Pairing-friendly field における超楕円曲線上のペアリングの並列化について

石井 将大† 猪俣 敦夫† 藤川 和利†

†奈良先端科学技術大学院大学
〒630-0192 奈良県生駒市高山町 8916-5

あらまし ペアリングは，楕円曲線上の点の集合に対し定義された双線形写像であり，ID ベース暗号やブロードキャスト暗号等に応用されている．一般的に，ペアリングに係る演算は，曲線上の演算に比べ複雑で，種数の高い代数曲線を選択すると計算コストはより高くなる．本稿では，pairing-friendly filed における演算の並列実装を行い，ペアリングに効率的な拡大体の構成法について述べる．拡大体の並列演算は Karatsuba 法に注目し，その並列化に適した曲線とペアリングアルゴリズムについて考察を与える．

A study of parallel computation of pairings on hyperelliptic curves with pairing-friendly fields

Masahiro ISHII† Atsuo INOMATA† Kazutoshi FUJIKAWA†

†Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, NARA 630-0192 JAPAN

Abstract Bilinear pairings on elliptic curves have been applied into many cryptographic schemes, for example ID-based cryptography and so on. Generally, the pairing computation is complex and its cost is much larger than the general arithmetic on curves, and much more using curves of higher genus such as hyperelliptic curves. In this paper, we consider a parallelized algorithm for pairing-friendly fields, and we report how to construct extension field effectively for pairings. We focus on parallel Karatsuba method for arithmetic in extension field, and also consider the pairing algorithm suitable for our parallelized algorithm.

1 Introduction

Koblitz [8] suggested a hyperelliptic cryptosystem such that using Jacobians of hyperelliptic curves as generalization of using arithmetic on groups of elliptic curves. Arithmetic on Jacobians of hyperelliptic curves is more complex than on elliptic curves groups. Alternatively, we can take smaller finite field if using curves of higher genus as keeping a same security level.

Pairings on elliptic curves or higher genus ones have attracted a lot of attention, and have been applied into many cryptographic schemes, for example ID-based cryptography and so on. Generally, the calculation method of pairings is complex and its cost on pairing is much larger than the arithmetic on curves, and much more by using algebraic curves of higher genus.

Nowadays GPGPU technology based on GPU computation has enhanced and it has rapidly spread in high level implementations for cryptography.

In this paper, we consider a parallelizaion of arithmetic on extension field and the pairing algorithm suitable for our parallel algorithm. Katoh et al. [6] implemented η_T pairing on GPU, similarly we parallelize arithmetic on extension field constructed by irreducible polynomial. So that we compute elements of

extension field as polynomials, and parallelize their arithmetic straightforwardly. Additionally, we consider an approach for combining the parallelization of Karatsuba method and parallel arithmetic on extension field as mentioned above. Finally, we mention about the algorithm of Eta pairing suitable for our parallelization of arithmetic on extension field.

This paper is organized as follows. We recall background on pairings on hyper elliptic curves, especially describe η_T pairing in detail in section 2. Section 3 gives a brief summary of pairig-friendly fields and Karatsuba method. Section 4 discusses the parallelization of Karatsuba method and arithmetic on extension fields, and we report timing result of implementation on GPU. Section 5 discusses the η_T pairing algorithm suitable for our parallel algorithm discussed in section 4. Finally, we draw our conclusion in section 6.

2 Eta pairing on hyperelliptic curves

In this section, we describe general form of *Tate-Lichtenbaum pairing* on hyeprelliptic curves and give overview of η_T pairing.

Let C be a hyperelliptic curve defined over $\mathbb{F}_q$ and let $\mathrm{Jac}_C(\simeq \mathrm{Pic}^0_C)$ denote Jacobian of C. Let r be a positive integer and suppose that $\mathbb{F}_{q^k}$ is an extension field of $\mathbb{F}_q$ such that $r|(q^k-1)$. For a divisor class $D \in \mathrm{Jac}_C(\mathbb{F}_{q^k})[r]$, $f_{r,D}$ denotes a rational function associated the principal divisor rD. Let $E = \sum n_P P$ be a divisor class disjoint from D. Then we call T_r the Tate-Lichtenbaum pairing as follows

$$T_r \colon \mathrm{Jac}_C(\mathbb{F}_{q^k})[r] \times \mathrm{Jac}_C(\mathbb{F}_{q^k})/r\mathrm{Jac}_C(\mathbb{F}_{q^k}) \to \mathbb{F}^{\times}_{q^k}/(\mathbb{F}^{\times}_{q^k})^r$$

$$(D, E) \mapsto f_{r,D}(E) = \prod_P f_{r,D}(P)^{n_P}.$$

The map T_r is bilinear, non-degenerate and the value of T_r is independent of representation of the divisor classes.

We describe η_T pairing [3] and give some its good properties. Barreto et al. exploited η_T pairing in [3] for supersingular curves as generalization of the Duursma and Lee technique [5].

Suppose that $C/\mathbb{F}_q$ is supersingular curve which has embedding degree $k > 1$, and there is a distortion map

$$\psi \colon C(\mathbb{F}_q) \to C(\mathbb{F}_{q^k})$$

which allows denominator elimination (i.e., for $P \in C(\mathbb{F}_q)$, $\psi(P) \in C(\mathbb{F}_{q^k})$ has x-coordinate in $\mathbb{F}_{q^{k/2}}$). Then for $T \in \mathbb{Z}$, *eta pairing (η_T pairing)* is given by

$$\eta_T \colon \mathrm{Jac}_C(\mathbb{F}_q)[r] \times \mathrm{Jac}_C(\mathbb{F}_q) \to \mu_r \subset \mathbb{F}^{\times}_{q^k}$$
$$(D, E) \mapsto f_{(T,D)}(\psi(E))^{(q^k-1)/r}.$$

In general, this map η_T is not non-degenerate, bilinear pairing. Barreto et al. give sufficient conditions on T under which η_T can be modified Tate-Lichtenbaum pairing.

η_T pairing is one of the twisted Ate pairing [2][§4.7] and can be often implemented more fastly than the other pairing. Barreto et al. generalized Durrsma-Lee techniques [5] such as effective calculation of divisors and using Frobenius map directly in Miller's algorithm. Especially, they succeeded to generalize loop shortening idea to many other cases.

3 Pairing-friendly fields and Karatsuba method

Koblitz and Menezes [7] suggested effective extension fields which called *pairing-friendly fields* for calculating pairings. In this section, we describe definition of pairing-friendly fields and Karatsuba method used for arithmetic extension field which constructed as pairing-friendly field.

An extension field $\mathbb{F}_{q^k}$ is said *pairing-friendly fields* if $p \equiv 1 \pmod{12}$ and k is of the form $2^i 3^j$ (if $j = 0$, need $p \equiv 1 \pmod 4$).

Suppose that an extension field $\mathbb{F}_{q^k}$ is pairing-friendly field, $\mathbb{F}_{q^k}$ can be constructed from $\mathbb{F}_q$ as a tower of quadratic and cubic extensions. If we first extend from $\mathbb{F}_q$ as cubic extension, that is constructed such as $\mathbb{F}_{q^3} \simeq \mathbb{F}_q[x]/(x^3 -$

β), then elements of $\mathbb{F}_{q^3}$ are written as a polynomial of degree 2 and arithmetic on field as calculation of polynomials.

In $\mathbb{F}_{q^3}$, Toom-Cook method reduces a multiplication to 5 multiplications in $\mathbb{F}_q$ rather than 9 multiplications by using Schoolbook method. Similarly, Karatsuba method reduces multiplication in quadratic extension field to 3 (rather than 4) multiplication. Thus the cost of multiplications in pairing-friendly field can be reduced by repeating Karatsuba or Toom-Cook method.

In this paper, we focus on Karatsuba method and we implement arithmetic on extension field by using only Karatsuba method. Karatsuba method can be generalized for polynomials of arbitrary degree [10][§3.2, Algorithm 2]. We consider two polynomials of degree d,

$$A(x) = \sum_{i=0}^{d} a_i x^i, \quad B(x) = \sum_{i=0}^{d} b_i x^i.$$

We compute for each $i = 0, ..., d$,

$$V_i := a_i b_i, \tag{1}$$

and for $0 \leq s < t \leq d$,

$$V_{s,t} = (a_s + a_t)(b_s + b_t), \tag{2}$$

then we can compute $a(x)b(x) = \sum_{i=0}^{2d} c_i x^i$ as follows

$$c_0 = V_0$$
$$c_{2d} = V_d$$
$$c_i = \begin{cases} \sum_{s+t=i} V_{s,t} - \sum_{s+t=i} (V_s + V_t) & i\text{: odd}, \\ \sum_{s+t=i} V_{s,t} - \sum_{s+t=i} (V_s + V_t) + V_{i/2} & i\text{: even}, \\ \text{for } 0 \leq s < t \leq d,\ 0 < i < 2d. & \end{cases} \tag{3}$$

Thus we can use Karatusba method for multiplication in extension field $\mathbb{F}_{q^k}$ and reduce a multiplication to respectively $3, 6, 21, 78$ multiplications in $\mathbb{F}_q$ if respectively $k = 2, 3, 6, 12$.

4 Parallelization of Karatsuba method and arithmetic on extension fields

In this section, we discusses the parallelization of arithmetic on extension fields. We focus on pairing-friendly fields and multiplication using Karatsuba method. We show how construct effectively extension fields as pairing-friendly fields suitable our parallelization.

4.1 Parallelization of arithmetic on finite field

Katoh et al. implemented η_T pairing on GPU by parallelizing Comb method on finite field [6][§3.2, Implementation II]. In this paper, we implement straightforward parallel computation of polynomials for arithmetic on extension field. For $a(x), b(x) \in \mathbb{F}_q[x]/(f(x))$,

$$a(x) = \sum_{i=0}^{m} a_i x^i,$$
$$b(x) = \sum_{i=0}^{m} b_i x^i,$$

we compute coefficients of $a(x)+b(x), a(x)b(x)$ in parallel. That is for $a(x)+b(x)$ we compute $a_i + b_i$ in parallel, and for $a(x)b(x)$ compute $c_k = \sum_{i+j=k} a_i b_j$ in parallel.

4.2 Parallelization of Karatsuba method

In addition above parallel method, we consider parallelization of Karatsuba method for arithmetic on pairing-friendly fields. As mentioned previous section, we use only Karatusba method for multiplication on pairing-friendly fields. We parallelize precomputation phase of Karatsuba method, first compute V_i (1) in parallel, and compute $(a_s + b_t)$, $(b_s + b_t)$ (2) in parallel then compute $V_{s,t}$ (2) in prallel. After that we compute c_i (3) in serial.

4.3 Combining the Parallelizations

We combine the parallel methods as mentioned above and adapt this method to arithmetic on

pairing-firendly fields. For efficient parallel implementation and computation of pairing, we consider finite field which has small characteristic p such as $p = 2, 3$. Supersingular hyperelliptic curves of genus 2 have embedding degree bounded by 12. We implement parallelized arithmetic on $\mathbb{F}_{q^k}$ when $k = 2, 3, 6, 12$ and $q = 2^m$ or $q = 3^m$ for efficient parallelized computation of η_T pairing. We implement arithmetic on $\mathbb{F}_{q^k}$ by three methods as follows.

I. We compute in serial.

II. We compute elements in $\mathbb{F}_p^m$ in parallel (4.1).

III. We combine parallelize methods that is compute elements in $\mathbb{F}_{q^k}$ by Karatsuba method in parallel (4.2), and compute each element in $\mathbb{F}_{p^m}$ shown as coefficients of Karatsuba polynomial in parallel (4.2).

We implement our parallel algorithm on GPU, NVIDIA GeForce GTX 590, and CUDA [4]. For comparison, the case I we compute on GPU in serial. We implement multiplication by Karatsuba method on $\mathbb{F}_{q^k}$ where $k = 2, 3, 6, 12$ and $q = 2^{79}, 2^{103}$ for η_T pairings on genus 2 curves, $q = 3^{97}, q = 3^{193}, q = 3^{509}$ for η_T pairings on elliptic curves. Calculate time seems to be depend on extend degrees m that is the degree of parallelism. Thus we show the case $q = 2^{103}, q = 3^{193}, q = 3^{509}$. We use `cudaEvent` part of CUDA Runtime API, for timing, and note that this calculate time is measured when calculating on GPU, thus do not take thought for timing to memory transfer on GPU. We call this timing *GPU time*, and call whole running time *Host time*. GPU time of calculating a multiplication in $\mathbb{F}_{p^{km}}$ by using Karatsuba method as follows. Note that in the timing tables, entries which has no element mean that we do not implement.

As shown Table 1,2, we can say that the computation cost of Karatsuba method in $\mathbb{F}_{3^{6m}}/\mathbb{F}_{3^m}$ is smaller than in $\mathbb{F}_{3^{6m}}/\mathbb{F}_{3^{3m}}/\mathbb{F}_{3^m}$ constructed as tower extension because a multiplication in $\mathbb{F}_{3^{6m}}$ equivalence 3 multiplications in $\mathbb{F}_{3^{3m}}$ by using Karatsuba method, and cost of addition is enough to small. Similarly,

Table 1: *GPU time* of a multiplication in extension field $\mathbb{F}_{3^{k\cdot 193}}$ over $\mathbb{F}_{3^{193}}$ (ms)

Implementation	I	II	III
$k = 2$	38.803	0.209	0.172
$k = 3$	80.863	0.456	0.153
$k = 6$	301.528	1.777	**0.383**
$k = 12$			1.765

Table 2: *GPU time* of a multiplication in extension field $\mathbb{F}_{3^{k\cdot 509}}$ over $\mathbb{F}_{3^{509}}$ (ms)

Implementation	I	II	III
$k = 2$	273.906	0.734	0.268
$k = 3$	575.911	1.503	0.507
$k = 6$	2162.24	5.437	**0.925**
$k = 12$			3.304

Table 3: *GPU time* of a multiplication in extension field $\mathbb{F}_{2^{k\cdot 103}}$ over $\mathbb{F}_{2^{103}}$ (ms)

Implementation	I	II	III
$k = 2$	10.408	0.132	0.094
$k = 3$	20.954	0.299	**0.103**
$k = 6$	75.580	1.231	0.318
$k = 12$			1.504

Table 4: *Host time* of a multiplication in extension field $\mathbb{F}_{3^{k\cdot 193}}$ over $\mathbb{F}_{3^{193}}$ (ms)

Implementation	I	II	III
$k = 2$	39.029	1.919	0.615
$k = 3$	81.141	4.804	0.790
$k = 6$	302.018	21.715	**2.931**
$k = 12$			38.767

Table 5: *Host time* of a multiplication in extension field $\mathbb{F}_{3^{k\cdot 509}}$ over $\mathbb{F}_{3^{509}}$ (ms)

Implementation	I	II	III
$k=2$	274.081	2.078	0.686
$k=3$	576.146	5.159	1.134
$k=6$	2162.74	23.071	**3.719**
$k=12$			41.383

Table 6: *Host time* of a multiplication in extension field $\mathbb{F}_{2^{k\cdot 103}}$ over $\mathbb{F}_{2^{103}}$ (ms)

Implementation	I	II	III
$k=2$	10.565	1.441	0.461
$k=3$	21.163	3.858	**0.661**
$k=6$	75.985	18.390	2.747
$k=12$			38.185

the cost of multiplication in $\mathbb{F}_{3^{6m}}/\mathbb{F}_{3^{2m}}/\mathbb{F}_{3^m}$ is higher. Thus if $k=6$, it is efficient to construct extension field directly for η_T pairing on elliptic curves.

In the same way as we consider above, and as shown Table 3, the computation cost of Karatsuba method in $\mathbb{F}_{3^{12m}}/\mathbb{F}_{3^{6m}}/\mathbb{F}_{3^{3m}}/\mathbb{F}_{3^m}$ is smaller than in $\mathbb{F}_{3^{12m}}/\mathbb{F}_{3^m}$. In the case, a multiplication in $\mathbb{F}_{3^{12m}}$ equivalence 9 multiplications $\mathbb{F}_{3^{3m}}$ by using Karatsuba method recursively.

If we consider a whole running time, Host time, as shown Table 4,5 it is efficient to construct extension field directly for η_T pairing on elliptic curves because an addition in costs $\mathbb{F}_{3^m}$ about 200 μs. Similarly, we can say that it is efficient to construct extension field by starting cubic extension for η_T pairing on hyperelliptic curves if $k=12$.

5 Computation of the Eta pairing

In this section, We discuss the algorithm of pairing on hyperelliptic curve with parallel computation on extension fields that we describe previous section. Barreto et al. described η_T pairing on genus 2 supersingular curve in detail in [3][§7]. We use this curve and consider η_T pairing in same condition.

We consider the supersingular curve

$$C\colon y^2+y=x^5+x^3$$

over $\mathbb{F}_{2^m}$ where m is coprime to 6. This curve has embedding degree 12, and as shown previous section we construct $\mathbb{F}_{2^{12m}}$ by starting cubic extension as

$$\mathbb{F}_{2^{12m}}/\mathbb{F}_{2^{6m}}/\mathbb{F}_{2^{3m}}/\mathbb{F}_{2^m}$$

for parallel arithmetic on extension field.

Now, we construct extension field that it is different from choice of basis of field in [3][§7.1]. We define $\mathbb{F}_{2^{3m}}$ using irreducible polynomial x^3+x+1 over $\mathbb{F}_{2^m}$ thus let w be one of the root of x^3+x+1, we represent elements $\mathbb{F}_{2^{3m}}$ with basis $\{1,w,w^2\}$ over $\mathbb{F}_{2^m}$. Similarly, we consider irreducible polynomial $y^2+y+w+1$ over $\mathbb{F}_{2^{3m}}$ and let s be one of the root of this polynomial, $\mathbb{F}_{2^{6m}}$ has the basis $\{1,w,w^2,s,sw,sw^2\}$. Finally, for irreducible polynomial $z^2+z+s+sw^2$ over $\mathbb{F}_{2^{6m}}$, let t is one of the root of this polynomial, thus we can represent elements of $\mathbb{F}_{2^{12m}}$ with basis.

$$\{1,w,w^2,s,sw,sw^2,t,tw,tw^2,st,stw,stw^2\}$$

Let ψ be a distortion map such as

$$\psi(x,y)=(x+s,y+t_2x^2+t_1x+t)$$

where $t_1=s^4+s^2$, $t_2=x^4+1$ ($x+s\in\mathbb{F}_{2^{12m/2}}$). Then we can construct η_T pairing in the same way as using technique described in [3][§7]. In the case, we can use octupling formula for computaion of divisors such that for a divisor $D=(P)-(\infty)$, $8D=(P')-(\infty)$ where $P'=\varphi\pi^6(P)$, π is 2-power Frobenius map and φ is an automorphism of C such as

$$\varphi(x,y)=(x+1,y+x^2+1).$$

Then we set $q=2^{3m}$, $\gamma=\varphi^m$, the same parameters in [3][§7.1, 7.2], we can see [3][§7.2 Lemma 9] is true in the case that we choose the basis of $\mathbb{F}_{2^{12m}}$ as above. Thus the conditions of

[3][§4 Theorem 1] which define the η_T pairing are also satisfied in our case.

In this paper, we do not describe detailed algorithm of pairing in this case and implement the pairing on GPU. We will tackle these as future work.

6 Conclusions

We show that parallelize algorithm of arithmetic on extension field and how to construct pairing-friendly field effectively for our parallelization. We focus on Karatsuba method for arithmetic in extension field, and consider to combine parallel methods of Karatsuba multiplication and arithmetic on base field. And we mention about how to construct the effective pairing-friendly field for pairings on hyperelliptic curves.

In addition, we describe that we can compute the η_T pairing on hyperelliptic curve [3][§7] with pairing-friendly field constructed suitable for our parallel method without transform distortion map and conditions of η_T pairing. However, we do not describe the algorithm of pairing in detail, therefore we are going to consider the algorithm and implement the pairing on GPU.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren: *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications. Chapman & Hall/CRC, 2006.

[2] Jennifer Balakrishnan, Juliana Belding, Sarah Chisholm, Kirsten Eisenträger, Katherine E. Stange, and Edlyn Teske: Pairings on hyperelliptic curves, CoRR, abs/0908.3731, 2009.

[3] P. S. L. M. Barreto, S. Galbraith, C. Ó hÉigeartaigh, and M. Scott: Efficient Pairing Computation on Supersingular Abelian Varieties, *Designs, Codes and Cryptography* **42**, pp. 239-271, 2007.

[4] NVIDIA, CUDA Zone, `http://developer.nvidia.com/category/zone/cuda-zone`.

[5] I. Duursma and H.-S. Lee: Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, Advances in Cryptology - Asiacrypt 2003, *Lecture Notes in Computer Science* **2894**, pp. 111-123, Springer-Verlag, 2003.

[6] Yosuke Katoh, Yun-Ju Huang, Chen-Mou Cheng, and Tsuyoshi Takagi: Efficient Implementation of the EtaT Pairing on GPU, 9th International Conference on Applied Cryptography and Network Security, ACNS 2011, Industrial Track, pp. 119-133, 2011.

[7] N. Koblitz and A. Menezes: Pairing-based cryptography at high security levels, Cryptography and Coding 2005, *Lecture Notes in Computer Science* **3796**, pp. 13-36, Springer-Verlag, 2005.

[8] N. Koblitz: Hyperelliptic cryptosystems, *Journal of Cryptography* **1**, pp. 139-150, 1989.

[9] N. Koblitz: *Algebraic Aspects of Cryptography. Algorithms and Computation in Mathematics **3***, Springer-Verlag, Berlin, 1998.

[10] A. Weimerskirch and C. Paar: Generalization of the Karatsuba Algorithm for Efficient Implementations. Cryptology ePrint Archive, Report 2006/224, Available: `http://eprint.iacr.org/2006/224`, 2006.