LETTER

Improvement of Final Exponentiation for Pairings on BLS Curves with Embedding Degree 15

Yuki NANJO[†a)], ***Student Member***, **Masaaki SHIRASE**[††b)], **Takuya KUSAKA**[†c)], ***and*** **Yasuyuki NOGAMI**[†d)], ***Members***

SUMMARY To be suitable in practice, pairings are typically carried out by two steps, which consist of the Miller loop and final exponentiation. To improve the final exponentiation step of a pairing on the BLS family of pairing-friendly elliptic curves with embedding degree 15, the authors provide a new representation of the exponent. The proposal can achieve a more reduction of the calculation cost of the final exponentiation than the previous method by Fouotsa et al.

key words: *pairing-based cryptography, BLS curves, final exponentiation*

1. Introduction

Pairings on elliptic curves enable innovative protocols, e.g., ID-based encryption [1], group signature authentication [2], searchable encryption [3], attribute-based encryption [4], and homomorphic encryption [5]. The elliptic curves on which pairings are defined are typically chosen from families of pairing-friendly elliptic curves, e.g., Barreto-Lynn-Scott (BLS) family [6], Barreto-Naehrig family [7], Kachisa-Schaefer-Scott family [8], and so on. One of the important facts is that these families have fixed polynomial formulas of a field characteristic p and group order r in terms of an integer parameter u where is chosen as both p and r are primes. These families also have a specific embedding degree k where is the smallest integer such that $r \mid (p^k - 1)$. In this paper, the authors focus on the BLS curves with $k = 15$ and try to improve the pairings on those curves, which are suggested for the pairings at the 128-bit security level in the recent works [9] and [10].

To be useful in cryptography, the pairings are typically carried out by two steps, which are the Miller loop and extra exponentiation in a finite field of order p^k to bring the output of the Miller loop to the unique value. This extra exponentiation is called a final exponentiation and that becomes more of a computational bottleneck with a large embedding degree k. In fact, the exponent of the final exponentiation is specifically given as $(p^k - 1)/r$. Since p and r are fixed by the polynomials corresponding to the families, Scott et al. gave a systematic method to find short vectorial addition chains to compute the final exponentiation in [11]. In [12], Fuentes et al. also presented a lattice-based method for determining a multiple of the exponent which results in at least as efficient final exponentiation as the method by Scott et al. [11].

For the BLS curves with $k = 15$, in [9], Fouotsa et al. found one of the best multiples of the exponent by using the lattice-based method [12] and provided the steps of computing the final exponentiation as a state-of-the-art method. In contrast, in this paper, the authors present another computation method with a new multiple of the exponent which results in more efficient final exponentiation than the previous method [9]. Indeed, the authors obtain that by using the property of the polynomial parameterization of p for the BLS family, which is also used for expanding the exponent for the BLS curves with $k = 27$ in [13] by Zhang et al. The authors also confirm that the proposal results in reducing at least two multiplications in a finite field of order p^{15} and two inversions in a cyclotomic subgroup from the previous method [9] for the pairing at the 128-bit security level.

The rest of this paper is organized as follows: Section 2 provides a brief fundamental of the final exponentiation. Section 3 describes the previous and proposed computations of the final exponentiation for the pairing on the BLS curves with $k = 15$. Section 4 presents the sample operation counts for the final exponentiation. Finally, Sect. 5 draws the conclusion.

2. The Final Exponentiation

The pairings such that the Tate pairing and its variants are typically computed by two steps, i.e., the Miller loop and final exponentiation. The final exponentiation step is given as a powering $(p^k - 1)/r$ in the finite field of order p^k. To achieve fast computation, the exponent is typically broken into two parts as follows [14]:

$$(p^k - 1)/r = [(p^k - 1)/\Phi_k(p)] \cdot [\Phi_k(p)/r], \tag{1}$$

where $\Phi_k(\cdot)$ is the k-th cyclotomic polynomial. The exponentiation by the first part is inexpensive and is called as a *easy part*, however, that of the second part, i.e, $d = \Phi_k(p)/r$, is more difficult to compute and is called as a *hard part*.

Since p and r are fixed by polynomials in base an integer u corresponding to the families, several optimizations can be available for the hard part computation. In [11],

Manuscript received April 27, 2020.
Manuscript revised July 5, 2020.
Manuscript publicized July 17, 2020.

[†]The authors are with Okayama University, Okayama-shi, 700-8530 Japan.
[††]The author is with Future University Hakodate, Hakodate-shi, 041-8655 Japan.
a) E-mail: yuki.nanjo@s.okayama-u.ac.jp
b) E-mail: shirase@fun.ac.jp
c) E-mail: takuya-t@okayama-u.ac.jp
d) E-mail: yasuyuki.nogami@okayama-u.ac.jp

DOI: 10.1587/transfun.2020EAL2046

Scott et al. gave a systematic method to reduce the computational complexity of the hard part by representing d to the polynomial in base p from the observation that p-th powering in the finite field is efficiently computed by the Frobenius endomorphism. In the context, d can be represented as $d = d_0 + d_1 p + \cdots + d_{n-1}p^{n-1}$ where n is the value of the Euler's totient function by k and d_i for $0 \le i \le (n-1)$ are polynomial coefficients in base u. Assuming f is an element after raising to the power of the easy part, one can find short vectorial addition chains to compute $f \mapsto f^d = f^{d_0} \cdot (f^{d_1})^p \cdots (f^{d_{n-1}})^{p^{n-1}}$. In [12], Fuentes et al. proposed to use a multiple d' of d such that $r \nmid d'$ and presented a lattice-based method for determining d' such that $f \mapsto f^{d'}$ can be computed at least as efficiently as $f \mapsto f^d$ applied [11]. An efficient d' can be found by constructing a rational matrix M' with dimensions $\deg(p) \times n \cdot \deg(p)$ and applying LLL algorithm [15] to M'.

3. The BLS Family of Pairing-Friendly Elliptic Curves with $k = 15$

The BLS family of pairing-friendly elliptic curves with $k = 15$ are parameterized as the following characteristic p and group order r.

$$p = m(u) \cdot \Phi_{15}(u) + u, \tag{2}$$
$$r = \Phi_{15}(u), \tag{3}$$

where $m(u) = (u-1)^2/3 \cdot (u^2+u+1)$, $\Phi_{15}(\cdot)$ is the fifteenth cyclotomic polynomial, and u is an integer making p and r being primes such that $u \equiv 1 \pmod 3$. The above parameterization is also found by Duan et al. in [16].

With the above, one can find an efficient representation of $(p^{15}-1)/r$ or multiple of that which results in a fast final exponentiation in the finite field of degree p^{15}, which is denoted as $\mathbb{F}_{p^{15}}$. In the following, the authors review the state-of-the-art method by Fouotsa et al. [9] in Sect. 3.1 and describe our proposed method in Sect. 3.2.

3.1 State-of-the-Art Method

In [9], Fouotsa et al. proposed to decompose the exponent as

$$(p^{15}-1)/r = [(p^5-1)] \cdot [\Phi_3(p^5)/r], \tag{4}$$

where $\Phi_3(\cdot)$ is the third cyclotomic polynomial. The first and second parts are corresponding to the easy and hard part, respectively. Note that they dared to use the above decomposition, however, the exponent is typically decomposed as shown in Eq. (1).

For $\tilde{d} = \Phi_3(p^5)/r$, they found one of the best multiple $\tilde{d}'$ of $\tilde{d}$ by the lattice-based method [12]. In the context, they found $\tilde{d}' = 3u^3 \cdot \tilde{d}$ which is represented as a polynomial in base p given as $\tilde{d}' = \tilde{d}'_0 + \tilde{d}'_1 p + \cdots + \tilde{d}'_9 p^9$ where $\tilde{d}'_i$ for $0 \le i \le 9$ are polynomial coefficients given as follows:

$$\tilde{d}'_0 = -u^6 + u^5 + u^3 - u^2, \tag{5a}$$
$$\tilde{d}'_1 = -u^5 + u^4 + u^2 - u, \tag{5b}$$
$$\tilde{d}'_2 = -u^4 + u^3 + u - 1, \tag{5c}$$
$$\tilde{d}'_3 = u^{11} - 2u^{10} + u^9 + u^6 - 2u^5 + u^4 - u^3 + u^2 + u + 2, \tag{5d}$$
$$\tilde{d}'_4 = u^{11} - u^{10} - u^9 + u^8 + u^6 - u^5 - u^4 + u^3 - u^2 + 2u + 2, \tag{5e}$$
$$\tilde{d}'_5 = u^{11} - u^{10} - u^8 + u^7 + 3, \tag{5f}$$
$$\tilde{d}'_6 = u^{10} - u^9 - u^7 + u^6, \tag{5g}$$
$$\tilde{d}'_7 = u^9 - u^8 - u^6 + u^5, \tag{5h}$$
$$\tilde{d}'_8 = u^8 - u^7 - u^5 + u^4 \tag{5i}$$
$$\tilde{d}'_9 = u^7 - u^6 - u^4 + u^3. \tag{5j}$$

These polynomials verify the following relations.

$$\tilde{d}'_2 = -(u-1)^2 \cdot (u^2+u+1), \quad \tilde{d}'_1 = u\tilde{d}'_2,$$
$$\tilde{d}'_0 = u\tilde{d}'_1, \quad \tilde{d}'_9 = -u\tilde{d}'_0,$$
$$\tilde{d}'_8 = u\tilde{d}'_9, \quad \tilde{d}'_7 = u\tilde{d}'_8,$$
$$\tilde{d}'_6 = u\tilde{d}'_7, \quad \tilde{d}'_5 = u\tilde{d}'_6 + 3,$$
$$\tilde{d}'_4 = v - (\tilde{d}'_1 + \tilde{d}'_7), \quad \tilde{d}'_3 = v - (\tilde{d}'_0 + \tilde{d}'_6 + \tilde{d}'_9),$$

where $v = \tilde{d}'_2 + \tilde{d}'_5 + \tilde{d}'_8$.

From the above, for an element $\tilde{f}$ after raising to the power of the easy part (p^5-1), the exponentiation by the hard part $\tilde{f} \mapsto \tilde{f}^{\tilde{d}'}$ is given by $\tilde{f}^{\tilde{d}'} = \mu_0 \cdot \mu_1^p \cdot \mu_2^{p^2} \cdot \mu_3^{p^3} \cdot \mu_4^{p^4} \cdot \mu_5^{p^5} \cdot \mu_6^{p^6} \cdot \mu_7^{p^7} \cdot \mu_8^{p^8} \cdot \mu_9^{p^9}$ where $\mu_i = \tilde{f}^{\tilde{d}'_i}$ for $0 \le i \le 9$ are computed by the following sequence of operations.

$$t_0 = (\tilde{f}^{u-1})^{u-1}, t_1 = t_0^u, t_2 = t_1^u, \mu_2 = (t_0 \cdot t_1 \cdot t_2)^{-1},$$
$$\mu_1 = \mu_2^u, \mu_0 = \mu_1^u, \mu_9 = (\mu_0^u)^{-1}, \mu_8 = \mu_9^u,$$
$$\mu_7 = \mu_8^u, \mu_6 = \mu_7^u, \mu_5 = \mu_6^u \cdot \tilde{f}^2 \cdot \tilde{f}, t_3 = \mu_2 \cdot \mu_5 \cdot \mu_8,$$
$$\mu_4 = t_3 \cdot (\mu_1 \cdot \mu_7)^{-1}, \mu_3 = t_3 \cdot (\mu_0 \cdot \mu_6 \cdot \mu_9)^{-1},$$

where t_i for $0 \le i \le 3$ are variables.

Applying the above method, the calculation cost of powering the easy part is one p^5-Frobenius endomorphism, one inversion, and one multiplication in $\mathbb{F}_{p^{15}}$. Besides, the calculation cost of powering the hard part is two exponentiations by $(u-1)$, nine exponentiations by u, twenty multiplications, one squaring, one p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, p^9-Frobenius endomorphisms, and four inversions in $\mathbb{F}_{p^{15}}$. Since $\tilde{f}$ is in the cyclotomic subgroup of order $\Phi_3(p^5) = p^{10} + p^5 + 1$, the inversion in the hard part is efficiently computed as shown in App. C. 1 in [9].

3.2 Proposed Method

Unlike Fouotsa et al.'s method [9], the authors decompose the exponent according to Eq. (1) as follows:

$$(p^{15}-1)/r = [(p^5-1) \cdot (p^2+p+1)] \cdot [\Phi_{15}(p)/r], \tag{6}$$

where the first and second parts are easy and hard parts of the final exponentiation, respectively. With the above decomposition, the authors propose to represent a multiple of $d = \Phi_{15}(p)/r$ as a polynomial in base p which are derived

by the following process.

Since p is parameterized by $p = m(u) \cdot r + u$, the hard part d is represented as a polynomial in base r such that $d = \Phi_{15}(m(u) \cdot r + u)/r$. Since the constant term of numerator of d in base r is $\Phi_{15}(u) = r$, the denominator of d is easily canceled. Then, the polynomial d in base r can be converted to a polynomial in base p by replacing r with $(p - u)/m(u)$ in a straightforward way. Note that in [13], Zhang et al. also expanded the polynomial of the hard part for the BLS curves with $k = 27$ by using the property of the characteristic of the form $p = m(u) \cdot r + u$ which leads to a recursion relation $p^{i+1} = m(u) \cdot r \cdot p^i + u \cdot p^i$ where i is a positive integer.

As a result, the authors found that $d = d_0 + d_1 p + \cdots + d_7 p^7$ where polynomial coefficients d_i for $0 \le i \le 7$ are given as follows:

$$d_0 = m(u) \cdot (u^7 - u^6 + u^4 - u^3 + u^2 - 1) + 1, \tag{7a}$$
$$d_1 = m(u) \cdot (u^6 - u^5 + u^3 - u^2 + u), \tag{7b}$$
$$d_2 = m(u) \cdot (u^5 - u^4 + u^2 - u + 1), \tag{7c}$$
$$d_3 = m(u) \cdot (u^4 - u^3 + u - 1), \tag{7d}$$
$$d_4 = m(u) \cdot (u^3 - u^2 + 1), \tag{7e}$$
$$d_5 = m(u) \cdot (u^2 - u), \tag{7f}$$
$$d_6 = m(u) \cdot (u - 1), \tag{7g}$$
$$d_7 = m(u), \tag{7h}$$

where $m(u) = (u - 1)^2/3 \cdot (u^2 + u + 1)$. Then, it is observed that the above polynomials already have the following simple relations before the LLL algorithm is applied.

$$d_7 = (u - 1)^2/3 \cdot (u^2 + u + 1), \quad d_6 = (u - 1) \cdot d_7,$$
$$d_5 = u d_6, \quad d_4 = u d_5 + d_7,$$
$$d_3 = u d_4 - d_7, \quad d_2 = u d_3 + d_7,$$
$$d_1 = u d_2, \quad d_0 = u d_1 - d_7 + 1,$$

which implies that the relations can provide one of the efficient computations for the final exponentiation. Indeed, since there exists a denominator 3 of d_7 which leads to a cube root computation, the authors propose to use a minimum multiple $d' = 3 \cdot d$ for a practical final exponentiation. Assuming $d' = d'_0 + d'_1 p + \cdots + d'_7 p^7$ where $d'_i = 3 \cdot d_i$ for $0 \le i \le 7$, the polynomials clearly verify the following simpler relations than that of the previous method [9].

$$d'_7 = (u - 1)^2 \cdot (u^2 + u + 1), \quad d'_6 = (u - 1) \cdot d'_7,$$
$$d'_5 = u d'_6, \quad d'_4 = u d'_5 + d'_7,$$
$$d'_3 = u d'_4 - d'_7, \quad d'_2 = u d'_3 + d'_7,$$
$$d'_1 = u d'_2, \quad d'_0 = u d'_1 - d'_7 + 3.$$

With the above, for an element f after raising to the power of the easy part given as $(p^5 - 1) \cdot (p^2 + p + 1)$, the exponentiation by the hard part $f \mapsto f^{d'}$ is computed as $f^{d'} = \nu_0 \cdot \nu_1^p \cdot \nu_2^{p^2} \cdot \nu_3^{p^3} \cdot \nu_4^{p^4} \cdot \nu_5^{p^5} \cdot \nu_6^{p^6} \cdot \nu_7^{p^7}$ where $\nu_i = f^{d'_i}$ for $0 \le i \le 7$ are computed by the following sequence of operations.

$$t_0 = (f^{u-1})^{u-1}, t_1 = t_0^u, t_2 = t_1^u, \nu_7 = t_0 \cdot t_1 \cdot t_2,$$
$$\nu_6 = \nu_7^{u-1}, \nu_5 = \nu_6^u, \nu_4 = \nu_5^u \cdot \nu_7, t_3 = \nu_7^{-1}, \nu_3 = \nu_4^u \cdot t_3$$
$$\nu_2 = \nu_3^u \cdot \nu_7, \nu_1 = \nu_2^u, \nu_0 = \nu_1^u \cdot t_3 \cdot f^2 \cdot f,$$

where t_i for $0 \le i \le 3$ are variables.

As a result, the calculation cost of powering the easy part is one p, p^2, p^5-Frobenius endomorphisms, one inversion, and three multiplications in $\mathbb{F}_{p^{15}}$. The calculation cost of powering the hard part is three exponentiations by $(u - 1)$, eight exponentiations by u, fifteen multiplications, one squaring, one p, p^2, p^3, p^4, p^5, p^6, p^7-Frobenius endomorphisms in $\mathbb{F}_{p^{15}}$, and one inversion in the cyclotomic subgroup of order $\Phi_3(p^5)$. Note that f is also an element in the cyclotomic subgroup of order $\Phi_3(p^5)$.

Comparing the previous and proposed methods, the proposed method results in reducing three multiplications, three inversions in the cyclotomic subgroup of order $\Phi_3(p^5)$, and one p^8, p^9-Frobenius endomorphisms, replacing one exponentiation by u with one exponentiation by $(u - 1)$, and increasing one p, p^2-Frobenius endomorphisms from the previous one. Thus, it is considered that the proposed method can achieve more efficient final exponentiation than the previous one.

Remark 1. One more important fact is that the derivation of the coefficients of the polynomial $\Phi_k(p)/r$ in base p by using the property that the parameterization of p can be available for the BLS curves with an arbitrary embedding degree k. Moreover, from the observation of Eqs. (7a) to (7h), there is a possibility that the coefficients are systematically obtained and those verify one of the simplest relations which leads to an efficient final exponentiation for arbitrary BLS curves.

4. Sample Operation Counts

In this section, the authors show the operation counts for the final exponentiation of the pairing at the 128-bit security level. In the following, let M_i, S_i, and I_i denote calculation costs of multiplication, squaring, inversion in a finite field of order p^i where i is a positive integer. Let I_c denote a calculation cost of an inversion in the cyclotomic subgroup of order $\Phi_3(p^5)$.

The authors use the parameter u which is proposed by Fouotsa et al. in [9] given as follows:

$$u = 2^{31} + 2^{19} + 2^5 + 2^2, \tag{8}$$

where u has a 32-bit length with a Hamming weight $\mathrm{HW}(u) = 4$. The parameter provides p and r with 383-bit and 249-bit length which is closed to the 256-bit as required to have 128-bit security on elliptic curves, respectively.

With the square-and-multiply algorithm, the exponentiation by u given in Eq. (8) in $\mathbb{F}_{p^{15}}$ which is appeared in the hard part is performed by $31S_{15} + 3M_{15}$. The exponentiation by $(u - 1)$ in $\mathbb{F}_{p^{15}}$ is also performed by $31S_{15} + 4M_{15} + I_c$. Thus, according to the calculation costs of the final exponentiation given in Sect. 3, the calculation cost of the proposed hard part is computed as $3 \cdot (31S_{15} + 4M_{15} + I_c) + 8 \cdot (31S_{15} +$

Table 1 The number of operations in $\mathbb{F}_{p^{15}}$ for computing single final exponentiation of the pairing at the 128-bit security level.

Method	M_{15}	S_{15}	I_{15}	I_c	Frob.								
					p	p^2	p^3	p^4	p^5	p^6	p^7	p^8	p^9
Fouotsa et al. [9]	56	342	1	6	1	1	1	1	2	1	1	1	1
This work	54	342	1	4	2	2	1	1	2	1	1	0	0

Table 2 The calculation cost of operations in $\mathbb{F}_{p^{15}}$.

Operations	Calculation Costs
Multiplication M_{15}	$45M_1$
Squaring S_{15}	$45S_1$
Inversion I_{15}	$126M_1 + 23S_1 + 1I_1$
Cyc. inversion I_c	$27M_1 + 27S_1$
Frobenius p^5;	$10M_1$
Frobenius p; p^2; p^3; p^4; p^6; p^7; p^8; p^9	$14M_1$

Table 3 The number of operations in $\mathbb{F}_p$ for computing single final exponentiation of the pairing at the 128-bit security level.

Method	M_1	S_1	I_1
Fouotsa et al. [9]	2,940	15,575	1
This work	2,796	15,521	1

$3M_{15}) + 15M_{15} + 1S_{15} + 1I_c = 51M_{15} + 342S_{15} + 4I_c$ with one p, p^2, p^3, p^4, p^5, p^6, p^7-Frobenius endomorphisms. Adding the cost of the easy part, i.e., $3M_{15} + 1I_{15}$ with one p, p^2, p^5-Frobenius endomorphisms, the proposed final exponentiation is performed by $54M_{15} + 342S_{15} + 1I_{15} + 4I_c$ with one p^3, p^4, p^6, p^7 and two p, p^2, p^5-Frobenius endomorphisms. In the same manner, the calculation cost of the previous one is obtained as shown in Sect. 8.1 in [9]. The details of the number of the operations in $\mathbb{F}_{p^{15}}$ for these final exponentiations are summarized in Table 1. According to [9], since the calculation costs of the operations in $\mathbb{F}_{p^{15}}$ can be written as Table 2, the number of operations in a prime field $\mathbb{F}_p$ for the final exponentiations are also determined as Table 3.

Comparing the operation counts of Table 1, the proposed method results in reducing $2M_{15} + 2I_c$ and one p^8, p^9-Frobenius endomorphisms from the previous final exponentiation. Although the proposal also results in increasing one p and p^2-Frobenius endomorphisms, the reduced calculation costs are still larger than the increased ones. Moreover, Table 3 also shows that the proposed method results in reducing $144M_1 + 54S_1$ from the previous ones. Thus, the authors conclude that the proposed method clearly more effective than the previous one.

5. Conclusion

In this paper, the authors present a new method of computing the final exponentiation for the pairing on the BLS family of pairing-friendly elliptic curves with $k = 15$ by using the property of the characteristic of the BLS family. The proposed method contributes more reduction of the calculation costs of the final exponentiation than the state-of-the-art one given by Fouotsa et al. As one of future works, the authors would like to confirm the possibility described in Remark 1 and try to improve the final exponentiation for arbitrary BLS curves.

Acknowledgments

This research was supported by JSPS KAKENHI Grant Numbers 19J2108612 and 19K11966.

References

[1] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol.17, no.4, pp.297–319, 2004.
[2] D. Boneh and X. Boyen, "Short signatures without random oracles," International Conference on the Theory and Applications of Cryptographic Techniques, pp.56–73, Springer, 2004.
[3] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," International conference on the theory and applications of cryptographic techniques, pp.506–522, Springer, 2004.
[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM conference on Computer and communications security, pp.89–98, ACM, 2006.
[5] T. Okamoto and K. Takashima, "Homomorphic encryption and signatures from vector decomposition," International Conference on Pairing-Based Cryptography, pp.57–74, Springer, 2008.
[6] P.S. Barreto, B. Lynn, and M. Scott, "Constructing elliptic curves with prescribed embedding degrees," International Conference on Security in Communication Networks, pp.257–267, Springer, 2002.
[7] P.S. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," International Workshop on Selected Areas in Cryptography, pp.319–331, Springer, 2005.
[8] E.J. Kachisa, E.F. Schaefer, and M. Scott, "Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field," International Conference on Pairing-Based Cryptography, pp.126–135, Springer, 2008.
[9] E. Fouotsa, N.E. Mrabet, and A. Pecha, "Optimal ate pairing on elliptic curves with embedding degree 9, 15 and 27," J. Groups, Complexity, Cryptology, vol.12, no.1, 2020. https://arxiv.org/abs/2002.11920
[10] R. Barbulescu, N. El Mrabet, and L. Ghammam, "A taxonomy of pairings, their security, their complexity," 2019. https://eprint.iacr.org/2019/485.pdf
[11] M. Scott, N. Benger, M. Charlemagne, L.J.D. Perez, and E.J. Kachisa, "On the final exponentiation for calculating pairings on ordinary elliptic curves," International Conference on Pairing-Based Cryptography, pp.78–88, Springer, 2009.
[12] L. Fuentes-Castaneda, E. Knapp, and F. Rodríguez-Henríquez, "Faster hashing to $\mathbb{G}_2$," International Workshop on Selected Areas in Cryptography, pp.412–430, Springer, 2011.
[13] X. Zhang and D. Lin, "Analysis of optimum pairing products at high security levels," International Conference on Cryptology in India, pp.412–430, Springer, 2012.
[14] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels," IMA International Conference on Cryptography and Coding, pp.13–36, Springer, 2005.
[15] H.W. Lenstra, A.K. Lenstra, L. Lovfiasz, et al., "Factoring polynomials with rational coeficients," 1982.
[16] P. Duan, S. Cui, and C.W. Chan, "Special polynomial families for generating more suitable elliptic curves for pairing-based cryptosystems," IACR Cryptology ePrint Archive, vol.2005, p.342, 2005.