Receipt-Free Electronic Voting Schemes for Large Scale Elections

Tatsuaki Okamoto

NTT Laboratories
Nippon Telegraph and Telephone Corporation
1-1 Hikarinooka, Yokosuka-shi, Kanagawa-ken, 239 Japan
Email: okamoto@sucaba.isl.ntt.co.jp
Tel: +81-468-59-2511
Fax: +81-468-59-3858

Abstract

This paper proposes practical receipt-free voting schemes which are suitable for (nation wide) large scale elections. One of the proposed scheme requires the help of the voting commission, and needs a physical assumption, the existence of an untappable channel. The other scheme does not require the help of the commission, but needs a stronger physical assumption, the existence of a voting booth. We define receipt-freeness, and prove that the proposed schemes satisfy receipt-freeness under such physical assumptions.

1 Introduction

Various types of electronic secret voting schemes have been proposed in the last ten years [BGW88, BT94, CCD88, CFSY96, Cha88, FOO92, GMW87, Ive92, JSI96, Oka96, SK94, SK95], and recently *receipt-free* voting schemes are attracting many researchers [BT94, JSI96, Oka96, SK95]. The receipt-free property means that voting system generates no receipt (evidence) of whom a voter voted for, where the receipt of a vote, which proves that a voter has voted for a candidate, could be used by another party to coerce the voter.

Benaloh and Tuinsra [BT94] introduced the concept of the receipt-free voting based on the framework of the voting scheme using higher degree residue encryption [BY86, CF85]. They used a physical assumption, the existence of a *voting booth*. Their scheme allows voters only yes/no voting and is very impractical for large scale elections, since a lot of communication and computation overhead is needed to prevent the dishonesty of voters by using zero-knowledge (like) protocols.

Sako and Kilian [SK94] and Cramer, Franklin, Schoenmaker and Yung [CFSY96] improved the efficiency of the underlying zero-knowledge protocols by using discrete logarithm encryption in place of the higher degree residue encryption used in [BY86, CF85, BT94]. However, their schemes do not satisfy receipt-freeness. Moreover, their scheme allows voters only yes/no voting, and if it is extended to multiple bit voting, their schemes are still inefficient in practice.

Sako and Kilian [SK95] proposed a receipt-free voting scheme based on the Mixnet framework [Cha81]. Their scheme uses a weaker physical assumption, the existence of an *untappable channel*, than the physical assumption, a voting booth, of [BT94]. Their solution also satisfies universal verifiability. However, their scheme allows voters only yes/no voting, and if it is extended to multiple bit voting, their scheme is very inefficient in practice, especially when it is used for a large scale voting system.

Here, an *untappable channel* for V is a physical apparatus by which only voter V can send a message to a party, and the message is perfectly secret to all other parties. A *voting booth* is a physical apparatus for V in which only voter V can interactively communicate with a party, and the communication is perfectly secret to all other parties.

Another practical approach for realizing electronic voting involves the schemes using blind signatures and anonymous channels [Cha88, FOO92, Oka96]. This approach is considered to be the most suitable and promising for large scale elections, since the communication and computation overhead is fairly small even if the number of voters is large. Moreover, this type of scheme naturally realizes multiple value voting, and is also very compatible with the framework of existing physical voting systems.

In addition, this type of scheme is universally acceptable, and this is the most important property in election systems, since otherwise many people should be suspicious about the voting result. We now explain the reason why this framework is universally acceptable. The procedures consist of four stages; the authorizing stage, voting stage, claiming stage, and counting stage. In the authorizing stage, the administrators issue blind signatures. In the voting stage, the voters send their votes with the administrator's signatures to the bulletin board (or counter) through anonymous channels. In the claiming stage, each voter can publicly claim if his/her vote is not found in the board, and in the counting stage, the votes on the board are verified and counted. Here, in the claiming stage, everyone has the chance to raise a claim if he/she is suspicious about the contents of the board, and anyone (e.g., judge) can clearly determine whether the claim is valid or not, by checking the validity of the administrator's signature included in the claim. Thus, at the end of the claiming stage, everyone should be satisfied with the contents of the board (otherwise he/she should have raised a claim and had it resolved), and should be satisfied with the voting result, since all can count the voting result from the contents of the board.

[Oka96] proposed a *receipt-free* voting scheme based on this framework. To our best knowledge, this scheme is the only receipt-free voting scheme that is based on this framework and is considered to be practical for large scale elections.

However, in this paper, we show a security flaw in the receipt-free property of this scheme, and propose some new voting schemes to overcome this security flaw. One scheme requires the help of a group of the voting commission, called the "parameter registration committee" (PRC), and needs the physical assumption of an *untappable channel*. Another scheme does not require the help of such a committee, but needs the stronger physical assumption of a *voting booth*. Since both solutions are still practical, the proposed receipt-free voting schemes are suitable for practical (nation wide) large scale elections.

One of the reasons why [Oka96] had such a flaw in receipt-freeness is that no formal definition and proof of receipt-freeness have been given in [Oka96]. Although Benaloh and Tuinstra [BT94] have defined receipt-freeness, their definition is specific to their framework, and cannot be used in our framework. Therefore, it is very important to define receipt-freeness based on our framework, and to prove that a voting scheme satisfies this definition.

This paper defines receipt-freeness based on our framework, and proves that our modified schemes satisfy receipt-freeness under physical assumptions (i.e., an untappable channel or a voting booth).

This paper is organized as follows: Section 2 introduces the previous voting scheme [Oka96], Section 3 shows a security flaw in [Oka96], and Section 4 gives the definition of receipt-freeness. In sections 5, 6 and 7, our voting schemes are presented and are proven to be receipt-free under physical assumptions.