Abstract

Electronic voting refers to the using of computers or computerized voting equipments to cast ballots in the election. The e-voting has been developed for more than 20 years. In the electronic voting, there are three stages: the registration stage, the voting stage, and the tally stage. Verifiable cryptographic voting systems use encryption technology to secure electorate’s votes and to avoid coerce them to vote for any particular candidate or to buy their votes, and any another threats. This research aims to obtain an electronic voting system could be used easily in the third world countries. In this research ten of existing cryptography verifiable voting systems have been studied, and especially focused on End-to-End verifiable voting systems, which is considered as the newest class of voting systems. In addition this paper took a system from another type of verifiable voting systems for a comparison purpose. The comparison between these systems has done according to a set of public evaluation contexts that is followed in any voting system such as: properties, cryptographic building block, ballot format, and models. This paper discusses seven of E2E voting systems, which are closer to deal with in the developing communities in order to modify any one of those systems for using in third world countries. This study concludes that most of the modern voting systems
Survey on End-to-End Verifiable Cryptographic Voting Systems

currently in place are not usable in the third world countries (despite the many positive achievements in many aspects) but can be adjusted to fit with these countries. In the future, the most appropriate E2E voting system will be chosen among systems which are mentioned in this study to be adjusted in order to fit in the third world countries.

References

- Cramer, Ronald and Damgrd, Ivan, "Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free?"; in Advances in Cryptology—CRYPTO&amp;apos;98(1998), pp. 424--441.
- Delaune, Stéphanie and Kremer, Steve and Ryan, Mark, "Verifying properties of electronic voting protocols"; in in&amp;quot; Proceedings of the IAVoSS Workshop On
Survey on End-to-End Verifiable Cryptographic Voting Systems

Trustworthy Elections (WOTE’06, 2006).
- Ryan, Peter YA and Schneider, Steve A, “Prêt à voter with re-encryption mixes” (Springer, 2006).
- Chaum, David and Carback, Richard T and Clark, Jeremy and Essex, Aleksander and
Survey on End-to-End Verifiable Cryptographic Voting Systems


- Bär, Michael and Henrich, Christian and Müller-Quade, Jörn and Röhrich, Stefan and Stüber, Carmen, "Real world experiences with Bingo Voting and a comparison of usability", in IAVoSS Workshop On Trustworthy Elections (WOTE 2008), (, 2008).

Index Terms
Keywords
Electronic voting  Usability of system  Third world societies.