는 것이다.

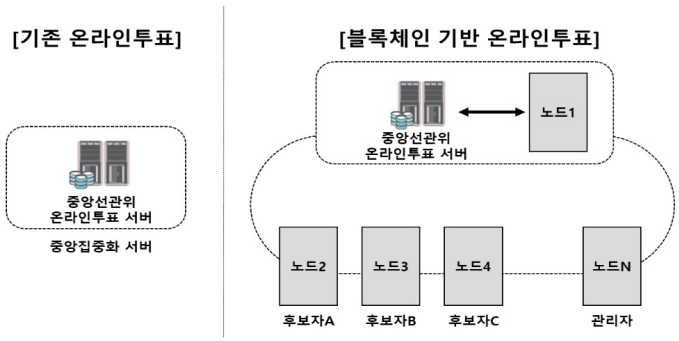


〈그림 2〉 온라인투표 보안기술

3.2.2.4 블록체인 투표와 믹스넷 익명화

상기의 과정들은 일반적으로 온라인투표시스템의 중앙화된 서버에서 수행되었다. 공직 선거라면 중앙선거관리위원회의 서버가 될 것이다. 만약 이것을 블록체인을 기반으로 수행하면 그 구조는 <그림 3>과 같이 된다.

여러 노드에 데이터를 분산 저장하는 블록체인은 위·변조가 어렵고 해킹으로부터 자유로운 데이터 저장소라는 강점을 지닌다. 만약 온라인투표 시스템에 블록체인을 적용한다면 안전하게 투표



〈그림 3〉 블록체인 기반 온라인투표의 시스템 구조(KSTEP, 2020, p.111로부터 발췌·수정)

데이터를 보호할 수 있다는 장점이 있다. 많은 투표 서비스들은 블록체인을 활용한다고 주장하지만 대부분은 투표 데이터를 저장하는 데에만 블록체인을 활용할 뿐 이후 개표를 위해 데이터를 수집하고 처리하는 과정은 별도의 서버에서 진행하는 경우가 많다. 별도 시스템에서는 얼마든지 데이터의 조작이나 해킹이 가능하므로, 데이터 위·변조 불가라는 블록체인의 장점은 퇴색된다(코인데스크코리아, 2020.11.12).

모든 과정이 블록체인상에서 처리된다 하여도 남아있는 중요한 문제가 있다. 블록체인 기반 투표의 더 큰 난제는 '비밀성 보장'에 있다. 블록체인에 기록된 데이터는 추적이 가능하기 때문이다(KISTEP, 2020; 하현수 등, 2017). 블록체인의 투명성이 비밀 보장 불가의 딜레마를 야기하는 것이다. 이를 해결하기 위해서는 고도의 기술적 과정이 요구된다.

먼저 투표 데이터는 일반 데이터베이스 저장과 마찬가지로 암호화되어 블록체인에 저장한다. 당연히 암호화키는 분할되어 관리된다. 다음으로 비밀성 문제를 해결해야 하는데, 이를 위해 믹스넷 기술을 추가해야 한다. 믹스넷은 입력데이터와 출력데이터 간의 연결고리를 제거함으로써 투표 데이터의 추적을 불가능하게 하는 기술이다. 데이터를 섞어서 어떤 유권자가 어떤 후보자를 찍었는지 그 연결고리가 보이지 않게 한다. 이때 남게 되는 이슈가 데이터 유효성 검증이다. 섞여진 데이터가 원래의 데이터와 여전히 동일한 것임을 증명해야 하는 것이다. 이를 위해 영지식증명을 사용한다. 영지식증명은 믹스넷의 출력데이터가 여전히 입력데이터와 동일한 것임을 수학적 연산을 통해 증명한다.

정리하자면, 중앙선거관리위원회의 온라인투표 가이드라인에서 제시하는 조건을 충족하려면 전술한 기술들이 <표 4>와 같이 항목별로 대응되

〈표 4〉 온라인투표시스템 표준가이드라인 준수와 해당 기술

항 목	상 세 내 용	구현기술
정확성	모든 정당한 유효 투표는 투표 결과에 정확히 집계되어야 함	암호화 은닉서명 믹스넷
완전성	부정투표자에 의한 방해를 차단하고 부정투표는 미집계 되어야 함	
기밀성	투표자와 투표결과의 비밀관계가 보장되어야 함	
공정성	투표 중의 집계결과가 남은 투표에 영향을 주지 않아야 함	키분할
확인성	투표결과 위조방지를 위한 검증수단이 있어야 함	비트위임 영지식증명
합법성	투표권이 없는 유권자의 투표참여가 불가해야 함	이중투표방지기술 전자투표용지기술
단일성	정당한 투표자는 오직 1회만 참여 가능해야 함	

어 구현되어야 한다. 본 논문에서 분석하고 있는 한국전자투표㈜의 온라인투표시스템은 이러한 기술이 모두 적용되어 있다는 점에서 공신력을 가진다.

3.3 온라인투표 서비스 현황 진단

그럼 현존하는 온라인투표서비스들은 상기의 가이드라인을 어느 정도 구현하고 있는지 분석해 본다. 먼저 온라인투표 데이터를 데이터베이스에 저장할 때 '투표값의 익명화'가 제대로 이루어지고 있는지부터 분석해보면, 당장 이 단계부터 문제가 존재한다. 다시 말해 'A라는 유권자가 기호 1번을 찍었다'는 식으로 투표자와 투표값의 연결 내용이 고스란이 시스템에 기록될 수 있다. 암호화되어 저장되므로 큰 문제가 아닌 것처럼 보일 수도 있다. 실제로 많은 온라인투표시스템들은 KCMVP라는 국정원 인증의 암호모듈을 적용하고 있다. KCMVP는 중요 정보를 보호하기 위해 도입하는 암호모듈의 안정성과 구현 적합성을 검증하는 제도로, 국산 알고리즘을 탑재한 암호모듈에 대한 구현의 적합성, 안정성 등을 검증한다(박찬희 등, 2019). 여기서 암호모듈은 데이터의 기밀성(개인키 · 공개키 암호화), 해시, 디지털서명, 인증 등을 포함한다.

하지만 온라인투표에서는 투표데이터의 기밀성만 해결한다고 해서 충분하지 않음을 설명한 바 있다. 데이터가 외부로부터는 보호되지만 시스템에 접근가능한 내부관리자 및 시스템 자체에게는 고스란히 공개되기 때문이다. 이러한 사유로 익명화가 침해되는 것이다. 내부자들이 투표 데이터를 조작하지는 않더라도 그 내용을 보는 것만으로도 문제가 된다. 상대방 후보들에게 불공정한 상황을 만들 수 있고 나아가 투표결과를 왜곡시킬 수도 있다. 투표용지에 대한 은닉서명, 키분할을 통한 관리자 부정방지, 비트위임에 의한 투표자 자가검증 등은 KCMVP 암호모듈만으로 구현되지 않는다. 이러한 보안기술이 추가적으로 적용되어야 하는 것이다. 하지만 지극히 일부의 온라인투표서비스에서만 이러한 제반 기술을 적용하고 있다.

키분할 기술을 적용한 경우 또한 매우 드물다. 단독으로 암호화키를 가진 관리자가 마음만 먹으면 투표 데이터를 언제든 들여다 볼 수 있기 때문이다. 이것은 일종의 단일 장애점 문제(SPF, Single Point of Failure)로 볼 수 있다(An, 2018). 해당 지점의 장애가 전체 시스템의 중단을 초래하는 단일 장애점 문제는 정보시스템 위험관리에서 가장 중요하게 다루어지는 문제 중 하나이며 현업의 IT관리자들은 이 문제의 심각성을 누구보다도 잘 알고 있다. 키분할이 되지 않고 하나의 지점(Single Point)에 보관되었을 때, 그리고 그 지점에서 키를 사용하여 복호화하였을 때 투표시스템 전체에 대한 신뢰가 무너지는 것이다. 하지만 이러한 장애를 외부에서는 인지조차 할 수 없다는 것이 더욱 심각하다.

비록 키분할이 이루어졌다 하더라도 투표 데이터를 복호화 했는데 전체 투표 내용이 익명화되지 않은 채 평문상태로 확인된다면 이 또한 문제이다. 민감한 개인정보일수록 상업적 가치가 상승하는 근래의 데이터 거래 시장에서 이렇게 '유권자A가 기호1번을 찍었다'는 식의 익명성이 전혀 보장되지 않은 투표데이터는 매우 매력적인 대상이 될 것이다. 이를 방지하기 위해서 '온라인투표시스템 가이드라인(<표 2>, <표 3>)'에서 제시한대로 투표값의 익명화가 철저하게 지켜져야 하고 블록체인과 같이 익명화가 어려울 경우 개표 전에 믹스넷을 적용하는 식의 추가적 익명화 적용이 반드시 필요하다.

결국 데이터 익명화와 키분할 기술이 결여된 데이터 암호화는 고식지계(姑息之計) 수준의 투표 비밀보장으로 언젠가 제2, 제3의 데이터 스캔들을 불러올 수 있다. 이 경우 발생할 수 있는 위험의 파급력은 오프라인투표와는 비교할 수 없을 것이다. 한순간에 모든 실체를 파악하고 쉽게 변경 · 조작 · 남용할 수 있는 온라인 기술의 특징 때문이다.

Ⅳ. 결 론

4.1 연구의 학술적 의의

기존 연구에서 제시되어온 온라인투표 기술들은 대부분 아이디어나 POC 수준으로 실용성 면에서의 검증이 결여된 한계가 있었다. 따라서 현실의 공직 및 민간 선거에 실제 적용하기에는 무리가 있었다. 나아가, 대부분의 연구에서는 투표 보안 및 검증을 위한 부분적 기술을 다룸으로써, 온라인투표 전반에 걸친 기술 개요와 그 필요성을 종합적으로 파악하기 어려웠다. 본 연구에서는 이론적으로 제시되었던 기술 요건들을 현재 서비스되고 온라인투표시스템을 기반으로 고찰함으로써, 현업에서 검증된 상황에서 분석했다는 점에서 의의를 갖는다. 뿐만 아니라 온라인투표 전반에 걸쳐 단계별 기술을 분석하였고, 적용된 각 기술들이 투표 단계별로 어떠한 요구조건을 충족시키고 있는 지 명확하게 제시함으로써 온라인투표시스템에 대한 종합적 이해를 도모하였다. <그림 2>에서 제시된 키분할, 은닉서명, 비트위임은 기본적인 데이터 암호화 외에 투표 속성상 요구되는 필수 보안 기술들이며, 이에 대한 이해를 투표 프로세스와 연관지어 제시하였다. <표 3>에서는 이러한 기술들이 투표의 요구 항목에 각각 어떻게 대응하는 지 상세하게 기술함으로써, 투표 보안기술에 대한 이해를 제고하였다. 이러한 시도는 선행 연구에서 축적되어온 다양한 기술들을 일련의 투표과정에서 정리하는 한편, 온라인투표시스템에 대한 보다 전문적 이해를 제시한다는 점에서 관련 연구를 진일보 시킬 것이다.

디지털 대전환을 맞이하는 현시점에 중요한 점 중 하나는 그간 대부분의 작업을 수행했던 오프라인 영역에서 '중앙 관리자의 위험'을 쉽게 간과해 왔다는 것이다. '선거관리위원회'와 같은 소위 '중앙집권적 신뢰기관'이 운영을 관할하므로 절대적으로 투표 운영의 공정성과 투명성을 믿어 왔다. 공직선거라면 '중앙선거관리위원회'라는 정부기관이 개입하지만 민간의 무수한 선거에서는 자체적으로 구성한 '선거관리위원회'가 존재한다. 여러 참관인 및 다단계 절차를 바탕으로 다중의 감시장치가 존재하는 전통적 '선거관리위원회'의 구성과 운영은 이미 체계를 확립하였고 그에 대한 유권자들의 신뢰로 인해 우리사회의 민주주의가 유지되고 있는 것은 부정할 수 없는 사실이다.

그런데 블록체인 네트워크의 탄생은 실제로 우리가 수차례 경험한 '중앙관리기관에 대한 불신'을 중요하게 지적한다(손주희, 문유석, 2020). 투표 영역에 적용해 보자면, 권력집단의 부정이 문제라기보다는 '인간의 개입'이 초래할 수 있는 오류나 부정의 필연적 개연성이 더 문제이다. 하지만, 철저하게 원칙을 고수하고 어떠한 오류나 예외를 초래하지 않는 '기술'이라는 도구는 우리에게 '자동화된 신뢰 시스템'의 가능성을 보여준다. 웹3.0의 도래와 블록체인 기반 디지털 경제의 확산 하에 이러한 신뢰 시스템을 더욱 완전하게 이해하고 활용하기 위한 노력은 더욱 확대되고 있다. 이러한 맥락에서 본 연구도 다양한 보안기술의 원리와 특성을 투표 프로세스의 본질에 근거하여 해석함으로써, 학문적 차원에서 이 사회의 디지털 전환 준비에 일조하고자 한다.

4.2 연구의 관리적 함의

온라인투표시스템에 대한 이해를 제고한다는 것은 민주주의와 사회적 거버넌스 성숙의 측면에서 의미있는 시도이다. 온라인 시스템에 있어 가장 큰 맹점은 보안에 허술함이 있어도 실제로 사고가 발생하지 않는 한 잘 드러나지 않는다는 것이다. 철저하게 준비되지 않은 시스템에 기반하여 온라인투표를 시행하는 것은 언제라도 보안사고가 발생할 수 있음을 의미한다. 투표라는 민감 행위에서 보안사고가 발생하게 되면 온라인투표에 대한 사회적 시선은 재빠르게 보수적으로 변할 수밖에 없다. 온라인투표의 장점은 배제되고 오프라인투표의 불편함을 당연하게 감수하는 상황이 되는

것이다. 이것은 디지털 대전환을 준비하는 매우 미숙한 접근이다. 사회적 차원에서도 고비용적, 비효율적 운영이다. 온라인투표기술에 대한 이해를 제고함으로써 시스템 요구조건을 종합적이고 전문성있게 사전 점검할 수 있다. 이는 사후적 비용을 사전적 대응으로 전환하여 디지털 전환의 효용을 사회적으로 향상시킨다는 점에서 의의를 갖는다.

본 논문은 K-Voting이라는 서비스명으로 중앙선거관리위원가 유수 공공선거에 적용하고 있는 온라인투표시스템을 바탕으로 기술되었다. 투표데이터 보안 및 개표 데이터 검증에 대해 이미 중앙선거관리위원회라는 정부조직에서 인정 및 채택한 공신력 있는 기술에 대해 분석함으로써 온라인투표시스템에 대한 사회적 이해를 제고하고, 온라인투표의 저변 확대에 기여할 수 있을 것이다.

효율과 합리성을 더욱 고려하는 일부 하위 법률에서는 온라인투표의 도입 근거를 이미 마련하였다. 상법의 경우 이미 10년 전에 법개정을 통해 주주총회에서 온라인투표를 공식적으로 도입하였다. 공동주택관리법의 경우 2014년에 전자투표 도입의 법률적 효력 근거를 마련하였고, 2021년에 온라인투표의 우선 사용을 권고하는 내용으로 개정하였는데, 이는 2021년 대한민국 최우수 법률상을 수상하였다(머니투데이, 20201.11.10). 온라인투표로 인한 공동주택관리의 장점과 효율성이 시대적 공감을 받을 만큼 디지털 전환에 대한 우리 사회의 니즈와 인식이 확대된 것으로 해석된다.

온라인투표가 우리 사회에 제공하는 가치는 무수하다. 대표적으로 오프라인 투표에서 관행적으로 발생했던 섀도우보팅(Shadow Voting)의 주총 악용 사례를 들 볼 수 있다(이해성, 김갑순, 2017). 섀도우보팅은 주총에 참여하지 못하는 주주들이 많을 경우, 그들의 투표권을 참석 주주들의 실제 표결 결과에 비례해서 반영하는 것이다. 그러다 보니 참여도가 낮은 소액주주들이나 지리적, 공간적, 시간적 이유로 참여하지 못한 주주들의 투표권이 대주주나 경영진에게 유리한 안건을 쉽게 통과시키는 수단으로 이용된 것이다. ESG를 위한 거버넌스의 투명성 및 자본주의 시장질서 확립이 강조되는 현시점에서 온라인 투표의 효용은 더욱 중용하게 부각된다. 공동주택 투표의 경우도 마찬가지이다. 관리사무소를 중심으로 한 회계부정 사례는 사회뉴스에 주기적으로 등장하는 단골 주제이다. 이를 위한 거버넌스 구축의 첫 단계로서 입주자대회를 구성하는 주민투표의 참여율을 높이는 것은 무엇보다 중요하다. 실제 온라인투표를 도입하고선 공동주택의 투표율은 크게 향상되었다(심선영, 2019).

에스토니아는 2005년 총선에서 세계 최초로 온라인투표를 도입하였다(조희정, 2008). 에스토니아가 당시 온라인투표를 도입할 수 있었던 주요 이유 중 하나는 에스토니아 국민의 80%가 eID 카드를 소지하고 있었기 때문이다. eID 카드는 직접선거의 원칙을 보장하는데 큰 역할을 수행하였다. 하지만 인터넷을 기반으로 원격지에서 수행된 투표인 만큼 비밀성 보장 및 공정성에 대한 다양한 반론이 가능했음에도 불구하고 당시 에스토니아가 온라인투표를 도입할 수 있었던 것은 '사회적 합의'라는 큰 전제가 있었기 때문이다(전응렬 등, 2011). 마치 수용을 위한 선결조건처럼 회자되어 온 '사회적 합의'는 투표와 같이 민감하고 중요한 영역의 디지털 전환을 위해 물론 중요다. 하지만, 최근 이루어진 온라인투표기술의 성숙은 오히려 '사회적 이해'를 요구하고 있다. 투표라는 행위와 이를 구현하는 기술에 대한 정확한 이해를 바탕으로 시스템에 대한 신뢰가 구축되고 수용 범위를 확대할 수 있을 것이다. 이런 점에서 본 연구가 우리 사회의 디지털 전환을 통한 민주적이고 직접적 의사결정을 보다 다양하게 확장하는데 기여하기를 바란다.

참 고 문 헌

[1] 강서일, 이임영, "전자 투표 시스템의 보안 기술 및 종이 영수증 동향", *정보보호학회지*,

제15권, 제5호, 2005, pp. 40-51.
[2] 김병록, “미국 대통령 선거의 ‘유권자 투표’(popular vote)와 ‘선거인단 투표’(Electoral College vote)에 관한 고찰-선거인단 제도를 중심으로”, *미국헌법연구*, 제32권, 제3호, 2021, pp. 1-44.
[3] 김용섭, *언컨택트, 더 많은 연결을 위한 새로운 시대 진화 코드*, 퍼블리온, 2020.
[4] 김종선, 이혁기, 정기정, 정연돈, *데이터 익명화 개념 이해 및 최신 기술 동향*, 휴먼싸이언스, 2018.
[5] 김철진, “신뢰성 향상을 위한 이더리움 블록체인 기반의온라인 투표 시스템”, *한국산학기술학회논문지*, 제19권, 제4호, 2018, pp. 563-570.
[6] 나장호, 김혜영, “블록체인에서 Schnorr 디지털서명의 사용 전망에 관한 연구”, *디지털콘텐츠학회논문지*, 제23권, 제4호, 2022, pp. 743-751.
[7] 노시완, 이경현, “블록체인 보안 이슈에 대한 분석과 해결 방안에 대한 연구”, *인터넷정보학회논문지*, 제20권, 제4호, 2019, pp. 1-11.
[8] 머니투데이, “그래도 법은 만든다…2021 최우수법률상 송기헌 ‘군사법원법’”, 20201.11.10, Available at https://news.mt.co.kr/mtview.php?no=2021111018422129350.
[9] 문은영, “선거의 원칙에 대한 재고찰-에스토니아 전자투표 사례를 중심으로”, *정보화정책*, 제29권, 제4호, 2022, pp. 67-90.
[10] 박근덕, 김창오, 염흥열, “분산 원장 기술을 활용한 온라인 투표에 대한 보안 위협과 대응 방안”, *정보보호학회논문지*, 제27권, 제5호, 2017, pp. 1201-1216.
[11] 박선영, 박상민, 박의성, 김현곤, “종단간 암호화와 전자서명 기능을 가진 안전한 메신저 프로그램”, *국통신학회 학술대회논문집*, 2016, pp. 305-306.
[12] 박찬형, 김재훈, “하이퍼레저 패브릭을 이용한 전자 투표 시스템”, *한국통신학회 학술대회논문집*, 2020, pp. 1096-1097.
[13] 박찬희, 김해용, 지장현, 이진재, 김호원, “KCMVP 검증을 위한 암호 모듈 설계 및 대응 방안”, *한국통신학회 학술대회논문집*, 2019, pp. 144-145.
[14] 박철용, 김기홍, 류재철, “이기종 전술통신망 종단간 암호화 통신을 위한 메커니즘”, *정보보호학회논문지*, 제24권, 제4호, 2014, pp. 625-634.
[15] 손주희, 문유석, “전자투표를 활용한 주민소환 활성화 방안: 블록체인을 활용한 전자투표를 중심으로”, *지방정부연구*, 제23권, 제4호, 2020, pp. 139-165.
[16] 심선영, “스마트 직접 민주주의를 위한 모바일 투표 활용방안-서울시 공동주택 관리방안을 중심으로”, *서울도시연구*, 제20권, 제2호, 2019, pp. 57-75.
[17] 월드코리안뉴스, “이종환칼럼: 이참에 온라인 투표 논의를 본격화하자”, 2020.03.31., Available at http://www.worldkorean.net/news/articleView.html?idxno=36693.
[18] 이광우, 이윤호, 원동호, 김승주, ″전자투표 신뢰성 향상을 위한 투표자 검증용 영수증 발급 기술”, *정보보호학회논문지*, 제16권, 제4호, 2006, pp. 119-126.
[19] 이루다, 임좌상, “블록체인을 활용한 전자투표 시스템 구축”, *한국정보통신학회논문지*, 제23권, 제1호, 2019, pp. 103-110.
[20] 이재영, 이지영, “디지털서명과 은닉서명에 관한 연구”, *한국OA학회논문지*, 제5권, 제3호, 2005, pp. 70-75.
[21] 이태혁, 강명조, 김미희, “블록체인 시스템에서의 프라이버시 보호 기술 동향 분석”, *한국정보처리학회 학술대회논문집*, 제29권, 제2호, 2022, pp. 82-84.
[22] 이해성, 김갑순, “섀도우보팅 이용 기업의 이익의 질과 조세회피”, *세무와 회계저널*, 제18권, 제4호, 2017, pp. 111-145.

[23] 장대익, “알고리즘 시대의 공감의 반경: 추천 알고리즘은 어떻게 우리를 더 폐쇄적으로 만드는가?”, *문명과 경계*, 제3권, 2020, pp. 17-42.

[24] 전웅렬, 원동호, “전자투표 기술 동향 분석”, *한국인터넷 정보학회*, 제13권, 제1호, 2012, pp. 39-47.

[25] 전웅렬, 이윤호, 원동호, “전자투표 시스템 실용화 현황과 전망”, *정보보호학회지*, 제21권, 제2호, 2011, pp. 83-92.

[26] 전형준, 김학린, “공공갈등 해결기제로서의 주민투표의 활용현황과 특징”, *분쟁해결연구*, 제11권, 제3호, 2013, pp. 5-26.

[27] 정익래, 이동훈, “명시적 수신자 은닉 서명”, *한국정보과학회 학술발표논문집*, 제30권, 제1A호, 2003, pp. 257-259.

[28] 조희정, “전자민주주의와 인터넷 투표 - 에스토니아 사례를 중심으로”, *한국정당학회 학회보*, 제7권, 제2호, 2008, pp. 159-187.

[29] 중앙선거관리위원회, “블록체인 기반 온라인 투표시스템”, *e-선거정보*, 2018-4호, 2018.04.22.

[30] 중앙선거관리위원회, “온라인투표시스템 표준가이드라인”, 2020.12, Available at https://pub.kvoting.go.kr/ReflibContentSelect.do.

[31] 중앙선거관리위원회, 보도자료, 22.02.25, Available at https://www.nec.go.kr/cmm/dozen/view.do?cbIdx=1090&bcIdx=163624&fileNo=2.

[32] 코인데스크코리아, “전자 투표는 어차피 올 미래다”, 2020.11.12, Available at https://www.coindeskkorea.com/news/articleView.html?idxno=71996.

[33] 하현수, 이선준, 정구익, 신용구, 김명호, 김영종, “Public Blockchain 기반의 익명성 전자투표 블록체인 플랫폼 모델”, *한국정보과학회 학술발표논문집*, 2017, pp. 1176-1178.

[34] 허원근, 김희선, 김광조, “전자선거 프로토콜의 요구사항 연구”, *정보보호학회지*, 제10권, 제1호, 2000, pp. 63-69.

[35] 홍재우, “민주주의와 선거관리: 원칙과 평가-제5회 전국동시지방선거를 중심으로”, *의정연구*, 제16권, 제3권, 2010, pp. 125-159.

[36] An, H. C., “Design and analysis of decentralized public key infrastructure with quantum-resistant signatures”, Mster’s Thesis in KAIST, 2018.

[37] Antonopoulos, A. M., Wood, G., Mastering ethereum: building smart contracts and dapps, O’reilly Media, 2018.

[38] BLOCKO, “블록체인 투표, 어디까지 왔나? 대선과 총선, 스마트폰으로 치를 수 있을까?”, Blockchain Report, 2020, Available at https://www.blocko.io/report/08-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%ED%88%AC%ED%91%9C-%EC%96%B4%EB%94%94%EA%B9%8C%EC%A7%80-%EC%99%94%EB%82%98-%EB%8C%80%EC%84%A0%EA%B3%BC-%EC%B4%9D%EC%84%A0-%EC%8A%A4%EB%A7%88%ED%8A%B8/.

[39] Brands, S., “Untraceable off-line cash in wallet with observers. In Advances in Cryptology—CRYPTO ’93”, *13th Annual International Cryptology Conference Santa Barbara*, California, USA August 22-26, *1993 Proceedings 13*, Springer Berlin Heidelberg, 1994, pp. 302-318.

[40] Camenisch, J., U. Maurer, and M. Stadler, “Digital payment systems with passive anonymity-revoking trustees”, *Journal of Computer Security*, Vol.5, No.1, 1997, pp. 69-89.

[41] Chaum, D. L., “Untraceable electronic mail, return addresses, and digital pseudonyms”, *Communications of the ACM*, Vol.24, No.2, 1981, pp. 84-90.

[42] Golle, P., M. Jakobsson, A. Juels, and P. Syverson, “Universal re-encryption for mixnets. In Topics in Cryptology–CT-RSA 2004”, *The Cryptographers’ Track at the RSA Conference 2004*, San

Francisco, CA, USA, February 23-27, Springer Berlin Heidelberg, 2004, pp. 163-178.

[43] Hyun, Y. G., J. T. Lim, J. H. Han, U. Chae, G. H. Lee, J. D. Ko, and J. Y. Lee, "A study on the development methodology for user-friendly interactive chatbot", *Journal of Digital Convergence*, Vol. 18, No. 11, 2020, pp. 215-226.

[44] Jafar, U., A. Juzaiddin, M. Aziz, and Z. Shukur, "Blockchain for electronic voting system－review and open research challenges", *Sensors*, Vol.21, No.17, 2021, pp. 5874-5895.

[45] Jakobsson, M., A. Juels, and R. L. Rivest, "Making mix nets robust for electronic voting by randomized partial checking", *USENIX Security Symposium*, 2002, August, pp. 339-353.

[46] Jeon, W. R., Y. H. Lee, and D. H. Won, "An efficient mixnet for electronic voting systems", *Journal of the Korea Institute of Information Security & Cryptology*, Vol.22, No.3, 2012, pp. 417-425.

[47] Jeong, I. R. and D. H. Lee, "Anonymity control in multi-bank E-cash system", *INDOCRYPT*, 2000, pp. 104-116.

[48] Kaliyamurthie, K. P., R. Udayakumar, D. Parameswari, and S. N. Mugunthan, "Highly secured online voting system over network", *Indian Journal of Science and Technology*, Vol.6, No.6, 2013, pp. 1-6.

[49] Kim, D. H., S. U. Yun, and Y. P. Lee, "IoT 서비스를 위한 보안", *Information and Communications Magazine*, Vol.30, No.8, 2013, pp. 53-59.

[50] Kshetri, N. and J. Voas, "Blockchain-enabled e-voting", *Ieee Software*, Vol.35, No.4, 2018, pp. 95-99.

[51] KSITEP, "2018년 기술영향평가 결과보고, 블록체인의 미래", 2019, Available at https://www.kistep.re.kr/boardDownload.es?bid=0002&list_no=34299&seq=10117.

[52] MBN, "[뉴스추적] 50cm 비례 투표용지…18년 만에 손 개표", 2020.03.28, Available at https://m.mbn.co.kr/tv/552/0/1239083.

[53] Neff, C. A., "A verifiable secret shuffle and its application to e-voting", In *Proceedings of the 8th ACM conference on Computer and Communications Security*, 2001, pp. 116-125.

[54] Sako, K. and J. Kilian, "Receipt-free mix-type voting scheme: A practical solution to the implementation of a voting booth In Advances in Cryptology－EUROCRYPT '95", *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques*, 14, Springer Berlin Heidelberg, 1995, pp. 393-403.

[55] Taghva, K., R. Beckley, and J. Coombs, "The effects of OCR error on the extraction of private information", *Document Analysis Systems*, Vol.3872, 2006, pp. 348-357.

[56] Won, D., *Modern Cryptology*, Green Press, 2006.

[57] Wong, P. W., "A public key watermark for image verification and authentication", In *Proceedings 1998 International Conference on Image Processing*, ICIP98(IEEE), Cat. No. 98CB36269, Vol. 1, 1998, pp. 455-459.

Information Systems Review
Volume 25 Number 4
November 2023

A Study on the Trust Mechanism of Online Voting: Based on the Security Technologies and Current Status of Online Voting Systems

Seonyoung Shim* · Sangho Dong**

Abstract

In this paper, we investigate how the online voting system can be a trust-based system from a technical perspective. Under four principles of voting, we finely evaluate the existing belief that offline voting is safer and more reliable than online voting based on procedural processes, technical principles. Many studies have suggested the ideas for implementing online voting system, but they have not attempted to strictly examine the technologies of online voting system from the perspective of voting requirements, and usually verification has been insufficient in terms of practical acceptance. Therefore, this study aims to analyze how the technologies are utilized to meet the demanding requirements of voting based on the technologies proven in the field. In addition to general data encryption, online voting requires more technologies for preventing data manipulation and verifying voting results. Moreover, high degree of confidentiality is required because voting data should not be exposed not only to outsiders but also to managers or the system itself. To this end, the security techniques such as Blind Signature, Bit Delegation and Key Division are used. In the case of blockchain-based voting, Mixnet and Zero-Knowledge Proof are required to ensure anonymity. In this study, the current status of the online voting system is analyzed based on the field system that actually serves. This study will enhance our understanding on online voting security technologies and contribute to build a more trust-based voting mechanism.

Keywords: ***Online Voting, Security Technology, Encryption, Fraud Detection, Data Manipulation, Blockchain, Data Confidentiality, Data Integrity***

* Corresponding Author, Professor, Department of Business Administration, Sungshin University
** Director of Research Institute, KEVOTING, Inc.

◐ 저 자 소 개 ◑

심 선 영 (syshim@sungshin.ac.kr)

한국과학기술원에서 박사학위를 취득하였으며, 현재 성신여자대학교 경영학과 교수로 재직 중이다. 주요 관심분야는 RPA 분석, 디지털 트랜스포메이션, 인공지능 비즈니스 융합, 전자투표 등이다.

동 상 호 (sangho.dong@kevoting.com)

포항공과대학교에서 전산과학을 전공하였으며, 현재 한국전자투표㈜에서 기술이사로 재직 중이다. 온라인 투표 시스템 및 관련 보안 프로그램의 개발 전문가이다.

논문접수일 : 2023년 02월 23일 **게재확정일 : 2023년 08월 03일**
1차 수정일 : 2023년 05월 08일 **2차 수정일 : 2023년 07월 04일**