Exponentiation Inversion Problem Reduced from Fixed Argument Pairing Inversion on Twistable Ate Pairing and Its Difficulty

Shoichi Akagi and Yasuyuki Nogami

Graduate School of Natural Science and Technology, Okayama University,
3–1–1, Tsushima–Naka, Okayama, Okayama 700-8530, Japan
yasuyuki.nogami@okayama-u.ac.jp

Abstract. As one of problems that guarantee the security of pairing–based cryptography, *pairing inversion* problem is studied. Some recent works have reduced *fixed argument pairing inversion* (FAPI) problem to exponentiation inversion (EI) problem. According to the results, FAPI problem is solved if EI problem of exponent $(q^k - 1)/\Phi_k(q)$ is solved, where q, k, and r are the characteristic, embedding degree, and order of pairing group, respectively. $\Phi_k(x)$ is the cyclotomic polynomial of order k. This paper shows an approach for reducing the exponent of EI problem to $q - 1$ especially on Ate pairing. For many embedding degrees, it is considerably reduced from the previous result $(q^k - 1)/\Phi_k(q)$. After that, the difficulty of the reduced EI problem is discussed based on the distribution of correct $(q - 1)$–th roots on a small example.

Keywords: pairing inversion problem, trace, Barreto–Naehrig curve.

1 Introduction

Fixed argument pairing inversion (FAPI) problem is one of important research targets for ensuring the security of pairing–based cryptography. According to some recent papers [4], [5], most of FAPI problems have been reduced to *exponentiation inversion* (EI) problems. In detail, let q, k, and r be the characteristic, embedding degree, and group order, respectively, the exponent of the reduced EI problem is $(q^k - 1)/\Phi_k(q)$, where $\Phi_k(x)$ is the cyclotomic polynomial of order k. Since recent efficient pairing calculations [1], [10] are based on Ate pairing[6], this paper deals with a class of FAPI problems on Ate pairing together with *twist* technique such as *sextic twist* that is available for the well known Barreto–Naehrig (BN) curve [2].

Pairing is a bilinear map that has two inputs P, Q (rational points) and one output z (a finite field element). As a typical setting in the context of Ate pairing of embedding degree k, the input rational points P and Q of order r are defined on an elliptic curve over prime field $\mathbb{F}_q$ and extension field $\mathbb{F}_{q^k}$, respectively. Throughout this paper, $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ denote a prime field of characteristic q and its m–th extension field, respectively. Then, the output z is calculated as a

M. Yoshida and K. Mouri (Eds.): IWSEC 2014, LNCS 8639, pp. 240–249, 2014.

non–zero element of order r in $\mathbb{F}_{q^k}$. As one of FAPI problems defined by these three values, this paper focuses on the following problem: Find *unknown* P from *given* Q and z. [1] This paper shows that the objective P is calculated if the *correct* $(q-1)$–th root of Tate pairing[7] is obtained[2]. The idea of the reduction from $(q^k-1)/\Phi_k(q)$ to $q-1$ is applicable for various pairing–friendly curves of even embedding degree such as BN curve. The reduced EI problem is still difficult even though the reduction is a significant achievement. Thus, this paper discusses the difficulty of the reduced EI problem based on the distribution of correct $(q-1)$–th roots on a small example.

2 Preliminaries

This section introduces some mathematical notations since this paper considers pairing inversion problems on Ate pairing with some curves. Especially, This paper focuses on some efficient pairing–friendly curves, such as Barreto–Naehrig (BN) curve[2], Brezing–Weng (BW) curve[3] and , Freeman curve[3], with *twist* technique[10] on Ate pairing.

2.1 Pairings

In what follows, let k, q, r and t be the embedding degree, characteristic, order of pairing group and trace of Frobenius[3], respectively. The following three pairings appear in this paper.

Ate Pairing and Ate$_i$ Pairing : Suppose the following three groups and Ate$_i$ pairing notation.

$$\begin{aligned} \mathbb{G}_1 &= E(\mathbb{F}_{q^k})[r] \cap \mathrm{Ker}(\phi - [1]), \\ \mathbb{G}_2 &= E(\mathbb{F}_{q^k})[r] \cap \mathrm{Ker}(\phi - [p]), \\ \mathbb{G}_T &= \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r, \end{aligned} \tag{1}$$

$$\alpha_i : \ \mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_T. \tag{2}$$

Ate$_1$ pairing is especially called **Ate pairing**. Then, let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, Ate pairing $\alpha(Q,P)$ and Ate$_i$ pairing $\alpha_i(Q,P)$ are given as follows, where $f_{s,Q}(P)$ is generally calculated by the Miller's algorithm with loop parameter s[9].

$$\alpha_i(Q,P) = f_{q^i \bmod r, Q}(P)^{\frac{q^k-1}{r}}. \tag{3}$$

$$\alpha(Q,P) = f_{t-1,Q}(P)^{\frac{q^k-1}{r}}. \tag{4}$$

[1] Let $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be groups of order r such that $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, and $z \in \mathbb{G}_T$, this type of FAPI is often called FAPI–2 [4].

[2] The result of Ate pairing is able to be translated to that of Tate pairing, therefore, this paper mainly uses Tate pairing notations.

Note that the bilinearity of Ate_i pairing holds after calculating the *final exponentiation* of $(q^k-1)/r$.

An important point is that $f_{q^i,Q}(P)$ whose loop parameter is just q^i without mod r holds the bilinearity without the final exponentiation[8].

Tate Pairing : Suppose three groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ defined as Eq. (1). Then, let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, Tate pairing $\tau(Q,P)$ is defined as follows.

$$\tau(Q,P) = f_{r,Q}(P)^{\frac{q^k-1}{r}}. \tag{5}$$

In the same of Ate_i pairing, the bilinearity holds after calculating the *final exponentiation*.

2.2 Divisor Theorem

In what follows, let $f_{a,Q}(P)$ be denoted as $f_{a,Q}$ in brief. Let $l_{P,Q}$ and v_T be the line and vertical line passing through rational points P, Q and T, respectively, then the following relations are given[5].

$$f_{-n,Q} = \frac{1}{f_{n,Q} \cdot v_{[n]Q}}. \tag{6a}$$

$$f_{a+b,Q} = f_{a,Q} \cdot f_{b,Q} \cdot \frac{l_{[a]Q,[b]Q}}{v_{[a+b]Q}}. \tag{6b}$$

$$f_{ab,Q} = f_{a,Q}^b \cdot f_{b,[a]Q} = f_{b,Q}^a \cdot f_{a,[b]Q}. \tag{6c}$$

According to the divisor theorem, it is shown that the three pairings are easily transformed to each other[5]. Thus, for simplicity, this paper in what follows mainly uses Tate pairing notations instead of Ate pairing.

3 Pairing Inversion Problem

In the case of Ate pairing, pairing inversion problems are roughly classified into the following three types:

FAPI–1 : Find $Q \in \mathbb{G}_2$ from given $P \in \mathbb{G}_1$ and $\alpha(Q,P) \in \mathbb{G}_T$.
FAPI–2 : Find $P \in \mathbb{G}_1$ from given $Q \in \mathbb{G}_2$ and $\alpha(Q,P) \in \mathbb{G}_T$.
GPI : Find $P' \in \mathbb{G}_1$ and $Q' \in \mathbb{G}_2$ satisfies $\alpha(Q',P') = \alpha(Q,P)$ from given $\alpha(Q,P) \in \mathbb{G}_T$.

The main target of this paper is FAPI-2 problem. The previous works [4], [5] have dealt with the general cases of FAPI problems and then shown that they are reduced to EI problem of exponent $(q^k-1)/\Phi_k(q)$. Then, another approach together with a smaller exponent, that is just $q-1$, is proposed in the case of BN curve. After that, it is shown that the approach is applicable for not only BN curve but also BW and Freeman curves. In detail, it is generalized for even embedding degrees through the case of Freeman curve.

3.1 Proposal

An Important Relation on Ate Pairing with BN Curve : In the case of BN curve of embedding degree 12, let $P(x_P, y_P) \in \mathbb{G}_1$ and $Q(x_Q, y_Q) \in \mathbb{G}_2$, it satisfies $[q^6+1]Q = \mathcal{O}$ since q^6+1 is divisible by the order r. Then, consider $f_{q^6+1,Q}(P)$ as follows.

$$f_{q^6+1,Q}(P) = f_{r\cdot\frac{q^6+1}{r},Q}(P) = f_{r,Q}^{\frac{q^6+1}{r}}(P) \cdot f_{\frac{q^6+1}{r},[r]Q}(P). \tag{7a}$$

On the other hand, the following relation is also obtained.

$$f_{q^6+1,Q}(P) = f_{q^6,Q}(P) \cdot f_{1,Q}(P) \cdot \frac{l_{[q^6]Q,Q}}{v_{[q^6+1]Q}} = f_{q^6,Q}(P) \cdot (x_P - x_Q). \tag{7b}$$

Thus, a relation shown below is obtained based on the above equations since $q^{12}-1 = (q^6-1)\cdot(q^6+1)$.

$$\frac{f_{r,Q}^{\frac{q^6+1}{r}}(P)}{f_{q^6,Q}(P)} = \frac{\sqrt[q^6-1]{\tau(Q,P)}}{f_{q^6,Q}(P)} = x_P - x_Q. \tag{8}$$

then the target of this problem is to obtain $X = x_P$ of P. As previously introduced, the denominator $f_{q^6,Q}(P)$ and $\tau(Q,P)$ are easily obtained as elements in $\mathbb{G}_T$ from $\alpha(Q,P)$. The above relation is furthermore improved by using higher degree traces and norm as follows.

Trace and Norm : First, powering both sides of Eq. (8) to $(q^6-1)/(q-1)$,

$$\frac{\sqrt[q-1]{\tau(Q,P)}}{f_{q^6,Q}(P)^{(q^6-1)/(q-1)}} = (X - x_Q)^{(q^6-1)/(q-1)}. \tag{9}$$

Let the left–hand side of the above equation be c that becomes a non–zero element in $\mathbb{F}_q$, then we have

$$(X - x_Q)^{(q^6-1)/(q-1)} - c = 0. \tag{10}$$

Since the objective X belongs to $\mathbb{F}_q$, the following relation holds.

$$\prod_{i=0}^{5}(X - x_Q^{q^i}) - c = 0. \tag{11}$$

In the case of BN curve, x_Q of $Q \in \mathbb{G}_2$ for Ate pairing belongs to the proper subfield $\mathbb{F}_{q^6}$ [10] as previously introduced. Thus, the trace and norm of x_Q leads to a simple relation as follows.

Let $\mathrm{M}_{x_Q}(X) = \prod_{i=0}^{5}(X - x_Q^{q^i})$ be the minimal polynomial of x_Q that is an irreducible polynomial of degree 6 over $\mathbb{F}_q$, it satisfies that

$$\mathrm{M}_{x_Q}(X) - c = X^6 - 3^{-1}\mathrm{Tr}\left(x_Q^3\right)X^3 + \mathrm{N}(x_Q) - c = 0. \tag{12}$$

$\mathrm{Tr}(\cdot)$ and $\mathrm{N}(\cdot)$ are trace and norm functions with respect to the prime field $\mathbb{F}_q$. Since x_Q is known as an input of this problem, these values are easily calculated. As shown in **App**. A, the feature of BN curve shows that the coefficients of $x^5,\ x^4,\ x^2,\ x$ of $\mathrm{M}_{x_Q}(X)$ always become 0. Therefore, calculating d and e in $\mathbb{F}_q$ such that

$$\mathrm{M}_{x_Q}(X) - c = (X^3 - d)(X^3 - e) = 0 \tag{13}$$

is not difficult. Thus, this FAPI problem is reduced to a smaller EI problem of exponent $q-1$ as shown in Eq. (9). In addition, the meaning of this problem is partially replaced to whether d or e becomes a cubic residue in $\mathbb{F}_q$. In detail, d or e needs to be a cubic residue in $\mathbb{F}_q$ such that its solution $X = x_P$ belongs to $\mathbb{F}_q$ as x–coordinate of $P \in \mathbb{G}_1$.

According to Eq. (9), if the correct $(q-1)$–th root of Tate pairing $\tau(Q,P)$ that could be inversely formulated as $\sqrt[q-1]{\tau(Q,P)} = f_{r,Q}(P)^{(q^{12}-1)/r(q-1)}$ is obtained, $X = x_P$ is obtained. Thus, it has been shown that this approach reduces EI problem on Ate pairing with BN curve to the exponent $q-1$.

3.2 EI Problem on Ate Pairing with BW Curve

In the case of BW curve of embedding degree 8, the following relation corresponding to Eq. (8) of BN curve is first obtained.

$$\frac{f_{r,Q}^{\frac{q^4+1}{r}}(P)}{f_{q^4,Q}(P)} = x_P - x_Q. \tag{14}$$

Then, powering both sides of Eq. (14) to $(q^4-1)/(q-1)$, the following relation corresponding to Eq. (9) is obtained.

$$\frac{\sqrt[q-1]{\tau(Q,P)}}{f_{q^4,Q}(P)^{(q^4-1)/(q-1)}} = (X - x_Q)^{(q^4-1)/(q-1)} = (X - x_Q)^{q^3+q^2+q+1}, \tag{15}$$

where $X = x_P$ as the target of this problem. Let the left–hand side of the above equation be $c \in \mathbb{F}_q$, as shown in **App**. A,

$$\mathrm{M}_{x_Q}(X) - c = x^4 + 2^{-1}\mathrm{Tr}\left(x_Q^2\right)x^2 + \mathrm{N}(x_Q) - c = (X^2 - d)(X^2 - e) = 0, \tag{16}$$

where $\mathrm{M}_{x_Q}(X)$ is the minimal polynomial of $x_Q \in \mathbb{F}_{q^4}$, that is an irreducible polynomial of degree 4 over $\mathbb{F}_q$. The above d and e are easily obtained as elements in $\mathbb{F}_q$ and one of them at least needs to be a quadratic residue in $\mathbb{F}_q$ since $\mathrm{M}_{x_Q}(X) - c = 0$ has a solution $X = x_P$ in $\mathbb{F}_q$.

Thus, it has been shown that this approach also reduces EI problem on Ate pairing with BW curve to the exponent $q-1$.

3.3 EI Problem on Ate Pairing with Freeman Curve

This section deals with Freeman curve for instance. Then, the discussion supports Ate pairing using pairing–friendly curves of even embedding degree.

In the case of Freeman curve of embedding degree 10, the following relation corresponding to Eq. (8) of BN curve is first obtained.

$$\frac{f_{\frac{q^5+1}{r},Q}(P)}{f_{q^5,Q}(P)} = x_P - x_Q. \tag{17}$$

Then, powering both sides of Eq. (17) to $(q^5-1)/(q-1)$, the following relation corresponding to Eq. (9) is obtained.

$$\frac{\sqrt[q-1]{\tau(Q,P)}}{f_{q^5,Q}(P)^{(q^5-1)/(q-1)}} = (X - x_Q)^{(q^5-1)/(q-1)} = (X - x_Q)^{q^4+q^3+q^2+q+1}, \tag{18}$$

where $X = x_P$ as the target of this problem. Let the left–hand side of the above equation be $c \in \mathbb{F}_q$ and let $\mathrm{M}_{x_Q}(X)$ be the minimal polynomial of $x_Q \in \mathbb{F}_{q^5}$, that is an irreducible polynomial of degree 5 over $\mathbb{F}_q$,

$$\mathrm{M}_{x_Q}(X) - c = 0. \tag{19}$$

Though the form of $\mathrm{M}_{x_Q}(X)$ for Freeman curve is not as simple as those for BN and BW curves, it is easily calculated. Then, $\mathrm{M}_{x_Q}(X) - c$ becomes reducible over $\mathbb{F}_q$ such that it has a solution $X = x_P$ in $\mathbb{F}_q$.

Thus, it has been also shown that this approach reduces EI problem on Ate pairing with Freeman curve, furthermore pairing–friendly curves of even embedding degree, to the exponent $q - 1$.

3.4 Difficulty of the Reduced EI Problem of FAPI-2

This section observes the difficulty of the reduced EI problem of FAPI–2 on BN curve with Eq. (9). Let the correct $(q-1)$–th root of Tate pairing $\tau(Q,P)$ be C and let $\hat{C}$ be a $(q-1)$–th root of $\tau(Q,P)$ such that $\hat{C} \in \mathbb{G}_3$[3]. $\hat{C}$ is easily and uniquely obtained in $\mathbb{G}_3$ since $q-1$ and r are coprime. It is found that $C/\hat{C}$ becomes a non–zero element in $\mathbb{F}_q^*$. Thus, in other words, the EI problem is solved if $C/\hat{C} \in \mathbb{F}_q^*$ is obtained.

As a small example, let the characteristic q and the order r of BN curve be 2143 and 2089, respectively, the distribution of $C/\hat{C}$ for all rational point pairs of pairing becomes as the histogram of **Fig**. 1. According to this figure, it seems that $C/\hat{C}$'s are uniformly distributed to show the difficulty of EI problem[4].

4 FAPI–1 Problem

The previous section has dealt with the case of FAPI–2 problem on Ate pairing. The approaches are also applicable to FAPI–1 problem and it reduces EI problem

[3] It is one of $(q-1)$–th roots of $\tau(Q,P)$ and explicitly determined in $\mathbb{G}_3$.

[4] Since sextic twist is available on BN curve, each number of occurrences in the histogram becomes 6 or some multiples of 6. In other words, certain six rational points associated with sextic twist have the same value of $C/\hat{C}$.

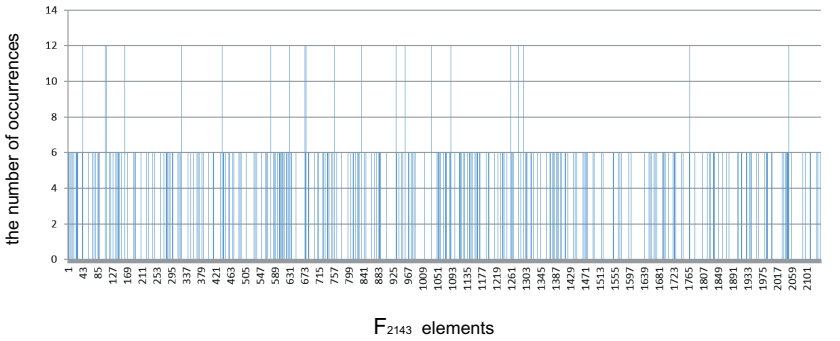

Fig. 1. Histogram of $C/\hat{C}$'s on BN curve with $q = 2143$

to exponent $q^{k/2} - 1$ at least when the embedding degree is even. In addition, when a pairing-friendly curve has another twist such as sextic twist, the exponent can be more reduced.

4.1 FAPI–1 : EI Problem on Ate Pairing with BN Curve

In the case of FAPI–1, this paper takes the same approach of the previous section. Noting that the objective of this problem is Q, $X = x_Q$ in this section. After Eq. (8), a similar approach to the previous section is usable.

Trace and Norm : In the case of FAPI–1, Eq. (10) is rewritten as follows.

$$(x_P - X)^{(q^6-1)/(q-1)} - c = 0. \tag{20}$$

Since the objective X belongs to $\mathbb{F}_{q^2}$, the following relation holds.

$$\prod_{i=0}^{5}(x_P - X^{q^i}) - c = \prod_{i=0}^{5}(X^{q^i} - x_P) - c = 0. \tag{21}$$

$Q(X, Y)$ have a corresponding rational point $Q'(X', Y')$ on $E'(\mathbb{F}_{q^2})[r][10]$. Let $v \in \mathbb{F}_{q^2}$ be a cubic non residue, X is written as

$$X = v^{1/3}X'. \tag{22}$$

As shown in **App**. A, noting that $X' \in \mathbb{F}_{q^2}$, the following equation is obtained from Eq. (21).

$$X'^3 X'^{3q} + {x_P}^3(X'^3 v + X'^{3q} v^q) + {x_P}^6 - c = 0. \tag{23}$$

As shown above, this equation causes another difficult problem to solve. Therefore, a slightly different approach is needed as follows.

Trace and Norm for FAPI–1 Problem : First, powering both sides of Eq. (8) to $(q^6-1)/(q^2-1)$ not $(q^6-1)/(q-1)$,

$$\frac{\sqrt[q^2-1]{\tau(Q,P)}}{f_{q^6,Q}(P)^{(q^6-1)/(q^2-1)}} = (x_P - X)^{(q^6-1)/(q^2-1)} = -\prod_{i=0}^{2}(X^{q^{2i}} - x_P). \tag{24}$$

Let c be the left–hand side of the above equation, as shown in **App**. A, the above equation is transformed as

$$X'^3 - v^{-1}(x_P^3 - c) = 0. \tag{25}$$

This equation has at least one solution ($X = x'_Q$). According to Eq. (24), if the correct (q^2-1)–th root of Tate pairing $\tau(Q,P)$ is obtained, X is obtained. Thus it has been shown that this approach for FAPI–1 problem reduces it to EI problem of the exponent q^2-1.

4.2 FAPI–1 : EI Problem on Ate Pairing with BW Curve

In the case of BW curve, powering both sides of Eq. (14) to $(q^4-1)/(q^2-1)$, the following relation corresponding to Eq. (24) is obtained.

$$\frac{\sqrt[q^2-1]{\tau(Q,P)}}{f_{q^4,Q}(P)^{(q^4-1)/(q^2-1)}} = (x_P - X)^{(q^4-1)/(q^2-1)} = (X - x_P)^{q^2+1}, \tag{26}$$

X is written as $v^{1/2}X'$ such that $X' \in \mathbb{F}_{q^2}$ since BW curve has twist curve[10]. Then let c be the left–hand side of the above equation, in the same of **App**. A, the above equation is transformed as

$$(X - x_P)^{q^2+1} - c = \prod_{i=0}^{1}((v^{1/2}X')^{q^{2i}} - x_P) - c = vX'^2 - (x_P^2 + c) = 0,$$

$$X'^2 - v^{-1}(x_P^2 + c) = 0. \tag{27}$$

Thus, it has been shown that this approach for FAPI–1 problem can reduce EI problem to the exponent q^2-1.

4.3 FAPI–1 : EI Problem on Ate Pairing with Freeman Curve

In the case of Freeman curve, there is no need to change Eq. (17) and the following relation corresponding to Eq. (24) is obtained.

$$\frac{f_{r,Q}^{\frac{q^5+1}{r}}(P)}{f_{q^5,Q}(P)} = x_P - X. \tag{28}$$

Let c be the left–hand side of the above equation, the above equation is transformed as

$$X + c - x_P = 0. \tag{29}$$

This approach can reduce EI problem to the exponent q^5-1. Thus it has been shown that EI problem is reduced to the exponent $q^{k/2}-1$ in the same way when the embedding degree k is even.

5 Conclusion and Future Works

As shown in this paper, one of FAPI problems on Ate pairing with BN curves, for example, has been reduced to EI problem of exponent $q-1$. It is considerably reduced from $(q^k-1)/\Phi_k(q)$ of the previous works. This approach is applicable for pairing–friendly curves of even embedding degree such as Freeman curve. As one of future works, it will be extended for odd embedding degrees.

Then, the reduced EI problem that is to solve the correct $(q-1)$–th root of Tate pairing, denoted by $\sqrt[q-1]{\tau(Q,P)}$ in this paper, will be still difficult. The difficulty has been discussed with a small example in this paper. Thus, as another future work, the size of EI problem needs to be furthermore reduced from $q-1$ though it may need some auxiliary input.

The approach shown in this paper will be appropriately modified for the other FAPI problems and not restricted to Ate pairing.

References

1. Aranha, D.F., Karabina, K., Longa, P., Gebotys, C.H., Lopez, J.: Faster Explicit Formulas for Computing Pairings over Ordinary Curves, Cryptology ePrint Archive, Report 2010/526 (2010)
2. Barreto, P.S.L.M., Naehrig, M.: Pairing-Friendly Elliptic Curves of Prime Order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006)
3. Freeman, D., Scott, M., Teske, E.: A Taxonomy of Pairing–Friendly Elliptic Curves, IACR ePrint archive, `http://eprint.iacr.org/2006/372.pdf`
4. Galbraith, S.D., Hess, F., Vercauteren, F.: Aspects of pairing inversion. IEEE Transactions on Information Theory 54(12), 5719–5728 (2008)
5. Kanayama, N., Okamoto, E.: Approach to Pairing Inversions Without Solving Miller Inversion. IEEE Transactions on Information Theory 58(2), 1248–1253 (2012)
6. Hess, F., Smart, N., Vercauteren, F.: The Eta Pairing Revisited. IEEE Trans. Information Theory, 4595–4602 (2006)
7. Galbraith, S.D., Harrison, K., Soldera, D.: Implemeting the Tate pairing. In: Fieker, C., Kohel, D.R. (eds.) ANTS 2002. LNCS, vol. 2369, pp. 324–337. Springer, Heidelberg (2002)
8. Matsuda, S., Kanayama, N., Hess, F., Okamoto, E.: Optimized versions of the Ate and Twisted Ate Pairings, Cryptology ePrint Archive, Report 2007/013 (2007), `http://eprint.iacr.org/2007/013.pdf`
9. Miller, V.S.: The Weil Pairing, and its Efficient Calculation. Journal of Cryptology 17, 235–261 (2004)
10. Nogami, Y., Akane, M., Sakemi, Y., Kato, H., Morikawa, Y.: Integer Variable χ–Based Ate Pairing. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 178–191. Springer, Heidelberg (2008)

A Minimal Polynomial $\mathrm{M}_{x_Q}(X)$ of x_Q over $\mathbb{F}_q$

Case of BN Curve

The minimal polynomial $\mathrm{M}_{x_Q}(X)$ of x_Q over $\mathbb{F}_q$ is given by

$$\mathrm{M}_{x_Q}(X) = \prod_{i=0}^{5}(X - x_Q^{q^i}). \tag{30}$$

When using a certain pair of $x'_Q \in \mathbb{F}_{q^2}$ and a cubic non residue $v \in \mathbb{F}_{q^2}$, x_Q is written as

$$x_Q = v^{1/3} x'_Q, \tag{31}$$

where $v^{1/3}$ belongs to $\mathbb{F}_{q^6}$ and thus x_Q also belongs to $\mathbb{F}_{q^6}$[10]. Note here that

$$v^{q^2/3} = v^{(q^2-1)/3} \cdot v^{1/3} = \epsilon v^{1/3}, \quad v^{q^4/3} = v^{(q^2-1)(q^2+1)/3} \cdot v^{1/3} = \epsilon^2 v^{1/3}, \tag{32}$$

where ϵ is a primitive third root[5] of unity in $\mathbb{F}_q$. Thus, it satisfies that $\epsilon^3 = 1$ and $1 + \epsilon + \epsilon^2 = 0$. Then, Eq. (30) is modified as

$$\begin{aligned} \mathrm{M}_{x_Q}(X) &= \prod_{i=0}^{5} (X - x_Q^{q^i}) = \prod_{i=0}^{2} (X - \epsilon^i \cdot v^{1/3} \cdot x'_Q) \prod_{i=0}^{2} (X - \epsilon^i \cdot v^{q/3} \cdot x'^q_Q), \\ &= (X^3 - v x'^3_Q)(X^3 - v^q x'^{3q}_Q) = X^6 - (v x'^3_Q + v^q x'^{3q}_Q) X^3 + (v x'^3_Q)^{1+q}. \end{aligned} \tag{33}$$

For the above equation,

$$\begin{aligned} \mathrm{Tr}\left(x_Q^3\right) &= \sum_{i=0}^{5} x_Q^{3q^i} = \sum_{i=0}^{5} (v^{1/3} x'_Q)^{3q^i}, \\ &= \sum_{i=0}^{2} (v x'^3_Q + v^q x'^{3q}_Q) = 3(v x'^3_Q + v^q x'^{3q}_Q), \end{aligned} \tag{34a}$$

$$\mathrm{N}(x_Q) = \prod_{i=0}^{5} x_Q^{q^i} = \prod_{i=0}^{2} (\epsilon^i \cdot v^{1/3} x'_Q)(\epsilon^i \cdot v^{q/3} x'^q_Q) = (v x'^3_Q)^{1+q}. \tag{34b}$$

Thus, ϵ is simply canceled and then Eq. (12) is obtained.

In the same way of the above, the equation

$$\prod_{i=0}^{2} (x_Q^{q^{2i}} - x_P) + c = 0, \tag{35}$$

is transformed as follows,

$$\begin{aligned} &\prod_{i=0}^{2} (x_Q^{q^{2i}} - x_P) + c = \prod_{i=0}^{2} (\epsilon^i \cdot v^{1/3} x'_Q - x_P) = v x'^3_Q - x_P^3 + c = 0, \\ &x'^3_Q - v^{-1}(x_P^3 - c) = 0. \end{aligned} \tag{36}$$

Let $X = x'_Q$, Eq. (25) is obtained.

[5] Since $q - 1$ is divisible by 3, it belongs to $\mathbb{F}_q$.