Multi-authority Electronic Voting Scheme Based on Elliptic Curves

Chinniah Porkodi, Ramalingam Arumuganathan, and Krishnasamy Vidya
(Corresponding author: Chinniah Porkodi)

Department of Mathematics and Computer Applications, PSG College of Technology
Peelamedu, Coimbatore, Tamilnadu- 641 004, India
(Email: {porkodi_c2003, ran_psgtech}@yahoo.co.in)
(Received May 25, 2009; revised and accepted Mar. 15, 2010)

Abstract

In this paper, a new multi authority electronic voting scheme based on elliptic curves is proposed. According to the proposed scheme, each voter casts the vote as a point on the elliptic curve and the final tally is computed with the assistance of multiple authorities. A trusted center is involved in the scheme to distribute the shared secret key among the authorities and the Shamir (t, n) threshold scheme is used for key distribution. The proposed scheme also meets the essential requirements of e-voting system. Ultimately, the proposed voting scheme fortifies the security properties of the electronic voting procedure, since the secrecy of the particularized vote is preserved by ElGamal cryptosystem and Elliptic curve discrete logarithm problem.

Keywords: ElGamal cryptosystem, elliptic curves, elliptic curve discrete, e-voting logarithm problem, homomorphic encryption

1 Introduction

Supporting group decisions has become an important topic in the field of computer applications and electronic voting (e-voting) has a great attention regarding this issue. Electronic voting has been intensively studied for over the past 20 years [2]. A multi authority electronic voting scheme is a set of protocols that allow a set of voters to cast their votes in a bulletin board and the final tally is computed with the assistance of a set of authorities.

Any e-voting scheme must accomplish the following requirements:

- **Privacy.** ensures that no one links the ballot to the voter.
- **Universal Verifiability.** provides the facility that anyone in the voting system should be able to independently verify that all valid votes have been counted correctly.
- **Robustness.** The system is robust, if it ensures that all the system can recover from the faulty behavior of any (reasonably sized) location of parties; i.e. Failure resulting from partial authorities or voters can be detected or tolerated.
- **Efficiency.** The computational loads must be light and able to be performed within a reasonable amount of time.
- **Eligibility.** Only the eligible voters, who pass the authentication process, can be allowed to vote.
- **Completeness.** It is unable to fake a vote, that is unable to remove a valid vote from the final tally, and unable to add an invalid vote to the final tally.
- **Uncoercibility.** No voter can be forced to vote in a particular way.

The first electronic voting scheme was introduced by Chaum [3], in which voters electronically cast their ballot over insecure networks. Cramer et al. [6, 7], proposed multi-authority secret-ballot election scheme and the performance in this scheme is optimal in the sense, that time and communication complexity is minimal both for the individual voters and the authorities, but it is a more complicated scheme, since, it is based on the q-th residuosity assumption.

Cohen and Fischer [5], proposed a robust and verifiable cryptographically secure election scheme based on a r-th residuosity assumption. Wang et al. [18], proposed an electronic voting scheme based on blind signature that distributes the powers to more administrators, but, if the voting center is not trustful and IP trace between the voting center and voters is available, then, the proposed scheme will be easily forgeable. Chun et al. [4] presented a one-server Private Information Retrieval (PIR) electronic voting scheme with secure coprocessor and it is suitable for small-scale election only, because of its high security, low cost and good efficiency.

Li et al. [12], developed an electronic voting scheme on ad hoh networks. Adida and Rivest [1] presented Scratch & Vote, a cryptographic voting system designed to minimize cost and complexity in which, any helper organization or the voter himself/herself can audit the ballot without interacting with election officials before the voter casts his/her ballot.

Liaw [13], proposed an e-voting protocol using smart cards, which allows the voter to ask the center to recount his vote by sending the receipt, if his/her vote has not been counted, but this approach does not satisfy the requirement of uncoercibility. Gang [8], Song et al. [16], Wei et al. [17], Liaw [13], Karro and Wang [9] and Liu [15] had done related work in e-voting.

Koblitz [10], introduced an efficient elliptic pubic key cryptosystem which uses considerably shorter key but offers the same level of security as other asymmetric algorithms using much larger keys. This security level is due to the fact that elliptic curve discrete logarithm problem appears to be much harder than the discrete logarithm problem in DSA and RSA. For example, an elliptic curve cryptosystem with public key size of 160 bits is as secure as RSA and DSA cryptosystems with the pubic key of size 1024 bits. Lee et al. [11] and Lin [14] had done related work in elliptic curves.

In this paper, a new multi authority electronic voting based on elliptic curves satisfying the requirements of electronic election is proposed. Elliptic curve discrete logarithm is the underlying principle for the security of the voting scheme. A trusted center is involved in the scheme to verify the authentication of voters and authorities. The trusted center is also responsible for constructing and distributing the shared secret keys to the authorities and publishing the public key of it and the authorities on the bulletin board.

All the existing voting schemes are developed on discrete logarithm problem and the parameters involved in the scheme chosen to those similar in DSA. Thus, these voting schemes require larger keys to offer higher security. The proposed e-voting scheme based on elliptic curves with smaller key size provides the same level security as the existing algorithms. The complex modular exponentiation is involved in the existing schemes; where as, the elliptic curve operations in the proposed scheme are not much complex. The proposed scheme satisfies all the requirements of e-voting. The scheme is illustrated numerically using Mat lab.

The paper in organized in such a way that, Section 2 gives Mathematical primitives behind the scheme, Section 3 discusses over view approach, Section 4 describes vote casting, Section 5 discusses tally computing, Section 6 provides proof of knowledge, Section 7 deals with analysis, Section 8 provides a numerical illustration, Section 9 discusses multi way election, Section 10 provides numerical illustration for multi way election and Section 11 concludes the paper.

2 Mathematical Primitives

2.1 Elliptic Curve

Let K be a field (either the field Q, R, C or F_p of characteristic $\neq 2$, 3, then an elliptic curve over K is the set of points (x, y) with $x, y \in K$ satisfying $E : y^2 = x^3 + ax + b$, (where the cubic on the right-hand side has no multiple roots, i.e., $4a^3 + 27b^2 \neq 0$) together with a single element O_E, called point at infinity.

2.2 Addition of Points on Elliptic Curve

Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ be two points on elliptic curve $y^2 = x^3 + ax + b$, then $P_3 = (x_3, y_3) = p_1 + p_2$ on E is computed as

$$\begin{aligned} P_1 + P_2 &= \begin{cases} O_E, & \text{if } x_1 = x_2 \& y_1 = -y_2 \text{ where,} \\ (x_3, y_3), & \text{otherwise} \end{cases} \\ (x_3, y_3) &= (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1), \text{ and} \\ \lambda &= \begin{cases} \frac{3x_1^2 + a}{2y_1}, & \text{if } P_1 = P_2 \\ \frac{y_2 - y_1}{x_2 - x_1}, & \text{otherwise} \end{cases} \end{aligned}$$

2.3 Elliptic Curve Discrete Logarithm Problem

Suppose $Q = xP$ represents that the point P on elliptic curve $E(F_p)$ is added to itself x times, then the elliptic curve discrete logarithm problem is to determine x given P and Q. It is relatively easy to calculate Q given x and P, but it is very hard to determine x given Q and P.

2.4 Analogue of the ElGamal Encryption

The communication between Alice and Bob is done as follows:

1) Alice and Bob choose an elliptic curve $E(F_p)$ and a random base point "P" of order "q".

2) Alice and Bob chooses secret keys as the random integers r_a and r_b. The public keys of Alice and Bob are r_a and r_b.

3) To send a message point "m" to Bob, Alice choose a random integer "k" and sends the pair of points $(kp, m + k(r_bP))$.

4) To read m, Bob computes $m + k(r_bP) - r_b(kP) = m$.

2.5 Homomorphic Encryption

Suppose $(c_1, c_2) = (\alpha P, m + \alpha(r_bP))$ and $(c_1^1, c_2^1) = (\alpha P^1, m^1 + \alpha^1(r_bP))$ are encryptions of messages m and m_1, then is an encryption for $(m + m_1)$.

$$\begin{aligned} \text{Since} \quad & (c_1, c_2) + (c_1^1, c_2^1) \\ = \; & (c_1 + c_1^1, c_2 + c_2^1) \\ = \; & (\alpha P + \alpha^1 P, m + \alpha(r_bP) + m^1 + \alpha^1(r_bP)) \\ = \; & ((\alpha + \alpha^1)P, (m + m^1) + (\alpha + \alpha^1)(r_bP)). \end{aligned}$$

Thus ElGamal encryption is homomorphic.

3 Overview of the Approach

3.1 Bulletin Board

The communication model required for the proposed scheme is best viewed as a publicly accessible memory, which is called a bulletin board. Each member has a designated section of the memory to post messages and no posted messages can be tampered. No party can erase any information from the bulletin board, but each active participant can append messages to its own designated section. Also it is assumed that, there is some authentication mechanism such as digital signatures to guarantee the origin of posted messages, which is to ensure only eligible voter can post messages in his/her section and authorities to post sub tally. Each published message is signed, so the validity can be easily verified by any third party. All Communication through the bulletin board can be read by any party.

To execute an election, the parties perform the following: Each voter selects the desired vote and constructs a ballot (encryption of the vote) and posts the ballot to the bulletin board together with a compact proof, that it contains a valid vote. However, with the assistance of a threshold number of authorities the final tally can be obtained.

3.2 Setting up the Scheme

The participants in the election scheme are the voters $V_1, V_2, \cdots V_m$, authorities $A_1, A_2, \cdots A_n$ and a trusted center. To set up the scheme, the trusted center chooses an elliptic curve $E(F_q)$ over a field F_p, a base point P of order q and secret $s \in Z_q^*$. The trusted center publishes $E(F_p)$, P, q and $h = sP$ on the bulletin board. Homomorphic encryption is used to encrypt the vote. Trusted center chooses a secret polynomial $f(x) = s + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1} (\mathrm{mod} q)$ and computes $s_1 = f(1), s_2 = f(2), \cdots, s_n = f(n)$. Trusted center sends the secret pair to the i^{th} authority A_i, where i is the identity of A_i. If at least t- authorities pool their secret shares, then the secret key of the trusted center s can be recovered using Shamir's (t, n)-threshold scheme. The pubic keys $h_1 = s_1P$ of the authorities are published on the bulletin board by the trusted center. In the described scheme, each voter selects his/her choice (yes or no), encrypts with a homomorphic encryption algorithm and signs the cryptogram. Particularly, yes vote is denoted by 1 and no vote by (-1).

4 Vote Casting

Each voter V_i chooses a secret $\alpha_i \; in Z_q^*$ and selects his/her vote $v_i \in \{1, -1\}$ and encrypts the vote by the encryption as $c_i = (c_{i,1}, c_{i,2}) = (\alpha_i P, \alpha_i h + v_i P)$ and posts it on the bulletin board. Here, it is assumed that V_i follows the protocol and correctly forms c_i. The voter has to perform a proof of knowledge discussed in Section 6, which shows that he/she really does; otherwise, the vote becomes invalid.

5 Tally Computing

Any one, who views the published details on the bulletin board, can compute

$$\begin{aligned} c &= (c_1, c_2) \\ &= (\sum_{i=1}^{m} c_{i,1}, \sum_{i=1}^{m} c_{i,2}) \\ &= ((\sum_{i=1}^{m} \alpha_i)P, (\sum_{i=1}^{m} \alpha_i)h + dP). \end{aligned}$$

Since the encryption is homomorphic. Thus $c = (c_1, c_2)$ is the encryption of dP, where $d = \sum_{i=1}^{m} v_i$ is the difference between the number of yes votes and no votes. Final tally is computed with the assistance of at least t- honest authorities out of n and let J be the set of these honest authorities. Each authority A_j posts $w_j = s_j(c_1)$ with his/her identity j. Here, it is assumed that the authorities are honest and follows the protocol described in Section 6. As soon as all $A_j \in J$ have posted their messages $w_j = s_j(c_1)$, any one can recover the final tally, by computing $c_2 - s_j(c_1)$. The value of sc_i is obtained from $w_j = s_j(c_1)$ as below.

$$\begin{aligned} \text{Now,} \quad & \sum_{j \in J} (\prod_{k \in J, k \neq j} (\frac{k}{k-j}) w_j) \\ &= \sum_{j \in J} (\prod_{k \in J, k \neq j} (\frac{k}{k-j})(s_j, c_1)) \\ &= \sum_{j \in J} (\prod_{k \in J, k \neq j} (\frac{k}{k-j}) s_j(c_1)) \\ &= s(c_1), \text{ by Shamir's threshold scheme.} \\ \text{Also, } c_2 - s(c_1) &= (\sum_{i=1}^{m} \alpha_i) sP + dP - s(\sum_{i=1}^{m} s\alpha_i)P, \\ &= (\sum_{i=1}^{m} \alpha_i) sP + dP - (\sum_{i=1}^{m} s\alpha_i)P, \\ &= dP, \text{ since } \alpha_i(sP) = (\alpha_i s)P. \end{aligned}$$

Thus, any tallier can compute from the information available on the bulletin board posted by the voters and authorities, where denotes the difference between the positive and negative votes.

The tallier obtains this difference d, by computing the points $m(-P), (m-1)(-P), \cdots, P, 2P, \cdots, mp$ and comparing with dP in each step. The number of yes votes x and the number of no votes y is obtained by solving $x - y = d, x + y = m$.

6 Proofs of Knowledge

6.1 Authority's Proof

In the decryption protocol, each authority has to prove that, he/she really posted $w_j = s_j c_1$, where s_j is the secret key. As $h_j = s_j P$ is published on the bulletin board, the authority has to prove that w_j and h_j have the same logarithm with respect to c_1 and P and that he/she knows this logarithm. The notation is simplified and an interactive proof of knowledge of the common logarithm k of $y_1 = kP_1$ and $y_2 = kP_2$ is described.

6.1.1 Interactive Proof of Knowledge

Proof of Log Equation (P_1, y_1, P_2, y_2):

1) Authority chooses $r \in Z_q$ at random, computes and sends $a = (a_1, a_2) = (rP_1, rp_2)$ to the verifier; i.e. the authority commits, that two points have the same logarithm r with respect to two different points P_1 and P_2.

2) Verifier chooses $c \in Z_q$ at random and sends to verifier, which is a challenge by the verifier.

3) Authority computes $b = r - ck$ and sends b to the verifier, which is the response by the authority.

4) Verifier accepts if only if, $a_1 = bP_1 + cy_1$ and $a_2 = bP_2 + cy_2$.

6.1.2 Non Interactive Proof of Knowledge

Proof of Log Equation (P_1, y_1, P_2, y_2): The interactive proof knowledge can be converted as a non interactive one by using a collision resistant hash function "hash". The authority chooses $r \in Z_q$ at random and sets $a = (a_1, a_2) = (rP_1, rP_2)$. Then he/she computes the challenge $c = hash(P_{1x} \| y_{1x} \| P_{1x} \| P_{2x} \| y_{2x} \| (bP_1 + cy_1) \| (bP_1 + cy_1))$ and sets $b = r - ck$, where $P_{1x}, y_{1x}, P_{2x}, y_{2x}, a_{1x}, a_{2x}$ denote the X-coordinates of P_1, y_1, P_2, y_2, a_1, and a_2 respectively. The verifier accepts only if, $c = hash(P_{1x} \| y_{1x} \| P_{2x} \| y_{2x} \| (bP_1 + cy_1)_x \| (bP_2 + cy_2)_x)$. The verifier need not know $a = (a_1, a_2)$ to check the verification condition. If one trusts the collision resistant function, from $hash(u) = hash(v)$, it can be concluded that $u = v$. Thus in election protocol, each authority and each voter completes his/her message with a non-interactive proof, which convinces everyone that he/she, followed the protocol.

6.1.3 Completeness

The equations $a_1 = bP_1 + cy_1$ and $a_2 = bP_2 + cy_2$ are satisfied only if, the authority and the verifier follow the protocol correctly and the authority knows a common logarithm for y_1 and y_2.

6.1.4 Soundness

A cheating prover Eve can convince the verifier with a probability $\frac{1}{q}$ in the following way:

1) Eve chooses $r, c^1 \in Z_q$ at random and sets $a = (a_1, a_2) = (rP_1 + c^1 y_1, rP_2 + c^2 y_2)$ and sends it to the verifier.

2) Verifier chooses $c \in Z_q$ at random and sends to Eve.

3) Eve sends "r" to the verifier.

4) Verifier accepts, if and only if $a_1 = bP_1 + cy_1$ and $a_2 = bP_2 + cy_2$. This is possible if and only if $c = c^1$. The event $c = c^1$ occurs with probability $\frac{1}{q}$. Thus, Eve succeeds in cheating with a probability $\frac{1}{q}$. If Eve can convince the verifier with a probability greater than $\frac{1}{q}$, then he/she has to answer at least two challenges correctly for a given commitment a. Suppose Eve knows an ordered pair (a_1, a_2) for which, he/she can answer two distinct challenges:

$$\begin{aligned} a_1 &= bP_1 + cy_1, \\ a_2 &= bP_2 + cy_2, \\ a_1 &= (b^1 P_1 + c^1 y_1), \\ a_2 &= b^1 P_2 + c^1 y_2) \end{aligned}$$

then he/she can compute

$$\begin{aligned} (b - b^1)P_1 &= (c^1 - c)y_1, \\ (b - b^1)P_2 &= (c^1 - c)y_2 \\ \frac{(b - b^1)}{c^1 - c}P_1 &= y_1, \\ \frac{b - b^1}{c^1 - c}P_2 &= y_2. \end{aligned}$$

Thus, Eve can find $\frac{(b-b^1)}{c^1-c)}$ from the above two equations which in turn implies that Eve can solve the computational hard elliptic curve discrete logarithm problem. Hence, the probability of successes of cheating prover is bounded by $\frac{1}{q}$.

6.2 Voter's Proof

In the vote- casting protocol, each voter has to prove that he/she really encrypted a vote $v_i P \in (P, -P)$; That is the voter V_i has to prove $c_i = (c_i, 1, c_i, 2) = (\alpha_i P, \alpha_i h + v_i P)$ and $v_i P \in (p, -P)$.

The voter performs a proof knowledge that he/she knows α_i for either $c_i = \alpha_i P$ and $c_{i,2} - P = \alpha_i h$, or $c_{i,1} = \alpha_i P$ and $c_{i,2} + P = a_i h$. Each of the two alternatives could be proven interactively or non-interactively as in authority's proof.

7 Analysis

The proposed voting scheme satisfies all the requirements of e-voting.

- **Eligibility:** The voters and authorities must register their identities to the trusted center, so that only authorized persons can post the messages.
- **Privacy:** During the voting phase, only encrypted ballot messages are published on the bulletin board. Hence, an attacker gains no knowledge from them and they cannot link the ballot to the voter.
- **Universal verifiability & Correctness:** The final ballot and the proof of validity are posted on the bulletin board and hence, any one can verify the validity of the final ballots, the correctness of the ballot collection and the final result. Thus, valid votes are counted correctly.
- **Fairness:** An attacker can decrypt the ballot messages only if, he/she has the knowledge of the secret key "s" of the system and to recover "s", and has to solve the elliptic curve discrete logarithm problem which is highly infeasible. Hence, no one can learn partial results of an election and the entire voted ballots are kept secret until the end of the voting process. The final tally is obtained, only after a minimum number of authorities post the messages.
- **Robustness:** The final tally is computed based on (t, n) threshold ElGamal encryption scheme, which can tolerate the failure of maximum $(n - t)$ authorities. Any invalid ballot can be detected and excluded from the tally.

8 Numerical Illustration

8.1 Setting up the Scheme

Assume that 8 voters and 6 authorities are involved in the voting scheme. The trusted center chooses the elliptic curve $E(F_p)$, given by $y^2 = x^3 - 4(\text{mod}211)$ with $p = 211$. The trusted center selects the base point $P = (94, 57)$ of order $q = 241$ and the secret polynomial $f(x) = 52 + 15x + 11x^2 + 14x^3 + 28x^4(\text{mod}241)$. The secret key of the trusted center is $s = 52$. The trusted center transmits the secret shares to the authority A_i, for through a secure channel; i.e. trusted center sends $(1, 120)$, $(2, 204)$, $(3, 191)$, $(4, 158)$, $(5, 131)$, $(6, 85)$ to the authorities securely.

The trusted center posts $E(F_p)$, p, P, q, $h = sP = (82, 134)$ and s_iP for $i = 1, 2, \cdots, 6$ on the bulletin board. The values of are $(196, 29)$, $(175, 155)$, $(6, 210)$, $(87, 50)$, $(118, 56)$, $(54, 138)$ respectively. As the degree of the secret polynomial is 4, the final tally is computed only if, at least 5 authorities post their messages on the bulletin board.

8.2 Encryption Phase

Each voter V_i encrypts his vote $v_iP \in \{P, -P\}$ as $(c_{i1}, c_{i2}) = (\alpha_iP, \alpha_ih + v_iP)$ and posts it in to the bulletin board. The encrypted votes of 8 Voters are given in the following table.

Table 1: Numerical values in vote casting phase - multi authority two way voting

Sl No	Voter V_i	$c_{i,1} = \alpha_iP$	$c_{i,2} = \alpha_ih + v_iP$
1	V_1	(50, 57)	(45, 179)
2	V_2	(195, 72)	(145, 127)
3	V_3	(159, 114)	(89, 196)
4	V_4	(20, 191)	(69, 191)
5	V_5	(159, 114)	(79, 136)
6	V_6	(191, 196)	(83, 124)
7	V_7	(17, 30)	(74, 210)
8	V_8	(20, 191)	(69, 191)

Table 2: Numerical values in tally computing phase - multi authority two way voting

Authorities	$w_j = S_jc_1$	$\prod_{k\in J,k\neq j}(\frac{k}{k-j})w_j$
A_1	(182, 100)	(34, 138)
A_2	(209, 58)	(183, 153)
A_3	(207, 96)	(181, 209)
A_4	(23, 66)	(111, 145)
A_5	(30, 153)	(64, 17)
A_6	(168, 205)	(168, 6)

8.3 Decryption Phase

Once the voters post the encrypted votes $(c_i, 1, c_i, 2)$ for $i = 1, 2, \cdots, 8$ on the bulletin board, any one who views the details on the bulletin board, can compute $c_1 = \sum_{i=1}^{8} c_i, 1 = (36, 34)$ and $c_2 = \sum_{i=1}^{8} c_i, 2 = (172, 16)$ including the authorities. Suppose, six authorities $j = \{A_1, A_2, \cdots, A_6\}$ post for $j = 1, 2, \cdots, 6$ on the bulletin board, then any tallier can compute $\prod_{k\in J,k\neq j}(\frac{k}{k-j})w_j$ for $j = 1, 2, \cdots, 6$ and inturn the value of sc_i. The values of w_j and $\prod_{k\in J,k\neq j}(\frac{k}{k-j})w_j$ are tabulated below.

Now, $sc_1 = \prod_{k\in J,k\neq j}(\frac{k}{k-j})w_j = (124, 119)$. The final tally is computed as $c_2 - sc_1 = dP = (124, 119)$. Now computing, $-8P$, $-7P$, $-6P$, $\cdots$, $-P$, $-2P$, $-3P$, $\cdots$, $-8P$, and comparing with dP, it is obtained that $d = 2$. Suppose the number of yes votes is x and the no votes y then, it is obtained that $x + y = 8$ and $x - y = 2$ and hence, the number yes votes is 5 and no votes is 3.

9 Extension to Multi Way Election

9.1 Encoding in Multi Way Election

Assume that participants $V_1, V_2, \cdots, V_m$ have choice of votes as $u_1, u_2, \cdots, u_r$ instead of the two choices [1, -1]. To encode these votes the trusted center chooses "r" base

points $P_1, P_2, \cdots, P_r$ and encodes v_j by P_j and publishes the encoding on the bulletin board.

9.2 Vote Casting

Each Voter V_i encrypts his/her vote u_j as $c_i = (c_{i,1}, c_{i,2}) = (\alpha_i P, \alpha_i h + P_j)$ and posts it on the bulletin board. Each voter shows by an interactive proof of knowledge that he/she knows $c_{i,1} = \alpha_i P$ and for exactly $\alpha_i h = c_{i2} - P_j$ one as in authority's proof.

9.3 Tally Computing

Any one, who views the bulletin board, can compute

$$\begin{aligned} c &= (c_1, c_2) \\ &= (\sum_{i=1}^{m} c_{i,1}, \sum_{i=1}^{m} c_{i,2}) \\ &= ((\sum_{i=1}^{m} \alpha_i)P, (\sum_{i=1}^{m} \alpha_i)h + (\sum_{j=1}^{r} d_1 P_j)) \end{aligned}$$

where, d_j denotes the number of votes favor to u_j. Thus $c = (c_1, c_2)$ is the encryption of the votes $u_1, u_2, \cdots, u_r$. Final tally is computed with the assistance of at least t-honest authorities out of "n" and let J be the set of these honest authorities. Each authority A_j posts his/her message $w_j = s_j(c_1)$ with their corresponding identity j. As soon as all $A_j \in J$ have posted $w_j = s_j(c_1)$, anyone, who views the bulletin board, can recover the final tally, by computing $c_2 = s(c_1) = \sum_{j=1}^{r} d_j P_j$. Now, any tallier can get final vote $(d_1, d_2, \cdots, d_r)$ by computing $\sum_{j=1}^{r} d_j P_j$ for values of satisfying $0 \le d_j \le m$, $\sum_{j=1}^{r} d_j = m$ and comparing with summation obtained from $c_2 - s(c_1)$. Here is uniquely determined by in the sense that computing a different solution $(d_1^1, d_2^1, \cdots, d_r^1)$ would contradict the elliptic curve discrete logarithm problem, because the base points were chosen independently.

9.4 Uniqueness of the Final Tally $(d_1, d_2, \cdots, d_r)$

9.4.1 The Representation Problem

Let $r \ge 2$ and $(P_1, P_2, \cdots, P_r)$ be distinct base points of $E(F_p)$, then $(P_1, P_2, \cdots, P_r)$ is called a generator of length r. For any $Q \in E(F_p)$, $d = (d_1, d_2, \cdots, d_r) \in Z_q^r$ is a representation if $Q = \sum_{j=1}^{r} d_j P_j$.

To represent Q, the elements $d_1, d_2, \cdots, d_{r-1}$ can be chosen arbitrarily. Thus, d_r is uniquely determined. Therefore, each $Q \in E(F_p)$ has q^{r-1} representations. Given $Q \in E(F_p)$, the probability that a randomly chosen $d \in Z_q^r$ is a representation of Q is $\frac{q^r - 1}{q^r} = \frac{1}{q}$.

Theorem 1. *No polynomial algorithm can exist which, on input of a randomly chosen of length $r \ge 2$, outputs $Q \in E(F_p)$ and two different representations of Q.*

Proof. Assume that such an algorithm exists. On input of randomly chosen generator $(P_1, P_2, \cdots, P_r)$, it outputs $Q \in E(F_p)$ and two different representations $d = (d_1, d_2, \cdots, d_r)$ and $d^1 = (d_1^1, d_2^1, \cdots, d_r^1)$ of Q. Then $d - d^1$ is a representation of O_E, since $O_E = Q - Q = \sum_{j=1}^{r} d_j P_j - \sum_{j=1}^{r} d_j^1 P_j = \sum_{j=1}^{r} (d_j - d_j^1) P_j$.

Thus, there exists a polynomial algorithm A, which on input a randomly chosen generator outputs a nontrivial representation of O_E. This algorithm A, may be used to define an algorithm B, which on input $P \in E(F_p)$, $P \ne O_E$ and $P^1 \in E(F_p)$ computes the discrete logarithm problem of P^1 with respect to P. □

Algorithm 1 Algorithm: B

1: Input P, P^1
2: repeat
3: select $i \in \{1, 2, \cdots, r\}$
4: select $u_j \in Z_q^*, 1 \le j \le r$, uniformly at random
5: $P_i \leftarrow u_i P^1$, $P_j \leftarrow u_i P^1$, $1 \le j \ne 1 \le r$
6: $(d_1, d_1, \cdots, d_r) \leftarrow A(P_1, P_2, \cdots, P_r)$
7: until $d_i u_i$ is not a multiple of q
8: return - $(d_i u_i)^{-1} \langle \sum_{i \ne j} d_j u_j \rangle (\mathrm{mod} q)$

The returned value is indeed the discrete logarithm of P^1, which is a contradiction to the fact that elliptic curve discrete logarithm is an computationally hard problem. Hence there exists no polynomial algorithm can exist which, on input of a randomly chosen of length $r \ge 2$, outputs $Q \in E(F_q)$ and two different representations of Q.

Corollary 1. *The returned value $-(d_i u_i)^{-1} \langle \sum_{i \ne j d_j u_j} \rangle$ (mod$q$) in algorithm B is discrete logarithm of P^1 with respect to P.*

Proof. Using algorithm A, a representation (d_1, d_2, $\cdots$, d_r) of O_E can be obtained. Therefore

$$\begin{aligned} \sum_{i=1}^{r} a_i P_i &= O_E \\ d_i P_i + \sum_{i \ne j} d_j P_j &= O_E \\ d_i u_i P_1 + \sum_{i \ne j} d_j u_j P &= O_E(\text{ by step 4}) \\ d_i u_i P_1 &= \sum_{i \ne j} d_j u_j P \\ P^1 &= -(d_i u_i)^{-1} \sum_{i \ne j} d_j u_j P. \end{aligned}$$

$-(d_i u_i)^{-1} \langle \sum_{i \ne j} d_j u_j \rangle \bmod q$ is the discrete logarithm of P^1 with respect to P.

□

Table 3: Numerical values in vote casting phase - multi authority multi way voting

S No	Voter V_i	$c_{i,1} = \alpha_i P$	$c_{i,2} = \alpha_i h + v_i P$
1	V_1	(60, 96)	(130, 203)
2	V_2	(39, 92)	(89, 196)
3	V_3	(174, 163)	(118, 56)
4	V_4	(206, 90)	(67, 57)
5	V_5	(144, 69)	(14, 29)
6	V_6	(95, 194)	(20, 20)
7	V_7	(16, 111)	(81, 136)
8	V_8	(93, 134)	(107, 87)
9	V_9	(150, 85)	(71, 126)
10	V_{10}	(130, 8)	(27, 181)

10 Numerical Illustration

10.1 Setting up the Scheme

Assume that 10 voters and 6 authorities are involved in the voting scheme. The trusted center chooses the elliptic curve $E(F_q)$, given by $y^2 = x^3 - 4(\text{mod}211)$ with $p = 211$. The trusted center selects the base point of order $q = 241$ and the secret polynomial $f(x) = 52 + 60x + 26x^2 + 24x^3 + 13x^4(\text{mod}241)$. The secret key of the trusted center is $s = 52$. The trusted center transmits the secret shares (i, $s_i = f(i)$) to the authority A_i, for $i = 1, 2, \cdots, 6$ through a secure channel; i.e. the trusted center sends (1, 175), (2, 194), (3, 239), (4, 29), (5, 77), (6, 3) to the authorities securely.

Suppose the participants have the choice of voting as u_1, u_2, u_3, u_4. The trusted center selects four distinct base points of the elliptic curve $E(F_p)$ other than $P = (94, 57)$, say $P_1 = (2, 2)$, $P_2 = (6, 1)$, $P_3 = (13, 100)$, $P_4 = (14, 29)$ and encodes u_1, u_2, u_3, u_4 as the points P_1, P_2, P_3, P_4 respectively. The trusted center posts, $E(F_q)$, p, q, $h = sP = (82, 134)$, and s_iP for $i = 1, 2, \cdots, 6$ on the bulletin board. The posted are (182, 100), (167, 30), (124, 92), (27, 30), (121, 210) and (137, 37) respectively. As the degree of the secret polynomial is 4, the final tally is computed only if at least 5 authorities post their messages on the bulletin board.

10.2 Encryption Phase

Each voter V_i encrypts his/her vote as $c_{1i}, c_{i2} = (\alpha_i P, \alpha_i h + P_j)$, where $P_j \in \{P_1, P_2, P_3, P_4\}$ and posts it into the bulletin board. The encrypted votes of 10 voters are given in the following table.

10.3 Decryption Phase

Once the voters post the encrypted votes $c_{i,1}, c_{i,2}$ for $i = 1, 2, \cdots, 10$ on the bulletin board, any one who views the bulletin board can compute $c_1 = \sum^1 0_{i=1} c_{i,1} = (119, 113)$ and $c_2 = \sum^1 0_{i=1} c_{i,2} = (87, 161)$ including the authorities. Suppose the six authorities $j = \{A_1, A_2, \cdots, A_6\}$

Table 4: Numerical values in tally computing phase - multi authority Multi way voting

Authorities	$w_j = S_j c_1$	$\prod_{k \in J, k \neq j} (\frac{k}{k-j}) w_j$
A_2	(80, 136)	(159, 97)
A_3	(72, 14)	(207, 115)
A_4	(51, 136)	(34, 73)
A_5	(50, 57)	(74, 10)
A_6	(168, 6)	(23, 66)
A_7	(179, 199)	(45, 32)

post $(j, w_j = s_j c_1)$ for on the bulletin board, then any tallier can compute $\prod_{k \in JK \neq j} (\frac{k}{k-j}) w_j$ for $j = 1, 2, \cdots, 6$ and inturn the value of sc_1. The values of and are tabulated below.

11 Conclusion

In this paper a new e-voting scheme based on elliptic curves is proposed. As far as the authors knowledge is concerned, the concept of elliptic curves has not previously been applied to multi authority election scheme. The elliptic curve cryptosystem requires considerably shorter key and offer the same level of security as other asymmetric algorithms RSA and DSA which need much larger keys. Hence, the proposed e-voting provides the same level of security as other e-voting schemes developed on ElGamal cryptosystem with parameter assumptions as in DSA. The modular exponentiation is involved in the existing voting schemes, where as, in the proposed scheme, the computation of the ballot requires only a few point additions; and hence, the scheme is computationally efficient. In this paper two multi authority election schemes were discussed. The first one is a multi authority voting scheme in which the vote v_i is selected from [-1, 1]. The second scheme multi way election is an extension of the first one in which the vote v_i has more than two choices $u_1, u_2, \cdots, u_r$. The proposed scheme satisfies well-known requirements such as privacy, universal verifiability and robustness of e-voting. The final tally computation is complicated in proposed scheme and hence the scheme is applicable at small scale.

Now $sc_1 = \sum_{j \in J} \prod_{k \in J, k \neq j} (\frac{k}{k-j}) w_j = (70, 200)$. Any one, who views the bulletin board, can recover the final tally $c_2 - s(c_1) = \sum_{j=1}^{4} d_j P_j = (99, 31)$.

References

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

[2] A. Azadmanesh, A. Farahani, and L. Najjar, "Fault tolerant weighted voting algorithms," *International Journal of Network Security*, vol. 7, no. 2, pp. 240-248, 2008.

[3] D. Chaum, "Untraceable electronic mail return addresses and digital pseudonyms," *CACM,* vol. 24, no. 2, pp. 84-88, 1981.
[4] C. H. Chen, C. M. Lan, and G. Horng, "A practical voting system for small-scale election", *3rd International Conference on InformationTechnology: Research and Education, ITRE*, pp. 322-326, 2005.
[5] J. Cohen and M. Fischer, "A robust and verifiable cryptographically secure election scheme," *Proceedings of 26th IEEE Symposium on Foundations of Computer Science (FOCS '85)*, pp. 372-382, 1985.
[6] R. Cramer, Ma. Franklin, B. Schoenmakers, and M. Yung, "Multi authority secret ballot elections with linear work," *Advances in Cryptology, Eurocrypt '96*, vol. 1070, pp. 72-83, LNCS, Springer-Verlag, 1996.
[7] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi authority election scheme," *Advances inCryptology Eurocrypt '97*, vol. 1233, pp. 103-118, LNCS, Springer-Verlag, 1997.
[8] C. Gang, "An electronic voting scheme based on secure multi-party computation," *ISCSCT '08*, pp. 292-294, 2008.
[9] J. Karro and J. Wang, "Towards a practical, secure, and very large scale online election," *ACSAC '99*, pp.161-16, 1999.
[10] N. Koblitz, "Elliptic Curves Cryptosystems," *Mathematics of computation*, vol. 48, pp. 203-209, 1987.
[11] J. Lee, H. Kim, Y. Lee, S. M. Hong, and H. Yoon, "Parallelized scalarmultiplication on elliptic curves defined over optimalextension field," *International Journal of Network Security*, vol. 4, no.1, pp. 99-106, 2007
[12] C. T. Li, M. S. Hwang, and C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, pp. 2534- 2540, 2008.
[13] H. T. Liaw, "A secure electronic voting protocol for general elections," *Computers & Security*, vol. 23, no. 2, pp. 107-119, 2004.
[14] T. C. Lin, "Algorithms on elliptic curves over fields of characteristic two with non-adjacent forms," *International Journal of Network Security*, vol. 9, no. 2, pp. 117-120, Sep. 2009.
[15] X. Liu and S. Tang, "Formal privacyanalysis of an electronic voting scheme," *International Conference on Computational Intelligence and Security 2008*, pp. 283-287.
[16] C. Song, X. Yin, and Y. Liu, "A practical electronic voting protocol based upon oblivious signature scheme," *International Conference on Computational Intelligence and Security*, pp. 381-384, 2008.
[17] H. Wei, Z. Dong, and K. F. Chen,"A receipt-free punch-hole ballot electronic voting scheme," *International IEEE Conference on Signal-Image Technologies and Internet-Based System*, pp. 355-360, 2008.
[18] L. Wang, J. Guo, and M. Luo, "A more effective voting scheme based on blind signature," *International Conference on Computational Intelligence and Security*, pp. 1507-1510, 2006.

Chinniah Porkodi is a Senior Lecturer in the Department of Mathematics and Computer Applications, PSG College of Technology, Coimbatore, India. She received M.Sc; M.Phil in Mathematics and currently pursuing Ph.D degree in the field of Cryptography. Her area of interest includes Number theory, Linear Algebra and Statistics.

Ramalingam Arumuganathan is a Professor in Department of Mathematics and Computer Applications, PSG College of Technology, Coimbatore, India. His area of interest includes Queuing theory, Cryptography, Number theory, Wavelet transforms and Linear Algebra.

Krishnasamy Vidya received M. Sc degree in Applied Mathematics.