An Anonymous Electronic Voting Protocol with the Latest Decision on Voters’ Intentions

Chun-I Fan
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd.
Tao-Yuan, Taiwan 326, R.O. C.
chunifan@ms35.hinet.net

Wei-Kuei Chen
Chien Hsin Institute of Technology
229, Chien-Hsin Road, Chung-Li
Taiwan 320, R.O.C.
weikchen@ms31.hinet.net

Abstract

In most of the anonymous electronic voting schemes presented in the literature, every voter must decide his intention for a voting before the tally center performs the signing operation on his vote. In these schemes, voters cannot modify or update their intentions embedded in the signed votes even if they have not been sent to the tally center for tallying yet. This paper presents a new anonymous voting protocol to cope with the problem such that voters do not need to determine their intentions until their votes are to be submitted to the tally center for tallying. Our method can be implemented on the electronic voting schemes in the literature to delay the intention decision for voters without affecting the infrastructures of these schemes, and the additional computation is just hashing.

1. Introduction

With the aid of network technologies, many advanced network applications have been proposed to take the advantages of the advanced techniques. One of the network applications is electronic voting (e-voting) [2, 5, 7, 8, 9, 11, 13, 15]. Because of e-voting, a voter can securely and efficiently cast his electronic vote (e-vote) through electronic communication networks. Typically, an electronic voting scheme contains two types of parties (a tally center and a group of voters) and the corresponding voting protocol consists of four stages (initializing, registering, unbinding, and casting). In the initializing stage, the tally center publishes some necessary information for the voting, such as the subject or the candidates of the voting. In the registering stage, every voter registers with the tally center and obtains an e-vote in a blinded version from the tally center. Then, in the unbinding stage, the voter unblinds his blinded e-vote to obtain a valid one. Finally, in the casting stage, every registered voter submits his e-vote with his own intention to the tally center, and then the tally center verifies and publishes these cast votes.

Ideally, a voter does not need to decide his intention until the casting stage. However, in most of the electronic voting schemes in the literature, voters have to determine their intentions before or during the registering stage. It turns out that voters cannot update or change their intentions embedded in their votes after the registering stage even if these votes have not been sent to the tally center in the casting stage yet. In this paper we adopt an efficient mechanism, i.e., dual hash chains, to solve the problem such that every voter can attach his intention to his vote when casting it to the tally center for tallying. Furthermore, the method can be applied to the electronic voting protocols in the literature without affecting their infrastructures, and the extra computation is just hashing.

The rest of this paper is organized as follows. In section 2, we review a typical anonymous electronic voting protocol based on a generic blind signature scheme. The proposed method is presented in section 3. In section 4, the security and privacy of the voting protocol are discussed. Finally, a concluding remark of this paper is given in section 5.

2. Preliminaries

In this section we introduce a generic blind signature scheme and show a typical anonymous electronic voting protocol based on the blind signature scheme.

2.1. A generic blind signature scheme

Two parties, a signer and a group of users, participate in a blind signature protocol. First, a user blinds a plaintext message by performing a blinding process on it. Then, the user submits the blinded message to the signer to request the signer’s signature on the blinded message. The signer signs