UDC 340.5

Gyoyong Sohn,
Department of Mathematics Education,
Daegu National University of Educaiton,
Republic of Korea
gysohn@dnue.ac.kr

SCALAR MULTIPLICATION ON CERTAIN MODELS OF ELLIPTIC CURVES USING THE FROBENIUS MAP

Abstract. Elliptic curve cryptography was independently proposed by Koblitz [9] and Miller [10] in 1985. The elliptic curve cryptosystem is a public key cryptosystem based on the discrete logarithm problem in the group of points on a curve. In elliptic curve cryptosystms, the efficiency depends essentially on the fundamental operation of the scalar multiplication $[n]P$ for a given point P on an elliptic curve E and an integer n. In general, the computational speed of scalar multiplication $[n]P$ depends on finite field operations, curve point operations, and representation of the scalar n [11,5].

There is vast literature on efficient methodes for computational speeding up scalar multiplication. For elliptic curves, the scalar multiplication can be done with various methods (a good reference is [1]). If an elliptic currve admits an efficient endomorphism, its use can speed up scalar multiplication. In [7], Iijima, Matsuo, Chao and Tsujii presented an efficiently computable homomorphism on elliptic curves using the Frobenius map on the quadratic twists of an elliptic curve. The Gallant-Lambert-Vanstone (GLV) gave suitable efficiently computable endomorphisms on elliptic curves for speeding up point multiplication [3, 4]. There are several models of elliptic curves to provide the efficient computation and implement for cryptography in recent year [2, 6, 8].

In this presentation, we consider efficient scalar multiplication on certain models of elliptic curves over a finite field using the Frobenius expansion. The Frobenius expansion is known as an efficient method to implement of point addition on elliptic curves. It has been applied to fast elliptic curve cryptosystem. Applying the Frobenius endomorphism on certain models of elliptic curves, we construct Frobeus maps defined on certain curves. To speed up the scalar multiplication on curves, we use the GLV method combined with the Frobenius endomorphism over the curves.

Key words . Elliptic curve, scalar muliplication, Frobenius map

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, Handbook of Elliptic and Hyperelliptic Cryptography, Chapman and Hall/CRC, 2006.

[2] H. M. Edwards, A normal form for elliptic curves, Bulletin of the American Mathematical Society 44(3) (2007), 393--422.

[3] S. D. Galbraith, X. Lin, M. Scott, Endomorphisms for faster elliptic curve cryptography on a large class of curves, J. Cryptology 24(3), 446--469, 2011.

[4] R. P. Gallant, R. J. Lambert and S. A. Vanstone, Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms, In J. Kilian (ed.), CRYPTO 2001, Springer LNCS 2139 (2001), 190--200.

[5] J. Guajardo and C. Paar, Itoh-tusji version in standard basis and its applicaiton in cryptography and codes, Design, Codes and Cryptography 25. 2002. N 2. P. 207-216.

[6] G. B. Huff, Diophantine problems in geometry and elliptic ternary forms, Duke Math. J., 15:443--453, 1948.

[7] T. Iijima, K. Matsuo, J. Chao and S. Tsujii, Construction of Frobenius Maps of Twists Elliptic Curves and its Application to Elliptic Scalar Multiplication, in SCIS 2002, IEICE Japan, January 2002, 699--702.

[8] M. Joye, M. Tibbouchi, and D. Vergnaud, Huff's Model for Elliptic Curves, Algorithmic Number Theory - ANTS-IX, Lecture Notes in Computer Science Vol. 6197, Springer, pp. 234-250, 2010.

[9] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 1987. N 48. P. 203-209.

[10] V. S. Miller, Use of elliptic curves in cryptography, In H. C. Williams, editor, Advances in Cryptology-CRYPTO'85, Lect. Notes Comput. Sci. 1986. N 218. P. 417-426.

[11] D. Yong and G. Feng, High speed modular divider based on GCD algorithm over GF($2m$)}, Journal of communications 29. 2008. N 10. P. 199-204.