Journal of Network and Computer Applications 42 (2014) 39–44

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Constructing credential-based E-voting systems from offline E-coin protocols

Víctor Mateu *, Francesc Sebé, Magda Valls

Department of Mathematics, Universitat de Lleida, Av. Jaume II 69, E-25001 Lleida, Spain

ARTICLE INFO

Article history:
Received 21 June 2013
Received in revised form
14 November 2013
Accepted 13 March 2014
Available online 26 March 2014

Keywords:
Cryptography
E-coin
E-voting

ABSTRACT

Mu and Varadharajan proposed a remote voting paradigm in which participants receive a blindly signed voting credential that permits them to cast a vote anonymously. If some participant tries to cheat by submitting more than one vote, her anonymity will be lifted. In the last years, several proposals following this paradigm, including Mu and Varadharajan's, have been shown to be cryptographically weak. In this paper we first show that a recent proposal by Baseri et al. is also weak. After that, we give a general construction that, employing an offline e-coin protocol as a building block, provides an anonymous voting system following the aforementioned paradigm.

1. Introduction

In the last years, traditional paper-based voting systems are being severely judged after having found, in some cases, evidences of misbehaving parties. The confidence on the fairness of an election is getting lower as some information about suspicious results gets filtered. The use of information technologies can help to revert this trend by adding security mechanisms that permit us to check the correctness of the process. Other advantages, like avoiding the need for voters to move to the polling station, are also possible.

Remote voting protocols permit an election to be carried out through communication networks without requiring the participants to move to the polling place. Such systems reduce the economic cost of an election and permit the ballots to be tallied in a fast and error-free way. A remote voting system has to provide some security properties:

Privacy: The identity of a voter cannot be linked to her vote. This is a key aspect for any election because it allows the voters to freely decide the option they prefer without making it public. There are some related properties like vote selling prevention or coercion resistance that are also desirable. In the first one, voters are not able to prove how they voted, despite being able to provide evidence that they have cast a vote. The fact that there is an evidence of their votes would make them easier to be coerced. Some coercion-resistance techniques provide tools that allow voters to cheat the coercers. Coercers are tricked into thinking that the voter has behaved under coercion.

Integrity: The result of the election cannot be altered in any way. Each voter should be confident about her vote being properly tallied. Additionally, she can be sure that the whole processing of the votes has been performed correctly. This means that all the votes have been cast as they were intended to be, and after that, the votes have not been altered during their processing. Integrity also ensures that only voters in the electoral roll are able to cast a vote, and that no more than one vote from each voter will be tallied.

Robustness: This property refers to the strength of the system against attacks. The system should be able to face situations in which some voters or authorities are misbehaving so as to try to disrupt the process.

Verifiability: The verifiability provided by traditional elections involves trusting in audit parties. This way has proven not to be successful as the confidence in some electoral processes has been decreasing in the last several years. By contrast, electronic elections allow the voters to verify the integrity of the voting process. There are two levels of verifiability:

- *Individual verifiability:* Each voter can check whether her vote has been properly received and tallied.
- *Public verifiability:* Anyone can check whether the reception and the tallying of all the votes have been performed properly.

* Corresponding author. Tel.: +34 973 702774.
E-mail addresses: vmateu@matematica.udl.cat (V. Mateu), fsebe@matematica.udl.cat (F. Sebé), magda@matematica.udl.cat (M. Valls).

http://dx.doi.org/10.1016/j.jnca.2014.03.009
1084-8045/

An election is end-to-end verifiable when all the phases of the election can be verified.

In the last decades, the design of secure e-voting systems has attracted the attention of the cryptographic community. Indeed, the fulfillment of the aforementioned security properties requires the use of cryptography. E-voting protocols can be classified into three main paradigms: *mix-type voting*, *homomorphic tallying* and *blind signature-based*. Our proposal is bounded on this last paradigm. More precisely, this paper is mainly devoted to provide a novel credential-based e-voting system, which exploits the usage of an underlying e-coin system. This e-voting protocol is proven to fulfill the security requirements, assuming that the e-coin system guarantees unforgeability and untraceability. Besides, we also show that a recent proposal by Baseri et al. is unsecure, by highlighting a security flaw.

This paper is organized as follows. Section 2 provides an overview of the main paradigms of e-voting systems, focusing on the proposals presented in the last decade and how security concerns have been addressed. Section 3 details a security weakness of Baseri et al.'s proposal. In Section 4 we review the main features of offline e-coin systems. Section 5 presents our proposal for building a credential-based e-voting system taking advantage of the usage of an e-coin system. Security issues are addressed in Section 6 while Section 7 includes a performance analysis. Finally, conclusions are sketched in Section 8.

2. E-voting paradigms

According to the employed cryptographic techniques, e-voting systems can be classified into three paradigms: *mix-type* (Peng, 2011; Peng et al., 2011; Sebé et al., 2010), *homomorphic tallying* (Kiayias and Yung, 2002; Peng et al., 2004) and *blind signature-based* (Fujioka et al., 1993; Ohkubo et al., 1999).

In mix-type protocols, the voter encrypts her vote into a ballot, signs it, and sends it to the polling station. Once the polling station has received all the ballots, it shuffles and re-encrypts them so as to break the link between ballots and voters. This shuffling and re-encryption operation is called a *mixing*. The polling station has to prove that the mixing has been performed properly by publishing a zero knowledge proof of correctness. Finally, the polling station decrypts the ballots and publishes the results.

Another approach is the homomorphic tallying paradigm. In this case, the voters encrypt their votes using an homomorphic public key cryptosystem. After that, each voter signs her ballot and sends it to the polling station together with a zero knowledge proof which proves that her ballot is a correct encryption of one of the candidates. The polling station checks the proof of each ballot prior to storing it. When all the ballots have been received, the polling station homomorphically aggregates them and decrypts the resulting ciphertext. The result of the election is then obtained from the decrypted value.

The mix-type and the homomorphic tallying paradigms require the use of complicated zero knowledge proofs to provide integrity and public verifiability. In the particular case of homomorphic tallying, the cost of the required proofs restricts them to be only usable for elections with a small range of candidates.

Fujioka et al. (1993) and later Ohkubo et al. (1999) proposed a paradigm using blind signatures. In this blind signature-based paradigm, a participant composes her vote, encrypts it and next authenticates herself to a trusted authority (the authentication server) who manages the electoral roll. If the authentication is successful and the participant has not voted yet, the authentication server blindly signs (Chaum, 1985) the participant's vote. After that, the participant casts her signed vote through an anonymous channel. The voting platform will only accept votes that have been signed by the authentication server. Once the voting period concludes, votes are decrypted and tallied. This approach does not require the use of complicated zero knowledge proofs but provides only individual verifiability. A voter can only verify that her vote has been counted while she has no evidence about correctness of the rest of the ballots other than the signature from the authentication server. If the authentication server is completely trusted, public verifiability can be considered to be achieved to some extent.

Radwin (1995) proposed a variant of this paradigm in which the voters have to move to the voting authority office (acting as an authentication authority) and ask for a pseudonym. Later, each voter will attach her blindly signed pseudonym to her vote and will send it to the polling station through an anonymous channel. If some voter tried to cheat by casting two or more votes, her identity could be disclosed. In this proposal, the vote is not blindly signed. Instead, a credential is needed which has been blindly signed by the authentication server. By means of this credential the voter can demonstrate that she appears in the electoral roll. This approach increases the robustness of the protocol against attacks to the authentication server because the blind signature can be performed in a non-capital moment (before the election begins).

Mu and Varadharajan (1998) proposed an improvement over the variant of Radwin (1995) in which the interaction between the authentication server and the voters can be carried out remotely. The proposal of Mu and Varadharajan (1998) presents several security flaws as shown in Chien et al. (2003), Lin et al. (2003), Yang et al. (2004) which allow dishonest voters to cast several votes without being detected. Moreover, the anonymity of any voter could be lifted by a dishonest authentication server. Lin et al. (2003) and later Yang et al. (2004) proposed some improvements to the scheme which they claimed to be secure. Hwang et al. (2005) showed a weakness on the system proposed by Lin et al. (2003) in which an authentication server could determine the identity of the voter related to a given voting credential, and gave a new protocol to solve this issue. Rodríguez-Henríquez et al. (2007) found a vulnerability in the proposal by Hwang et al. (2005) that also affected the proposal by Yang et al. (2004) which allows, in some particular cases, the authentication server to prevent some voters from casting a vote. Rodríguez-Henríquez et al. (2007) also presented a new proposal that Asadpour and Jalili (2009) proved to be weak in the sense that a coalition of two dishonest voters would be able to vote several times. Baseri et al. (2011) described some security flaws on the improvement proposed by Asadpour and Jalili (2009), and presented a new proposal.

In this paper we first show that the contribution by Baseri et al. (2011) has a security flaw that permits any entity to compute the private key of the authentication server given only the public setup parameters.

After that, we give a general construction, using off-line e-coin systems, that provides a voting system based on blindly signed credentials with identity disclosure in case of double voting. The advantage of this construction is that its security is proven to hold on the security of the underlying offline e-coin protocol that, in most proposals, has been formally proven. As a result, our construction does not require the design of novel ad hoc cryptosystems that, in all the previous works, have turned out to be weak.

3. Baseri et al. scheme and its failure

The scheme of Baseri et al. (2011) consists of an RSA-type cryptosystem whose security holds on the assumed intractability of the *integer factorization*, *RSA*, *discrete logarithm* and *representation* problems.