ABSTRACT

Since its first invention, Elliptic Curve Cryptography (ECC) has been considered one very ideal option for implementing public key cryptography. Due to the small size of the lock, it can be used on devices with limited specifications. ECC needs to be upgraded as one of the public key cryptography checks the data or messages sent regarding security from the sender. It is used to meet the validation security requirements. One of the Zero Knowledge Proof (ZKP) protocols is the Fiat-Shamir protocol.

This final project aims to apply the ECC algorithm based on Fiat Shamir and Elliptic Curve Diffie Hellman (ECDH) using a Massage Authorization Code (MAC) which was optimized in previous studies by combining computational techniques with several mathematical formulas. The Fiat Shamir and ECDH algorithms using MAC will be implemented on IoT devices to analyze their computing power and network performance.

The outputs of this final project are: (i) the total computation time, (ii) delay, (iii) amount of memory usage, and (iv) communication cost. The results of this final project are expected to be able to be applied as a cryptography algorithm for devices that have low specifications, especially in Indonesia.

Keywords: Elliptic Curve Cryptography, Elliptic Curve Diffie-Hellman, Massage Authentication Code ,Internet of Things, Zero Knowledge Protocol, Fiat-Shamir.