ABSTRAK

Sejak penemuan pertamanya, *Elliptic Curve Cryptography* (ECC) telah dianggap satu pilihan yang sangat ideal untuk mengimplementasikan kriptografi kunci publik. Karena ukuran kuncinya yang kecil, dapat digunakan pada perangkat dengan spesifikasi terbatas. ECC perlu ditingkatkan sebagai salah satu kriptografi kunci publik Periksa data atau pesan yang dikirim terkait keamanan Dari pengirim. Ini digunakan untuk memenuhi kebutuhan keamanan validasi Salah satu protokol *Zero Knowledge Proof* (ZKP) digunakan Protokol *Fiat-Shamir*.

Tugas akhir ini bertujuan untuk menerapkan algoritma ECC berbasis Fiat Shamir dan *Elliptic Curve Diffie Hellman* (ECDH) menggunakan *Massage Authorization Code* (MAC) yang dioptimalkan pada penelitian sebelumnya dengan menggabungkan teknik komputasi dengan beberapa rumus matematika. Algoritma Fiat Shamir dan ECDH menggunakan MAC akan diimplementasikan pada perangkat IoT untuk menganalisis daya komputasi dan kinerja jaringannya.

Luaran Tugas Akhir ini adalah: (i) total waktu komputasinya, (ii) *delay*, (iii) jumlah pemakaian memori dan (iv) *communication cost*. Hasil Tugas Akhir ini diharapkan mampu diterapkan sebagai algoritma kriptografi untuk perangkat yang memiliki spesifikasi rendah khususnya di Indonesia.

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