Individual Verifiability with ReturnCodes: Manipulation Detection Efficacy

Paul Tim Th¨ urw¨ achter1, Melanie Volkamer1(B), and Oksana Kulyk

1 Karlsruhe Institute of Technology, Karlsruhe, Germany  
paul.thuerwaechter@student.kit.edu, melanie.volkamer@kit.edu  
2 IT University of Copenhagen, Copenhagen, Denmark  
okku@itu.dk

Brief Description of the Topic

Cryptographic end-to-end verifiability helps detect election integrity violations, but individual verifiability is challenging for voters. A study by Kulyk et al. at E-Vote-ID 2021[1] showed that QR-code-based code voting should be used in certain elections as it avoids reliance on trustworthy clients and positively affects manipulation detection rates. Studies on verifiable voting systems have shown mixed results on their effectiveness in e-voting systems. A code-voting approach aims to reduce trust in vote secrecy, but limited evaluations have been conducted.

The Swiss voting system uses a postal service to send voters an individual code sheet, which contains an initialization code, check codes for each voting option, confirmation code, and finalization code. The system generates an election-specific election key pair for each voter, with the private key deduced from the initialization code.[3]

Researchers at E-Vote-ID 2021 proposed an extension of Switzerland's verifiable voting scheme to improve vote secrecy. However, they did not evaluate (two groups with video and without video) its effectiveness in manipulating voters. A user study found that 65% of those receiving the video detected manipulation, while 75% and 63% of those not watching the video detected it. The researchers discuss ways to increase detection rates.[2]

Conclusions of the Paper

Online voting for political elections usually involves using verifiable voting systems, which guarantee vote confidentiality only in cases where the voting client is reliable. This problem can be solved by code voting, which offers a workable improvement to the current approach that can improve manipulation-detection effectiveness without compromising usability. According to this research, code-voting verifiable voting schemes may be an acceptable solution since simple steps like scanning QR codes can take the place of difficult human voting code entry steps. Although the analysed technique has a greater manipulation-detection efficacy, there is still potential for improvement. The study comes to the conclusion that increasing manipulation-detection efficacy requires a close examination of alternative interventions and a focus on verifiability.

Critical Opinion of the Paper

This paper focused on cryptographic end-to-end for election integrity violations. Also, evaluate and detect manipulation in electronic voting and attacks. with using a QR code base in the code voting system. They use of blockchain technology in e-voting to address voters between voters. In real they used the Swiss voting system and E-Vote-ID 2021 to detect manipulation of voting and Improve that system with descriptive video. for the swiss system, voting uses a postal and send code sheet which is a private code for one person. The system became easier using a QR code and scanning with a camera. Then improve with descriptive video.

The E-Vote-ID-2021 proposal outperforms the original system in detection manipulation rates of course, this system improved to description of video and participation divided to video and no video But No significant differences were found between the no-video-group and video-group. It is better to use E-Vote-ID-2021 proposal.

1. Kulyk, O., Volkamer, M., M¨ uller, M., Renaud, K.: Towards improving the efficacyof code-based verification in internet voting. In: Bernhard, M., et al. (eds.) FC2020. LNCS, vol. 12063, pp. 291–309. Springer, Cham (2020). https://doi.org/10.  
   1007/978-3-030-54455-3 21
2. Kulyk, O., Ludwig, J., Volkamer, M., Koenig, R.E., Locher, P.: Usable verifiable secrecy-preserving e-voting. In: Electronic Voting: 6th International Joint Conference, E-Vote-ID. University of Tartu Press (2021)
3. Haines, T., Lewis, S.J., Pereira, O., Teague, V.: How not to prove your election outcome. In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 644–660. IEEE (2020)

Citation /Reference: Use **APA** format

Thürwächter, P. T., Volkamer, M., & Kulyk, O. (2022, September). Individual Verifiability with Return Codes: Manipulation Detection Efficacy. In *International Joint Conference on Electronic Voting* (pp. 139-156). Cham: Springer International Publishing.‏