Abstract

Suppose that we are performing an elliptic curve point multiplication kP using an $r \times c$ combing table T. After precomputation the point multiplication will require $c-1$ doubles and $M-1$ additions, where M is the number of non-zero columns in T. Thus the cost of performing a point multiplication using a combing table can be reduced if we can create combing tables with fewer non-zero columns. In this paper we present an algorithm which will generate combing tables, using a signed binary representation, with fewer non-zero columns and at most one more column than the combing table formed with the same number of rows using the binary representation of k. We further show that a generalization of Solinas' joint sparse form (JSF) [4] of two integers to more than two integers can be derived from these zero columned combing tables. By considering this generalization of Solinas' JSF we consider the optimality of the zero columned combing tables among all combing tables containing signed binary representations.