Journal of Network and Computer Applications 40 (2014) 139–150

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

An electronic voting mechanism for fighting bribery and coercion

Zhen-Yu Wu [a], Ju-Chuan Wu [a], Sung-Chiang Lin [a,*], Charlotte Wang [b]

[a] Department of Information Management, National Penghu University of Science and Technology, No. 300 Liuhe Road, Magong City, Penghu County 880, Taiwan

[b] Institute of Epidemiology and Preventive Medicine, National Taiwan University, No. 17 Xu-Zhou Road, Taipei 100, Taiwan

ARTICLE INFO

Article history:
Received 16 November 2012
Received in revised form
9 May 2013
Accepted 4 September 2013
Available online 4 October 2013

Keywords:
Long-term private key assumption
Anonymity
Bribery
Coercion
Mobility

ABSTRACT

This paper proposes an electronic voting scheme that can be implemented on the current Internet without any secure channel. Under the long-term private key assumption, this scheme not only satisfies most important security requirements proposed before, such as fairness, eligibility, uniqueness, accuracy, anonymity and so on, but also prevents bribery and coercion. Furthermore, the scheme offers voters mobility and convenience so they can securely and easily cast their vote from any location and on any device using a stable Internet connection, which has a potential for raising voter turnout rates and facilitating the voting process.

1. Introduction

Electronic voting is a convenient approach that can be used to significantly reduce the limitations of traditional voting, such as a specific place, a large number of manpower inputs, abundant documentation and related costs. Furthermore, the flourishing rise in the development of IT and the Internet have brought about practical implementations of various electronic paperless mechanisms in many fields and has helped to achieve effective management and utilization in organizations. Obviously, through the use of the Internet, the constraints of physical space and time can possibly be resolved, so voters around the world can vote anywhere in a particular period without concerns about bribery and coercion.

While the potential advantages of electronic voting have been recognized, and many electronic schemes have been developed, from the security perspective, electronic voting is still not widely used in formal elections.

Electronic voting schemes have been in development for several years. Below is an overview of the security requirements of such schemes.

(1) Anonymity: No one can trace the relation between voters and their ballots.
(2) Accuracy: No one can alter, remove, or duplicate a legal ballot.
(3) Eligibility: Voters are allowed to vote after passing the authentication phase.
(4) Fairness: No one can know the immediate result of election before it is officially announced.
(5) Mobility: Instead of being restricted to a specific location, voters can cast their ballots from any location.
(6) Uniqueness: In an election, an eligible voter can vote only once.
(7) Verifiability: All voters can verify if their ballots have been counted correctly.

Most of schemes (Chaum, 1981; Fujioka et al., 1992; Cranor and Crtron, 1997; Jan et al., 2001; Lin et al., 2003; Dini, 2003; Hwang et al., 2004; Chen et al., 2004) use blind signatures (Chaum, 1982, 1983) to attain anonymity, i.e. although the Election Center knows the content of the ballot, it cannot trace the ballot back to the voter due to the blind factor. Furthermore, voters' ballots are each combined with a unique number, giving them uniqueness. Thus, through the final result, voters can verify whether their ballots have been counted correctly with the help of the unique number; and this method has been adopted in several schemes (Nurmi et al., 1991; Fujioka et al., 1992; Cranor and Crtron, 1997; Jan et al., 2001; Lin et al., 2003; Dini, 2003; Hwang et al., 2004). Moreover, accuracy and eligibility are two other mentioned requirements. They can be achieved by the verification and authentication of the election center (Chaum, 1981, 1982, 1983; Nurmi et al., 1991; Fujioka et al., 1992; Cranor and Crtron, 1997; Benaloh and Tuinstra, 1994; Sako and Kilian, 1995; Cramer et al., 1996, 1997; Juang and Lei, 1997; Jan et al., 2001; Lin et al., 2003; Dini, 2003; Hwang et al.,

* Corresponding author. Tel.: +886 6 9264115 5420; fax: +886 6 9277401.
E-mail address: lschiang@gms.npu.edu.tw (S.-C. Lin).

1084-8045/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2013.09.011

2004; Chen et al., 2004; Juels et al., 2005). Each scheme has employed different methods to carry out the mobility and fairness requirements. For example, (Chen et al., 2004) used randomly encryption to achieve fairness, and (Lin et al., 2003) proposed a protocol which is suitable for the Internet to obtain mobility and the other requirements.

Although the above-mentioned schemes satisfied the demands of the electronic voting schemes they were considering, they were not designed to avoid bribery and coercion. Bribery is a situation where an entity, called the briber, provides voters benefits such as banquets, money, or valuables, in exchange for control over their ballots. Coercion is a situation where a person, called a coercer, threatens voters, forcing them to cast their votes according to his instruction. In spite of the fact that their definitions are not the same, the common target of both of these methods is to make the result of the voting follow a briber or a coercer's will, and both of them are regarded as the same problem. By examining the unique number mentioned above, the coercer/briber can verify election results to confirm the voters' ballots, so bribery and coercion can easily happen.

Therefore, Benaloh and Tuinstra (1994) proposed a scheme that could effectively prevent bribery and coercion. In their proposal, they defined a non-coercibility requirement, indicating that their scheme could avoid bribery and coercion. They employed private voting spaces and physical voting booths (as in traditional elections) to prevent other voters from knowing the content of ballots; this allowed voters to vote freely instead of making true their promises to a coercer/briber. Unfortunately, the essential cumbersome physical requirements of this scheme made it impossible to exhibit the special feature, mobility, of electronic voting (Liaw, 2004); in addition, the erection cost of the machines is also too high. In reality, this protocol is not suitable for implementation.

Sako and Kilian (1995) proposed another scheme that could avoid bribery under two assumptions. First, the channel of communication is untappable. Second, the briber cannot coerce the voter to reveal private information. This scheme permits voters to verify their ballots universally and individually. Universal verifiability indicates that each voter can confirm the correctness of the voting results by some information from other voters or the authorities. Individual verifiability indicates that the voter can use his private message or receipt to prove his ballot was counted correctly. Since the private information used to check ballots is unknown to others, the scheme achieves non-coercibility.

Meanwhile, other e-voting schemes with non-coercibility were proposed. Cramer et al., 1996 used multiple voting authorities in their scheme. Gennaro and Schoenmakers made improvements on the time complexity and communication complexity of the Cramer et al. (1997) scheme. Juang and Lei (1997) showed that the early research had vote-buying problems. Though these schemes prevented bribery effectively, they needed assumptions, i.e. cumbersome physical requirements, untappable channels, and specific hypotheses. Hence, after 2000, instead of emphasizing non-coercibility, most researchers, like Jan et al. (2001), Lin et al. (2003), Dini (2003), and Hwang et al. (2004), stressed proposals of a practical mechanism that could work well in the present network environment.

Chen et al. (2004) proposed a scheme that could avoid bribery and coercion and at the same time run on the current Internet with SSL. It barred voters from verifying their ballots so as to prevent the briber from confirming the voting results. In other words, voters were unable to determine if their ballots had been counted correctly. Hence, the scheme incorporates a Supervisor Center to help the voter monitor the counting stage. When a vote is to be announced, the two entities, the Election Center and the Supervisor Center, must work together because of the decrypting information shared between the two. Consequently, the Election Center will not be able to alter, remove, or duplicate the ballots. Nevertheless, this scheme cannot achieve non-coercibility because of an important value, called a temporary pseudonym, used as proof that a legal voter can be extorted or bought by a coercer/briber, thus creating another act of bribery and coercive behavior. Additionally, the scheme has complex time complexity with regard to computation since each ballot requires two exponent operations at the time of the count.

Recently, Juels et al. (2005) proposed a scheme that focused on resisting coercion. In their paper, they clearly defined three types of coercion attacks. The first was called a randomization attack, where the attacker forces a voter to submit randomly the composed balloting material. The second type is a forced-abstention attack, where the attacker absolutely forbids the voter to vote, and the third is a simulation attack, where the attacker casts a ballot using pre-obtained private voter information. In order to avert these three kinds of attacks, Juels's scheme allowed the voter to create a legal credential resembling the one created by the Election Center. However, only the vote of the Election Center-made credential can be counted in the counting phase. This way, coercers would be uncertain regarding the credential. Even if a vote was cast according to the coercer's wish, the coercer could not discern it. Spontaneously, these attacks fail. Juels et al.'s idea seemed great, but it requires a great deal of computation (Weber, 2006). Therefore, Smith (2005), and Schweisgut (2006) improved the efficiency of the Juels et al. scheme.

Although there are many methods that can be used to prevent bribery and coercion problems in the schemes introduced above, unfortunately, they always need some strong assumptions or requirements. For instance, some schemes must rely on an untappable channel, which exists only in theory (Fujioka et al., 1992; Cranor and Crtron, 1997; Benaloh and Tuinstra, 1994; Sako and Kilian, 1995). The other schemes have cumbersome physical requirements, e.g. physical voting booths to prevent bribery and coercion (Benaloh and Tuinstra, 1994; Sako and Kilian, 1995; Cramer et al., 1996, 1997); therefore, they are unable to achieve the mobility requirement. In order to overcome the above shortcomings, we propose a practical and efficient scheme to solve these problems.

The rest of the paper is organized as follows: Section 2 introduces the techniques adapted in this work. Section 3 contains our proposed e-voting scheme, including the entities, the process adopted, and detailed procedures, and a security analysis is presented in Section 4. Future works are discussed, and conclusions are drawn in Section 5.

2. Preliminary

In this study, two techniques were adapted, the first one is Mixnet, in which a mixer (Abe, 1998) jumbles up the order of the messages sent and received, causing the receiver to not be able to trace the relation between the message and its sender. And the second one is a blind signature, whose main function is to let a signer sign without knowing the content of the message. Thus, even if verifiers confirm its validity, signers still don't know in whose place they signed the message. These two techniques play a very important role in enabling our e-voting scheme to meet the requirements of a secret ballot.

2.1. Mixnet

The idea of Mixnet was first proposed by Chaum (1981). The main function of Mixnet is to allow a set of senders to