Chapter 10
Cryptographic Voting Protocols

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

Jayanthi Mathanan
Mepco Schlenk Engineering College, India

ABSTRACT
Most of the voting protocols proposed so far can be categorized into two main types based on the approach taken: schemes using blind signatures and schemes using homomorphic encryption. In the schemes using blind signatures, the voter initially obtains a token – a blindly signed message unknown to anyone except himself. In the schemes using homomorphic encryption the voter cooperates with the authorities in order to construct an encryption of his vote. Due to the homomorphic property, an encryption of the sum of the votes is obtained by multiplying the encrypted votes of all voters. This chapter reviews schemes based on blind signatures and homomorphic encryption and proposes improvements to the existing schemes.

INTRODUCTION
With the advent of the digital era, Electronic Voting has become common. Many issues remain to be solved in electronic voting schemes. This chapter explores the use of cryptographic protocols in electronic voting especially the application of homomorphic encryption to electronic voting. Most of the existing voting protocols can be categorized into two main types based on the approach taken: schemes using blind signatures and schemes using homomorphic encryption. In the schemes using blind signatures, the voter initially obtains a token – a blindly signed message unknown to anyone except himself. Next, the voter sends his token together with his vote anonymously. These schemes require voter’s participation in many rounds. In the schemes using homomorphic encryption, the voter cooperates with the authorities in order to construct an encryption of his vote. Due to the homomorphic property, an encryption of the sum of the votes is obtained by multiplying the encrypted votes of all voters. Finally, the result of the election is computed from the sum of the votes which is jointly decrypted by the authorities. This chapter reviews schemes based on blind signatures and homomorphic encryption and proposes improvements to the existing schemes.
FORMULATION OF THE VOTING PROBLEM

A voting scheme must ensure not only that the voter can keep his vote private, but also that he must keep it private. In other words, the voter should not be able to prove to the third party that he has cast a particular vote. He must not be able to construct a receipt proving the content of his vote. This property is referred to as receipt-freeness.

Only a few schemes guaranteeing receipt-freeness have been proposed. Known receipt-free scheme using blind signatures (Okamoto, 1997), assumes the existence of a special anonymous untappable channel. Achieving both secure and anonymous communication would, however, be extremely difficult. As for the schemes using homomorphic encryption, some efficient receipt-free schemes have already been proposed. Only the scheme proposed by Hirt and Sako (Hirt et al., 2000).

The Voting committee takes count of the voters: It allows only eligible voters to vote, and it ensures that every voter votes at most once. After the elections, the voting committee counts the votes and publishes the result. The votes remain secret. No one should not be able to say how anyone has voted. Even if the person says how he has voted, we cannot believe him, since he can lie. On the other hand, a person casting his vote cannot be absolutely sure that his vote was really counted. Everyone has to believe that the voting committee is honest and it would not disrupt the elections.

Basic Model

The participants in our schemes are voters and authorities. Let the number of Voters be M and the number of authorities be N. M is usually much greater than N. In general, the voters need not concern themselves with the voting process—they simply need to cast their votes. A voter can abstain from voting if he wishes to. Further we can assume, that he can store some amount of data in some secret place inaccessible to anyone except himself.

The authorities manage the elections. They have large computing power and they can store large amount of data in secret. Authorities can also act as voters. Of course, some number of authorities will be faulty. The maximum of faulty authorities will be assumed to be $t$. We assume that the remaining N-t authorities will do their prescribed work correctly and honestly.

The structure of Votes depends on the election (Rjaskova, 2002). The following types of elections are usually considered.

- **Yes/No Voting**: Voter’s answer is yes or no. Vote is one bit: 1 for yes, 0 for no.
- **1-out-of-L Voting**: Here, the voter has L possibilities and the voter chooses one of them. The vote is a number in the range 1…L.
- **K-Out-of-L Voting**: Voter selects K different elements from the set of L possibilities. The order of the selected elements is not important. The Vote is a K-tuple ($v_1 \cdots v_K$).
- **K-Out-of-L Ordered Voting**: The Voter select K different elements in order from the set of L possibilities. Vote is an ordered K-tuple ($v_1 \cdots v_K$).
- **1-L-K Voting**: Voter picks out one of the L sets of possibilities, and from the selected set he chooses K elements. Vote is a K+1-tuple (i, $a_1 \cdots a_K$); $a_1 \cdots a_K$ are elements of the ith set.
- **Structured Voting**: Voting is done from sets of possibilities in $n$ levels.
- **Write-In Voting**: Voter formulates his own answer and writes it down. Vote is a string with a specified maximum length.