Chapter 16

Protecting a Distributed Voting Schema for Anonymous and Secure Voting Against Attacks of Malicious Partners

Sebastian Obermeier
ABB Corporate Research, Switzerland

Stefan Böttcher
Universität Paderborn, Germany

ABSTRACT

A distributed protocol is presented for anonymous and secure voting that is failure-tolerant with respect to malicious behavior of individual participants and that does not rely on a trusted third party. The proposed voting protocol was designed to be executed on a fixed group of N known participants, each of them casting one vote that may be a vote for abstention. Several attack vectors on the protocol are presented, and the detection of malicious behavior like spying, suppressing, inventing, and modifying protocol messages or votes by the protocol is shown. If some participants stop the protocol, a fair information exchange is achieved in the sense that either all votes are guaranteed to be valid and accessible to all participants, or malicious behavior has been detected and the protocol is stopped, but the votes are not disclosed.

INTRODUCTION

Electronic voting is not only of interest for governmental elections; there are additional applications that motivate the development of a secure electronic voting schema that works without a trusted authority. An example is the energy market respective smart grids. In this scenario, end users use interconnected energy meters, which allows energy utilities to change prices due to demand. Within such scenario, an anonymous voting of smart meter users, for instance on their private
Protecting a Distributed Voting Schema for Anonymous and Secure Voting

energy consumption, is an application for energy demand prediction, but such scenario clearly has to prevent a large variety of malicious behavior, which ranges from manipulating or suppressing the distribution of the voting result, to spying or manipulating single votes, i.e., suppressing, inventing or modifying votes, to spying or manipulating protocol messages, e.g. suppressing, inventing or modifying messages, to stopping cooperation or even stopping the protocol when an unwanted outcome of the electronic voting process is obvious.

Another different example where anonymous voting mechanism can be used is the computation of the union of different statements. In this case, participants do not choose from a fixed set of possible results, but are free to phrase the content of their vote. In this case, properties of an anonymous voting schema such as vote integrity and the limitation to a fixed set of participants that is allowed to vote motivate the use of such a voting schema.

Therefore, whenever participants may behave malicious, it is crucial that a voting protocol can detect such kinds of malicious behavior. In contrast to traditional paper based voting mechanisms, we consider detecting these kinds of malicious behavior after some votes have been disclosed as being not sufficient. When some votes have already been disclosed, other participants may vote differently in a repetition depending on the previously disclosed votes.

This is why we additionally require a secure anonymous voting protocol to meet the following requirements:

1. The protocol prohibits disclosure of votes as long as malicious behavior can prevent a fair voting process, and even more, the protocol prohibits the disclosure of votes as long as the protocol execution can be stopped by the malicious behavior of a single participant.
2. Whenever votes have been disclosed, even malicious behavior cannot prevent the voting protocol to terminate “correctly”. Informally speaking, Correct Termination means that every cooperative participant will get provable information about the correct voting result.

If only limited anonymity is required, i.e. if there is a trusted party which fulfills the following two requirements: every participant trust this third party (i.e. assumes that this trusted party does not act maliciously) and every participant allows this third party to know his vote (i.e. it does not require anonymity of his vote with respect to this party), there is the following straight forward solution. This trusted third party collects all votes, prevents duplicate votes, and distributes the voting result.

However, we argue that in many voting situations, this limited anonymity is not sufficient and a party trusted by every participant is not always given, i.e. when votes shall not be disclosed to any voting authority. For the smart grid scenario, competing energy utilities and an open market impede the establishment of a third party organization that collects sensitive data.

Therefore, we focus on the significantly more difficult situation where no trusted party is given, and full anonymity is required, i.e. the voter’s identity shall not be disclosed to anybody, not even to a voting authority. Here, a special challenge is to achieve two goals which seem to be contradictory, i.e. guaranteeing that the final voting result contains exactly one uncorrupted vote of each participant and guaranteeing voter anonymity at the same time.

**Problem Description and Requirements**

Fair and secure anonymous voting has to solve a variety of requirements at the same time that seem to be contradictory.

According to Cranor and Cytron (1996), the following requirements have to be met by an anonymous voting schema: