An investigatioin of efficient scalar multiplication of elliptic curve cryptography

Yoshio Kawamo(s1010901)

School of Information Science,
Japan Advanced Institute of Science and Technology

February, 2013

Key word: elliptic curve, cryptosystem, efficient, Double-base number system, scalar multiplication

There are two types of cryptosystem, public key cryptosystem and secret key cryptosystem. While a secret key cryptosystem uses the same key for encryption and decryption, a public key cryptosystem uses different key for encryption and decryption. A secret key cryptosystem requests us to keep the key secret, and it is necessary to exchange the key between sender and receiver securely before cryptocommunication. On the other hand, it can allow smaller key length and faster encryption and decryption compared with a public key cryptosystem. A public key cryptosystem needs a secret key and a public key, where the public key can be known to any one. It is not necessary to exchange the secret key between a sender and a receiver before cryptocommunication. On the other hand, it needs longer key length and slower encryption and decryption compared with secret key cryptosystem. So, secret key cryptosystem is mainly used for data encryption and public key cryptosystem is mainly used for key exchange and digital signature.

Elliptic curve cryptosystem(ECC) is one of the public key cryptosystem, whose security level is higher than RSA, one of the public key cryptosystem developed earlier than ECC. So it is expected to be used for small devices with small capacity processor like smart card. It is necessary for widely use of ECC to speed up its encryption and decryption, so there are many existing researches.

Main operation of encryption and decryption of ECC is a scalar multiplication to compute $kP = P + \cdots + P(k \text{ times})$, where k and P is called a scalar and a base point, respectively. Scalar multiplication is consists of elliptic curve addition (ADD) and doubling (DBL) and operation on finite field such as prime field and binary field. It is necessary for speed-up of scalar multiplication to reduce number of elliptic-curve operations. It is important for reducing the number of elliptic-curve operations to reduce the density of non-zero digits. For example the NAF and w-NAF reduce the number of non-zero digits of binary. On the other hand, to improve ECC operation, some previous methods reduce the number of operations on finite field using such as conversion of coodinates and re-use of same operation.

Double-base number system(DBNS) is a representation of a scalar k by a sum of integers of the form 2^b3^t. It can drastically reduce the number of non-zero digits compared with binary, NAF, w-NAF method. For example, for scalar k of 160 bits, binary method and NAF need 80 and 53 non-zero digits respectively, but DBNS needs only 22 non-zero digits. In this paper, we focus on first term of DBNS and propose a new

method. We also implement our method and as a result, experiment shows that our method can speed up scalar multiplication by 6.71 percent compared with the previous method. Also we further propose a new method of converting scalar k into DBNS, which needs only $O(\log(\log k)$, although the previous method needs $O(\log k)$.