

An anonymous and flexible t -out-of- n electronic voting scheme

Chin-Chen Chang^{1,2*}

Jung-San Lee^{2†}

¹*Department of Information Engineering and Computer Science*

Feng Chia University

100 Wenhwa Rd., Seatwen

Taichung 40724

Taiwan

R.O.C.

²*Department of Computer Science and Information Engineering*

National Chung Cheng University

Chiayi

Taiwan, 621

R.O.C.

Abstract

Voting is always considered as the most important hallmarks in the democratic society. However, there are plenty of problems of the traditional election such as inconvenience, non-mobility, unfairness, non-anonymity, and so on. Furthermore, the cost of the traditional voting often places a heavy burden on the nation. To solve the problems of the traditional election, the concept of “electronic voting” is proposed, where people are allowed to vote over the Internet. The properties of mobility and convenience are the most significant reasons why people may adopt the electronic voting mechanism in the future. In this article, we are going to present an efficient and flexible voting scheme which allows the voter having at most t out of n choices at the same time by employing Chaum’s blind signature scheme and the concept of an oblivious transfer protocol, where n is the number of candidates. Our proposed electronic voting scheme not only achieves lots of essential requirements of general electronic voting schemes but also possesses better efficiency than that of other related works.

Keywords : *Electronic voting, blind signature, oblivious transfer, anonymity.*

*E-mail: ccc@cs.ccu.edu.tw

†E-mail: ljs@cs.ccu.edu.tw

Journal of Discrete Mathematical Sciences & Cryptography

Vol. 9 (2006), No. 1, pp. 133–151

© Taru Publications