CORR 2002-03

A Fast Parallel Elliptic curve Multiplication Resistant against Side Channel Attacks

Tetsuya Izu*, Tsuyoshi Takagi*

Abstract This paper proposes a fast elliptic curve multiplication algorithm applicable for any types of curves over finite fields $\mathbb{F}_p$ (p a prime), based on [Mon87], together with criteria which make our algorithm resistant against the side channel attacks (SCA). The algorithm improves both on an addition chain and an addition formula in the scalar multiplication. Our addition chain requires no table look-up (or a very small number of precomputed points) and a prominent property is that it can be implemented in parallel. The computing time for n-bit scalar multiplication is one ECDBL $+(n-1)$ ECADDs in the parallel case and $(n-1)$ ECDBLs $+(n-1)$ ECADDs in the single case. We also propose faster addition formulas which only use the x-coordinates of the points. By combination of our addition chain and addition formulas, we establish a faster scalar multiplication resistant against the SCA in both single and parallel computation. The improvement of our scalar multiplications over the previous method is about 37% for two processors and 17.1% for a single processor. Our scalar multiplication is suitable for implementation on smart cards.

Keywords elliptic curve cryptosystem, scalar multiplication, parallel computation, side channel attack