Title	楕円曲線暗号の効率的な実装に関する研究
Author(s)	永田，智芳
Citation	
Issue Date	2010-09
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/9146
Rights	
Description	Supervisor:宮地充子，情報科学研究科，修士

A Study on Efficient Implementation of Elliptic Curve Cryptosystem

Tomoyoshi Nagata (0710902)

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

August 7, 2010

Keywords: Elliptic curve, Scalar multiplication, Multiple precision arithmetic, OpenSSL, ARM.

Elliptic curve cryptosystem can achieve high security with shorter key length, faster speed, lower power consumption, and smaller memory spaces than conventional cryptosystems. In order to implement efficient elliptic curve cryptosystem, we need to compute scalar multiplications on a curve effectively. It is necessary to calculate a multiplication in polynomial time because scalars are represented with multi-precisional values over 160-bit.

Many studies on fast implementation have been done for years. The most basic idea is Binary Method. Binary Method is improved to Sliding Window Method, which is applied to Interleaving Exponentiation implemented in open source code, OpenSSL library.

Scalar multiplication algorithms depend on doublings and additions on an elliptic curve. The latest result that speeds up operations on an elliptic curve enables us to implement faster EC-doublings and additions with OpenSSL crypto library.

Inside the EC-doubling and addition, modular reduction is executed for multi-precisional valuables. One of the researches on modular reduction is called Incomplete Reduction. It is the fast algorithm of the arithmetic operations in the finite field GF_p with an arbitrary prime modulus p. The method adopts word-level operations which is significantly faster than bitlevel operations. We can improve EC-doubling and addition with Incomplete Reduction.

Modular reduction repeatedly executes multiple precision arithmetics. Therefore, speeding up multi-precisional operations has a large effect on scalar multiplication. Cutting down conditional branches and merging operations have been proposed to increase the performance of multi-precisional arithmetics. Though the method was proposed for x86 processors, it is applicable to the other platforms, such as ARM processors. ARM is generally build into embedded devices such as mobile phones to which elliptic curve cryptosystem is able to contributes.

We examined multi-precisional arithmetics on an ARM9 processor and found that squaring is slower than multiplying on 160-bit multiple precision values. The cause is a frequency of accessing memories. Here, we propose a new merged operation to solve the problem. ARM is good at shifting values which can reduce the number of additions in the multi-precisional squaring algorithm. Also ARM is good at data transferring operations which can move several words at a time. With taking advantage of shifting and data transferring operations on ARM, we finally reduced the number of accessing memories around 80%, and got the result that multi-precision squaring become faster about 20% than the speed of previous implementation. Furthermore, we examined the merged operation on an iPhone device which is also based on ARM architecture. The proposed method gained around 80% speed up compared with the existing algorithm. Finally, combining the proposed operation and the latest EC-operations, we achieved speed up to 63.09% to execute scalar multiplication on an elliptic curve.