Single authority electronic voting based on elliptic curves

C. Porkodi *
R. Arumuganathan †
K. Vidya
Department of Mathematics and Computer Applications
PSG College of Technology
Coimbatore 641 004
Tamilnadu, India

Abstract

In this paper, a new single authority electronic voting scheme is proposed, based on elliptic curves. 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 a single trusted authority. 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 and phrases : *e-voting, elliptic curves, elliptic curve discrete logarithm problem, elgamal cryptosystem, 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. A single 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 the authority.

Any e-voting scheme must accomplish the following requirements.

* *E-mail*: porkodi_c2003yahoo.co.in
† *E-mail*: ran_psgtech@yahoo.co.in

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 3, pp. 209–217