ABSTRACT

Security becomes an important aspect to secure the data exchanged and to ensure that the data is received by a legitimate user. Some aspects that must be considered while exchanging information are authentication, confidentiality, and integrity. In the electronic voting system, authentication is used to ensure that the voter is legitimate without knowing his/her identity, while the vote collectors verify that the data is received from a legitimate user without knowing the identity of the voter. An authentication scheme that fulfilled this requirement is called a deniable authentication scheme. The deniable authentication as advance authentication where the receiver can prove the source of the message and the receiver cannot prove the source of the given message to another party. In 2013, Li-Takagi et al. [15] proposed a deniable authentication scheme. The leak of Li-Takagi's scheme is that the receiver can prove the source of a given message to the third party when the receiver fully cooperates with the third party, as described by Mashid et al. [20]. In the proposed method, zero-knowledge proof is introduced to maintain the anonymity of the deniable authentication scheme when the receiver fully cooperates with the third party. In this case, the sender and the receiver generate a random number used to construct a shared secret key for mutual authentication. Message integrity is used to ensure the originality of the message. If the receiver forwards the message to the third party, the third party only knows the receiver as the source of the given message. Based on the analysis, the proposed scheme fulfils the requirement of the deniable authentication scheme when the receiver fully cooperates with the third party. However, the proposed scheme has additional computation cost for securing the shared secret key. Two attack schemes carried out on both Li-Takagi and the proposed scheme are the MITM attack and the impersonation attack. The probability of breaking the proposed scheme using MITM attack is lower than when using Li-Takagi's scheme, but the probability of breaking the proposed scheme using impersonation attack is the same as Li-Takagi's scheme.

Keywords: Deniable authentication, fully cooperated, electronic voting system, MITM attack, Impersonation attack.