ABSTRACT

The explosive growth in the use of mobile and wireless devices demands a public key cryptosystem (PCK) achieving aspects of information security with accommodate limitations on power and bandwidth, at the same time keeping with high level of security.

Elliptic curve cryptosystem (ECC) are new generation of public key cryptosystems that has smaller key sizes for the same level of security. The exponentiation in elliptic curve is the most important operation in ECC, So when put the ECC into practice, the major problem is how to enhance the speed of the exponentiation. It is thus of great interest to develop algorithms for exponentiation, which allow efficient implementations of ECC.

In this thesis, we improve efficient algorithm for exponentiation on elliptic curve defined over $\mathbf{F}_p$ in terms of affine coordinates. The algorithm computes $2^{n_2}(2^{n_1}P+Q)$ directly from random points P and Q on an elliptic curve, without computing the intermediate points. Moreover, we apply this algorithm on exponentiation on elliptic curve with wMOF and analyze their computational complexity. This algorithm can speed the wMOF exponentiation of elliptic curve of size 160-bit about (21.7 %) as a result of its implementation with respect to affine coordinates.