A Secure Multi authority Electronic Voting Protocol based on Blind Signature

Sujata Mohanty
Dept. of Computer Science and Engineering
National Institute of Technology
Rourkela, India
sujata.nitrkl@gmail.com

Banshidhar Majhi
Dept. of Computer Science and Engineering
National Institute of Technology
Rourkela, India
bmajhi@nitrkl.ac.in

***Abstract*— Electronic voting is an emerging application of cryptographic protocols. In this paper we propose a simple multi-authority electronic voting protocol based on blind signature, which meets security requirements such as privacy, accuracy, verifiability, anonymity, fairness and uniqueness. In this scheme bit wise XOR operation is used for vote generation and blind signature scheme for its authentication. The proposed scheme is secure as none of the authority involved in this scheme can have sufficient information to link a vote to corresponding voter.**

Keywords- electronic voting, blind signature, cryptography, anonymity, verifiability

I. INTRODUCTION

With the rapid development of the Internet and the massive improvements in cryptographic and security technologies, electronic voting is a promising concept to afford convenience to voters and to increase election turnouts. In all democratic systems, it is essential that the voting system must provide privacy, security and fairness during the election process. Electronic voting is an excellent mechanism that does not require geographical proximity of voters, i.e. the voters need not come to the poll station to participate in voting process [5, 6, 7]. A secure and trusted electronic voting protocol must satisfy the following security requirements [3, 4].

- Eligibility: Only eligible or legitimate voters can take part in the election.
- Accuracy: The voting authority can not alter vote of any voter.
- Anonymity: No one, even the voting authority can link a vote to the voter who cast it.
- Privacy: The privacy of the voter must be preserved.
- Uniqueness: Each voter can cast vote only once.
- Fairness: Intermediate results of the election process should not be leaked out.
- Verifiability: Each voter should ale to be verify his casted vote is considered in the counting process.
- Uncoercibility: Each voter must be able to cast the vote according to his/her own conscience and no voter can be forced to vote in a particular way, which will prevent vote buying and selling.

In this paper we propose a simple anonymous, multi-authority electronic voting protocol based on Chaum's blind signature and bit-wise XOR operations. This proposed scheme is an enhancement over the Yes/No e-voting protocol suggested in [2].It is verified that the proposed scheme meets security criteria such as anonymity, verifiability, privacy, fairness and accuracy.

The rest of the work is organized as follows. In Section 2 we present the general architecture of the proposed scheme. Section 3 shows the security analysis of the proposed scheme. Finally conclusion and future work are made in Section 4.

II. THE PROPOSED SCHEME

The proposed scheme is an improvement over the Yes/No electronic voting protocol as in [1]. We propose an e-voting protocol which provides any number of voting options, thereby, suitable for a large scale general election. The notations used in the proposed scheme are described in Table 1.

The proposed scheme consists of four parties: a set of N voters, Authority of authentication (U_1) which issues blind signature of vote to legitimate voter V_i, Authority of Certification (U_2) which registers voters and an Authority of Publication which counts votes and publishes election result. The entire process composed of three phases: registration, voting phase and counting phase. Fig. 1 shows the communication between various authorities and voters. The phases of the proposed protocol are described below.

A. Registration Phase

This is the initiation of the voting protocol and proceds as follows.

978-0-7695-4058-0/10 $26.00 © 2010 IEEE
DOI 10.1109/ACE.2010.82

TABLE 1. Notations used in the proposed scheme

Notations	Descriptions
V_i	Voter *i*, *i*=1 to N
v_i	Vote of V_i, *i*=1 to N
Z_n	{0, 1, 2,..,n−1}
Z_n^*	{0, 1, 2,..,n−1}, n is prime
$S(P_i)$	Signed vote
N	Total number of votes
m	Total number of options

a) The voters willing to participate in election must register himself in the Authority of certification (U_2) before the election date.
b) The U_2 checks necessary details of each voter and gives a digital certificate to each legitimate voter V_i along with a unique string B_i requesting him to keep B_i secret.

B. Voting Phase

The activities of this phase are described below.

a) Each voter V_i generates a random string S_i whose length is same as B_i.
b) Then the voter V_i constructs his vote v_i as per a simple method. If he/she chooses for option j, then the j^{th} bit of the sequence $\mathbf{S}_i$ is set as "1" and all the remaining bits set to zeros. The constructed vote v_i is given as, $v_i = B_i \oplus S_i$
c) After constructing vote, each voter V_i randomly chooses a bit sequence $C_i \in F_2^N$ and computes $P_i=v_i \oplus C_i$. Then the voter sends P_i to the authority of authentication for a blind signature and sends C_i to the authority of authentication.
d) The authority of authentication puts a signature on P_i and sends it to the voter. The detail of the blind signature scheme is given in Section 2. Each voter can get the signature $S(P_i)$ of his vote and submits the signed vote to the authority of publication.
e) The authority of certification computes B as

$$B=B_1 \oplus B_2 \oplus B_3 \oplus .. \oplus B_N$$

where $B \in F_2^N$. Then sends B to the authority of publication.
f) The authority of authentication computes C as

$$C=C_1 \oplus C_2 \oplus C_3 \oplus \ldots \oplus C_N$$

where $C \in F_2^N$. It then sends C to the authority of publication.
g) The authority of publication verifies the validity of different votes by deciphering $S(P_1)$, $S(P_2)$, . . , $S(P_N)$ obtaining P_1, P_2, …., P_N. Then it computes P as follows.

$$P=P_1 \oplus P_2 \oplus P_3 \oplus \ldots \oplus P_N$$

Then it computes $P \oplus C$ which is equivalent to V, which is shown in proof 1. Then it computes the value of $V \oplus B$.

C. Counting Phase

The authority of collection has the following set of data: B, P, C and V. Then it computes $S=V \oplus B$. The number of votes for each option is computed as follows.
The number of votes for option 1, option 2, option 3,. . , and option m are n_1, n_2, n_3, n_m respectively. Hence,

$$n_1+n_2+n_3+\ldots+n_m=N,$$

where N is the total number of votes. It takes a String S_k having same length as string S_i. The number of votes for option j (j=1 to m, m<N) will equal to
N− {(n_1 times XOR of string S_{k1}) (n_2 times XOR of string S_{k2}) (n_3 times XOR of string S_{k3})… (n_m times XOR of string S_{kj}). Here S_{k1}indicates the first bit of string S_k is 1 and rest bits are zeros. Similarly, S_{k2} indicates the 2^{nd} bit of string S_k is set as 1 and rest are zeros, and so on.

Finally, the authority of publication displays the value of C and the sequence P_1, P_2, …., P_N in the bulletin board along with the voting result so that each voter can verify that his/her vote is counted properly.

III. Security Analysis of Proposed Scheme

In this proposed scheme, the voter constructs his/her vote by randomizing his/her voting option by a random string B_i provided by the authority of authentication. The constructed vote v_i is blinded by the voter with a random bit string C_i. Then the voter requests blind signature of the constructed vote to the authority of certification. After obtaining the signature of the vote, the voter sends the signed vote to the authority of collection. The authority of collection collects all votes, verifies their validity, counts the votes and publishes the result of the election.
In this section we will verify that the proposed protocol satisfies the basic requirements to any electronic voting system.

- *Anonymity:* None of the three authorities that participate in the election process can determine the vote of any voter. The authority of certification knows the bit sequence C_i but does not know B_i. So it is impossible to determine v_i from only C_i. Similarly, the authority of authentication only knows the bit sequence B_i. He cannot determine the content of vote as C_i is unknown to him. Finally, the authority of collection knows the value of P, C, S and B. Even if the value of S is available to the authority of collection, which is the XOR of all individual voting options, it is impossible to trace the vote v_i to his/her vote. It is impossible to know vote v_i of a voter from all these available values. Hence anonymity is maintained in our e-voting protocol.

- Verifiability: Each voter Vi can verify that his/her vote has been counted in the election as the bit sequence P_1, P_2,., P_N and C are displayed in the bulletin board. The voter calculates $P_i=v_i \oplus C_i$. If the value of Pi calculated

by the voter is same as the value displayed in the bulletin board, then it is verified that the vote is counted correctly in the election process.

- *Uniqueness:* Each voter cannot vote more than once. As each voter is supplied with only one value of Bi, he can construct only one legitimate vote. Also the voter has to submit the value of C_i to the authority of certification. So a voter can not cast more than one vote. Hence uniqueness is achieved.

- *Privacy:* Privacy of voter is maintained as the concept of blind signature is used. The authority of certification provides blind signature of vote v_i without knowing its content. Also none of the trusted party can know the content of the vote.

- *Unlinkability:* No one can link or identify the vote with the voter.

- *Uncoercibility:* Nobody can force the voter to cast vote against their will. This is because when the vote v_i is constructed, the bit string selected by the voter is randomized by another bit string B_i is given by the authority. Even if someone force to choose the bit string Si in a certain way, he cannot know the content of the vote as vote is constructed by $B_i \oplus S_i$. This prevents vote buying and vote selling.

Proof 1: The authority of collection computes P⊕C which is equals to XOR of all votes (V)

$$P \oplus C = [P_1 \oplus P_2 \oplus P_3 \oplus \ldots \oplus P_N] \oplus [C_1 \oplus C_2 \oplus C_3 \oplus \ldots \oplus C_N]$$
$$= v_1 \oplus v_2 \oplus v_3 \oplus .. \oplus v_N = V,$$
$$\text{as } P_i = v_i \oplus C_i$$

Advantages of the proposed scheme are:

a) Suitable for large scale general election as there are more options available and there is no provision of only two options: either Yes or No.

b) The bit length of the random bit sequence S_i generated by voter for the construction of vote is independent of total number of voters. That implies if the number of voters is increased, we do not have to increase the bit length of S_i. Hence complexity of computation is reduced.

The complexity of this scheme is much less as XOR operation is used in most of the cases. None of the three authorities have enough information that they could know the ballot's content or can link the ballot with the corresponding voter. Hence this scheme is very much secure.

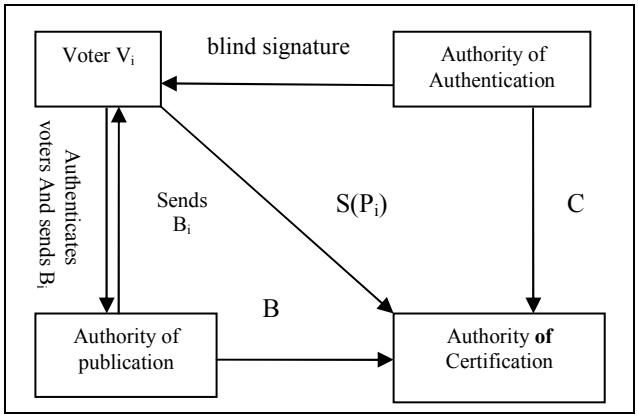

FIGURE 1. Topology of the proposed scheme

IV. CONCLUSION AND FUTURE WORK

In this paper, we present a simple, multiparty, anonymous electronic voting protocol that satisfies the core properties of a secure voting system. None of the three authorities have enough information that they could know the ballot's content or can link the ballot with the corresponding voter. Hence this scheme is secure. Here also a voter can choose among multiple options. Hence it can be applied to general election.

REFERENCES

[1]. B. C. Pardos, A. H. Encinas, S. H. White, A. M. Rey and G. R. Sanchez, "A Simple Protocol for Yes-No Electronic Voting", IJCSNS International Journal of Computer Science and Network Security, Vol. 7, No. 7, July 2007.

[2]. D Chaum. "Blind Signatures for Untraceable Payments", Advances in Cryptology Proceedings of Crypto 82, pp 199-203, 1983.

[3]. J.L Lin, H Lin, C. Chen, C. Chang, " A Multiauthority Electronic Voting Protocol based upon a Blind Multisignature Scheme", IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No 12, December, 2006.

[4]. Chun Li, Min s Hwang, Yan C Lai, " A verifiable Electronic voting Scheme over Internet", 6th International conference on Information Technology, IEEE Computer Society, 2009.

[5]. Liaw HT. "A secure electronic voting protocol for general elections". Computers and Security 2004;Vol-23: pp- 107–19.

[6]. Martin Hirt and Kazue Sako, "Efficient receipt-free voting based on homomorphic encryption," In Proceeding of EUROCRYPT '00, LNCS 1807,pp.539–556,2000.

[7]. Lin, M. Hwang, C. Chang, Security enhancement for anonymous secure e-voting over a network, Comput. Stand. Interfaces 25 (2) (2003), 131–139.