22

An Improvement of Cyclic Vector Multiplication Algorithm

Hidehiro Kato, Yasuyuki Nogami, Tomoki Yoshida, Kenta Nekado,
Shoichi Takeuchi, and Yoshitaka Morikawa
Okayama University
Japan

1. Introduction

Pairing-based cryptographic applications such as ID-based cryptography (Boneh et al., 2001) and group signature authentication (Nakanishi & Funabiki, 2005) have received much attentions. Such an application needs a pairing-friendly elliptic curve and arithmetic operations in a certain extension field F_{p^m}. The extension degree is especially called *embedding degree*. In general, corresponding to the pairing-friendly curve, characteristic p is restricted so as to satisfy a certain condition and m is fixed to a certain positive integer. For example, Barreto-Naehrig (BN) curve (Barreto & Naehrig, 2005) and Freeman curve (Freeman, 2006) are well known pairing – friendly curves. In the case of BN curve, characteristic p needs to be given with an integer χ as

$$p = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1 \tag{1}$$

and m is fixed to 12. In the case of Freeman curve,

$$p = 25\chi^4 - 25\chi^3 + 25\chi^2 - 10\chi + 3 \tag{2}$$

and embedding degree m is fixed to 10. In order to make those cryptographic applications practical, definition field F_{p^m} needs to have fast arithmetic operations, especially multiplication. However, some of these restrictions cannot satisfy the conditions for fast arithmetic operations inversely.

Optimal extension field (OEF) (Bailey & Paar, 1998) has fast arithmetic operations and is widely used (Devegili et al., 2007). Since OEF uses Karatsuba-based polynomial multiplication and an irreducible binomial as the modular polynomial, a multiplication in OEF is efficiently carried out. However, in order to construct F_{p^m} as OEF, each prime factor needs to divide p - 1. It is a critical condition for Freeman curve, for example, because characteristic p of Freeman curve is given by Eq.(2) and thus can never satisfy it. On the other hand, type-<k,m> Gauss period normal basis (GNB) can be easily prepared in F_{p^m} whenever $4p$ does not divide $m(p - 1)$ (Kato et al., 2007). As previously introduced, m is relatively small than p, therefore this condition is always satisfied. In addition, the authors have proposed an efficient multiplication algorithm using GNB (Kato et al, 2007). It is called *cyclic vector multiplication algorithm* (CVMA). In the previous work (Kato et al, 2007), CVMA

Source: Convergence and Hybrid Information Technologies, Book edited by: Marius Crisan,
ISBN 978-953-307-068-1, pp. 426, March 2010, INTECH, Croatia, downloaded from SCIYO.COM

is quite efficient when m is small such as for the use of pairing-based cryptographic applications. However, the calculation cost of CVMA becomes worse as k becomes larger. As shown in (Kato et al, 2007), most of cases have small k within 5 but it sometimes becomes large.

In this paper, a symmetric feature that appears in the calculation of CVMA is first introduced. Then, based on the feature, an improvement of CVMA is proposed. From some simulation results, it is shown that the improved CVMA efficiently carries out a multiplication in extension field even if parameter k is large.

Throughout this paper, p and m denote the characteristic and the extension degree, respectively, where p is a prime number. F_{p^m} denotes an m-th extension field over F_p. Without any additional explanation, lower and upper case letters show elements in prime field and extension field, respectively, and a Greek alphabet shows a zero of modular polynomial. In this paper, a subtraction in F_p is counted up as an addition in F_p. M_1, A_1 and D_1 denote the calculation costs of a multiplication, addition and doubling in F_p.

2. Fundamentals

This section briefly reviews Gauss period normal basis, cyclic vector multiplication algorithm (CVMA), and then shows a problem of CVMA.

2.1 Gauss period normal basis

Type-<k,m> Gauss period normal basis in F_{p^m} is defined with an integer k as follows (Gao, 1993).

Definition 1 *Let* $km + 1$ be *a prime number not equal to p and suppose that* $\gcd(km/e,m) = 1$, *where e is the order of p modulo* $km + 1$. *Then, for any primitive k-th root* θ *of unity in* F_{km+1},

$$\gamma = \sum_{i=0}^{k-1} \beta^{\theta^i} \tag{3}$$

generates a normal basis $\{\gamma, \gamma^p, \ldots, \gamma^{p^{m-1}}\}$ *in* F_{p^m}, *where* β *is a* $(km + 1)$*-st root of unity that belongs to* F_{p^e}. *This normal basis Eq.*(3) *is called type-*<k,m> *Gauss period normal basis*. ■

For an arbitrary extension degree m, there is an infinite number of k's such that $km + 1$ becomes a prime number. It is well-known as the Dirichlet's theorem on arithmetic progressions(Apostol, 1976). Moreover, when p is odd and $4p$ does not divide $m(p - 1)$, it is known that type-<k,m> Gauss period normal basis with a certain integer k always exists for an arbitrary pair of p and m (Gao, 1993).

2.2 TypeI-X GNB and CVMA

Consider a class of Gauss period normal basis of which the order e shown in Def.1 is $km+1$. When k is equal to 1, it is typeI optimal normal basis (Cohen & Frey, 2005), thus in what follows we call the class of Gauss period normal basis *typeI–X* (typeI eXtended) GNB.

The authors have shown a multiplication algorithm with typeI–X Gauss period normal basis called *cyclic vector multiplication algorithm* (CVMA) (Kato et al., 2007). Fig.1 shows CVMA with typeI-X GNB in F_{p^m}. In the algorithm Fig.1, <x> denotes x mod $km + 1$

The calculation cost of CVMA is given by

$$\left\{\frac{m(m+1)}{2}+1\right\}M_1 + \left\{\frac{m(m-1)(k+2)}{2}+m\right\}A_1, \tag{4}$$

where M_1 and A_1 denote the calculation costs of a multiplication and an addition in F_p, respectively. Different from OEF (optimal extension field) that restricts the characteristic p and extension degree m (Bailey & Paar, 1998)[1], our proposed multiplication algorithm, that is CVMA, is widely applicable since it is based on Gauss period normal basis (Kato et al, 2007). Especially, CVMA is efficient when extension degree m is small.

Input: $X = \sum_{i=0}^{m-1} x_i \gamma^{p^i}$, $Y = \sum_{i=0}^{m-1} y_i \gamma^{p^i}$.

Output: $Z = XY = \sum_{i=0}^{m-1} z_i \gamma^{p^i}$.

Preparation:

1. Determine k that satisfies the conditions in Def.1.
2. for i = 0 to m do
3. $q[i] \leftarrow 0$
4. for t = 0 to m - 1 do
5. for h = 0 to k - 1 do
6. $g[<p^{t+hm}>] \leftarrow t + 1$
7. $g[0] \leftarrow 0$

Procedure:

1. for i = 0 to m - 1 do
2. $q[i+1] \leftarrow x_i y_i$
3. for i = 0 to m - 2 do
4. for $j = i+1$ to m – 1 do
5. $M_{ij} \leftarrow (x_i - x_j)(y_i - y_j)$
6. for h = 0 to k - 1 do
7. $q[g[<p^i+p^{j+hm}>]] \leftarrow q[g[<p^i+p^{j+hm}>]] + M_{ij}$
8. for i = 0 to m - 1 do
9. $z_i \leftarrow kq[0] - q[i+1]$

(End of algorithm)

Fig. 1. CVMA with TypeI-X Gauss period normal basis in F_{p^m}

2.3 A problem in conventional CVMA

As shown in Eq.(4), the calculation cost of CVMA depends on the integer k. In general, A_1 is much smaller than M_1; however, if k is large, it will not be negligible. As shown in our previous work (Kato et al, 2007), the minimal integer k such that the conditions for type I-X Gauss period normal basis tends to be small such as within 5 but sometimes becomes large. When we can appropriately set the parameters p and m such that the corresponding minimal integer k becomes small, it will not be a critical problem. However, when these parameters are restricted as pairing-based cryptographies, it is out of options for CVMA. Thus, for such a case, this paper shows an improvement of CVMA.

3. Improvement of CVMA

This section shows an improvement of CVMA by which the number of F_p-additions needed for a multiplication in F_{p^m} with CVMA is efficiently reduced.

[1] Each prime factor must divide p-1.

3.1 Pre-Computation

According to the original CVMA Fig.1, the temporary data M_{ij} shown at Step 3 of the procedure is prepared with corresponding to i and j. Then, at Step 5, it is added to k coefficients among $q[l]$, $0 \le l \le m$.

The k coefficients to which the temporary data M_{ij} is added are determined from not only I and j but also p and m. It can be previously computed. In order to explain the basic idea, let us consider the following simple example. Let (p, m, k) be (41, 3, 6), respectively, and let X, Y be given as

$$X = x_0\gamma + x_1\gamma^p + x_2\gamma^{p^2}, \tag{5a}$$

$$Y = y_0\gamma + y_1\gamma^p + y_2\gamma^{p^2}. \tag{5b}$$

Suppose that not only x_0y_0, x_1y_1, x_2y_2 but also M_{01}, M_{02}, M_{12} have been calculated as the temporary values, then we need to calculate $q[0]$, $q[1]$, $q[2]$, and $q[3]$. In this case, those temporary values are used as

$$q[0] = 0, \tag{6a}$$

$$q[1] = x_0y_0 + M_{01} + 2M_{02} + 3M_{12}, \tag{6b}$$

$$q[2] = x_1y_1 + 2M_{01} + 3M_{02} + M_{12}, \tag{6c}$$

$$q[3] = x_2y_2 + 3M_{01} + M_{02} + 2M_{12}, \tag{6d}$$

Note that M_{01}, M_{02}, and M_{12} are given as

$$M_{01} = (x_0 - x_1)(y_0 - y_1), \tag{7a}$$

$$M_{02} = (x_0 - x_2)(y_0 - y_2), \tag{7b}$$

$$M_{12} = (x_1 - x_2)(y_1 - y_2), \tag{7c}$$

In our previous work (Kato et al, 2007), it has been shown that $q[0]$ becomes 0 when k is even. As shown in Eqs.(6), six M_{01}'s in total are added to $q[1]$, $q[2]$, and $q[3]$. M_{02}'s and M_{12}'s are similarly added to $q[1]$, $q[2]$, and $q[3]$. Thus, it is found that the number of additions increases as k becomes larger.

Based on Eqs.(6), consider the following $m \times {}_mC_2$ matrix given from the coefficients related to k:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}. \tag{8}$$

As shown in Eq.(8), finite field theory often demonstrates such a symmetric feature. In what follows, we consider how to reduce the number of such additions. Such a matrix can be previously computed because it only depends on p, m, and k.

3.2 Improvement with tree structure

Eq.(8) can be decomposed as

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}. \tag{9}$$

Thus, the decomposed equation also has the symmetric feature. Then, consider C_{101}, C_{011}, and C_{110} as

$$C_{101} = M_{01} + 2M_{12}, \tag{10a}$$

$$C_{011} = M_{02} + 2M_{01}, \tag{10b}$$

$$C_{110} = M_{12} + 2M_{02}. \tag{10c}$$

The lower suffixes correspond to the column vectors of the first matrix of the right-hand side of Eq.(9) and thus it is led from Eq.(9). Then, using C_{101}, C_{011}, and C_{110}, $q[1]$, $q[2]$, and $q[3]$ are calculated by

$$q[1] = x_0 y_0 + C_{101} + C_{110}, \tag{11a}$$

$$q[2] = x_1 y_1 + C_{110} + C_{011}, \tag{11b}$$

$$q[3] = x_2 y_2 + C_{101} + C_{011}, \tag{11c}$$

Though Eqs.(6) needs 18 additions, Eqs.(11) needs only 12 additions. This example is one of the most efficient cases. However, since the lower suffixes are efficiently controlled with *tree structure*, this technique can be widely applied for more general cases. In other words, using *tree structure*, $q[0]$ to $q[m]$ are systematically recomposed with temporary calculated values such as C_{110}, C_{101}, and C_{011}.

4. Simulation

In order to show the efficiency of the improvement, this section simulates the improved CVMA with some practical parameter settings.

4.1 Parameter settings

This section considers a more practical case. Since pairing-based cryptographies often considers 158-bit characteristic p and extension degree m = 6, for simulation we consider m = 6 and the following p:

$$\begin{aligned} p = {} & 218673105437695088256450591/ \\ & 949649001738589593793. (158\text{bit}) \end{aligned} \tag{12}$$

In this case, the minimal k that satisfies the conditions for the existence of type I-X Gauss period normal basis in F_{p^6} is 12. Noting that k is even in the same of the preceding example, consider $q[1]$ to $q[6]$ in this case. Then, the $m \times {}_m C_2$ becomes

$$\begin{pmatrix} 0 & 2 & 2 & 3 & 2 & 3 & 3 & 1 & 3 & 1 & 0 & 3 & 3 & 1 & 3 \\ 2 & 3 & 3 & 1 & 3 & 0 & 2 & 2 & 3 & 3 & 3 & 1 & 1 & 0 & 3 \\ 3 & 3 & 1 & 0 & 3 & 2 & 3 & 3 & 1 & 0 & 2 & 2 & 3 & 3 & 1 \\ 3 & 1 & 2 & 3 & 1 & 3 & 3 & 1 & 0 & 2 & 3 & 3 & 0 & 2 & 3 \\ 1 & 0 & 3 & 2 & 3 & 3 & 1 & 2 & 3 & 3 & 3 & 1 & 2 & 3 & 0 \\ 3 & 3 & 1 & 3 & 0 & 1 & 0 & 3 & 2 & 3 & 1 & 2 & 3 & 3 & 2 \end{pmatrix}. \tag{13}$$

In this case, it is decomposed as Eq.(14).

$$\begin{pmatrix} 0 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 0 & 2 & 0 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 \\ 2 & 2 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 2 & 2 & 2 & 2 & 0 \\ 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 2 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 0 \\ 2 & 2 & 0 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}. \tag{14}$$

Thus, while the original CVMA needs

$$21M_1 + 210A_1, \tag{15a}$$

the improved CVMA needs

$$21M_1 + 86A_1 + 15D_1. \tag{15b}$$

4.2 Simulation result

Let characteristic p be 158–bit prime, Table 1 shows calculation costs and simulation results of the original CVMA for some pairs of extension degree m and k, Table 2 shows those of the improved CVMA. The simulation result shows that the improved CVMA becomes more efficient than the original.

extension degree m	parameter k	without the improvement†	with the improvement†
6	1	(21,50,-)	-
	2	(21,60,-)	-
	6	(21,120,-)	(21,80,15)
	12	(21,210,-)	(21,86,15)
12	1	(78,198,-)	-
	2	(78,343,-)	(78,321,1)
	6	(78,528,-)	(78,393,36)
	12	(78,660,-)	(78,426,60)

†(21, 80, 15) denotes $21M_1 + 80A_1 + 15D_1$, for example.

Table 1. Calculation cost of CVMA

5. Conclusion

This paper has first introduced *cyclic vector multiplication algorithm* (CVMA) that is a multiplication algorithm in extension field. Then, it was also introduced that CVMA was

extension degree m	parameter k	without the improvement [μs]‡	with the improvement [μs]‡
6	1	(21,50,-)	-
	2	(21,60,-)	-
	6	(21,120,-)	(21,80,15)
	12	(21,210,-)	(21,86,15)
12	1	(78,198,-)	-
	2	(78,343,-)	(78,321,1)
	6	(78,528,-)	(78,393,36)
	12	(78,660,-)	(78,426,60)

‡The authors used Pentium4 (3.6GHz), C language, and GMP4.2.2 library.

Table 2. Timing of a multiplication with CVMA

useful under the tight restrictions of *pairing-based cryptographies*. Then, this paper pointed out a problem about the calculation cost of CVMA. For this problem, this paper proposed an improvement. According to some simulation results, it was shown that the improvement made CVMA much more efficient.

6. References

Apostol, T. (1976). *Introduction to Analytic Number Theory*, Springer-Verlag, ISBN: 978-0-387-90163-3

Bailey, D. & Paar, C. (1998). Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms, *Proceedings of CRYPT'98*, pp.472-485, ISBN: 978-3-540-64892-5, USA, August 1998, Springer-Verlag, Santa Barbara, California

Barreto, P. S. L. M. & Naehrig, M. (2006). Pairing-Friendly Elliptic Curves of Prime Order, *Proceedings of SAC2005*, pp. 319-331, ISBN: 978-3-540-33108-7, Canada, August 2005, Springer-Verlag, Kingston

Boneh, D.; Lynn, B. & Shacham, H. (2001). Short signatures from the Weil pairing, *Proceedings of Asiacrypt2001,* pp. 514-532, ISBN: 978-3-540-42987-6, Australia, December 2001, Springer-Verlag, Gold Coast

Cohen, H. & Frey, G. (2005). *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall CRC, ISBN: 1584885181

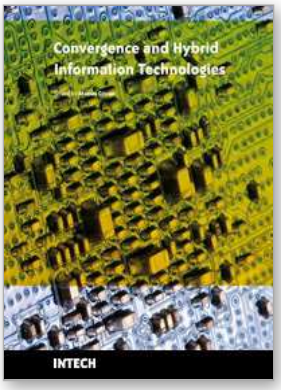
Devegili, A. J.; Scott, M. & Dahab, R. (2007). Implementing Cryptographic Pairings over Barreto-Naehrig Curves, *Proceedings of Pairing2007*, pp. 197-207, ISBN: 978-3-540-73488-8, Japan, July 2007, Springer-Verlag, Tokyo

Freeman, D. (2006). Constructing pairing-friendly elliptic curves with embedding degree 10, *Proceedings of ANTS-VII*, pp. 248-258, ISBN: 978-3-540-36075-9, Germany, July 2006, Springer-Verlag, Berlin

Gao, S. (1993). Normal Bases over Finite Fields. *Doctoral thesis*, Waterloo, Ontario, Canada GNU Multiple Precision Arithmetic Library, http://gmplib.org/

Kato, H.; Nogami, Y. & Morikawa, Y. (2007) Cyclic Vector Multiplication Algorithm Based on a Special Class of Gauss Period Normal Basis. *ETRI Journal*, Vol. 29, No. 6, December 2007, 768-778, ISSN: 1225-6463

Nakanishi, T. & Funabiki, N. (2005). Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps, *Proceedings of Asiacrypt2005,* pp. 443-454, ISBN: 978-3-540-30684-9, India, December 2005, Springer-Verlag, Chennai



Convergence and Hybrid Information Technologies

Edited by Marius Crisan

ISBN 978-953-307-068-1
Hard cover, 426 pages
Publisher InTech
Published online 01, March, 2010
Published in print edition March, 2010

Starting a journey on the new path of converging information technologies is the aim of the present book. Extended on 27 chapters, the book provides the reader with some leading-edge research results regarding algorithms and information models, software frameworks, multimedia, information security, communication networks, and applications. Information technologies are only at the dawn of a massive transformation and adaptation to the complex demands of the new upcoming information society. It is not possible to achieve a thorough view of the field in one book. Nonetheless, the editor hopes that the book can at least offer the first step into the convergence domain of information technologies, and the reader will find it instructive and stimulating.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821