A Lightweight Certificateless Aggregate Ring Signature Scheme for Privacy-preserving in Smart Grids

Huiwen Wang (✉ 17853727747@163.com)

Shanghai University of Electric Power <https://orcid.org/0000-0001-6207-840X>

Liangliang Wang

Shanghai University of Electric Power <https://orcid.org/0000-0003-0389-3281>

Mi Wen

Shanghai University of Electric Power

Kefei Chen

Hangzhou Normal University

Yiyuan Luo

Huizhou University

Research Article

Keywords: Certificateless cryptosystem , Ring signature , Aggregate signature , Privacy-preservation , Random oracle , Smart grid

Posted Date: June 4th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-498186/v1>

License: This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Abstract

There exists a problem of user privacy leakage in the smart grids (SGs) that malicious attackers may intercept or tamper with electricity data and associate the stolen data with real users to commit crimes. Besides, node equipment resources in the SGs are limited. Aiming at the problems above, most of the existing privacy-preserving schemes apply aggregate signature to ensure the integrity of message and improve communication efficiency. However, they cannot realize the anonymity of users to block link attacks, and most of the aggregate signature verification has a high computational cost. Therefore, we propose a certificateless aggregate ring signature (CLARS) scheme based on computational Diffie-Hellman problem and decisional Diffie-Hellman problem. Our scheme is suitable for privacy-preserving in SGs. In this scheme, certificateless cryptosystem is used to avoid key escrow and certificates management problems and ring signature is used to ensure the unconditional anonymity of users. In addition, our scheme is proved to be unforgeability and unconditional anonymity under adaptively chosen message attacks against Type I and Type II adversaries in the random oracle model. Compared with previous certificateless aggregate signature (CLAS) schemes, our CLARS scheme has lower computational cost, which only needs two pairing operations.

Full Text

This preprint is available for [download as a PDF](#).

Figures

Figure 1

System model

Figure 2

Computational cost comparison

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [spmpsci.bst](#)