

## ELLIPTIC CURVE POINT MULTIPLICATION USING WZOT

Hani Mimi

*Alzaytoonah University of Jordan – Computer Science*

*University Sains Malaysia – Computer Sciences*

*Hani\_mimi@yahoo.com*

Azman Samsudin

*University Sains Malaysia – Computer Sciences*

*Azman@cs.usm.my*

Shahram Jahani

*University Sains Malaysia – Computer Sciences*

*Jahani2001@yahoo.com*

### **Abstract:**

*The dominant operation in elliptic curve cryptography schemes is the point multiplication of the form  $kP$ . A radix-2 representation of  $k$  is called  $w$ -NAF if  $w \geq 2$  and the window values are in the digit set  $B = \{\mp 1, \mp 3, \dots, \mp 2^w - 1\}$ . Researchers have been trying to enhance the EC point multiplication by employing the window methods, such as  $w$ -NAF method. ZOT is a new recoding technique that uses different digit set. The left-to-right property is addressed as one of the advantages of ZOT. Moreover, it uses the available memory in more efficient way since you can limit the number of precomputed points. Thus, it is more suitable for limited storage devices.*