Evaluating Composite EC Operations and their Applicability to the on-the-fly and non-window Multiplication Methods

International Journal of Computer Applications
© 2014 by IJCA Journal

Volume 105 - Number 6
Year of Publication: 2014

Authors:
Mohammad Rasmi
Hani Mimi
Mohammad Sharif

10.5120/18382-9621

Abstract

In order to improve the efficiency of elliptic curve multiplication methods, extended and composite elliptic curve operations such as nP,mP+Q, where n>2 and m>2, and repeated doublings were proposed. These operations have lower complexity, in terms of field operations, than that for classical methods. Moreover, they are supposed to replace the classical methods. In this paper, repeated doublings and odd point computation are deeply analyzed in order to measure their actual efficiency. According to the gained results, the improvement ratio in the execution time is not the same as the improvement ratio measured in terms of field operations. Moreover, different implementations of Sakai repeated doubling method yield different results. For example, implementing 4P as a separate function gives lower complexity than implementing repeated doublings as a general function. On the other hand, other methods for computing nP, where n is odd, have been analyzed. Dahmen method failed to meet the expected results for computing odd points in elliptic curve multiplication methods that employ the on-the-fly strategy since its time complexity was more than that for classical methods. It was also found that new techniques should be devised to improve the efficiency of window methods for calculating odd points such as: 5P, 7P, and 15P, which have lower cost than that for classical method.
Evaluating Composite EC Operations and their Applicability to the on-the-fly and non-window Multiplication Methods

References


Index Terms

Computer Science

Information Science

Keywords

Repeated doublings, extended elliptic curve operations, pre-computations, single scalar multiplications, recoding methods
Evaluating Composite EC Operations and their Applicability to the on-the-fly and non-window Multiplication Methods