

Usage of Optimal Extension Fields for Elliptic Curve Cryptosystems

Tetsutaro Kobayashi, Kazumaro Aoki, Fumitaka Hoshino, Kunio Kobayashi,
and Hikaru Morita

NTT Laboratories

Abstract. In IEEE P1363, two kinds of finite fields, “Prime Finite Fields” and “Characteristic Two Finite Fields” have been standardized. We propose “Optimal Extension Fields (OEF)” in addition to the two fields. OEF is efficient to compute [1–3].

1 Introduction

Elliptic curves over $\text{GF}(p)$ (p is a prime) or $\text{GF}(2^n)$ have been implemented by many companies and standardized by several organizations such as IEEE P1363 and ISO/IEC JTC1/SC27.

On the other hand, if you select $\lceil \log_2 p \rceil$ (the number of the bits of a prime number p) to match the operation unit of an individual computer, the scalar multiplication of $\text{GF}(p^m)$ could be calculated faster than that of $\text{GF}(p)$ or $\text{GF}(2^n)$ where $\lceil \log_2 p^m \rceil$ should be close to $\lceil \log_2 p \rceil$ or $\lceil \log_2 2^n \rceil (= n)$ under the condition of the same security level. Bailey and Paar newly proposed an elliptic curve scheme on OEF (Optimal Extension Fields), or an $\text{GF}(p^m)$ type at Crypto’98 [1]. Their method represents elliptic curve points using a polynomial basis. They showed that OEF accelerates multiplication significantly by introducing a binomial as a minimal polynomial. Further studies [2, 3] on OEF were presented.

2 Definitions

2.1 Definition of OEF

The *Optimal Extension Fields (OEF)* are finite fields whose number of elements is a power of p . If $m \geq 1$, then there is a unique field $\text{GF}(p^m)$.

We define OEF as $\text{GF}(p^m)$ that satisfies the following:

- p is a prime less than but close to the word size of the processor,
- $p = 2^n \pm c$, where $\log_2 c \leq n/2$ and

For purposes of conversion, the element of $\text{GF}(p^m)$ should be represented by a sequence of m words. For example, we can use the following basis representation.

2.2 Polynomial Basis

This representation is determined by choosing an irreducible binomial $f(x)$ of degree m . If the polynomial basis representation over $\text{GF}(p)$ is used, then, for purposes of conversion, the word sequence

$$(a_0, a_1, \dots, a_{m-1})$$

shall be taken to represent the polynomial

$$a_0 + a_1t + a_2t^2 + \dots + a_{m-1}t^{m-1}$$

where the coefficients a_i are elements of $\text{GF}(p)$.

In particular, for purposes of conversion, the additive identity (zero) element of the field is represented by $(0, 0, 0, \dots, 0, 0)$, and the multiplicative identity (one) element of the field is represented by $(1, 0, 0, \dots, 0, 0)$.

3 Claimed Attributes and Advantages

Scalar multiplication over OEF runs very fast. For example, in [2] it is about ten times as fast as characteristic two finite fields.

Table 1 [2] shows the results of an elliptic curve implementation over OEF.

4 Security Considerations

There are no general security considerations for the OEF representation; This is merely alternate definition fields.

References

1. D. V. Bailey and C. Paar, "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms," *Advances in Cryptology – CRYPTO '98*, Lecture Notes in Computer Science 1462, pp.472-485, Springer, 1998.
2. T. Kobayashi, H. Morita, K. Kobayashi and F. Hoshino, "Fast Elliptic Curve Algorithm Combining Frobenius Map and Table Reference to Adapt to Higher Characteristic," *Advances in Cryptology – EUROCRYPT '99*, Lecture Notes in Computer Science 1592, pp.176-189, Springer, 1999.
3. D. V. Bailey and C. Paar, "Inversion in Optimal Extension Fields," *Conference on The Mathematics of Public Key Cryptography, The Fields Institute for Research in the Mathematical Sciences Toronto, Ontario, June 12-17, 1999*
4. V. Müller, "Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two," *Journal of Cryptology*(1998) 11, pp.219-234, 1998.
5. E. De Win, A. Bosselaers and S. Vandenberghe, "A Fast Software Implementation for Arithmetic Operations in $\text{GF}(2^n)$," *Advances in Cryptology – ASIACRYPT'96*, Lecture Notes in Computer Science 1163, pp.65-76, Springer-Verlag, 1996.

Table 1. Scalar Multiplication Speed

Base- ϕ Expansion Method

Platform	Order (bit)	Size of Base Field	EC-Add (μsec)	EC-Double (μsec)	Scalar Mult. (msec)	
P II 400	186	$2^{31} - 1$	19.7	13.2	1.95	Base-ϕ
P II 400	186	$2^{31} - 1$	19.7	13.2	3.89	Signed Binary
P II 400	156	$2^{13} - 1$	32.1	22.3	2.66	Base-ϕ
P II 400	156	$2^{13} - 1$	32.1	22.3	5.50	Signed Binary

“P II 400” denotes 400 MHz Pentium II PC.

Affine Coordinates

Platform	Order (bit)	Size of Base Field	EC-Add (μsec)	EC-Double (μsec)	Scalar Mult. (msec)	
Alpha 500	183	$2^{61} - 1$	4.64	5.25	0.994	Affine
Alpha 500	183	$2^{61} - 1$	7.8	6.24	1.58	Jacobian(Bailey[1])

“Alpha 500” denotes DEC Alpha workstation that equips 500MHz 21164A.

Speed in Previous Works

Platform	Order (bit)	Size of Base Field	EC-Add (μsec)	EC-Double (μsec)	Scalar Mult. (msec)	
Sparc4	180	2^5	* ^a	* ^a	59.2	Muller[4]
P 133	177	2	306	309	72	De Win[5]
Alpha 500	160	$2^{32} - 5$	20	16.2	3.62	Bailey[1]
Alpha 500	160	$2^{16} - 165$	207	166	37.1	Bailey[1]

“Sparc4” denotes SparcStation4.

“P 133” denotes 133 MHz Pentium PC.

^a No information in [4].