ABSTRACT

Nowadays the use of internet in daily life is increasing such that data exchange is frequently conducted. Especially in the case of business transactions, data communication security (such as for banking transaction, contract) is necessary. Sony, et al. [1] proposed a method for securing a contract by introducing ECDSA for signing a contract based on blockchain. However, Sony's method requires high time complexity and not resistant against quantum computing attacks. Therefore, this research proposed a method to reduce the time complexity and resistant against quantum computing attack. To overcome the quantum attack and reduce the time complexity of digital signing based on blockchain, McElliece Cryptosystem and digital signature based on Niederreiter are introduced for signing the contract. Since McElliece Cryptosystem and Niederreiter based signature uses scalar multiplication then the processing time is less than ECDSA. Based on the experiment result, it is proven that the execution time for signing process using the proposed method may reach up to 51.1% less than signing execution time of Sony's method, and for verification process up to 77.8% less than verification execution time of Sony's method. It is also proven that the proposed method is resistant against quantum attack.

Keywords: McElliece Cryptosystem, Niederreiter, Digital Signature, Blockchain