九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Efficient Implementation of ηT Pairing on Supersingular Elliptic Curves in Characteristic 3

川原, 祐人
九州大学大学院数理学府

https://doi.org/10.15017/21704

出版情報：九州大学, 2011, 博士（機能数理学）, 課程博士
バージョン：
権利関係：

氏　　名：川原　祐人

論文題目：Efficient Implementation of η_T Pairing on Supersingular Elliptic Curves in Characteristic 3
（標数 3 の超特異楕円曲線上のη_Tペアリングの高速実装）

区　　分：甲

論　文　内　容　の　要　旨

Pairing-based cryptosystems can provide cryptographic schemes which have novel and useful properties, such as Identity-based encryption schemes, and they have been attracted in cryptography. These schemes are constructed by using pairings, such as the Tate and Weil pairings, hash functions, and group computations. Miller proposed the first polynomial-time algorithm for computing the Weil pairing on algebraic curves, and various pairings are indicated until now. η_T pairing over F_{3^m} is one of the fastest pairings now.

We propose efficient algorithms of addition and subtraction in F_3 and MapToPoint, which is a hash function to compute a point on elliptic curves, for efficient implementation of the η_T pairing over F_{3^m}. Firstly, we construct instruction sequences of addition and subtraction in F_3 with the minimum number of logical instructions, since all functions of the η_T pairing is based on them. Every F_3-element is assigned to two bits, and the F_3-addition and subtraction is considered as a map $(\mathrm{F}_2)^2 \times (\mathrm{F}_2)^2 \to (\mathrm{F}_2)^2$. We perform an exhaustive search for finding the instruction sequences of the F_3-addition that use seven or fewer logical instructions. Indeed, we find many implementations of the F_3-addition and subtraction with only six logical instructions, and no sequence that can compute them with less than six logical instructions for any assignment of elements or logical instructions. In other words, we have proven that the minimum number of logical instructions required for the F_3-addition and subtraction is six.

MapToPoint algorithm is used to compute a point of an elliptic curve from identity. There exists two conventional algorithms for supersingular elliptic curves over F_{3^m}: one is computed by using a square root computation in F_{3^m}, which needs $O(\log m)$ multiplications and $O(m)$ cubings in F_{3^m}; another is computed by using an $(m-1) \times (m-1)$ matrix over F_3, which needs the off-line memory to store it. We construct an efficient MapToPoint algorithm on the supersingular elliptic curves by using *1/3-trace* over F_{3^m}. The *1/3-trace* can compute a solution x of $x^3 - x = c$ by using no multiplication in F_{3^m}. The proposed algorithm is computed by $O(1)$ multiplications and $O(m)$ cubings in F_{3^m}, and it requires less than m F_3-elements to be stored in the off-line memory to efficiently compute *trace* over F_{3^m}.

Finally, the implementation of the η_T pairing, arithmetic over $E(\mathrm{F}_{3^m})$ and F_{3^m} are described. We implement them in C and Java as programming languages, and measure the running time of these functions on an Intel Core i7-950 processor.