ABSTRACT

Electronic voting is a technique where votes are recorded or counted using electronic equipment. Election systems often face severe challenges regarding security and trust. Threats such as vote falsification and lack of transparency in vote counting have shaken the integrity of elections in various countries. Blockchain technology in e-voting has been proposed as an attractive solution to overcome this problem. Several studies use blockchain to secure electronic voting systems, such as research by Wu & Yang. In this research, has a weakness in verifying the sender. This weakness makes the potential for impersonation attacks and man-in-the-middle attacks against the sender possible. This research proposes a new scheme to strengthen a blockchain-based e-voting system. The proposed scheme uses The Goldreich-Goldwasser-Halevi (GGH) signature scheme. Digital signatures generated using Goldreich-Goldwasser-Halevi (GGH) can strengthen the message sender's identity so that attacker cannot imitate someone. In this research, the voter's public key is still used, and an anonymous ID is only used, which is then used by the voter to maintain the voter's anonymity. Meanwhile, Wu & Yang's research provides a new pair of keys generated and used by voters to maintain voter anonymity. Based on the experimental results, it can be concluded that the proposed scheme is stronger than the previous scheme because the probability of success in impersonating the sender with the proposed scheme using an impersonation attack and man-in-the-middle attack is smaller than the Wu & Yang scheme.

Keywords: Impersonation Attack, Man-in-the-middle Attack, Goldreich-Goldwasser-Halevi (GGH) Signature scheme, Anonymous ID, Voter Anonymity.