Matrix Based Single Authority Electronic Voting Schemes

Porkodi C[1] and Sangavai K[2]
{[1]cpg.maths@psgtech.ac.in, [2]sks.maths@psgtech.ac.in }

Professors, Department of Mathematics, PSG College of Technology, Coimbatore[1,2]

Abstract. The developments of electronic communication have made the world in to a global village and provide the opportunity for interactive communication with distant people with in short duration. Cost, time and energy are saved by the digital technologies like electronic commerce, electronic voting and so on.Electronic voting is a form of digital-mediated voting in which voters make their selections with the aid of a computer or a mobile or a PDA and so on. In this paper, two electronic voting schemes namely single authority two way and single authority multi way voting schemes based on matrices are discussed in detail. Illustration is done using Wolfram cloud.

Keywords: e-voting, circulant matrices, bulletin board, trusted authority, interactive proof of knowledge.

1 Introduction

Taking group decisions is an essential subject in the field of computer applications and electronic voting (e-voting) has a great interest in this issue. Electronic voting has been the primary focus of electronic commerce in the recent years, because it minimises the cost, increases the processing speed and provides security. The main objective of electronic voting is to speed up, provide user-friendliness for disabled and old age voters, minimise cost involved in casting and tally computing the votes and announce the results faster. Everyone knows that the world is now severely suffering by the pandemic. In this situation, conducting elections by gathering crowds is not an advisable one. In such occasions electronic voting is an appropriate alternative to conventional mode of voting and it is attained through the devices like computers, laptops, mobile phones, PDA´s, smart cards and so on from the voters place itself.

The following are essential for any e-voting scheme.

- **Privacy** -make sure that no third party associates the ballot to the voter.
- **Universal Verifiability-** any authorised participant in the voting scheme can check independently that all valid votes are counted
- **Robustness-** identifies detection of failure from partial authorities or voters.
- **Efficiency-** processing time must becomputational.
- **Eligibility-** Only authenticated voters must be allowed to vote
- **Completeness** - no fake or invalid vote is added into final tally and no valid vote is removed from the final tally.
- **Uncoercibility** - no voter is forced to vote in a specific way

ICCAP 2021, December 07-08, Chennai, India

DOI 10.4108/eai.7-12-2021.2314706

The main phases of e - voting are:

- **registration phase -** A participant must be registered as an authenticated voter
- **voting phase** - authenticated voter cast his/her vote
- **counting phase** – the final tally of the casted votes is computed with the support of a set of authorities

Cryptographic algorithms are used to design secure electronic voting schemes. Chaum[2] introduced in which votes were casted electronically through insecure networks. A robust and verifiable cryptographically secure election scheme based on an r-thresiduosity was proposed by Cohen and Fischer [4]. Ronald Cramer et al [5, 6] designed an exponentiation based ballot election scheme involving multiple authorities. Smart cards based electronic voting protocol was discussed by Liaw [9], in which the voter has the provision of asking the center to recount the votes by sending the receipt. Private Information Retrieval (PIR) electronic voting scheme appropriate for small-scale election using one server and secure coprocessor was proposed by Chun Hua Chen et.al [3]. Lina Wang et al [16]analyzed a blind signature based electronic voting scheme involving more than one administrator, and a forgeable one when the voting center is not trustful and IP trace between the voting center and voters is available. Ben Adida and Rivest[1] designed a scratch & vote cryptographic voting system, that minimize the cost and complexity, in which the voter can audit the ballot without interacting with election officials before casting. Xun Yi et al [18] proposed an electronic voting for mobile communications based on blind signatures. Chun-Ta Li et al [8] developed an ad hoc networks based electronic voting scheme. Zhen-YuWuet al [20] proposed an internet based electronic voting schemewhich 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.Porkodi et al [12, 13] proposed single and multi authority electronic voting schemes based on elliptic curves, in which two ways as well as multi ways of voting are discussed.Liu Y et al [19] proposed an e- voting scheme using secret sharing and k-anonymity, in which no computational hard problem is involved. Ralf Kusters et al [14] analysed general formal frameworks and solid formulations of fundamental security requirements for e - voting. Cao Gang [7], Karro and Wang [10],Chunlai Song et al [15] and H. Wei[17] et al had done related work in e-voting. Mukesh Kumar Singh [11] introduced public key cryptosystem using matrices based on the concept matrix multiplication is commutative for circulant matrices.

In this paper, single authority two ways and multi ways e-voting schemes using circulant matrices are developed. In section 2 the basic terminologies related to the scheme are given. In section 3,single authority two ways electronic voting scheme is explained elaborately. In section 4 single authority multi way electronic voting scheme is presented and in section 5 analysis of the scheme is given.

2 Basic Terminologies

2.1 Mode of Communication

The voters and authorities involved in the voting schemes communicate through, two means of communication a bulletin board and private channels.

2.1.1 Bulletin board

To execute the single authority electronic voting scheme, each participant involved in the voting scheme are in need of publicly accessible memory known as bulletin board in the cloud. Every participant is assigned with a portion of memory to cast their votes in the encrypted form and no casted vote is tampered. Also each participant has the liberty of adding messages in the assigned section but cannot remove the posted information later. Further it is supposed that, there is some in built authentication mechanism to provide assurance for the origin of posted messages, so that only eligible persons post their messages in their respective section. To verify the validity by any third party, each posted message is digitally signed.

To implement the voting scheme, every voter constructs the ballot in the encrypted form and posts it on the bulletin board along with a proof for validity. The final tally is computed with the support of trusted authorities. Every voter posts vote as a matrix on the bulletin board.

2.1.2 Private channels

Communication between voters and authority is done through private channels and in the case of single authority electronic voting, encrypted secret keys are transmitted to the trusted authority through these private channel.

2.2. Circulant matrix

A circulant matrix is a square matrix in which all row vectors are composed of the same elements and each row vector is rotated one element to the right relative to the preceding row vector.

Example: A 4 x 4 circulant matrix is of the form A = $\begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix}$

3 Single Authority Two Way Electronic Voting Scheme Based on Matrices

In this section, the vote casting and tally computing of a two way election scheme with the assistance of a single authorityisdiscussed.It is assumed that ‘n’ voters are involved in the scheme. The processes of initialization, vote casting and tally computing are depicted in Fig 1.

3.1 Initialization phase:

The trusted authority publishes following parameters on the bulletin board.

- Composite number N which is a product of two large primes p and q
- A matrix $G_{r\,x\,r}$ of elements $g_{ij} \in Z_N$
- Selects two secret circulant matrices A_T and B_T with entries from Z_N and publishes its public key $P_T = A_T G B_T (\text{mod } N)$

3.2 Ballot: For a two way voting scheme on a specific subject,thedecision‘Yes’ is encoded as an r x rmessage matrix $M_i = M_{r\,x\,r}$ with leading diagonal element M_{11} as ‘1’ and rest of the elements ‘0’. The decision‘No’ is encoded as an r x r message matrix$M_i = O_{r\,x\,r}$ with all entries ‘0’ i.e, a zero matrix.

3.3 Vote casting

To vote on an issue,

- Every voter V_i selects r x r secret random circulant matrices A_i and B_i with entries from Z_N, computes $C_{i,1} = A_i P_T B_i + M_i (\text{mod } N)$, where $r \geq 2$ and M_i is the message matrix.
- V_i and posts the encrypted vote $C_{i,1}$ on the bulletin board.
- $V_i$encryptsthe secret keys A_i and B_i, using public parameter G as$C_{i,2}=A_i G B_i (\text{modN})$and sends it to the trusted authority through private channel.

3.4 Tally computing

Trusted authority

- Determines thesum $S = \sum_{i=1}^{n} C_{i,2} (\text{modN}) = \sum_{i=1}^{n} A_i G B_i (\text{mod N})$and $C_2 = A_T S B_T (\text{mod N})$
- Posts C_2 on the bulletin board.
- Using the data published on the bulletin board any authenticated person computes $C_1 = \sum_{i=1}^{n} C_{i,1} (\text{mod N})$ and in turn $C_1 - C_2 = \sum_{i=1}^{n} M_i$.
- Since $C_1 - C_2 = \sum_{i=1}^{n} C_{i,1} (\text{mod N}) - A_T S B_T (\text{mod N})$

$= \sum_{i=1}^{n} (A_i P_T B_i + M_i) (\text{mod N}) - A_T (\sum_{i=1}^{n} A_i G B_i) B_T (\text{mod N}) =$

$\sum_{1}^{n} M_i (\text{mod N})$. Since circulant matrices satisfies commutative property with respect to multiplication.

- The first leading diagonal element say 'f' gives number of votes casted in favour to the particular subject and 'n-f' gives number of votes casted against the subject.

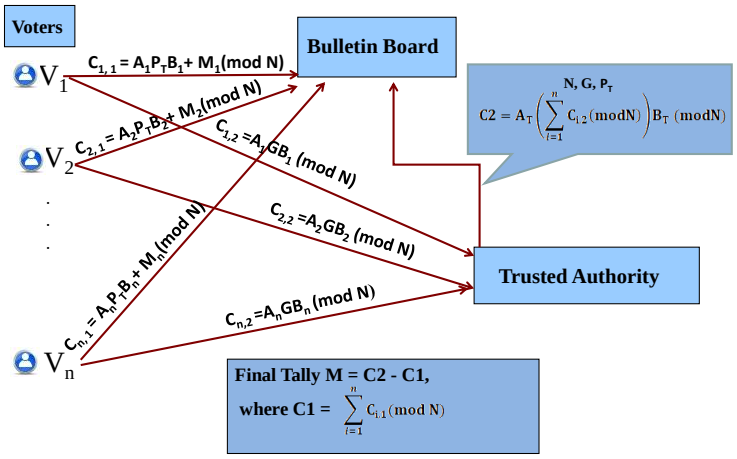

Fig 1: Voting Phase and Tally Computing Phase

3.5 Voter's Proof

In the vote casting protocol, every voter has to prove that he/she really encrypted a vote the matrix $M_i = M_{r x r}$ with leading diagonal element M_{11} as '1' and rest of the elements '0' or the matrix$M_i = O_{r x r}$ with all entries '0' i.e., a zero matrix.

The voter V_i performs a proof knowledge, to show that whether he/she knows A_i and B_i for either $C_{i,2}=A_i G B_i (\text{modN})$ and $C_{i,1} - O_{r x r}$, or $C_{i,2}=A_i G B_i (\text{modN})$ and $C_{i,1} - M_{r x r} (\text{modN})$. Each of the two alternatives could be proven through the interactive proof of knowledge between the voter and authority.

3.6 Interactive Proof of Knowledge

An interactive proof of knowledge of the common logarithm X of $Y_1 = XG_1$ and $Y_2 = XG_2$ is described below.

1. Voter chooses a circulant matrix R with entries from Z_N and sets $A = (RG_1, RG_2)$ and sends to the authority (verifier). i.e. the voter commits, that two different matrices G_1 and G_2 have the same logarithm R.
2. Verifier chooses a circulant matrix C with entries from Z_N at random and sends to authority, which is a challenge by the verifier.
3. Voter computes $B = R - CX$ and sends to the verifier, which is the response.
4. Verifier accepts, if and only if, $A = (BG_1+CY_1, BG_2+CY_2)$

3.7 Completeness

The equation $A = (BG_1+CY_1, BG_2+CY_2)$ is satisfied only if the voter and the authority follow the protocol correctly and the voter knows a common logarithm for Y_1 and Y_2.

3.8 Illustration:

In this section, single authority two way electronic voting scheme based on circulant matrices is illustrated with an example. In the voting scheme 10 voters are involved.

Trusted authority selects two prime numbers p = 7, q =11 and posts the public parameters N = 77 and $G = \begin{pmatrix} 4 & 9 \\ 5 & 12 \end{pmatrix}$ on the bulletin board. Trusted authority selects secret circulant matrices $A_T = \begin{pmatrix} 4 & 15 \\ 15 & 4 \end{pmatrix}$ and $B_T = \begin{pmatrix} 8 & 10 \\ 10 & 8 \end{pmatrix}$ and computes its public key $P_T = A_T\ G\ B_T = \begin{pmatrix} 39 & 20 \\ 6 & 31 \end{pmatrix}$ and posts P_T on the bulletin board.Voters V_i for i=1, 2, ...,10, selects secret keys A_i & B_i and transmits their encrypted secret keys $C_{i,2}$ to the trusted authority through private channels. Also voters V_i for i=1, 2, ...,10, encrypts their vote and post $C_{i,1}$ on the bulletin board. The encrypted secret keys details and encrypted vote details are given by table 1 and table 2 respectively.

Voters	**Secret keys A_i & B_i**	**Encrypted Secret keys $C_{i,2}$**
V_1	$\begin{pmatrix} 2 & 7 \\ 7 & 2 \end{pmatrix} \& \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$	$\begin{pmatrix} 52 & 75 \\ 37 & 30 \end{pmatrix}$
V_2	$\begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix} \& \begin{pmatrix} 6 & 10 \\ 10 & 6 \end{pmatrix}$	$\begin{pmatrix} 15 & 34 \\ 51 & 62 \end{pmatrix}$
V_3	$\begin{pmatrix} 12 & 5 \\ 5 & 12 \end{pmatrix} \& \begin{pmatrix} 15 & 12 \\ 12 & 15 \end{pmatrix}$	$\begin{pmatrix} 31 & 8 \\ 3 & 22 \end{pmatrix}$
V_4	$\begin{pmatrix} 20 & 2 \\ 2 & 20 \end{pmatrix} \& \begin{pmatrix} 16 & 4 \\ 4 & 16 \end{pmatrix}$	$\begin{pmatrix} 23 & 5 \\ 65 & 17 \end{pmatrix}$
V_5	$\begin{pmatrix} 5 & 7 \\ 7 & 5 \end{pmatrix} \& \begin{pmatrix} 40 & 3 \\ 3 & 40 \end{pmatrix}$	$\begin{pmatrix} 46 & 12 \\ 25 & 74 \end{pmatrix}$
V_6	$\begin{pmatrix} 35 & 8 \\ 8 & 35 \end{pmatrix} \& \begin{pmatrix} 30 & 12 \\ 12 & 30 \end{pmatrix}$	$\begin{pmatrix} 14 & 14 \\ 25 & 73 \end{pmatrix}$
V_7	$\begin{pmatrix} 12 & 5 \\ 5 & 12 \end{pmatrix} \& \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$	$\begin{pmatrix} 26 & 44 \\ 40 & 72 \end{pmatrix}$
V_8	$\begin{pmatrix} 15 & 14 \\ 14 & 15 \end{pmatrix} \& \begin{pmatrix} 7 & 4 \\ 4 & 7 \end{pmatrix}$	$\begin{pmatrix} 43 & 23 \\ 62 & 48 \end{pmatrix}$
V_9	$\begin{pmatrix} 2 & 7 \\ 7 & 2 \end{pmatrix} \& \begin{pmatrix} 11 & 4 \\ 4 & 11 \end{pmatrix}$	$\begin{pmatrix} 34 & 62 \\ 73 & 31 \end{pmatrix}$
V_{10}	$\begin{pmatrix} 9 & 5 \\ 5 & 9 \end{pmatrix} \& \begin{pmatrix} 18 & 4 \\ 4 & 18 \end{pmatrix}$	$\begin{pmatrix} 45 & 10 \\ 11 & 11 \end{pmatrix}$

Table1: Encrypted Secret keys transmitted to Trusted Authority

Voters	Voting Choice	Encoded Voting Choice	Encrypted votes $C_{i,1}$
V_1	Yes	$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}53 & 1\\8 & 67\end{pmatrix}$
V_2	Yes	$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}12 & 69\\1 & 36\end{pmatrix}$
V_3	Yes	$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}45 & 43\\44 & 43\end{pmatrix}$
V_4	No	$\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}44 & 11\\33 & 33\end{pmatrix}$
V_5	Yes	$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}37 & 70\\69 & 4\end{pmatrix}$
V_6	Yes	$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}21 & 43\\31 & 32\end{pmatrix}$
V_7	No	$\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}20 & 71\\20 & 71\end{pmatrix}$
V_8	No	$\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}73 & 37\\40 & 59\end{pmatrix}$
V_9	Yes	$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}39 & 73\\16 & 51\end{pmatrix}$
V_{10}	Yes	$\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$	$\begin{pmatrix}67 & 41\\23 & 52\end{pmatrix}$

Table 2: Encrypted Votes published on the bulletin board

Trusted authority computes $S = \sum_{i=1}^{n} C_{i,2} (\text{mod } 77) = \begin{pmatrix}21 & 56\\7 & 55\end{pmatrix}$, in turn $C_2 = A_T S B_T$ (mod 77) = $\begin{pmatrix}67 & 41\\23 & 52\end{pmatrix}$ and posts C_2 on the bulletin board. Anyone who has the rights to view the bulletin board computes $C_1 = \sum_{i=1}^{n} C_{i,1} (\text{mod } 77) = \begin{pmatrix}74 & 41\\23 & 52\end{pmatrix}$ and in turn $C_1 - C_2 = \begin{pmatrix}7 & 0\\0 & 0\end{pmatrix}$. From which it can be concluded that 7 voters casted in favour of the subject and 3 against the subject.

4 Single Authority Multi Way Electronic Voting Scheme Based on Matrices

In a decision making problem, if there are only two choices {Yes, No}, then the two way voting scheme can be adopted. There is real time scenario, like elect one person for a post out of 10 candidates by 100 voters somewhat similar to legislative assembly election or local body election. In such cases, single authority two ways electronic voting scheme based on circulant matrices can be extended to multi way voting also.

4.1 Ballot

Suppose that the voters have 'k' choices, for example 'k' contestants contest for a secretary post. In this case of multiway voting scheme, i^{th} choice is encoded as an 'k x k' message matrix $M = M_{k \times k}$ with leading diagonal element M_{ii} as '1' and rest of the elements '0'. i.e, the first choice denoted as a matrix M with first leading element as '1' and rest of the elements to be zero.

4.2 Illustration:

In this section, single authority multi way electronic voting scheme based on circulant matrices is illustrated with an example. In the voting scheme, 10 voters are involved and they need to vote for 4 contestants. The ballots for 4 contestants 1, 2, 3, 4 are encoded as $M_1=\begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$, $M_2=\begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$, $M_3=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}$, $M_4=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{pmatrix}$

Trusted authority selects two random prime numbers p = 7, q =11 and a random matrix G $=\begin{pmatrix}4&10&7&3\\5&14&10&7\\7&5&14&0\\0&17&9&4\end{pmatrix}$ with entries from Z_{77} and posts the public parametersN = 77 and G on the bulletin board. Trusted authority chooses random secret circulant matrices $A_T = \begin{pmatrix}4&12&1&15\\15&4&12&1\\1&15&4&12\\12&1&15&4\end{pmatrix}$ and $B_T=\begin{pmatrix}8&1&2&10\\10&8&1&2\\2&10&8&1\\1&2&10&8\end{pmatrix}$ and computes its public key $P_T = A_T\ G$ $B_T=\begin{pmatrix}11&25&27&0\\12&27&30&64\\11&20&12&62\\76&40&53&20\end{pmatrix}$ and posts P_T on the bulletin board. Voters V_i for i=1, 2, ...,10, selects secret keys A_i & B_i and transmits their encrypted secret keys $C_{i,\,2}$ to the trusted authority through private channels. Also voters V_i for i=1, 2, ...,10, encrypts their vote and post $C_{i,\,1}$ on the bulletin board. The encrypted secret keys are given by table 3 .

Voters	**Secret keys A_i & B_i**	**Encrypted Secret keys $C_{i,\,2}$**
V_1	$\begin{pmatrix}4&0&7&5\\5&4&0&7\\7&5&4&0\\0&7&5&4\end{pmatrix}$ & $\begin{pmatrix}5&4&3&11\\11&5&4&3\\3&11&5&4\\4&3&11&5\end{pmatrix}$	$\begin{pmatrix}31&34&40&37\\62&13&27&20\\5&71&41&38\\5&55&28&62\end{pmatrix}$
V_2	$\begin{pmatrix}5&14&0&11\\11&5&14&0\\0&11&5&14\\14&0&11&5\end{pmatrix}$ & $\begin{pmatrix}2&9&31&33\\33&2&9&31\\31&33&2&9\\9&31&33&2\end{pmatrix}$	$\begin{pmatrix}26&63&66&24\\0&67&12&4\\49&23&50&76\\70&38&39&60\end{pmatrix}$
V_3	$\begin{pmatrix}12&5&25&1\\1&12&5&25\\25&1&12&5\\5&25&1&12\end{pmatrix}$ & $\begin{pmatrix}15&10&7&7\\7&15&10&7\\7&7&15&10\\10&7&7&15\end{pmatrix}$	$\begin{pmatrix}4&40&40&28\\2&43&59&25\\33&52&8&71\\68&1&64&31\end{pmatrix}$
V_4	$\begin{pmatrix}20&40&24&2\\2&20&40&24\\24&2&20&40\\40&24&2&20\end{pmatrix}$ & $\begin{pmatrix}16&70&65&4\\4&16&70&65\\65&4&16&70\\70&65&4&16\end{pmatrix}$	$\begin{pmatrix}47&31&72&67\\39&9&21&72\\12&6&17&23\\46&31&65&24\end{pmatrix}$
V_5	$\begin{pmatrix}5&0&11&7\\7&5&0&11\\11&7&5&0\\0&11&7&5\end{pmatrix}$ & $\begin{pmatrix}40&2&52&3\\3&40&2&52\\52&3&40&2\\2&52&3&40\end{pmatrix}$	$\begin{pmatrix}32&57&70&72\\45&38&3&76\\74&64&74&2\\6&31&43&4\end{pmatrix}$

V_6	$\begin{pmatrix}35&4&56&8\\8&35&4&56\\56&8&35&4\\4&56&8&35\end{pmatrix}$ & $\begin{pmatrix}30&3&3&12\\12&30&3&3\\3&12&30&3\\3&3&12&30\end{pmatrix}$	$\begin{pmatrix}4&1&61&61\\55&53&33&32\\11&16&55&28\\20&41&61&15\end{pmatrix}$
V_7	$\begin{pmatrix}12&0&1&5\\5&12&0&1\\1&5&12&0\\0&1&5&12\end{pmatrix}$ & $\begin{pmatrix}4&72&13&3\\3&4&72&13\\13&3&4&72\\72&13&3&4\end{pmatrix}$	$\begin{pmatrix}42&28&20&17\\24&61&60&38\\65&9&12&31\\55&49&68&18\end{pmatrix}$
V_8	$\begin{pmatrix}15&6&9&14\\14&15&6&9\\9&14&15&6\\6&9&14&15\end{pmatrix}$ & $\begin{pmatrix}7&12&75&4\\4&7&12&75\\75&4&7&12\\12&75&4&7\end{pmatrix}$	$\begin{pmatrix}17&61&72&39\\16&9&48&11\\25&28&67&20\\52&67&55&29\end{pmatrix}$
V_9	$\begin{pmatrix}2&35&42&7\\7&2&35&42\\42&7&2&35\\35&42&7&2\end{pmatrix}$ & $\begin{pmatrix}11&15&60&4\\4&11&15&60\\60&4&11&15\\15&60&4&11\end{pmatrix}$	$\begin{pmatrix}76&70&48&10\\29&76&15&25\\25&28&67&20\\52&67&55&29\end{pmatrix}$
V_{10}	$\begin{pmatrix}9&14&27&5\\5&9&14&27\\27&5&9&14\\14&27&5&9\end{pmatrix}$ & $\begin{pmatrix}18&50&37&4\\4&18&50&37\\37&4&18&50\\50&37&4&18\end{pmatrix}$	$\begin{pmatrix}16&3&15&66\\40&25&48&73\\62&5&34&45\\58&55&57&47\end{pmatrix}$

Table3: Encrypted Secret keys transmitted to Trusted Authority

The encrypted vote details are given table 4

Voters	**Voting Choice Contestants**	**Encoded Voting Choice**	**Encrypted votes $C_{i,1}$**
V_1	1	$\begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}73&53&26&10\\37&12&47&72\\4&11&45&3\\17&52&46&18\end{pmatrix}$
V_2	2	$\begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}60&38&37&75\\20&6&27&46\\26&13&33&68\\33&68&32&42\end{pmatrix}$
V_3	1	$\begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}5&35&70&45\\61&65&50&6\\9&21&1&36\\40&38&43&73\end{pmatrix}$
V_4	1	$\begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}67&76&25&71\\42&68&70&23\\69&34&71&22\\16&31&26&4\end{pmatrix}$
V_5	1	$\begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}28&3&63&19\\27&37&44&67\\49&56&24&39\\38&55&21&68\end{pmatrix}$
V_6	2	$\begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}67&65&64&49\\50&18&71&65\\16&31&25&61\\66&57&18&34\end{pmatrix}$

V_7	4	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}29&63&5&43\\53&72&65&48\\18&57&33&67\\16&70&39&30\end{pmatrix}$
V_8	3	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}60&6&45&22\\44&36&3&22\\17&5&55&22\\11&52&52&11\end{pmatrix}$
V_9	4	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}0&25&46&13\\8&61&62&23\\41&11&55&61\\55&41&61&19\end{pmatrix}$
V_{10}	3	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}63&74&5&40\\64&55&74&38\\47&47&18&15\\46&33&47&28\end{pmatrix}$

Table 4: Encrypted Votes published on the bulletin board

Trusted authority computes $S = \sum_{i=1}^{n} C_{i,2} (\text{mod } 77) = \begin{pmatrix}64&3&42&36\\4&9&18&68\\76&34&67&31\\8&6&2&35\end{pmatrix}$ and $C_2 = A_T S B_T \text{ (mod 77)} = \begin{pmatrix}63&53&1&2\\21&43&51&25\\65&58&50&9\\30&35&0&19\end{pmatrix}$ and posts C_2 on the bulletin board. Anyone who has the rights to view the bulletin board computes $C_1 = \sum_{i=1}^{n} C_{i,1} (\text{mod } 77) = \begin{pmatrix}67&53&1&2\\21&45&51&25\\65&58&52&9\\30&35&0&21\end{pmatrix}$ and in turn $C_1 - C_2 = \begin{pmatrix}4&0&0&0\\0&2&0&0\\0&0&2&0\\0&0&0&2\end{pmatrix}$. From which it can be concluded that 4, 2, 2, 2 voters casted in favour of the contestants 1, 2, 3 and 4 respectively.

5 Analysis of the Schemes:

The basic requirements of e-votingare satisfied in the proposed schemes. As the voters individually cast their votes in the encrypted form in the bulletin board, no third party associates the ballot to the voter and in turn privacy is maintained in the scheme.Once the hidden value C_2 of the voters and trusted authority's secret keys is posted by the trusted authority on the bulletin board, any authorised participant in the voting scheme can check independently that all valid votes are counted and thus universal Verifiability is achieved in the scheme. As the processing time is computational, the scheme is efficient. As it is assumed that some authentication mechanism to be adopted in the beginning itself, eligibilityis also attained. Also voter and authority has no rights to add or delete the posted messages on the

bulletin board, no fake or invalid vote is added into final tally and no valid vote is removed from the final tally and thus completeness is accomplished in the proposed scheme.

6 Conclusion

In future traditional based voting may be replaced with cryptographically secured electronic voting scheme because of the current pandemic situations.But designing such an e-voting scheme satisfying all requirements is still a great challenge. In this paper, a public key cryptography based on matrices is used to develop an e- voting scheme. The e-voting is done with the support of a trusted authority. The requirements like privacy, universal verifiability are satisfied in the proposed scheme.

References

[1] B. Adida and R. L. Rivest, Scratch vote self-contained paper-based cryptographic voting, WPES'06, Alexandria, Virginia, USA, 2006, pp. 29–39.

[2] D. Chaum, Untraceable electronic mail return addresses and digital pseudonyms, Communications of the ACM, Vol. 24(2), 1981, pp. 84– 88.

[3] C. H. Chen, C. M. Lan and G. Horng, A practical voting system for small-scale election, IEEE, 2005, pp. 322–326.

[4] J. Cohen and M. Fischer, A robust and verifiable cryptographically secure election scheme, in Proceedings of 26th IEEE Symposium on 14 Foundations of Computer Science, 1985, pp. 372–382.

[5] R. Cramer, M. Franklin, B. Schoenmakers and M. Yung, Multi authority secret ballot elections with linear work, in Advances in Cryptology, EUROCRYPT'96, Vol. 1070, Lecture Notes in Computer Science, Springer-Verlag, 1996, pp. 72–83.

[6] R. Cramer, R. Gennaro and B. Schoenmakers, A secure and optimally efficient multi-authority election scheme, in Advances in Cryptology – EUROCRYPT'97, Vol. 1233, Lecture Notes in Computer Science, 36 Springer-Verlag, 1997, pp. 103–118.

[7] C. Gang, An electronic voting scheme based on secure multi-party computation, International Symposium on Computer Science and Computational Technology, 2008, pp. 292–294.

[8] C. T. Li, M. S. Hwang and C. Y. Liu, An electronic voting protocol with deniable authentication for mobile ad hoc networks, Journal of 8 Computer Communications, Vol. 31, 2008, pp. 2534–2540.

[9] H. T. Liaw, A secure electronic voting protocol for general elections, Computers & Security, Vol. 23 2004, pp. 107–119.

[10] J. Karro and J. Wang, Towards a practical, secure, and very large scale online election, in Proceedings of the Annual Computer Security Applications Conference, 1999, pp. 161–169.

[11] Mukesh Kumar Singh, Public Key Cryptography with Matrices, Proceedings of the 2004 IEEE Workshop on Information Assurance United States Military Academy, pp.146-152, 2004.

[12] C.Porkodi , R.Arumugnathan, K.Vidya, Single authority e-voting based on elliptic curves, Journal of Discrete Mathematical Sciences & Cryptography, Vol.13, No.03, pp. 209–217, 2010.

[13] C.Porkodi , R.Arumugnathan, K.Vidya, Multi-authority Electronic Voting Scheme Based on Elliptic Curves, International Journal of Network Security, Vol. 12, No. 2, 2011, pp. 84-91.

[14] Ralf Kusters and Johannes Muller, Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations, Springer International Publishing AG 2017 R. Krimmer et al. (Eds.): E-Vote-ID 2017, LNCS 10615, pp. 21–41, 2017.

[15] C. Song, X. Yin and Y. Liu, A practical electronic voting protocol based upon oblivious signature scheme, International Conference on Computational Intelligence and Security, 2008, pp. 381–384.

[16] L. Wang, J. Guo and M. Luo, A more effective voting scheme based on blind signature, 2006, pp. 1507–1510.
[17] H. Wei, Z. Dong and C. K. Fei, A receipt-free punch-hole ballot electronic voting scheme, in 3rd International IEEE Conference on Signal Image Technologies and Internet-Based System, 2008, pp. 355–360.
[18] Xun Yi, P. Cerone and Yanchun Zhang, "Secure Electronic Voting for Mobile Communications," *IEEE 63rd Vehicular Technology Conference*, 2006, pp. 836-840.
[19] Liu, Y., Zhao, Q. E-voting scheme using secret sharing and K-anonymity. World Wide Web 22, (2019), pp. 1657–1667.
[20] Zhen-Yu Wu, Ju-Chuan Wu, Sung-Chiang Lin, Charlotte Wang, An electronic voting mechanism for fighting bribery and coercion, Journal of Network and Computer Applications, Vol. 40, 2014, pp. 139-150.