Implementation of e-Voting system using new blinding signature protocol

Prakash Kuppuswamy[1], Omar Saeed Ali Al-Mushayt[2]
Department of Computer Engineering & Networks, Jazan University, KSA
College of Computer science & Information system, Jazan University, KSA

Abstract: *Electronic voting has attracted much interest recently and a variety of schemes have been proposed. Generally speaking, all these schemes can be divided into three main approaches: based on blind signature, based on mix networks and based on homomorphism encryption. Schemes based on blind signature are thought to be simple, efficient, and suitable for large scale elections. With the help of networking and internet we can easily replace the traditional election process with the electronic voting system. In the proposed cryptographic technique we are implementing new blind signature based on linear matrix function and modulation. The new scheme fully conforms to the requirement of large scale election such as privacy, fairness and security. The voter's private key for digital signature is protected by using linear square matrix based on block cipher algorithm and it can be make many combination so that only valid voter can use it. In the cryptography history, block cipher used in symmetric key algorithm, this is first time we are introducing block cipher as a public key algorithm.*

Keywords: *E-voting system (EVS), Blinding, Signing, Unblinding, Block cipher, Ballot, Authenticator, Registrar etc.,*

I. Introduction

The traditional process of election is quite tedious, time consuming, cumbersome because voter's come in person and vote at pre-assigned voting booth. But in era of networking and internet, we can overcome this problem by using the electronic voting system (EVS). EVS is expected to make our modern social life more convenient, efficient, inexpensive and. without disturbing the daily routine life. It is possible by voter to vote to its desire candidate in the National Election Day from his home or at working place.[1]

Electronic voting has attracted much interest recently and a variety of schemes have been introduced. Some papers [11, 12] give a good general introduction to different e-voting approaches, their mechanisms, security requirements, and so on. In this paper, we will not repeat them, but only focus on three security properties, receipt-freeness, and individual verifiability and no-cheating, which are the focuses of this paper.

Each voter encrypts his/her vote and then gets the encryption blindly signed by a validator. The voter un-blinds the signature and sends the encryption and the signature to a voting authority via an anonymous channel, for privacy. At the end of the voting period the authority posts all encrypted votes and their blind signatures on a bulletin board .Each voter checks that his/her encrypted vote is on the board and then sends the decryption key to the authority, also anonymously. The authority decrypts the votes and posts the tally on the board. An advantage of blind signature election schemes is that their communication and computation overhead is fairly small even when the number of voters is large.

Many extensive researches on electronic voting have been conducted and therefore there are now extensive lists of security requirements available. Without these security requirements, numerous opportunities for a widespread fraud and corruption may exist. In order to overcome these problems, an election should have the following requirements. [8, 9]

- Accuracy
- Convenience
- Flexibility
- Invulnerability
- Privacy
- Verifiability
- Fairness

The basic idea is the following. A sends a piece of information to B which B signs and returns to A. From this signature, A can compute B's signature on an a priori message m of A's choice. At the completion of the protocol, B knows neither the message m nor the signature associated with it. The purpose of a blind signature is to prevent the signer B from observing the message it signs and the signature; hence, it is later unable to associate the signed message with the sender A.

In this paper, we will propose a simple and efficient method to improve individual verifiability to the scheme, meanwhile maintaining all other security properties. The proposed blind signature scheme is organized as follows: In Section 2, it has been described in brief the relative researches in public key security algorithm based on block cipher or hill cipher. In Section 3 provides the method and detailed steps on the proposed method of digital signature scheme, It can be used electronic voting system based on public key security algorithm. An implementation and the illustration are demonstrated in Section 4. In Section 5, the design of the experimental results and performance analysis is discussed; finally, in Section6 offers conclusions.

II. Related Works

Zhe Xia, Steve Schneider proposed A New Receipt-Free E-Voting Scheme Based on Blind Signature in 2006. It is a simple and efficient method, applying the secret ballot technique introduced by the voter scheme to improve individual verifiability to the later work. The scheme is the only receipt-free scheme in which voters can verify both the ballot recording process and the ballot counting process.[10]

Subariah Ibrahim, Maznah Kamat, Mazleena Salleh, Shah Rizan Abdul Aziz proposed Secure E-Voting With Blind Signature in 2008. In this proposal, they suggested a new electronic voting system, E-Voting for a general election. The provider, which is an open source library, is used to provide the secure communication channel. The voter's private key for digital signature is protected by using password-based encryption with SHA and Twofish-CBC algorithm so that only valid voter can use it.[2]

Patil V.M. proposed in 2010 Secure EVS by using blind signature and cryptography for voter's privacy & authentication. In that proposed protocol secure for large scale election system. The bio-matrix authentication system provides the uniqueness. i.e., only one person one registration & one person one vote in a election period possible that need a extra H/w & S/w. There is no any link between pseudo key & registration of voter hence it fallow the voter privacy & confidentially & universal & individual verifiability of voter is main objective of the protocol.[1]

Nidhi Gupta, Praveen Kumar and Satish Chhokar proposed in 2011 "A Secure Blind Signature Applications in E- Voting". In this paper we apply a technique called blind signatures to a voter's ballot so that it is impossible for anyone to trace the ballot back to voter. E-voting employs cryptographic technique to overcome the security issues in the election process. The proposed scheme fully conforms to the requirement of large scale election such as privacy, fairness, unreusability.[7]

The proposed blinding signature scheme new algorithm based on Hill cipher's or linear block cipher. The block cipher is susceptible to cryptanalysis and unusable in practice, but still serves an important pedagogical role in both cryptology and linear algebra. In general, the key space of the Hill cipher is precisely GL(r, Z_m) the group of r x r matrices that are invertible over Z_m for a predetermined modulus m.[4]

III. Proposed Scheme

A large number of protocols and more generalised schemes for electronic voting have been proposed since 1981. Many of them share some common characteristics, a fact that has been utilised as the criterion for their rough classification presented next. The general procedure of the electronic voting process is presented in the following sections.

3.1 Registration Phase

A voter must register with the registrar, identifying himself as an eligible voter. Upon registering, the registrar assigns a unique identification number to the voter, places the voter's name and ID in the registered voter list, and sends the ID without the name to the authenticator. The authenticator generates a unique pair of public/private keys for the ID it received, stores them in a list, and sends the pair of the public keys and the ID to the registrar. The registrar then sends the pair back to the voter.

3.2 Voting Phase

In order to vote, the voter contacts the distributor and asks for a ballot. The distributor randomly selects a ballot and sends it to the voter, who, in turn, requests and receives the matching pair for the received ballot from the matcher. The voter then signs the encrypted version of the desired vote using his signature key and sends them to the authenticator, along with the ballot's ID number and the voter's own ID. The voter also informs the registrar that he has cast a vote but it is not required to tell the registrar which ballot ID it used. The authenticator checks the signature to authenticate the voter and verifies that the authenticated voter is permitted to vote in the given election. Once authenticated, the authenticator passes only the legitimate encrypted vote and the ballot's ID to the counter. The voter gets a receipt, confirming that the authenticator has received the ballot packets.

3.3 Tallying and Verification

For verifying the vote tally, the counter simply decrypts the votes it has received. After the tallying of the votes, each authority releases certain information to the public. To verify the integrity of the election, the verifier compares certain published lists. The authenticator publishes the list containing the encrypted ballots and the ballot ID. The counter publishes its version of the same list and the verifier confirms that these lists are identical.

The most widely using RSA equation for encryption and decryption are as follows:
Encryption: $C = M^e \bmod n$
Decryption: $M= C^d \bmod n$

In E-Voting, digital signature is created by using RSA encryption.
Signature, $S = H^d \bmod n$
To verify the message, the receiver will hash the message, M by using the same digest function. At the same time, the signature, ***S*** is decrypted using the receiver's public key.
$H = S^e \bmod n$. The results of the two processes are then compared.

3.1.1 RSA Protocol

1. *Notation.* B's RSA public and private keys are (n, e) and d, respectively. k is a random secret integer chosen by A satisfying $0 \leq k \leq n - 1$ and gcd(n; k) = 1.
2. *Protocol actions.*

(a) Blinding: A calculates $m^* = mk^e \bmod n$ and sends this to B.
(b) signing: B computes $s^* = (m^*)^d \bmod n$ which it sends to A.
(c) unblinding: A computes $s = k^{-1}s^* \bmod n$, which is B's signature on m.[4]

3.1.2 New Protocol

1. Notation. B's New proposed algorithm's public and private keys are (n=37, e) and d. k is a random secret integer chosen by A satisfying $0 \leq k \leq n - 1$ and
2. gcd(n; k) = 1
3. Protocol actions

(a) Blinding $m^*=(m \bullet k \bullet e) \bmod n$
(b) Signing $s^* = (m^* \bullet d \bmod n) \bmod n$
(c) Unblinding $S=(s^* \bullet k^{-1}) \bmod n$. It is B's signature on m

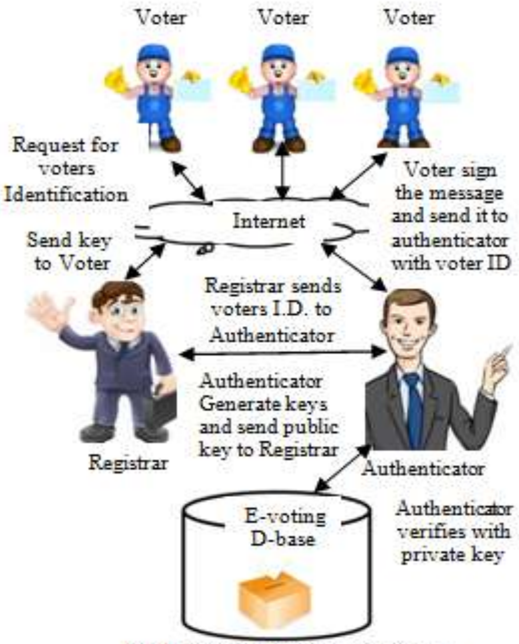
Voter
Voter
Voter
Request for voters Identification
Internet
Voter sign the message and send it to authenticator with voter ID
Send key to Voter
Registrar sends voters I.D. to Authenticator
Authenticator Generate keys and send public key to Registrar
Registrar
Authenticator
E-voting D-base
Authenticator verifies with private key

Fig.1 E-voting system architecture

Implementation

Select Square matrix $\begin{pmatrix} 3 & 2 \\ 3 & 4 \end{pmatrix}$

Finding inverse of matrix
C_{11} $[-1]^{1+1}$ x [4] = $[-1]^{2}$ x [4] = 4
C_{12} $[-1]^{1+2}$ x [3] = $[-1]^{3}$ x [3] = -3
C_{21} $[-1]^{2+1}$ x [3] = $[-1]^{3}$ x [2] = -2
C_{22} $[-1]^{2+2}$ x [4] = $[-1]^{4}$ x [3] = 3

$$-6 * \begin{pmatrix} 4 & -2 \\ -3 & 3 \end{pmatrix} \text{mod } 37 = \begin{pmatrix} -24 & 12 \\ 18 & -18 \end{pmatrix} \text{mod} 37 = \begin{pmatrix} 13 & 12 \\ 18 & 19 \end{pmatrix}$$

Now we have

$$.k = \begin{pmatrix} 3 & 2 \\ 3 & 4 \end{pmatrix} \quad \text{and } k^{-1} = \begin{pmatrix} 13 & 12 \\ 18 & 19 \end{pmatrix}$$

And select random integer e=5 and d=15
(Verification 5*15 mod 37 =1)

In the list of Candidate we select candidate ‘3’
Again, we confirm the letter with ‘C’
Now message is ‘3C’ i.e (30, 3)

i) Blinding m^{*}=(m • k • e) mod n

$$.m^* = \begin{pmatrix} 30 \\ 3 \end{pmatrix} * \begin{pmatrix} 3 & 2 \\ 3 & 4 \end{pmatrix} *5 \text{ mod } 37 = \begin{pmatrix} 480 \\ 510 \end{pmatrix} \text{mod } 37 = \begin{pmatrix} 36 \\ 29 \end{pmatrix}$$

ii) Signing $s^{*} = (m^{*} \bullet d \text{ mod } n) \text{ mod } n$

$$s^{*} = \begin{pmatrix} 36 \\ 29 \end{pmatrix} * 15 \text{ mod } 37 = \begin{pmatrix} 22 \\ 28 \end{pmatrix}$$

iii) Unblinding $S=(s^{*} \bullet k^{-1}) \text{ mod } n$

$$S = \begin{pmatrix} 22 \\ 28 \end{pmatrix} * \begin{pmatrix} 13 & 12 \\ 18 & 19 \end{pmatrix} \text{mod } 37 = \begin{pmatrix} 622 \\ 928 \end{pmatrix} \text{ mod } 37 = \begin{pmatrix} 30 \\ 3 \end{pmatrix}$$

Now blinding message and unblinding messages are same, So, Signing accepted.

IV. Result Analysis

The algorithm executes on PC computer of CPU Intel Pentium 4, 2.2 MHz Dual Core. The programs implemented using MATLAB and messages are stored in 3 different arrays for blinding, signing and unblinding scheme. It is tested with the length of 100 characters.

TABLE I
COMPARISON OF EVS

Electronic Voting System	Blinding/Signing/Unblinding Executing Time
RSA EVS	33 Sec.
Chaum’s EVS	28 Sec.
New proposed EVS	27 Sec.
No. of characters 100	

The above result shows system prototype that implements security protocols that meet the security requirements of an EVS. With this system, electronic ballots are generated automatically. The participation rate of voting is expected to increase because voters do not have to line-up in a long queue anymore. With electronic ballots, results can be obtained faster than the traditional voting.

V. Conclusion

The proposed new protocol system is fully secure for large scale election system. The employment of electronic voting systems for organising and conducting large-scale elections in a secure way is feasible, provided that certain deficiencies of existing voting protocols are successfully addressed. Specifically, the block cipher has been demonstrated that several security requirements are contradicting each other, thus requiring special treatment, while there are requirements that can either not be fulfilled, given the currently available technology, or they can be handled provided that a substantial increase in cost and complexity is accepted. The new e-voting system demonstrated by the fact that none of the existing voting protocols supports reasonable cost, complexity and security.

References

Journal Papers:

[1] Patil V.M. “Secure EVS by using blind signature and cryptography for voter’s privacy & Authentication”, Journal of Signal and Image Processing, Vol. 1, Issue 1, 2010, PP-01-06.

[2] Subariah Ibrahim, Maznah Kamat, Mazleena Salleh, Shah Rizan Abdul Aziz, “Secure E-Voting With Blind Signature”, 3262/1/ieee02 in 2008.

[3] Prakash Kuppuswamy, Dr.C. Chandrasekar, “Enrichment of Security through Cryptographic Public key Algorithm Based on Block cipher”, IJCSE, ISSN : 0976-5166 Vol. 2 No. 3 Jun-Jul 2011 PP 347-355.

Books:

[4] John C. Bowman, Math 422 Coding Theory & Cryptography, University of Alberta, Edmonton, Canada.

[5] Denning, D.E. “Cryptography and Data Security. Reading (MA)”: Addison-Wesley, 1982.

[6] Diffie, W. & Landau, S. “Privacy on the Line. Boston”, MIT Press, 1998.

Proceedings Papers:

[7] Nidhi Gupta, Praveen Kumar and Satish Chhokar, “A Secure Blind Signature Application in E Voting”, Proceedings of the 5th National Conference; Computing For Nation Development, New Delhi, March,2011.

[8] R. Cramer, R. Gennaro, and B. Schoenmakers, and M. Yung, “Multi-Authority Secret-Ballot Elections with Linear Works”, Eurocrypt ’96, LNCS 1070, pp 72 – 83, 1996.

[9] L.R. Cranor, and R.K. Cytron, “Design and Implementation of a Practical Security-Conscious Electronic Pollind System,” Washington University: Computer Science Technical Report, 1996.

[10] Zhe Xia, Steve Schneider, “A New Receipt-Free E-Voting Scheme Based on Blind Signature”, may 25, 2006.

[11] A. Juels, D. Catalano, and M. Jakobsson, “Coercion-resistant electronic elections”, Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pages 61–70, 2005.

[12] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, “Providing receipt-freeness in mixnet-based voting protocols”, Proceedings of ICISC’03, LNCS 2971:245–258, 2003.

Dr.Omar Saeed Ali Al-Mushayt is an Associate Professor and Dean of the College of Computer Science & Information System, Jazan University, Kingdom of Saudi Arabia. He obtained his Master's degree from University of Illinois, Chicago - United States of America and Ph. D University of Loughborough, United Kingdom. He is the Member of the Board of Jazan University, Member of the Committee for Scientific Collaboration of Jazan University with (IRF) Information Research Facility, Board member of the Council of the University of Jazan, Elected member of the municipal council of the municipality of Khamis Mushayt (2005-2011) and Associate member of the Arab Thought Foundation. He participated as a Reviewer in many international conferences worldwide. His research interests include Information Security, E-governance and Artificial Intelligence. He published many Research papers in National/International Journals and Conferences

Prakash Kuppuswamy Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar proceeding in ‘Dravidian University’. He has published few journals/Technical papers and participated in many international conferences in Rep. of Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and Network algorithms