Abstract

The successful application to elliptic curve cryptography of side-channel attacks, in which information about the secret key can be recovered from the observation of side channels like power consumption or timing, has motivated the recent development of unified formul for elliptic curve point operations. In this paper, we give a version of a previously-developed family of unified point addition formul that uses projective coordinates for improved efficiency. We discuss the applicability of a recent attack by Walter on this family of projective formul and describe how the field arithmetic can be implemented to obtain fully unified formul and avoid this type of attack. Keywords: elliptic-curve cryptography, side-channel attacks, unified point addition formul, projective coordinates.