Cryptology ePrint Archive: Report 2011/569

Analysis of the Hamming Weight of the Extended wmbNAF

Ming Li, Ali Miri and Daming Zhu

Abstract: Scalar multiplication is an important operation in elliptic curve cryptosystems(ECC). The algorithms for computing scalar multiplication are mostly based on the binary expansions of scalars, such as the non-adjacent form (NAF) and wNAF (sliding window method). Representing scalars using more bases can speed up the scalar multiplication, such as mbNAF, wmbNAF and extended wmbNAF, which was proposed by Longa and Miri in 2008. In this paper, we give a formal analysis of the Hamming weight of the extended wmbNAF method for scalar multiplication on general elliptic curves over large prime fields. Then the cost of this method is compared with NAF and other double-base methods. The analysis shows that we obtain the most efficient algorithm when using (2; 3; 5)NAF_{1;1;0}, which is 9:0% faster than the NAF method without extra storage requirement. Moreover, the recoding algorithm of the extended wmbNAF method is just as simple and fast as that of the NAF method.

Category / Keywords: public-key cryptography / elliptic curve cryptography, multibase representation, scalar multiplication

Date: received 20 Oct 2011

Contact author: luaming at msn com