ABSTRACT – CAN. J. ELECT. COMPUT. ENG., VOL. 27, NO. 2, APRIL 2002, PP. 61–65

A fast algorithm for multiplication on elliptic curves

Un algorithme rapide pour la multiplication des courbes elliptiques

Hua Li and Chang N. Zhang*

Large-integer modular multiplication is an arithmetic primitive required by public-key cryptosystems, including elliptic curve cryptography (ECC). In this paper, a new fast algorithm for multiplication of a point on the elliptic curve by a large integer based on non-adjacent-form (NAF) Frobenius expansion is proposed. The improved algorithm runs 66% faster than the binary algorithm and 33% faster than the regular Frobenius expansion method. In addition, the proposed algorithm is shown to be simpler than previous methods and can be efficiently implemented by hardware.

La multiplication modulaire de grands entiers est une primitive arithmétique qui est requise dans les systèmes d'encryptage avec clé publique, incluant l'encryptage par courbe elliptique (ECC). Cet article présente un nouvel algorithme rapide pour la multiplication d'un point sur une courbe elliptique avec un grand nombre entier. L'algorithme se base sur une expansion en forme non adjacente de Frobenius (NAF). Le nouvel algorithme s'exécute 66% plus vite que l'algorithme binaire et 33% plus vite que l'algorithme basé sur l'expansion de Frobenius classique. De plus, l'algorithme est plus simple que les autres méthodes et peut être implanté en hardware.

Keywords: elliptic curves, multiplication, Frobenius expansion, Frobenius endomorphism, encryption

*The authors are with the Department of Computer Science, TR-Labs, University of Regina, Regina, Saskatchewan S4S 0A2. E-mail: {huali,zhang} @cs.uregina.ca