Chapter 12
Secure Electronic Voting with Cryptography

Xunhua Wang
James Madison University, USA

Ralph Grove
James Madison University, USA

M. Hossain Heydari
James Madison University, USA

ABSTRACT

In recent years, computer and network-based voting technologies have been gradually adopted for various elections. However, due to the fragile nature of electronic ballots and voting software, computer voting has posed serious security challenges. This chapter studies the security of computer voting and focuses on a cryptographic solution based on mix-nets. Like traditional voting systems, mix-net-based computer voting provides voter privacy and prevents vote selling/buying and vote coercion. Unlike traditional voting systems, mix-net-based computer voting has several additional advantages: 1) it offers vote verifiability, allowing individual voters to directly verify whether their votes have been counted and counted correctly; 2) it allows voters to check the behavior of potentially malicious computer voting machines and thus does not require voters to blindly trust computer voting machines. In this chapter, we give the full details of the building blocks for the mix-net-based computer voting scheme, including semantically secure encryption, threshold decryption, mix-net, and robust mix-net. Future research directions on secure electronic voting are also discussed.

INTRODUCTION

"Those who vote determine nothing; those who count the votes determine everything."—Joseph Stalin

Fair elections are the foundation of democracy. The integrity of an election depends heavily on the voting technologies used. In human history, several voting technologies have been used in various elections, including *stone*s, *colored balls or beans*, *paper ballots*, *mechanical lever machines*, *punched cards*, *optical scanners*, and most recently, *computers*. Computer voting is

DOI: 10.4018/978-1-61520-783-1.ch012

also called *electronic voting* and computer voting machines are often called *Direct Recording Electronics* (DRE).

Just as in many other applications, computers have the potential to make ballot casting, vote tallying, and vote recounting much easier and faster. On the other hand, computer voting also poses a big security challenge as it uses *electronic* ballots, not the traditional *paper* ballots.

Unlike paper ballots, electronic ballots can be easily modified, forged, and discarded without a trace. Such modification, forgery, and removal of electronic ballots can happen in all stages of electronic voting, including the *casting* (e.g., by faulty or malicious voting software), *storage*, *transferring*, and *tallying* of electronic ballots. The following examples of computer voting glitches happened in the November 4th, 2004 election.

- Carteret county, North Carolina, used an electronic voting system with a storage unit that has capacity of 3005 votes. The voting system allowed 7535 electronic ballots to be cast without reporting any errors. As a result, more than 4500 votes were lost (USA Today, 2004).
- One precinct in Franklin county, Ohio, used computer voting and reported 4258 votes for Bush. But records showed that only 638 voters cast their ballots in that precinct (McCarthy, 2004).
- Broward county, Florida, used computer voting equipment with faulty software that could not handle more than 32,000 votes in a precinct. When more than 32,000 votes were counted, the tallying software started counting backward. As a result, the outcome of Amendment 4 in the ballot was erroneously reported (Internet Broadcasting Systems, 2004).
- Sarpy county, Nebraska, used computer voting equipment and a computer problem caused double votes in half the county's precincts, leading to about 3000 phantom votes (WOWT.COM, 2004).

Because of the fragility of electronic ballots and voting and tallying software, it is desirable to have a paper trail for each electronic vote (for example, let each voter bring home a *paper receipt*). In case of a dispute, this paper receipt can be used at a later time for tracing the vote and for vote recounting.

However, this idea of a paper receipt may jeopardize several other properties of the voting system. First, the voter can use a plain paper receipt to prove to a candidate how the vote is cast, thus making vote selling possible: the candidate may pay a fee to the voter upon proof that the vote is actually for the candidate. Second, paper receipts also make vote coercion possible: a rogue candidate may seek revenge if a paper receipt shows that the vote is not for him. Thus, introducing plain paper receipts into electronic voting may improve accountability but will negatively impact the integrity of an election.

To overcome these difficulties, (Benaloh, 1988; Benaloh & Tuinstra, 1994; Chaum, 2004a, 2004b) developed the concept of *secret-ballot receipt*, which is an *encrypted* ballot. The resulting computer voting solution is essentially a *cryptography-based voting scheme* and is sometimes called *secret-ballot voting* or *receipt-free voting*. For this cryptographic solution, several issues need to be resolved: what cryptographic key and encryption algorithm are used? How are the encrypted ballots tallied? How is the integrity of the encrypted ballots guaranteed?

The introduction of *encrypted* paper receipts into computer voting may bring several additional desirable properties that do *not* exist in non-electronic traditional voting systems. First, in traditional voting systems, there is no direct method for a voter to verify that his/her vote is actually counted or counted correctly. A voter has to place his/her trust in the voting system for counting votes. As we shall see in this chapter, vote verifiability is achievable in cryptography-based computer voting systems.

Second, cryptography-based computer voting also allows individual voters to check the behavior