Information Sciences 181 (2011) 1493–1502

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

New receipt-free voting scheme using double-trapdoor commitment ☆

Xiaofeng Chen [a,*], Qianhong Wu [b], Fangguo Zhang [c], Haibo Tian [c], Baodian Wei [c], Byoungcheon Lee [d], Hyunrok Lee [e], Kwangjo Kim [e]

[a] Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071, PR China
[b] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan University, Wuhan 430079, PR China
[c] School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, PR China
[d] Department of Information Security, Joongbu University, Chungnam 312-702, Republic of Korea
[e] Department of Computer Science, KAIST, Daejeon 305-714, Republic of Korea

ARTICLE INFO

Article history:
Received 18 April 2009
Received in revised form 28 January 2010
Accepted 18 December 2010
Available online 28 December 2010

Keywords:
Electronic voting
Receipt-freeness
Blind signature
Double-trapdoor commitment

ABSTRACT

It is considered to be the most suitable solution for large scale elections to design an electronic voting scheme using blind signatures and anonymous channels. Based on this framework, Okamoto first proposed a receipt-free voting scheme [30] for large scale elections. However, in the following paper, Okamoto [31] proved that the scheme [30] was not receipt-free and presented two improved schemes. One scheme requires the help of the parameter registration committee and the other needs a stronger physical assumption of the voting booth. In this paper, we utilize the double-trapdoor commitment to propose a new receipt-free voting scheme based on blind signatures for large scale elections. Neither the parameter registration committee nor the voting booth is required in our scheme. We also present a more efficient zero-knowledge proof for secret permutation. Therefore, our scheme is much more efficient than Okamoto's schemes [30,31] with the weaker physical assumptions. Moreover, we prove that our scheme can achieve the desired security properties.

1. Introduction

Electronic voting is one of the most significant applications of cryptography. Plenty of research work has been done in the past 20 years. The existing electronic voting schemes can be categorized by their research approaches into three types: schemes using blind signatures [21,30,31], schemes using mix-nets [1,3,10,26,32,33,36], and schemes using homomorphic encryption [7–9,17–19,24,25,35].

One essential property of electronic voting is the privacy of the ballot. If a voter is not required to keep his/her ballot secret, the voter could be coerced by a political boss or an employer with power or money into casting a certain ballot. This will affect the final result of the voting and destroy the fairness of the election. In some sense, democracy cannot be achieved since it depends on a proper and fair administration of the election. Therefore, the content of a vote should never be revealed before the counting stage of the voting. Moreover, a voter could not provide a receipt to any third party to prove that a certain vote was casted.

Benaloh and Tuinstra [8] firstly introduced the concept of receipt-freeness to solve the problems of "vote buying" or "coercion" in the electronic voting. Based on the assumption of a voting booth, they also proposed two voting schemes using homo-

☆ An extended abstract of this paper has been presented at the Eighth International Workshop on Information Security Applications, 2007, pp. 395–409 [16].

* Corresponding author.
E-mail address: xfchen@xidian.edu.cn (X. Chen).

0020-0255/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2010.12.012

morphic encryption. The first one is a single-authority voting scheme and fails to maintain vote secrecy. The second scheme is extended to a multi-authority scheme achieving vote secrecy. However, Hirt and Sako [24] proved that the scheme could not satisfy the property of receipt-free and proposed the first practical receipt-free voting scheme based on homomorphic encryption.

Receipt-free voting protocol based on a mix-net channel was first proposed by Sako and Kilian [36], which only assumes one-way secret communication from the authorities to the voters. However, a significant disadvantage of this protocol is the heavy processing load required for tallying in mix-net schemes.

The only two receipt-free voting schemes using blind signatures were proposed by Okamoto [31], where a single-trapdoor commitment is used to ensure the receipt-freeness. However, the first scheme requires the help of the parameter registration committee and the second one needs a stronger physical assumption of the voting booth.

Our contribution. In this paper, we point out that the traditional single-trapdoor commitment is unsuitable for design receipt-free voting schemes. We then use the double-trapdoor commitment to propose a new receipt-free voting scheme based on blind signatures. Neither the parameter registration committee nor the voting booth is required in the proposed voting scheme. So, it is more efficient and practical for large scale elections than Okamoto's voting schemes [31].

1.1. Related work

Blind signatures, introduced by Chaum [11], allow a recipient to obtain a signature on message m without revealing anything about the message to the signer. Blind signatures play an important role in a plenty of applications such as electronic voting [21,30,28], electronic cash [11,20] where anonymity is of great concern.

Fujioka, Okamoto, and Ohta [21] proposed the first practical voting scheme for large scale elections based on blind signatures. Moreover, Cranor and Cytron designed and implemented a voting system named Sensus based on this scheme. The main disadvantage of [21] is that all voters have to join the ballot counting process. This is because in the counting stage the tally authority needs the help of each voter to open the commitment (ballot) in the bit-commitment scheme. Ohkubo et al. [28] proposed an improved voting scheme based on blind signatures which allowed the voters to walk away once they finished casting their votes. The scheme used a threshold encryption scheme instead of a bit-commitment scheme [27]. However, the scheme is not receipt-free.

Okamoto [30] proposed a new voting scheme based on blind signatures. The scheme tried to use a trapdoor commitment scheme [6] to ahieve the receipt-freeness. The concept of trapdoor commitment (also called chameleon commitment) was first introduced by Brassard, Chaum, and Crepeau [6] for zero-knowledge proofs. In a trapdoor commitment scheme, the holder with a trapdoor knowledge can open a commitment in any possible way in the open phase. Therefore, the scheme satisfies the property of receipt-free only if the trapdoor information is known by the voters. Okamoto [31] then proposed two improved voting schemes which ensure that the voters know the trapdoor information, therefore both of the schemes can satisfy the receipt-freeness. The first scheme requires an untappable channel and a group of parameter registration committee, and the second one requires the stronger physical assumption of a voting booth, where a voter provides a zero-knowledge proof that he/she knows the trapdoor information.

In other electronic commerce protocols such as electronic auction and contract signing, similar concepts were also introduced to prevent the corresponding crimes. For example, Abe and Suziki [2] introduced the idea of receipt-free auctions to prevent bid-rigging in the auction protocol. In the contract signing, if a party can provide a proof that he is capable of choosing whether to validate or invalidate the contract, he may obtain a better contract. Garay et al. [23] first introduced the concept of abuse-free contract signing to solve this problem.

1.2. Organization

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Okamoto's receipt-free voting schemes are revisited in Section 3. The proposed receipt-free voting scheme and its security and efficiency analysis are given in Section 4. The non-interactive zero-knowledge proof required in our voting scheme is presented in Section 5. Finally, conclusions will be made in Section 6.

2. Preliminaries

In this section, we first describe the model and security requirements of electronic voting, and then introduce the notion of trapdoor commitment.

2.1. Electronic voting

The participants of an electronic voting scheme are voters, administrator authorities, and tally authorities. Also, there are four kinds of physical assumption about the communication channel between participants in voting schemes.

- *Untappable channel:* it is a one-way channel between two participants. Communication through an untappable channel is perfectly secret to all other parties.