SSE-504

Signcryption Scheme for Secure Voting Empowered by Lattice-based Cryptography

Sourav Choudhary* and Rifaqat Ali

Department of Mathematics and Scientific Computing, National Institute of Technology Hamirpur, 177005, Himachal Pradesh, India

*Corresponding author's e-mail: sourav.ch8529@gmail.com

ABSTRACT

In electronic voting systems, privacy and verifiability are essential security criteria, crucial especially in the era of quantum computing. To achieve quantum immunity and high efficiency in electronic voting, we propose the Signcryption Scheme for Voting System using Lattice-Based Cryptography (SVS-LBC) in this article. The security of this scheme relies on solving the learning with error problem (LWE problem) and the small integer solution problem (SIS problem). The rejection sampling technique is employed to generate the ring signature, greatly improving the signature speed. SVS-LBC provides quantum immunity, unconditional anonymity, and unforgeability, proving its safety in the random oracle model. Furthermore, efficiency analysis and comparison results demonstrate that the proposed scheme is more efficient than similar literature. Due to its ability to enhance the electronic voting process and reduce the cost of electronic voting, SVS-LBC is deemed suitable for use in electronic voting systems.

Keywords: Signcryption Scheme, Lattice-based cryptography, ROR Model

How to Cite

S. Choudhary and R. Ali, "Signcryption Scheme for Secure Voting Empowered by Lattice-based Cryptography", *AIJR Abstracts*, pp. 72–72, Feb. 2024.

DOI: 10.21467/abstracts.165 ISBN: 978-81-965621-7-5 (eBook), 978-81-965621-4-4 (Paperback)