Chapter XII

Secure Multiparty/Multicandidate Electronic Elections

Tassos Dimitriou, Athens Information Technology, Greece

Dimitris Foteinakis, University of Thessaly, Greece

ABSTRACT

In this chapter, we present a methodology for proving in Zero Knowledge the validity of selecting a subset of a set belonging to predefined family of sets. We apply this methodology in electronic voting to provide for extended ballot options. Our proposed voting scheme supports multiple parties and the selection of a number of candidates from one and only one of these parties. We have implemented this system and provided measures of its computational and communication complexity. We show that the complexity is linear with respect to the total number of candidates and the number of parties participating in the election.
INTRODUCTION

With the explosion of growth of the World Wide Web, the increase of computational power, computer memory, and the storage capacity, we have the ability to communicate more information faster, cheaper, and more reliably. The general trend toward a paperless society has affected the area of voting. Many attempts have been made to create systems that would allow modern computer-based technology to emulate the secure desirable properties valued in centuries of public voting.

Remote electronic voting refers to an election process whereby people can cast their votes over the internet, from the comfort of their home, or possibly any other location where they can get internet access. There are many aspects of elections besides security that bring this type of voting into question. The primary ones are:

- **Coercibility**: The danger that outside of a public polling place, a voter could be coerced into voting for a particular candidate
- **Vote selling**: The opportunity for voters to sell their vote
- **Vote solicitation**: The danger that outside of a public polling place, it is much more difficult to control vote solicitation by political parties at the time of voting
- **Invalid registration**: The issue of whether or not to allow online registration, and if so, how to control the level of fraud

The possibility of widely distributed locations where votes can be cast changes many aspects of our carefully controlled elections, as we know them. The relevant issues are of great importance and could very well influence whether or not such election processes are desirable. However, in this chapter, we do not discuss issues like the vulnerability of the internet to denial of service attacks, the unreliability of the Domain Name Service, or the various threats the supporting hosts are liable to, but we focus instead on the security considerations of the voting process.

Thanks to the advances in the fields of cryptography, an electronic voting system can satisfy the requirements that are considered self-evident for paper-based systems and at the same time be efficient and reduce the cost of large-scale elections. Fujioka, Okamoto, and Ohta (1992) define the properties of a secure, secret election:

- **Completeness**: All valid votes must be counted correctly
- **Soundness**: The dishonest voter cannot disrupt the voting process
- **Privacy and integrity**: All votes must be and remain secret and cannot be altered in transit. Hence, effective encryption must be used to protect the votes from being disclosed to third parties during transmission
- **Anonymity**: The voting system must support the voters’ right to secrecy of their vote. Hence, the vote recording mechanism must not identify the individual voter.