Elliptic Curve Point Multiplication Algorithm Using Precomputation

HANI MIMI, AZMAN SAMSUDIN, SHAHRAM JAHANI
Universiti Sains Malaysia
Al-Zaytoonah University of Jordan
hani_mimi@yahoo.com

Abstract: - Window-based elliptic curve multiplication algorithms are more attractive than non-window techniques if precomputation is allowed. Reducing the complexity of elliptic curve point multiplication of the form , which is the dominant operation in elliptic curve cryptography schemes, will reduces the overall complexity of the cryptographic protocol. The wBD is a new window-based elliptic curve multiplication method. It is based on new recoding method called window big-digit (wBD). The wBD is a bidirectional method that can be calculated in both directions based on the amount of the available memory. The available memory is invested in an efficient way since wBD has little number of precomputed points compared to other window methods wich make it more suitable for limited storage devices. The BD recoding method requires only one pass to transform the exponent *k* from its binary representation to its wBD representation. Moreover, the wBD keys has the lowest zero-run length among other window methods. Finally, the number of elliptic curve operations in addition to the execution time of wBD method is measured. Consequently, the wBD is efficient as other window-based methods.

Key-Words: - Window methods, Single Scalar EC multiplication, Big-digit Recoding, Public key cryptography