ABSTRACT

Most identity-based cryptography systems in the blockchain can overcome the challenges of complicated certificate management, privacy protection, and security in traditional authentication systems. A decentralized private key management system avoids complicated certificate management and improves privacy protection, security enhancement, privacy, and efficiency. However, with the high computational cost of the bilinear pair, the system overhead is large. Therefore, the efficiency of the computing process is required. This research aims to implement a low-computation lightweight identity-based cryptography so that it can be applied to devices with limited computing power.

Keywords: Identity-based cryptography, light-weight identity-based cryptograpy, blockchain, lightweight computation