Available online at www.sciencedirect.com

ScienceDirect

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

Blinded additively homomorphic encryption schemes for self-tallying voting

Jérôme Dossogne [b,*], Frédéric Lafitte [a]

[a] Department of Mathematics, Royal Military Academy, Brussels, Belgium
[b] Département d'Informatique, Université Libre de Bruxelles, Brussels, Belgium

ARTICLE INFO

Article history:
Available online 19 August 2014

Keywords:
Self-tallying
e-Voting
Homomorphism
Blinding
Helios

ABSTRACT

In this paper, we propose a self-tallying election protocol based public key homomorphic encryption. The additive homomorphism allows a set of participants (voters) to publish an encrypted value (ballot) and to compute the encrypted sum of all these values based on their ciphertexts. Our scheme has the particularity that anyone can decrypt the sum, but only once all participants have contributed to its computation. More precisely, the sum can be decrypted at all times, but remains blinded until all participants have contributed their vote, which contains a share of the unblinding key. Additionally, we propose an adaptation of Helios in order to provide self-tallying.

1. Introduction

With the increased use of electronic voting around the world, for governmental as well as corporate applications (Burnand, 2010; Gonzalez, 2012; Rfi.fr, 2012; Sensei Enterprises and I, 2004; Vabariigi Valimiskomisjon, 2011; Weber and Taglioni, 2011), concerns arise regarding the security of the implementations and of their underlying schemes. While the process of validating the implementation (e.g. source code, hardware, ...) is still relevant (Ryan, 2006), recent advances aim to achieve "end-to-end verifiability" (E2E) (Clark, 2011; Kramer and Ryan, 2011; Yi et al., 2011), i.e. allowing auditors to validate the system without relying entirely on its implementation. Using cryptographic proofs, receipts, credentials (Juels et al., 2005), it is possible to provide certain guarantees to each participants regarding the requirements of the election (correctness, ballot privacy, coercion-freeness (Dossogne et al., 2011a), ...). Another step in this direction would consist in allowing every participant (organizers as well as voters) to audit the system. This would diminish the need to trust other participants (such as official auditors). In this paper, we intend to focus on this aspect, referred as self-tallying, by providing the voters with the capacity to compute the tally revealing neither the content of their individual vote nor the content of partial results of the election.

1.1. *Objectives*

In this paper, we investigate a generic self-tallying blinding homomorphic technique and its application to choose "1-out-of-l" elections. The technique is generic in the sense that it can be based on most encryption algorithms, without modifying their implementation.

This lead us to the second objective which consists in illustrating the genericity of the technique on both the Elgamal and the Paillier encryption scheme. Notice that Elgamal is originally multiplicatively homomorphic compared to Paillier which is naturally additively homomorphic.

* *Corresponding author.*
E-mail addresses: jdossogn@ulb.ac.be (J. Dossogne), frederic.lafitte@rma.ac.be (F. Lafitte).

http://dx.doi.org/10.1016/j.jisa.2014.07.002
2214-2126/© 2014 Elsevier Ltd. All rights reserved.

A third objective is to apply this technique to an existing voting scheme (of which an implementation exist and which has already been used large scale practical situation, namely Helios).

1.2. Outline

Section 4 introduces the notations, the assumptions and describes the protocol in a generic way (i.e. without instantiating the public key algorithm). Section 5.1 presents the scheme based on Elgamal, section 5.2 based on Paillier and section 5.3 present an adaptation of the Helios election voting system by adding a self-tallying mechanism. We conclude in section 6.

2. Related work

Homomorphic encryption has been applied in different ways to electronic voting, sometimes together with threshold cryptography. However this is not sufficient for self-tallying as it relies on a trusted authority to decrypt the tally.

Related work includes (Groth and Juels, 2004; Li et al., 2012) who improved upon the scheme of Kiayias et al. (2002) where the notion of self-tallying is introduced. In late 2012, Li et al. published an independent work (Li et al., 2012) with similar self-tallying or "blinding" features based on DC-net (Dining Cryptographer Network) (Chaum, 1988). (Li et al., 2012) presents a scheme for referendum ("yes/no" voting) that requires the existence of a complete bidirectional graph of absolutely secret communication channels amongst the voters (2 by 2) as required by the DC-net.

Compared to (Li et al., 2012), our first proposal is not completely decentralized and thus does not require such a graph nor the setup of a DC-net. Furthermore, our proposal is directly oriented towards "1-out-of-l" candidates type of election instead of referendums.[1]

(Li et al., 2012) leverage the complete graph of communication channels as well as the DC-net deployed on it to provide anonymity as well as other interesting properties for such a voting scheme (such as internal verifiability as described below).

For instance, the scheme allows for internal universal verifiability. This means that only voters can perform any form of audit to control the validity of the ballots. In our proposal, we suggest a different approach allowing anyone (voters, authorities, third parties, …) to perform verification on the elections.

In Li et al. (2012), such audit is performed by an interactive proof of ballot validity protocol (verify the assertion "ballot contains -1 or 1" without revealing if its "-1" or "1"). This protocol needs to be performed for each ballot between each voter and every other voters (for a single ballot, between the author of the ballot and all the other voters who wish to audit the ballot) using these distinct channel. If n is the number of voter, the scheme requires n $(n-1)$ communication channels and requires to perform, for instance, $n(n-1)$ execution of the verification protocol. The complexity (number of computations, interactions by and between voters, …) is thus dependent on the number of voters. These characteristics and requirements makes their proposal, as mentioned by the authors, suitable only for small scale referendums. In our proposal, we adopt a more asynchronous and indirect approach. A voter is not required to execute any protocol a number of times dependent on the number of other participants meaning that the cost for each participant to participate to the election (cast his ballot) is not dependent on the number of voters. However, to audit the ballot of others, an auditor still has to perform the verification algorithm on each of the other ballots, therefore the complexity of the audit is still linear in the number of ballots and thus on the total number participants.

Both proposals (Li et al., 2012's and ours) use similar approach to blind the votes. However, since (Li et al., 2012) focus their scheme on referendum and thus limits the number of choices/candidates available to the voter to "yes/no", it allows them adequately to use simpler mathematics (encoding of a ballot is simply "yes $=1$", "no $=-1$" and an addition is enough to blind the vote whereas we perform a multiplication for the blinding and the encoding of the ballot is done by exponentiation).

The scheme proposed in Li et al. (2012) occurs in several rounds. Cheating is detectable in any round and requires the scheme to be restarted which limits the robustness of the scheme. Identification of a single cheater (called "solving dispute") can be done in at most n restart (with $\sum_{i=n}^{2} i = (n+1)n/2 - 1$ as the maximum number of times the whole scheme has to be restarted from scratch in case of all but one cheating participants). However, to evade identification, a cheater can cheat up to $n-1$ times which makes the scheme suitable mostly for yes/no referendum with only a small amount of participants and an even smaller amount of dishonest participants. In our proposal, the cheater is identified after cheating only once.

Li et al. (2012) claims to have unconditionally perfect ballot secrecy using their scheme (Kiayias et al., 2002). This ballot secrecy is provided by the common approach to ballot binding between our proposal and their scheme. However, suggesting a distributed setup for their construction, the requirements to deploy the infrastructure to obtain this unconditional ballot secrecy are relatively hard to satisfy. The authors suggest for instance that each participants exchange with every others a DVD containing encryption keys via postal means. Thus, the "unconditional" aspect of their and our proposal relies in fact in underlying trustworthiness hypothesis (either of a key generation server, of a postal office, …).

3. Material and methods

Our proposal allows the reuse of existing implementation to provide an additional property called blinding. It can be applied to several context and is therefore illustrated using two different encryption scheme (allowing the reader to directly apply the contribution in either of both cases) namely El Gamal (1985) and Paillier and Stern (1999) which are

[1] While some aspect of their referendum scheme are not detailed, the scheme and requirement up to the proof of validity is relatively clear. Before analyzing their referendum scheme, the authors mention the possibility to extend their scheme beyond the "yes/no" type of election without, however, providing a detailed presentation of such a result nor the corresponding security analysis.