

Abstract: A Practical and Secure Electronic Voting System Based on Digital Signature

Jianping Chen*, Bo Yu, Xiang Gu, Quan Shi
School of Computer Science and Technology, Nantong University
Nantong, Jiangsu, 226019, P. R. China
chen.jp@ntu.edu.cn

Abstract

The design of electronic voting systems is an important research topic in the area of information security. This paper proposes a new design scheme for electronic voting systems. In the design, the RSA encryption algorithm is used to protect the secrecy of ballot papers; the temporary identification and the blind signature are used to ensure the anonymity of voters; and the bit commitment is used to guarantee the justice of the voting process. With this system the major problems of an electronic voting system including the ballot collision, halfway abstention and cheating practice can be solved to a significant extent. System performance and security analysis shows that the new electronic voting system is practical and reliable.

Acknowledgements

Financial supports from the National Natural Science Foundation (No. 61171132), the Jiangsu Provincial Natural Science Foundation (No. BK2010280) and the Nantong Municipal Application Research Program (No. BK2011026) of China are acknowledged.