논문 19-44-01-23 The Journal of Korean Institute of Communications and Information Sciences '19-01 Vol.44 No.01
https://doi.org/10.7840/kics.2019.44.1.171

동형암호를 사용한 블록체인 기반 전자투표 시스템 개발

한 상 우◆, 배 민 수*, 황 경 호°

Development of Electronic Voting System Based on Blockchain using Homomorphic Encryption

Sang-Woo Han◆, Min-Su Bae*, Gyung-Ho Hwang°

요 약

전자투표와 종이투표 방식은 기술적으로 신뢰성이 낮고 비밀선거의 원칙을 보장하기가 어렵다. 본 논문에서는 투표 내역을 블록체인에 안전하게 저장하고 동형암호로 암호화하여 비밀선거의 원칙을 보장하는 전자투표 시스템을 구현하였다. 유권자의 투표 내용을 동형암호로 암호화 한 후 이더리움 플랫폼의 블록체인으로 저장하였고, 투표 시간이 종료되면 암호화한 투표용지들을 동형암호 덧셈 연산을 통해 집계할 수 있었다.

Key Words : Electronic Voting System, Blockchain, Ethereum, IPFS, Homomorphic Encryption

ABSTRACT

Electronic voting and paper voting are technically unreliable and it is difficult to ensure the principle of secret election. In this letter, we implemented an electronic voting system that securely stores the voting history in the Etherium based blockchain and encrypts the ballots with the homomorphic encryption to ensure the principle of secret election. After voting time, the ballots are tallied by addition operation of the homomorphic encryption and the secret election is ensured.

Ⅰ. 서 론

기존의 전자투표 시스템은 투표 내역과 집계 과정 중의 신뢰성이 낮고, 현재의 종이투표 방식은 선거에 따른 비용 증가와 부정확한 집계로 인해 선거 결과의 신뢰성이 낮다[1]. 또한 선거의 4원칙 중 하나인 비밀선거 원칙은 유권자가 누구에게 투표했는지를 알 수 없게 하는 제도로, 이를 위해 유권자의 투표 내역을 암호화하여 숨겨야하는데 기존의 암호화 방식을 사용한 전자투표 시스템은 선거 기관이 선거 기간 중에 투표 내역을 노출하거나 투표를 집계할 때 투표 내역과 함께 유권자의 정보를 노출할 위험성이 있다.

기존의 데이터베이스를 사용하는 것에 비해 이더리움 플랫폼의 블록체인을 사용한다면 분산하여 저장된 투표 내역의 일관성으로 인해 신뢰성을 보장할 수 있다. 또한 기존의 SHA나 RSA와 같은 암호화 방식을 사용하는 것에 비해 동형암호를 사용하여 유권자의 투표 내역을 암호화하여 숨길 수 있으며, 유권자들의 투표 내역을 암호화된 상태로 모두 더하여 집계를 할 수 있다. 이러한 동형암호의 성질을 이용하여 비밀선거의 원칙을 보장한다.

따라서 투표와 집계에 대한 신뢰성을 높이고, 비밀선거의 원칙을 보장하는 새로운 방법으로 이더리움의 블록체인과 동형암호를 사용하는 방법을 제안한다. 본 논문에서는 블록체인으로 투표 내역을 저장하고, 동형암호로 투표 과정을 모두 암호화하여 정보의 노출을 막고, 암호화된 상태에서도 연산을 가능케 하여 투표 집계 결과를 낼 수 있는 전자투표 시스템을 구현하였다[2].

Ⅱ. 전자투표 시스템의 구성

제안하는 전자투표 시스템은 <그림 1>과 같이 사용자, 탈중앙화 애플리케이션인 ĐApp 서버, 데이터베이스 및 블록체인들로 구성한다. 블록체인은 이더리움과 IPFS(Inter Planetary File System) 플랫폼을 사용하며, 데이터베이스는 MongoDB를 사용한다.

사용자는 Chrome 웹 환경을 통해 ĐApp 서버에

◆ First Author : (ORCID:0000-0001-8062-6860)Dept. Computer Engineering, Hanbat National University, tkddn204@gmail.com, 정회원
° Corresponding Author : (ORCID:0000-0001-6795-8086)Dept. Computer Engineering, Hanbat National University, gabriel@hanbat.ac.kr, 종신회원
* (ORCID:0000-0003-3958-1773)Dept. Computer Engineering, Hanbat National University, kluge0221@gmail.com
논문번호 : 201810-314-D-LU, Received Ocotber 8, 2018; Revised December 11, 2018; Accepted December 18, 2018

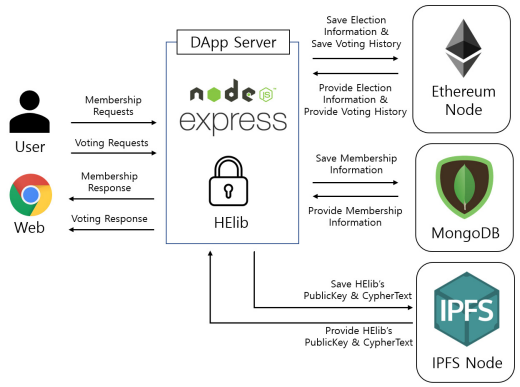

그림 1. 전자투표 시스템 구성도
Fig. 1. Architecture of Electronic Voting System

접근할 수 있다. ĐApp 서버는 Ubuntu 18.02 환경에서 Node.js 플랫폼과 express.js 서버를 운용하여 사용자와 서버 간 데이터베이스 및 블록체인의 접근을 제어한다. 동형암호는 관련 연구에 따르면 6번 이상의 암호화 연산을 수행할 때 여러 동형암호 라이브러리 중 HElib가 가장 연산 속도가 빠르다[3]. 보통 투표 집계를 할 때, 선거 인원이 6명 이상일 경우가 대부분이므로, 동형암호 라이브러리로 HElib를 사용한다. 본 논문에서 사용하는 이더리움 노드는 프라이빗 네트워크로써 메인 네트워크와 독립된 네트워크를 형성하여 사용한다. 이더리움의 블록체인에는 선거 정보와 유권자의 투표 내역을 저장한다. MongoDB에는 사용자 정보를 저장한다. IPFS 노드는 퍼블릭 환경의 노드를 사용한다. IPFS에는 동형암호의 공개키와 암호화된 정보를 저장한다. IPFS는 파일을 업로드하면 SHA-1 hash 값의 식별자를 반환한다. 이더리움에 동형암호 공개키 파일이나 암호문 파일을 직접 저장하면 이더리움 트랜잭션 수수료인 GAS의 소모량이 높기 때문에 이를 줄이기 위해 파일을 직접 저장하지 않고, IPFS의 hash 값 식별자를 저장한다.

Ⅲ. 전자투표 시스템의 설계

전자투표 시스템의 절차는 <그림 2>와 같이 크게 선거 개설, 투표, 집계의 세 단계를 거쳐 진행한다.

3.1 선거 개설 단계

회원으로 가입한 사용자라면 누구나 서버 관리자에게 선거 개설 요청을 할 수 있다. 관리자는 사용자가 요청한 선거 정보를 토대로 선거용 스마트 컨트랙트 계정을 만든다. 계정을 만든 후 해당 선거에서만 사용

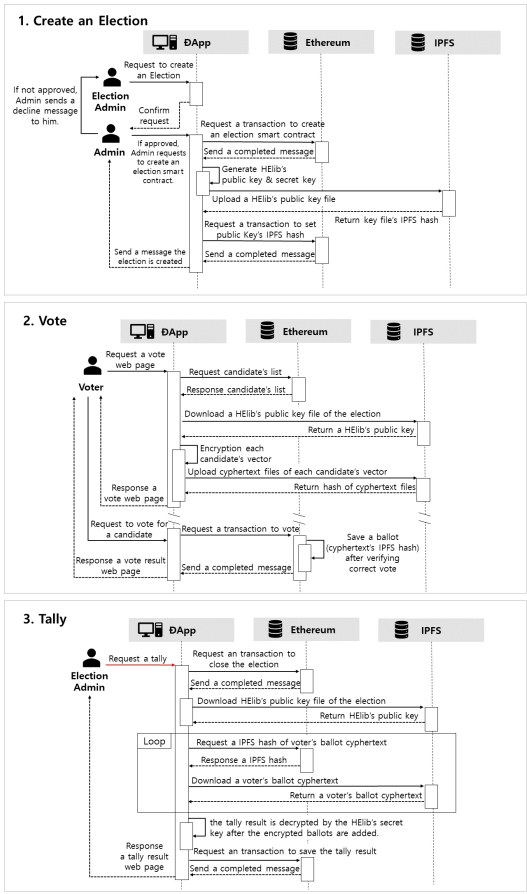

그림 2. 전자투표 시스템의 각 투표 단계 절차
Fig. 2. Procedures of Electronic Voting System

할 수 있는 동형암호 공개키와 비밀키를 생성한다. 키를 생성할 때, HElib은 특정 파라미터 값으로 키를 생성하도록 설계되어 있다. 본 논문에서는 파라미터 값을 HElib의 테스트 코드에서 권장하는 값으로 설정한다. 다만, 권장하는 값이 없는 파라미터인 소수 p와 레벨값 L은 임의로 설정한다. 본 논문에서 사용한 소수 값은 10007이며, 레벨값은 7로 설정했다. 이 값으로 키를 생성하여 이진 파일로 내보내면, 비밀키의 파일 크기는 92MB, 공개키의 파일 크기는 46MB 정도이다. 공개키는 IPFS에 저장한 후 파일의 식별자인 hash 값을 선거 스마트 컨트랙트에 저장한다. 비밀키는 ĐApp 서버의 파일 시스템에 저장한다. 이후 DB의 사용자 정보에 계정 주소를 저장하고, 관리자는 사용자에게 선거를 개설 완료하였다는 메시지를 보낸다.

3.2 투표 단계

선거의 상태가 진행 중이면 선거 기간 동안 유권자

는 투표를 진행 할 수 있다. 유권자가 투표에 참여하겠다는 요청을 ĐApp 서버로 보내면, 서버에서는 해당 선거의 후보자 목록을 이더리움에서 가져온다. 서버는 유권자가 가진 이더리움 계정 주소와 해당 선거의 동형암호 공개키를 사용하여 후보자 목록을 암호화한다. 공개키는 서버의 파일 시스템에 저장되어 있으면 그것을 사용하고, 없을 경우 IPFS에서 공개키를 다운로드한다. 각각의 후보자는 다항식 벡터인 [1, 0, 0]과 같은 형태로 암호화를 진행한다. 완전 동형암호의 특성상 암호화를 진행하거나 암호화된 상태로 연산을 할 때마다 노이즈가 발생하기 때문에 계정마다 달리 암호화를 진행하면 암호문의 내용을 유추하기 어려워진다[2][4]. 정리하면, 암호문은 사용자가 후보자에게 투표한 벡터를 암호화한 것이며, 이는 노이즈로 더욱 보안이 강화된다. 이러한 암호화는 제3자는 유권자가 어느 후보자에게 투표했는지 알기 어려울 것이다. 암호화를 후보 수만큼 진행한 뒤 ASCII 문자로 이루어진 암호문 파일을 생성한다. 암호문 파일의 크기는 700KB 정도이다. 이 파일들은 모두 IPFS에 저장한다.

ĐApp 서버는 후보들의 IPFS hash 값과 함께 투표 웹페이지를 유권자에게 전달한다. 유권자가 투표하고자 하는 후보를 선택하면, 선택한 후보의 IPFS hash 값을 서버로 전달한다. 이 값이 하나의 투표용지가 된다. 서버는 선거 스마트 컨트랙트에 투표용지를 저장하고 유권자의 상태를 투표 완료 상태로 변경한다. 스마트 컨트렉트에 저장된 유권자의 상태가 투표 완료 상태가 되면 해당 유권자는 그 선거에 더 이상 투표를 할 수 없다.

3.3 집계 단계

선거를 개설한 사용자가 선거를 종료 상태로 변경하면 ĐApp 서버에서 집계를 진행한다. <그림 3>은 3개의 투표용지에 동형암호의 덧셈 연산 결과를 통해 2번 후보가 당선되는 과정이다.

ĐApp 서버는 스마트 컨트랙트에 저장한 투표용지의 IPFS hash 값으로 IPFS에서 투표용지 암호문들을 다운로드한다. 동형암호 공개키로 투표용지 암호문들을 모두 더한 뒤 동형암호의 비밀키로 최종 암호 값을 복호화하여 투표를 집계한다. 집계한 결과 값을 선거 컨트랙트에 저장한다. 이후 선거의 상태를 종료 상태로 변경한다.

Ⅳ. 구현 결과

본 논문의 전자투표 시스템은 <그림 4>와 같이 웹 환경으로 개발하였다. 투표 내역이 이더리움에 저장되기 때문에 기존의 중앙집중된 데이터를 이용하는 전자투표 시스템보다 투명성과 신뢰성을 높일 수 있으며 이더리움에 저장된 정보를 탈취하더라도 동형암호 사용으로 인해 비밀선거 원칙을 유지할 수 있다. 본 논문에서는 프라이빗 환경의 이더리움을 사용하여 이더리움에 참여할 수 있는 권한이 있는 노드만 투표 내역을 저장할 수 있다. 프라이빗 환경은 퍼블릭 환경에서 투표 내역을 저장하는 것보다 블록체인에 대한 관리가 용이하며 이더리움 설정이 유연하고 트랜잭션 전송 속도가 빠르다. 하지만 투표 내역에 대한 투명성이 없어 제 3자가 투표 내역을 쉽게 신뢰하지 못한다는 단점을 가지고 있다. 제 3자가 동형암호의 비밀키를 습득하면 사용자가 투표한 암호화된 투표용지를 복호화할 수 있는 문제점이 있어 서버 관리자는 비밀키에 대해 폐쇄적인 정책을 세울 필요가 있다.

동형암호는 2세대 완전동형암호인 HElib을 사용하였다. HElib 이외 Paillier의 부분동형암호를 사용한 전자투표 시스템 개발 사례가 있다. 부분동형암호를 사용하면 암호화 속도가 빠르다는 장점이 있지만 덧셈이나 곱셈 중 하나의 연산만을 수행할 수 있다. 그러나 완전동형암호는 복수의 연산이 가능하기 때문에 유연성이 높고, 집계 시에 단순히 덧셈만을 하는 것이

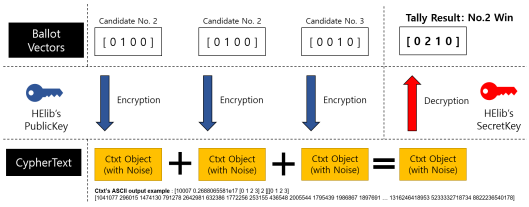

그림 3. 동형암호를 사용한 투표 집계
Fig. 3. Tallying the ballots using Homomorphic Encryption

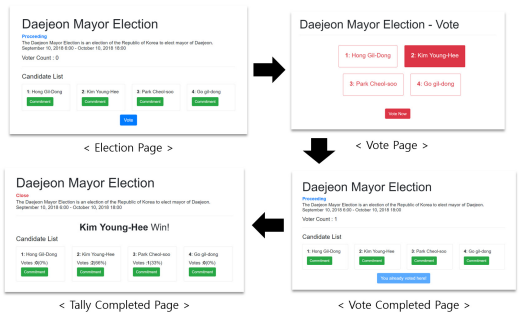

그림 4. 전자투표 시스템의 웹사이트 화면
Fig. 4. Web UI of Electronic Voting System

아니라, 비트마스킹 연산이나 소수 계산을 한다면 보안성을 높인 시스템을 구축할 수 있다[4].

V. 결 론

본 논문에서는 동형암호를 사용한 전자투표 시스템을 구현하고 이를 통해 사용자가 선거를 개설하고 투표를 진행할 수 있는 ĐApp을 개발하였다. 테스트를 위해 ĐApp 서버를 아마존 클라우드 서버에 배포하여 이더리움 테스트 노드를 운용하였고 구현 결과 비밀선거 원칙과 이더리움의 블록체인을 적용한 데이터 위변조에 대한 보안성을 기대할 수 있었다.

References

[1] K. Lee, Y. Lee, D. Won, and S. Kim, "A voter verifiable receipt in electronic voting with improved reliability," *J. KIISC,* vol. 16, no. 4, pp. 119-126, Aug. 2006.

[2] J.-H. Kim, S.-K. Yoo, and S.-H. Lee, "Fully homomorphic encryption scheme without key switching," *J. KICS*, vol. 38, no. 5, pp. 428-433, May 2013.

[3] E.-J. Jo, S.-B. Moon, and Y. Lee, "Performance analysis of fully homomorphic encryption libraries," *J. KIIT*, vol. 16, no. 2, pp. 131-143, Feb. 2018.

[4] A. Azougaghe, M. Hedabou, and M. Belkasmi, "An electronic voting system based on homomorphic encryption and prime numbers," *11th Int. Conf. Inf. Assurance and Secur.*, pp. 140-145, Marrakech, Morocco, Dec. 2015.