SN Computer Science (2020) 1:51
https://doi.org/10.1007/s42979-019-0053-5

ORIGINAL RESEARCH

Fast Hashing to $\mathbb{G}_2$ on Aurifeuillean Pairing-Friendly Elliptic Curves

Emmanuel Fouotsa[1] · **Laurian Azebaze Guimagang**[2]

Received: 1 August 2019 / Accepted: 3 December 2019 / Published online: 17 December 2019

Abstract
In pairing-based cryptography, the computation of asymmetric pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ requires input points of prime order r. The process of getting those r-torsion point is known as hashing into $\mathbb{G}_1$ or $\mathbb{G}_2$ and is in general costly. Few recent works have considered the Scott et al.'s method and Fuentes et al.'s method for hashing on specific families of pairing-friendly curves. In this work, we apply those two methods on the recently discovered Scott–Guillevic Aurifeuillean curves with embedding degree $k = 6, 9, 15, 18, 27$ and 54. The results obtained show that the Fuentes et al.'s method is at least twice faster than the Scott et al.'s method in terms of group operations. In addition, the computational cost of hashing into $\mathbb{G}_2$ studied in this work is higher compared to the previous work done with BN curves, KSS curves and BLS curves at comparable embedding degrees.

Keywords Hashing · Aurifeuillean curves · Pairing-based cryptography

Introduction

A cryptographic pairing is a non-degenerate bilinear map from certain pairs of points of elliptic curves to a multiplicative subgroup of appropriate order of finite fields. Whereas some research papers such as Boneh and Franklin's identity-based encryption scheme [1], Lynn and Shacham's short signature scheme [2] used pairings in a constructive manner to implement novel protocols, and Joux's one round tripartite key exchange [3] used pairing to improve existing protocol which was in two rounds. There are several types of pairings such as the Weil pairing [4, 5], the Tate pairing [6], and its variants: the ate pairing [7], the R-ate pairing [8].

The original algorithm for computing pairings is due to Miller and is named the Miller algorithm. What the algorithm does is the efficient evaluation of a rational function associated with an r-torsion point of the elliptic curve.

✉ Emmanuel Fouotsa
emmanuelfouotsa@yahoo.fr

Laurian Azebaze Guimagang
azebazelaurian@yahoo.fr

[1] Department of Mathematics, Higher Teacher Training College, The University of Bamenda, Bamenda, Cameroon

[2] Department of Mathematics, Faculty of Science, University of Yaounde 1, Yaounde, Cameroon

Let $E(F_p)$ denote the set of rational points of an elliptic curve E over a finite field F_p. Let r be the large prime divisor of $\#E(\mathbb{F}_p)$ and c the integer, such that $\#E(\mathbb{F}_p) = c \cdot r$. For the Tate pairing for example, the group $\mathbb{G}_1$ is the subgroup $E(\mathbb{F}_p)[r]$ of r-torsion points in $E(\mathbb{F}_p)$, so that a point in $\mathbb{G}_1$ can be obtained by the scalar multiplication by c. The group $\mathbb{G}_2$ appears as the r-torsion subgroup of $\tilde{E}(\mathbb{F}_{p^{k/d}})$, where $\tilde{E}$ is the degree-d twist of the elliptic curve E. Hashing can be done exactly as in the case of $\mathbb{G}_1$, but the cofactor c in this case is quite large making the scalar multiplication costly, and it is thus a major concern to make it as fast as possible.

Two methods are used for efficient hashing into $\mathbb{G}_2$: the Scott et al.'s method [9] and Fuentes et al.'s method [10]. Those methods have been applied to BN curves and BLS curves [11] and other curves [9]. This work continues the same line of research in which we consider hashing into $\mathbb{G}_2$ on the newly constructed pairing-friendly curves introduced by Scott and Guillevic [12]. For the case study with both methods, our results show that the Fuentes et al.'s method is at least twice faster than the Scott et al.'s method in terms of group operations. In addition, the computational cost of Hashing into $\mathbb{G}_2$ studied in this work is higher compared to the previous work done with BN curves, KSS curves, and BLS curves at comparable embedding degrees.

The rest of this paper is organised as follows: in the next section, we bring out some preliminary on elliptic curves and pairings useful for the understanding of this work. The

following section describes and applies hashing into $\mathbb{G}_2$ with Scott et al. method to Aurifeuillean curves with embedding degree $k \in \{6, 9, 15, 18, 27, 54\}$, as well as hashing into $\mathbb{G}_2$ with Fuentes et al.'s method to the same elliptic curves, but not for $k = 15$, since a certain condition was not satisfy. We also bring up a comparison between computational cost of hashing with Aurifeuillean curves and other pairing-friendly elliptic curves in this section. The last section concludes the work.

Preliminary on Elliptic Curves and Pairings

This section recalls some preliminaries on elliptic curves useful to understand the remainder of this work. We refer the reader to the book [4] for more details.

Elliptic Curves

Let $\mathbb{F}_p$ denote the finite field with p elements. $\overline{\mathbb{F}}_p$ denotes its algebraic closure, $\overline{\mathbb{F}}_p = \cup_{m\geq 1}\mathbb{F}_{p^m}$. When the characteristic of $\mathbb{F}_p$ is different from 2 and 3 the Weierstrass elliptic curve is the set of points in $(x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ satisfying the equation:

$$E : y^2 = x^3 + ax + b, \tag{1}$$

where $a, b \in \overline{\mathbb{F}}_p$ together with an extra point at infinity $\mathcal{O}$. If $a, b \in \mathbb{F}_p$, then E is said to be defined over $\mathbb{F}_p$ and we denote this by $E/\mathbb{F}_p$. If E is defined over $\mathbb{F}_p$, then the set of $\mathbb{F}_p$-rational points of E, denoted $E(\mathbb{F}_p)$ is the set of points with coordinates in $\mathbb{F}_p$.

Group Law

Let E be the elliptic curve given by the Weierstrass Eq. (1). The addition rule is given below. For any point P_1 and P_2 of the curve where $P_i(x_i, y_i)$ for $i = 1, 2$.

(i) $P_1 + \mathcal{O} = \mathcal{O} + P_1 = P_1$.
(ii) $-\mathcal{O} = \mathcal{O}$,
(iii) Let $P_1(x_1, y_1) \neq \mathcal{O}$, $-P_1$ has as coordinates $-P_1(x_1, -y_1)$ and $P_1 + (-P_1) = \mathcal{O}$.
(iv) $P_1 + P_2$ is of coordinates (x_3, y_3) with

$$x_3 = \lambda^2 - x_1 - x_2 \quad y_3 = \lambda(x_1 - x_3) - y_1$$

where

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2}, & si \quad P_1 \neq \pm P_2 \\ \dfrac{3x_1^2 + a}{2y_1} & si \quad P_1 = P_2. \end{cases}$$

Theorem 1 *The set $(E(\mathbb{F}_p), +)$ consisting of the elliptic curve given by the Weierstrass Eq. (1) together with addition defined above is an abelian group with identity element $\mathcal{O}$.*

The Frobenius endomorphism on the elliptic curve is defined by $\pi : E(\overline{\mathbb{F}}_p) \longrightarrow E(\overline{\mathbb{F}}_p) : (x, y) \longmapsto (x^p, y^p)$ and $\mathcal{O} \longmapsto \mathcal{O}$. The following theorem gives a bound of the number of points of an elliptic curve.

Theorem 2 (Hasse) *Let E the elliptic curve on finite field $\mathbb{F}_q$, with $q = p^n$ then*

$$\#E(\mathbb{F}_q) = q + 1 - t \quad with \quad |t| \leq 2\sqrt{q}.$$

Theorem 3 *Let E the elliptic curve on finite field $\mathbb{F}_q$, then*

$$\pi^2 - t\pi + q = \mathcal{O},$$

where t is the unique integer equal to $q + 1 - \#E(\mathbb{F}_q)$, called the trace of the Frobenius map on the elliptic curve.

There are two categories of elliptic curves: supersingular elliptic curves and ordinary elliptic curves. If $t = 0$ or $\#E(\mathbb{F}_q) \equiv 1 \mod p$, the curve is said to be supersingular otherwise it is an ordinary curve.

Definition 1 Let E and $\tilde{E}$ be two elliptic curves defined over the finite field $\mathbb{F}_q$. then, $\tilde{E}$ is called the twist of degree d of E if there exists an isomorphism ψ_d from $\tilde{E}$ to E over $\mathbb{F}_{q^d}$ such that d is minimal.

r-Torsion Points

Definition 2 For $P \in E(\overline{\mathbb{F}}_p)$, P is a r-torsion point if $[r]P = \mathcal{O}$.

The set of r-torsion points of $E(\overline{\mathbb{F}}_p)$ is denoted

$$E[r] = \left\{ P \in E(\overline{\mathbb{F}}_p) : [r]P = \mathcal{O} \right\}.$$

Definition 3 Let r be a large prime number dividing $\#E(\mathbb{F}_q)$, the embedding degree of the elliptic curve E relatively to r is the least integer k, such that $r/q^k - 1$.

Remark 1 The embedding degree k is the minimal degree of extension field $\mathbb{F}_q$ such that $E[r] \subset E(\mathbb{F}_{q^k})$.

Pairings

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ be three groups of order r, a pairing is non-degenerate bilinear map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_3.$$

Consequence

$$\forall j \in \mathbb{N}, \quad e([j]P;Q) = e(P;Q)^j = e(P;[j]Q).$$

On an elliptic curve E over $\mathbb{F}_q$, the following groups are defined:

- $\mathbb{G}_1$ is the group $E(\mathbb{F}_p)[r]$ of r-torsion points in $E(\mathbb{F}_p)$,
- $\mathbb{G}_2$ is a group $\tilde{E}(\mathbb{F}_{p^{k/d}})$ of r-torsion points, where $\tilde{E}$ is the degree d twist of E over a lower degree extension $\mathbb{F}_{p^{k/d}}$.
- $\mathbb{G}_3$ the group of rth roots of unity in $\mathbb{F}_{q^k}$.

The Tate pairing is the map

$$\begin{aligned} e_T : \mathbb{G}_1 \times \mathbb{G}_2 &\longrightarrow \mathbb{G}_3 \\ (P, Q) &\longmapsto (f_{r;P}(Q))^{\frac{p^k-1}{r}} \end{aligned}$$

where $f_{r;P}$ is the Miller function, the rational function $f_{r;P}$ verifying $div(f_{r;R}) = s(R) - ([s]R) - (s-1)\mathcal{O}$.

Order of Elliptic Curves and Its Twist

Consider an elliptic curve E defined over $\mathbb{F}_p$. The number of points of E is defined as $\#E(\mathbb{F}_p) = p + 1 - t$, where t is the trace of the p-power Frobenius of E, which obeys the Hasse bound $t \leqslant 2\sqrt{p}$. The trace t_m of the p^m-power Frobenius on E for an arbitrary m can be determined using the recursion:

$$\begin{aligned} t_0 &= 2 \\ t_1 &= t \\ t_{i+1} &= t \cdot t_i - p \cdot t_{i-1} \end{aligned}$$

for all $i \geqslant 1$.

Therefore, the number of points of an elliptic curve E over $\mathbb{F}_{p^m}$ is defined as

$$\begin{aligned} \#E(\mathbb{F}_{p^2}) &= p^2 + 1 - (t^2 - 2p), \quad \text{for} \quad m = 2, \\ \#E(\mathbb{F}_{p^3}) &= p^3 + 1 - (t^3 - 3tp), \quad \text{for} \quad m = 3, \\ \#E(\mathbb{F}_{p^m}) &= p^m + 1 - t_m, \quad \text{for} \quad m \geqslant 2. \end{aligned}$$

If E admits a twist $\tilde{E}$ of degree d dividing k and $q = p^{k/d}$, then for $d = 2$,

$$\#\tilde{E}(\mathbb{F}_q) = q + 1 + t.$$

For $d = 3$

$$\begin{aligned} \#\tilde{E}(\mathbb{F}_q) &= q + 1 - (3f - t)/2, \quad \text{or} \\ \#\tilde{E}(\mathbb{F}_q) &= q + 1 - (-3f - t)/2, \end{aligned}$$

with $t^2 - 4q = -3f^2$.

For $d = 4$

$$\begin{aligned} \#\tilde{E}(\mathbb{F}_q) &= q + 1 + f, \quad \text{or} \\ \#\tilde{E}(\mathbb{F}_q) &= q + 1 - f, \end{aligned}$$

with $t^2 - 4q = -f^2$.

For $d = 6$

$$\begin{aligned} \#\tilde{E}(\mathbb{F}_q) &= q + 1 - (-3f + t)/2, \quad \text{or} \\ \#\tilde{E}(\mathbb{F}_q) &= q + 1 - (3f + t)/2, \end{aligned}$$

with $t^2 - 4q = -3f^2$ (see [9] for more explanation).

Addition Chain

Definition 4 (*Basic definition*) An addition chain for positive integer n is a sequence of positive integers $\{e_0, e_1, e_2, \ldots, e_s\}$, such that

(i) $e_0 = 1, e_1 = 2$ and $e_s = n$
(ii) for each i, $1 < i < s$, there exist $k, j < i$ such that $e_i = e_j + e_k$

A generalisation of the following definition take into consideration several integers.

Definition 5 (*Generalisation*) A generalisation of an addition chain of length l for a set of positive integers $\{n_1, n_2, \ldots, n_s\}$ is a sequence of positive integers $\{e_0, e_1, e_2, \ldots, e_l\}$ which include $\{n_1, n_2, \ldots, n_s\}$, such that

(i) $e_0 = 1, e_1 = 2$ and $e_s = n_s$
(ii) for each i, $1 < i < l$, there exist $k, j < i$ such that $e_i = e_j + e_k$

Such a chain defines a correct sequence of additions/substraction and doublings required for performing a scalar multiplication operation, $[c]P$; with P an element of an arbitrary Abelian group.

By means of Olivos theorem [13], group operations with the addition chain of length l can be accomplished with $l + s - 1$ operations in the group including squaring and addition of element of the group. However, it has been shown that finding a minimal length addition sequence is an NP-hard problem.

Hashing into $\mathbb{G}_2$

Real protocols such as Franklin's identity-based encryption scheme require hashing of identities to $\mathbb{G}_1$ or $\mathbb{G}_2$. The general approach to construct secure hash functions for hashing an identity to the group G of order r on an elliptic curve $E(\mathbb{F}_p)$ consists to: first step to transform an arbitrary binary message (the identity) to an element x of $\mathbb{F}_p$. Second step

solves the quadratic curve equation on $\mathbb{F}_p$ to find a y coordinate (change x if y does not exist) and finally carry the point P of coordinate (x, y) to some elliptic curve subgroup $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$ or $\mathbb{G}_2 = \tilde{E}(\mathbb{F}_{p^{k/d}})[r]$ by multiplying the point P by cofactor c, where $\#\tilde{E}(\mathbb{F}_p) = c.r$.

When hashing to $\mathbb{G}_1$, the cofactor c and p / r have almost the same size and the hashing is considered to be easier than when hashing to $\mathbb{G}_2$. In fact, in $\mathbb{G}_2$, the length of c increases and it is of the same size with $p^{k/d}/r$, so that the scalar multiplication becomes really costly. Therefore, it is of great interest to make hashing into $\mathbb{G}_2$ fast.

Hashing into $\mathbb{G}_2$ with Scott et al. Method

Let $\phi : \tilde{E} \to E$ be the twist isomorphism from $\tilde{E}$ to E and π be the pth power Frobenius on E. Scott et al. realized that the endomorphism $\psi = \phi^{-1} \circ \pi \circ \phi$ can be used to quicken the computation of $c \cdot P$ (this was noted in [14]).

The endomorphism ψ satisfies

$$\psi^2(P) - [t]\psi(P) + [p]P = \mathcal{O}. \tag{2}$$

The idea of Scott is to first express c to the base p as

$$c = c_0 + c_1 p + c_2 p^2 + \cdots + c_l p^l$$

and then use the identity $[p]P = [t]\psi(P) - \psi^2(P)$, so

$$\begin{aligned}[c]P &= [c_0]P + [c_1 p]P + [c_2 p^2]P + \cdots + [c_l p^l]P,\\ &= [c_0]P + [c_1 t]\psi(P) + [-c_1 + c_2 t^2]\psi^2(P) + \cdots,\\ &= [g_0]P + [g_1]\psi(P) + [g_2]\psi^2(P) + \cdots + [g_{2l}]\psi^{2l}(P).\end{aligned}$$

where every g_i is a polynomial in x with degree smaller than the degree of p.

For a parameterized family of curves, the method requires first to pre-calculate the cardinality $\tilde{n} \in \mathbb{Q}[x]$ of $\tilde{E}(\mathbb{F}_{q^{k/d}})$, where d is from the set of possible twist degrees $\{1;2;3;4;6\}$, and is usually the maximum from this set that divides k. The application ends by the execution of the algorithm 2 in [9] which determine the coefficients of the polynomial $[c(x)]P$ in $\psi(P)$ where $c(x) = \frac{\tilde{n}}{r(x)}$.

In what follows the Scott et al. hashing method is applied to Aurifeuillean curves [12] having embedding degree k equal to 6, 9, 15, 27 and 54.

Aurifeuillean Curves-6

The Aurifeuillean pairing-friendly curves-6 has an embedding degree of $k = 6$. We consider the zero j-invariant curves having twist curves $\tilde{E}$ with degree $d = 6$. This defines the group $\mathbb{G}_2$ as $\mathbb{G}_2 = \tilde{E}(\mathbb{F}_{p^{k/d}})(r) = \tilde{E}(\mathbb{F}_p)(r)$. The curve is parametrized by the polynomials:

$$\begin{aligned}p &= 9x^4 + 18x^3 + 18x^2 + 6x + 1\\ r &= 3x^2 + 3x + 1\\ t &= 3x^2 + 1,\end{aligned}$$

The order of the group $\tilde{E}(\mathbb{F}_p)$ is $c(x)r(x)$, where $c(x)$

$$c(x) = 3x^2 + 3x + 3.$$

for some rational point $P \in \tilde{E}(\mathbb{F}_p)$,

$$[c(x)]P = [3x^2 + 3x + 3]P.$$

To evaluate the cost of the operations $[c(x)]P$, we first calculate $[2]P + P = [3]P$ then $[x]([3]P) = [3x]P$ and $[x]([3x]P) = [3x^2]P$. It is made of three point additions, one point doubling and two scalar multiplications by x.

Aurifeuillean Curves-9

The Aurifeuillean curves-9 family of elliptic curves has an embedding degree of $k = 9$, and an associated twist curve $\tilde{E}$ with degree $d = 3$. This defines the group $\mathbb{G}_2$ as $\mathbb{G}_2 = \tilde{E}(\mathbb{F}_{p^{k/d}})(r) = \tilde{E}(\mathbb{F}_{p^3})(r)$. The curve is parametrized by the polynomials:

$$\begin{aligned}p &= 81\,x^8 + 27\,x^6 + 27\,x^5 - 18\,x^4 + 9\,x^3 + 3\,x^2 - 3\,x + 1\\ r &= 27x^6 + 9x^3 + 1\\ t &= -18x^4 - 3x + 1\end{aligned}$$

The cofactor of $\#\tilde{E}(\mathbb{F}_{p^3})$ relatively to $r(x)$ yields,

$$\begin{aligned}c(x) = {} & 19683\,x^{18} + 19683\,x^{16} + 13122\,x^{15} - 6561\,x^{14}\\ & + 13122\,x^{13} - 4374\,x^{12} - 2187\,x^{11}\\ & + 5103\,x^{10} - 3402\,x^9 + 972\,x^8 + 729\,x^7 - 891\,x^6\\ & + 486\,x^5 - 99\,x^3 + 45\,x^2 - 9\,x + 1.\end{aligned}$$

Applying Scott et al. method (algorithm 2 in [9]), the scalar multiplication $[c(x)]P$, for some rational point $P \in \tilde{E}(\mathbb{F}_{p^3})$, is reduced to

$$\begin{aligned}[c(x)]P = {} & \left[-27\,x^6 + 81\,x^5 - 27\,x^3 + 6\,x^2 + 18\,x^4\right]P\\ & + \left[-54\,x^6 - 9\,x^3 + 9\,x^2 - 27\,x^4 - 3\,x\right]\psi(P)\\ & + \left[1 - 54\,x^6 - 27\,x^4 - 9\,x^3 - 3\,x\right]\psi^2(P)\\ & + \left[36\,x^4 - 108\,x^6 + 6\,x - 18\,x^3 - 2 - 6\,x^2\right]\psi^3(P)\\ & + [-9\,x^2 + 1]\psi^4(P).\end{aligned}$$

In addition, we put into factor the common coefficients:

$$
\begin{aligned}
[c(x)]P = {} & [108](\psi^3([x^6]P)) + [81]([x^5]P) \\
& + [54]\big(-\psi([x^6P]) - \psi^2([x^6]P)\big) + [36](\psi^3([x^4]P)) \\
& + [27]\big(-[x^3]P - [x^6]P - \psi([x^4]P) - \psi^2([x^4]P)\big) \\
& + [18]([x^4]P - \psi^3([x^3]P)) \\
& + [9]\big(-\psi([x^3]P) + \psi([x^2]P) - \psi^2([x^3]P) - \psi^4([x^2]P)\big) \\
& + [6]\big([x^2]P + \psi^3([x]P)\big) \\
& + [3]\big(-\psi([x]P) - \psi^2([x]P)\big) + [2](-\psi^3(P)) \\
& + [1]\big(\psi^2(P) + \psi^4(P)\big)
\end{aligned}
$$

There are 11 point additions inside the brackets. Then, extracting all the $s = 11$ coefficients below and constructing the addition chain:

$$\left\{1, \boxed{2}, 3, \boxed{6}, 9, \boxed{18}, 27, 36, 54, 81, 108\right\}$$

of length $l = 10$. The numbers in box are results of adding a number that comes before by itself. By Olivos theorem [13], the number of group operations is $l + s - 1 = 10 + 11 - 1 = 20$, which includes 3 point doubling (number of elements in box) and 17 extra point additions. To evaluate the rest of cost operations, we first calculate $[x]P$, $[x^2]P = [x].([x]P)$, $[x^3]P = [x].([x^2]P)$, $[x^4]P = [x].([x^3]P)$, $[x^5]P = [x].([x^4]P)$, $[x^6]P = [x].([x^5]P)$. For $i = 1$ to 4 we evaluate $\psi^i(P)$, $\psi^i([x]P)$, $\psi^i([x^2]P)$, $\psi^i([x^3]P)$, $\psi^i([x^4]P)$, $\psi^i([x^5]P)$ and $\psi^i([x^6]P)$. Just the values which appeared in the decomposition of $[c(x)]P$ are needed.

In total, hashing to $\mathbb{G}_2$ in this family of curves has a cost of twenty eight point additions, three point doubling, six scalar multiplications by the parameter x and twenty ψ maps.

Aurifeuillean Curves-18

This family of curves has embedding degree $k = 18$ and is parameterised by the polynomials:

$$
\begin{aligned}
p &= 243x^{10} + 1 - 162x^8 + 81x^7 + 27x^6 - 54x^5 + 9x^4 + 9x^3 - 3x^2. \\
r &= 27x^6 + 9x^3 + 1 \\
t &= 3x^2 + 1
\end{aligned}
$$

The zero j-invariant curves have twists of order 6. In this case, the group $\mathbb{G}_2$ is expressed as a subgroup of $\tilde{E}(\mathbb{F}_{p^3})$. Then, $c(x)$ is of degree 24. Applying Scott et al. method, $[c(x)]P$, for $P \in \tilde{E}(\mathbb{F}_{p^3})$, is reduced to

$$
\begin{aligned}
[c(x)]P = {} & \Big[2 + 81x^8 - 243x^7 + 81x^5 \\
& - 45x^4 - 18x^3 + 243x^9 + 9x^2 + 27x^6\Big]P \\
& + \Big[-27x^6 + 81x^8 - 9x^4 + 3x^2\Big]\psi(P) \\
& + \Big[81x^8 + 1 - 27x^6 - 3x^2\Big]\psi^2(P) \\
& + \Big[6x^2 - 54x^6 + 18x^4 - 2\Big]\psi^3(P) \\
& + \Big[9x^4 - 6x^2 + 1\Big]\psi^4(P).
\end{aligned}
$$

The construction of addition chain yields, $\{1, \boxed{2}, 3, \boxed{6}, 9, \boxed{18}, 27, 45, \boxed{54}, 81, \underline{\boxed{162}}, 243\}$ of length $l = 11$. The underline number is not among coefficients of the expression of $[c(x)]P$, but added to build addition chain. By Olivos theorem, the number of group operations is $l + s - 1 = 11 + 11 - 1 = 21$ plus 12 extra operations which from the number of additions of points of the same coefficient. The final cost is made by 5 point doublings, 28 point additions, 9 scalar multiplications by the parameter x, and 20 applications of ψ.

Aurifeuillean Curves-15

This family of curves has embedding degree $k = 15$ and is parametrized by the polynomials:

$$
\begin{aligned}
p &= 729x^{12} + 243x^{10} + 81x^7 + 54x^6 + 27x^5 + 3x^2 + 3x + 1. \\
r &= 81x^8 + 81x^7 + 54x^6 + 27x^5 + 9x^4 + 9x^3 + 6x^2 + 3x + 1 \\
t &= 54x^6 + 3x + 1
\end{aligned}
$$

In this case, the group $\mathbb{G}_2$ is expressed as a subgroup of $\tilde{E}(\mathbb{F}_{p^5})$. Then, $c(x)$ is of degree 52. Applying Scott et al. method, $[c(x)]P$, for $P \in \tilde{\mathbf{E}}(\mathbb{F}_{p^5})$, is reduced to

$$[\lambda_0]P + \sum_{i=1}^{7}[\lambda_i]\psi^i(P) \tag{3}$$

where $\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6$ and λ_7 are polynomials of $\mathbb{Z}[x]$ of degree less than or equal to 11. To ease the readability, these polynomials are fully reported in Appendix A. The scalar multiplication $[c(x)]P$ can be calculated at the cost of 11 scalar multiplications by x and 83 applications of ψ.

Aurifeuillean Curves-27

The Aurifeuillean curves-27 has embedding degree $k = 27$ and twists of degree $d = 3$ The curve is giving by the following polynomial parametrization:

$$p = 177147\,x^{22} + 1 + 118098\,x^{20} + 19683\,x^{18} + 2187\,x^{13} + 1458\,x^{11} + 243\,x^9 + 9\,x^4 + 3\,x^2$$
$$r = 19683\,x^{18} + 243\,x^9 + 1$$
$$t = -3\,x^2 + 1$$

The group $\mathbb{G}_2$ is expressed as a subgroup of $\tilde{E}(\mathbb{F}_{p^9})$. Then, $c(x)$ is of degree 180. Applying Scott et al method, $[c(x)]P$, for $P \in \tilde{E}(\mathbb{F}_{p^9})$, is reduced to

$$[\lambda_0]P + \sum_{i=1}^{16} [\lambda_i]\psi^i(P) \tag{4}$$

where λ_i, for $i = 0, 1, \ldots, 16$ are polynomials of $\mathbb{Z}[x]$ of degree less than or equal to 21 (see Appendix B for their complete expressions). The multiplication $[c(x)]P$ can be calculated at the cost of 21 scalar multiplications by x and 240 applications of ψ.

Aurifeuillean Curves-54

The Aurifeuillean curves-54 has embedding degree $k = 54$ and is parametrized by the polynomials:

$$p = 59049\,x^{20} + 59049\,x^{19} + 19683\,x^{18} + 1 + 729\,x^{11} + 972\,x^{10} + 243\,x^9 + 3\,x^2 + 3\,x.$$
$$r = 19683\,x^{18} + 243\,x^9 + 1$$
$$t = 243\,x^{10} + 1,$$

The corresponding zero j-invariant curve has twist of degree $d = 6$, and the group $\mathbb{G}_2$ is expressed as a subgroup of $\tilde{E}(\mathbb{F}_{p^9})$, then the cofactor is $c(x)$ of degree 162. Applying Scott et al method, $[c(x)]P$, for $P \in \tilde{\mathbf{E}}(\mathbb{F}_{p^9})$, is reduced to

$$[\lambda_0]P + \sum_{i=1}^{10} [\lambda_i]\psi^i(P), \tag{5}$$

where $\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8, \lambda_9$ and λ_{10} are polynomials of $\mathbb{Z}[x]$ of degree less than or equal to 19 (see Appendix C for their complete forms). The multiplication $[c(x)]P$ can be calculated at the cost 19 scalar multiplications by x and 159 applications of ψ.

Comparison with Others Pairing-Friendly Elliptic Curves

Previous works [9, 11] on hashing into $\mathbb{G}_2$ using the Scott et al.'s method with BLS curves, MNT curves, KSS curves, and Freeman curves provided some computational costs that we confront to the results obtained in this work. We consider the notations A for point addition, D for point doubling, X for a scalar multiplication by the parameter x and ψ an application of the endomorphism $\psi(.)$. The endomorphism ψ can be efficiently calculated, whereas the multiplication by x, is most costly, since x is large and the algorithm to compute large scalar multiplications require many point additions and doubling. The comparison is given in Table 1.

Hashing into $\mathbb{G}_2$ with Fuentes et al. Method

Fuentes et al. discovered that instead of multiplying the polynomial $c(x)$ by the point P of elliptic curve as in the Scott et al. method, and it is sufficient to multiply P by c' a multiple of c, such that c' do not vanish modulo r.

Indeed, let f and $\tilde{f}$ be such that $t^2 - 4p = Df^2$ and $\tilde{t}^2 - 4q = D\tilde{f}^2$, where D is the discriminant, $n + t = p + 1$ and $\tilde{n} + \tilde{t} = q + 1$ where $n = \#E(\mathbb{F}_p)$, $\tilde{n} = \#\tilde{E}(\mathbb{F}_q)$ and q a power of p. The Lemma 1 shows that $\tilde{E}(\mathbb{F}_q)$ is stable by ψ, and the Lemma 2 illustrates the effect of ψ on the element of twisted curve $\tilde{E}(\mathbb{F}_q)$. (see [10] for evidence)

Lemma 1 *If* $p \equiv 1 \mod d$, *then* $\psi(Q) \in \tilde{E}(\mathbb{F}_q)$ *for all* $Q \in \tilde{E}(\mathbb{F}_q)$.

Lemma 2 *If* $p \equiv 1 \mod d, gcd(\tilde{f}, \tilde{n}) = 1$ *and* $\tilde{E}(\mathbb{F}_q)$ *is a cyclic group, then* $\psi(Q) = aQ$ *for all* $Q \in \tilde{E}(\mathbb{F}_q)$, *where a is*

$$\frac{t}{2} + \frac{f(\tilde{t} - 2)}{2\tilde{f}} \quad or \quad \frac{t}{2} - \frac{f(\tilde{t} - 2)}{2\tilde{f}}. \tag{6}$$

Table 1 Cost summary of hashing into $\mathbb{G}_2$ using the Scott et al.

Aurifeuillean curves	Scoot et al. method this work	Other curves	Scoot et al. method previous works in [9, 11]
AU-6	3A,1D,2X	MNT-6	1 A, 1 D, 1 X, 2 ψ
AU-9	28A, 3D, 6X, 20 ψ	Freeman-10	20 A, 5 D, 3 X, 4 ψ
AU-15	11X, 83 ψ	BLS-12	6A, 2 D, 3 X, 3 ψ
AU-18	28A, 5D, 9X, 20 ψ	KSS-18	51A, 5 D, 7 X, 38 ψ
AU-27	21 X, 240 ψ	BLS-30	82 A, 16 D, 11 X, 67 ψ
AU-54	19 X, 159 ψ	BLS-48	132 A, 120 D, 16 X, 130 ψ

Theorem 4 [10] *Suppose that* $\tilde{E}(\mathbb{F}_q)$ *is cyclic and* $p \equiv 1 \mod d$.

Then, there exists a polynomial

$$h(z) = h_0 + h_1 z + \cdots + h_{\varphi(k)-1} z^{\varphi(k)-1}$$

in $\mathbb{Z}[z]$ *such that* $[h(\psi)]Q$ *is a multiple of* $[c]Q$ *for all* $Q \in \tilde{E}(\mathbb{F}_q)$ *and* $|h_i|^{\varphi(k)} \leq \#\tilde{E}(\mathbb{F}_q)/r$ *for all* i.

Fuentes noticed that polynomials $h \in \mathbb{Z}[z]$, such that $h(a) \equiv 0 \mod c$ correspond to points in the integer lattice generated by the matrix:

$$M = \left(\begin{array}{c|c} c & 0 \\ \hline A & I_{\varphi(k)-1} \end{array}\right)$$

where A is a column vector with ith entry $-a^i \mod c$, $i = 1, 2, \ldots, \varphi(k) - 1$.

The method begins as the Scott et al. method for obtaining $\tilde{n}$ the order of twisted curve $\tilde{E}$ and $c(x)$ its cofactor relatively to $r(x)$. We also find $a(x)$ as defined in Lemma 2 and set the matrix M. Then used LLL algorithm [15] to reduce the coefficients of the matrix M. The linear combination of the rows of the reduced matrix obtained yields

$$h(z) = h_0(x) + h_1(x)z + h_2(x)z^2 + \cdots$$

and the final step of hashing into $\mathbb{G}_2$ with Fuentes et al. method is

$$[h(\psi)]P = [h_0(x)]P + [h_1(x)]\psi(P) + [h_2(x)]\psi(P)^2 + \cdots$$

The pre-computation is done using the software Maple and the LLL reduction is done using Magma V2.24-1 calculator

We applied Fuentes et al. hashing method to Aurifeuillean curves having embedding degree k equal to 6, 9, 18, 27 and 54. But we does not applied the method for $k = 15$, because the condition that the cyclotomic polynomial map to a (see Eq. 6) modulo the order of the twisted curve does not hold.

Aurifeuillean Curves-6

For the Aurifeuillean curves with $k = 6$,, the parameter a from Lemma2 is the following polynomial in x.

$$\begin{aligned} a(x) &= \frac{t}{2} + \frac{f(\tilde{t}-2)}{2\tilde{f}} \mod \tilde{n}(x) \\ &= 12x^2 + 6x^3 + 8x + 3 \end{aligned}$$

We set

$$M = \left(\begin{array}{c|c} c(x) & 0 \\ -a(x) \mod c(x) & 1 \end{array}\right).$$

and the LLL reduction of M yields

$$LLL(M) = \begin{bmatrix} -\frac{13}{4}x + 1/4 & 0 \\ x + 3/4 & 1/4 \end{bmatrix}.$$

By multiplying the last row by 4 and setting $h(z) = (4x + 3) + z$, $h(a(x)) = 2(x + 1)c(x) \mod \tilde{n}(x)$, with $gcd(2x + 2, r(x)) = 1$. Hence, if $P \in E(\mathbb{F}_{p(x)})$, then $[h(a)]P$ is a multiple of $[c]P$ and $[h(a)]P = [h(\psi)]P$, so

$$[h(\psi)]P = [4x + 3]P + \psi(P).$$

$[3]P = [2]P + P$,$[4x]P = [x]([2]([2]P))$, then $[h(\psi)]P$ can be computed at the cost of 3 point additions, 2 point doubling, 1 scalar multiplication by the parameter x and 1 applications of ψ.

Aurifeuillean Curves-9

For the Aurifeuillean curves with $k = 9$, the parameter a is given by

$$\begin{aligned} a(x) = &-\frac{2424212632}{217993987}x + \frac{5143304439}{217993987}x^2 \\ &- \frac{2610122718}{217993987}x^3 - \frac{28189433622483}{217993987}x^{18} \\ &+ \frac{2506275703512}{217993987}x^{16} - \frac{12796629413985}{217993987}x^{15} \\ &+ \frac{1222024507191}{217993987}x^{14} + \frac{1016530951635}{217993987}x^{13} \\ &- \frac{3969053944218}{217993987}x^{12} + \frac{1767566638755}{217993987}x^{11} \\ &- \frac{302386560777}{217993987}x^{10} - \frac{838029510945}{217993987}x^9 \\ &+ \frac{547494386031}{217993987}x^8 - \frac{185168432511}{217993987}x^7 \\ &- \frac{94951444725}{217993987}x^6 + \frac{81127529640}{217993987}x^5 \\ &- \frac{10251013101543}{217993987}x^{22} - \frac{428418209700}{2986219}x^{21} \\ &- \frac{38370288560094}{217993987}x^{20} - \frac{5671787322267}{217993987}x^{19} \\ &+ \frac{359339840}{217993987} - \frac{11556879138387}{217993987}x^{17} \\ &- \frac{34656702615}{217993987}x^4 - \frac{27153033524343}{217993987}x^{23}. \end{aligned}$$

Setting

$$M = \left(\begin{array}{c|ccccc} c(x) & 0 & 0 & 0 & 0 & 0 \\ -a(x) \mod c(x) & 1 & 0 & 0 & 0 & 0 \\ -a(x)^2 \mod c(x) & 0 & 1 & 0 & 0 & 0 \\ -a(x)^3 \mod c(x) & 0 & 0 & 1 & 0 & 0 \\ -a(x)^4 \mod c(x) & 0 & 0 & 0 & 1 & 0 \\ -a(x)^5 \mod c(x) & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

and using LLL algorithm, we obtain the matrix with small coefficients:

$$\begin{bmatrix} -1/3\,x^2-1/3\,x & 1/3\,x-1/9 & -2/3\,x^2+2/9 & 1/3\,x^2-1/3\,x & 1/3\,x+1/9 & x^3-1/3\,x^2+1/9 \\ 1/3\,x-1/9 & -2/3\,x^2+2/9 & 2/3\,x^2 & 1/3\,x+1/9 & x^3-1/3\,x^2+1/9 & 1/3\,x^2+1/3\,x \\ -2/3\,x^2+2/9 & 2/3\,x^2 & 2/9 & x^3-1/3\,x^2+1/9 & 1/3\,x^2+1/3\,x & -1/3\,x+1/9 \\ 2/3\,x^2 & 2/9 & x^3+1/3\,x^2-1/9 & 1/3\,x^2+1/3\,x & -1/3\,x+1/9 & 2/3\,x^2-2/9 \\ 2/9 & x^3+1/3\,x^2-1/9 & -1/3\,x^2+1/3\,x & -1/3\,x+1/9 & 2/3\,x^2-2/9 & -2/3\,x^2 \\ x^3+1/3\,x^2-1/9 & -1/3\,x^2+1/3\,x & -1/3\,x-1/9 & 2/3\,x^2-2/9 & -2/3\,x^2 & -2/9 \end{bmatrix}$$

Taking the 6th row of the above matrix when multiplied by 9 we defined the polynomial:

$$h(z) = 9\,x^3+3\,x^2-1+\left(-3\,x^2+3\,x\right)z + (-3\,x-1)z^2+\left(6\,x^2-2\right)z^3-6\,x^2z^4-2\,z^5.$$

$h(a(x)) \equiv (9x^3+1)c(x) \mod \tilde{n}(x)$, with $\gcd(r(x), 9x^3+1) = 1$. Hence if $P \in \tilde{E}(\mathbb{F}_{p(x)^2})$, then $[h(a)]P$ is a multiple of $[c]P$ and $[h(a)]P = [h(\psi)]P$.

$$[h(\psi)]P = [9\,x^3+3\,x^2-1]P+\left[-3\,x^2+3\,x\right]\psi(P) + [-3\,x-1]\psi(P)^2+\left[6\,x^2-2\right]\psi(P)^3 - [6\,x^2]\psi(P)^4-[2]\,\psi(P)^5.$$

That can be computed at the cost of 12 point additions,2 point doublings, 3 scalar multiplications by the parameter x and 11 applications of ψ.

Aurifeuillean Curves-18

For Aurifeuillean curves with $k = 18$, we follow the same process as above and obtain the polynomial:

$$h(z) = -3\,x^3+x-1+\left(9\,x^4-3\,x^2+x\right)z+\left(3\,x^2-1\right)z^2 + \left(-3\,x^3+x+1\right)z^3-2\,xz^4$$

with $h(a(x)) \equiv -3(9x^3+2)c(x) \mod \tilde{n}(x)$ and $\gcd(r(x), -3(9x^3+2)) = 1$.

For every $P \in \tilde{E}(\mathbb{F}_{p(x)^3})$,

$$[h(\psi)]P = [-3\,x^3+x-1]P+\left[9\,x^4-3\,x^2+x\right]\psi(P) + \left[3\,x^2-1\right]\psi(P)^2 + [-3\,x^3+x+1]\psi(P)^3+[-2x]\,\psi(P)^4.$$

That can be computed at the cost of 14 point additions, 2 point doublings, 4 scalar multiplications by the parameter x and 13 applications of ψ.

Aurifeuillean Curves-27

For Aurifeuillean curves with $k = 27$, the polynomial yields

$$\begin{aligned} h(z) = {} & 81x^9+27x^7+1+(-27x^7-9x^5)z \\ & +(9x^5+3x^3)z^2+(-3x^3-x)z^3 \\ & +(-243x^{10}-81x^8-x)z^4+(81x^8+27x^6)z^5 \\ & +(-27x^6-9x^4)z^6+(9x^4+3x^2)z^7 \\ & +(-3x^2-1)z^8+(-81x^9-27x^7+1)z^9 \\ & +(27x^7+9x^5)z^{10}+(-9x^5-3x^3)z^{11} \\ & +(3x^3+x)z^{12}+(-2x)z^{13} \end{aligned}$$

with $h(a(x)) \equiv 81x^9c(x) \mod \tilde{n}(x)$ and $\gcd(r(x), 81x^9) = 1$. For every $P \in \tilde{E}(\mathbb{F}_{p(x)^9})$,

$$\begin{aligned} [h(\psi)]P = {} & [81x^9+27x^7+1]P+[-27x^7-9x^5]\psi(P) \\ & +[9x^5+3x^3]\psi(P)^2+[-3x^3-x]\psi(P)^3 \\ & +[-243x^10-81x^8-x]\,\psi(P)^4 \\ & +[81x^8+27x^6]\,\psi(P)^5 \\ & +[-27x^6-9x^4]\,\psi(P)^6+[9x^4+3x^2]\,\psi(P)^7 \\ & +[-3x^2-1]\,\psi(P)^8 \\ & +[-81x^9-27x^7+1]\,\psi(P)^9 \\ & +[27x^7+9x^5]\,\psi(P)^{10}+[-9x^5-3x^3]\,\psi(P)^{11} \\ & +[3x^3+x]\,\psi(P)^{12}+[-2x]\,\psi(P)^{13}. \end{aligned}$$

That can be computed at the cost of 33 point additions, 5 point doublings, 10 scalar multiplications by the parameter x and 94 applications of ψ.

Aurifeuillean Curves-54

For Aurifeuillean curves with $k = 54$, we obtain the following polynomial:

$$\begin{aligned} h(z) = {} & 2x+1+(81x^9-1)z+(27x^7)z^2 \\ & +(-27x^7-27x^6)z^3+(27x^6+18x^5)z^4 \\ & +(-18x^5-9x^4)z^5+(9x^4+3x^3)z^6 \\ & +(-3x^3)z^7+(-x)z^8+(-x)z^9 \\ & +(81x^9+81x^8+1)z^{10}+(-81x^8-54x^7)z^{11} \\ & +(54x^7+27x^6)z^{12}+(-27x^6-9x^5)z^{13} \\ & +(9x^5)z^{14}+(3x^3)z^{15} \\ & +(-3x^3-3x^2)z^{16}+(3x^2+2x)z^{17} \end{aligned}$$

with $h(a(x)) \equiv 3x(81x^9+1)c(x) \mod \tilde{n}(x)$ and $\gcd(r(x), 3x(81x^9+1)) = 1$. For every $P \in \tilde{E}(\mathbb{F}_{p(x)^9})$,

$$\begin{aligned}[h(\psi)]P = {} & [2x+1]P + \left[81x^9-1\right]\psi(P) + \left[27x^7\right]\psi(P)^2 \\ & + [-27x^7 - 27x^6]\psi(P)^3 + [27x^6 + 18x^5]\,\psi(P)^4 \\ & + [-18x^5 - 9x^4]\,\psi(P)^5 + [9x^4 + 3x^3]\,\psi(P)^6 \\ & + [-3x^3]\,\psi(P)^7 + [-x]\,\psi(P)^8 + [-x]\,\psi(P)^9 \\ & + [81x^9 + 81x^8 + 1]\,\psi(P)^{10} + [-81x^8 - 54x^7]\,\psi(P)^{11} \\ & + [54x^7 + 27x^6]\,\psi(P)^{12} + [-27x^6 - 9x^5]\,\psi(P)^{13} \\ & + [9x^5]\,\psi(P)^{14} + [3x^3]\,\psi(P)^{15} + [-3x^3 - 3x^2]\,\psi(P)^{16} \\ & + [3x^2 + 2x]\,\psi(P)^{17}.\end{aligned}$$

That can be computed at the cost of 33A point additions, 4 point doublings, 9 scalar multiplications by the parameter x and 126 applications of ψ.

Comparison with Others Pairing Friendly Elliptic Curves

In Table 2, we recapitulate the computational costs of hashing into $\mathbb{G}_2$ using Fuentes et al. method with Aurifeuillean curves, KSS curves, Freeman curve and BN curves. As with Scott et al.'s method for $k = 18$ hashing with KSS curve is more efficient than with Aurifeuillean curve as far as group operations is concerned.

In Table 3, we carry out the computational costs of hashing into $\mathbb{G}_2$ using the Scott et al.'s and Fuentes et al.'s methods with Aurifeuillean curves with embedding degrees $k = 6, 9, 18, 27$ and $k = 54$. We observe that for the two first cases, the Fuentes et al.'s method is twice as fast than the one of Scott et al. method. For $k = 18, 27$ and 54, the Fuentes et al.'s method determines a 9/4, 21/10 and 19/8-fold improvement respectively. Previous works show that is it more efficient to hashing into $\mathbb{G}_2$ using the Fuentes et al.'s method with BLS, BN, and KSS curves. Our results on Aurifeuillean curve also confirm this assertion.

Table 3 Comparison between the computational cost of each hash map

Curve	Scott et al. method	Fuentes et al. method
AU-6	3 A, 1 D, 2 X	3 A, 2 D, 1 X, 1ψ
AU-9	28 A, 3 D, 6 X, 20 ψ	12 A, 2 D, 3 X, 11 ψ
AU-18	28 A, 5 D, 9 X, 20 ψ	14 A, 2 D, 4 X, 13 ψ
AU-27	21 X, 240 ψ	33 A, 5 D, 10 X, 94 ψ
AU-54	19 X, 159 ψ	33 A, 4 D, 9 X, 126 ψ

Conclusion

This work investigated on an efficient hashing into $\mathbb{G}_2$ to on the recent Scott–Guillevic Aurifeuillean curves. We applied the two existing hashing methods namely the Scott et al. and Fuentes et al. methods. Our results show that hashing on Auriffeuillean curves with embedding degree $k = 6, 9, 18, 27$ and 54 is more costly than hashing on the well known BLS curves, KSS curves, or BN curves for comparable embedding degrees. Our results also confirm that hashing into $\mathbb{G}_2$ using the Fuentes et al.'s method is more efficient that using the Scott et al. method as reported in the previous work on the literature.

Acknowledgements The authors deeply thank Aurore Guillevic who provided a magma code for obtaining the coefficient matrix representation of the polynomial matrix in Theorem 4. Indeed She helped to obtain matrices with rational coefficients instead of polynomial coefficients to which the application of the LLL algorithm was infeasible for high embedding degrees 27 and 54. The authors also thank the reviewers for their comments which helped to improve the work.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Table 2 Cost summary of hashing into $\mathbb{G}_2$ using the Fuentes et al.

Curve	Fuentes et al. method this work	Curve	Fuentes et al. method previous work in [11, 16]
AU-6	3 A,2 D,1 X 1 ψ	KSS-8	7 A, 3 D, 2 X, 3 ψ
AU-9	12 A, 2 D, 3 X, 11 ψ	Freeman-10	14 A, 4 D, 3 X, 4 ψ
AU-15	–	BN-12	4 A, 1 D, 1 X, 3 ψ
AU-18	14 A, 2 D, 4 X, 13 ψ	KSS-18	16 A, 2 D, 3 X, 5 ψ
AU-27	33 A, 5 D, 10 X, 94 ψ	BLS-24	9 A, 1 D, 4 X, 10 ψ
AU-54	33 A, 4 D, 9 X, 126 ψ	BLS-48	17 A, 1 D, 8 X, 36 ψ

Appendix A: Aurifeuillean Curves-15

For any rational $P \in \tilde{E}(\mathbb{F}_{p^5})$, the hash map obtained in (3) yields $[c(x)]P = [\lambda_0]P + \sum_{i=1}^{7}[\lambda_i]\psi^i(P)$ where:

$$\begin{aligned}
\lambda_0 &= 786\,x + 286 - 369\,x^4 + 12285\,x^6 \\
&\quad - 6318\,x^9 + 3240\,x^7 + 7857\,x^5 - 1116\,x^3 \\
&\quad - 19359\,x^8 + 89667\,x^{10} + 6561\,x^{11} + 126\,x^2 \\
\lambda_1 &= -436 - 1233\,x - 414\,x^4 \\
&\quad - 19305\,x^6 + 2673\,x^9 - 2187\,x^7 \\
&\quad - 6210\,x^5 + 1557\,x^3 + 25353\,x^8 \\
&\quad - 69741\,x^{10} - 12393\,x^{11} + 288\,x^2 \\
\lambda_2 &= 375 + 423\,x + 783\,x^4 + 6966\,x^6 + 3402\,x^9 \\
&\quad - 1053\,x^7 + 378\,x^5 - 378\,x^3 - 6480\,x^8 \\
&\quad + 243\,x^{10} + 1458\,x^{11} - 564\,x^2 \\
\lambda_3 &= 168\,x + 72\,x^4 - 87 + 162\,x^6 - 162\,x^7 + 27\,x^5 \\
&\quad - 153\,x^3 + 243\,x^8 + 1458\,x^{11} + 36\,x^2 \\
\lambda_4 &= -60 + 162\,x^6 + 27\,x^5 + 72\,x^3 + 243\,x^8 \\
&\quad + 1458\,x^{11} - 162\,x^7 - 63\,x^4 + 126\,x^2 - 147\,x \\
\lambda_5 &= 179 + 726\,x - 1368\,x^4 + 15417\,x^6 - 24786\,x^9 \\
&\quad + 14742\,x^7 + 3510\,x^5 - 306\,x^3 - 6156\,x^8 \\
&\quad + 36450\,x^{10} + 110808\,x^{11} + 702\,x^2 \\
\lambda_6 &= -176 - 921\,x + 1377\,x^4 - 15768\,x^6 + 25758\,x^9 \\
&\quad - 19926\,x^7 - 3213\,x^5 + 990\,x^3 + 11340\,x^8 \\
&\quad - 25758\,x^{10} - 81648\,x^{11} - 1017\,x^2 \\
\lambda_7 &= 117 + 429\,x + 45\,x^4 + 3240\,x^6 - 1944\,x^9 + 5832\,x^7 \\
&\quad + 972\,x^5 - 729\,x^3 - 5184\,x^8 + 1944\,x^{10} + 222\,x^2.
\end{aligned}$$

Appendix B: Aurifeuillean Curves-27

For any rational $P \in \tilde{E}(\mathbb{F}_{p^9})$, the hash map obtained in (4) yields $[c(x)]P = [\lambda_0]P + \sum_{i=1}^{16}[\lambda_i]\psi^i(P)$ where:

$$\begin{aligned}
\lambda_0 &= -2480058\,x^{21} + 6561\,x^{16} + 6 - 405\,x^5 \\
&\quad - 30618\,x^{10} - 78732\,x^{18} - 10935\,x^{13} + 810\,x^6 \\
&\quad - 2480058\,x^{19} - 275562\,x^{17} + 59049\,x^{20} \\
&\quad + 144342\,x^{15} - 84\,x + 1053\,x^7 - 4374\,x^{11} \\
&\quad - 243\,x^9 - 162\,x^4 72\,x^3 - 52488\,x^{12} + 39366\,x^{14} \\
\lambda_1 &= -9 + 9920232\,x^{21} - 65610\,x^{16} \\
&\quad + 1674\,x^5 - 27\,x^2 + 68526\,x^{10} + 19683\,x^{18} \\
&\quad + 63423\,x^{13} - 6804\,x^8 - 1458\,x^6 \\
&\quad + 6613488\,x^{19} + 59049\,x^{20} - 406782\,x^{15} \\
&\quad + 234\,x - 1782\,x^7 + 14580\,x^{11} - 3645\,x^9 \\
&\quad + 648\,x^4 - 117\,x^3 + 174960\,x^{12} - 21870\,x^{14}, \\
\lambda_2 &= 9 - 11337408\,x^{21} - 1269\,x^5 + 135\,x^2 \\
&\quad - 37908\,x^{10} + 19683\,x^{18} - 137781\,x^{13} \\
&\quad + 15552\,x^8 - 648\,x^6 - 5196312\,x^{19} \\
&\quad + 1102248\,x^{17} + 59049\,x^{20} + 367416\,x^{15} \\
&\quad - 309\,x - 10206\,x^{11} + 6075\,x^9 - 972\,x^4 \\
&\quad + 540\,x^3 - 172044\,x^{12} - 17496\,x^{14}, \\
\lambda_3 &= 3 + 3720087\,x^{21} - 189\,x^2 - 14094\,x^{10} \\
&\quad + 19683\,x^{18} + 129033\,x^{13} - 9963\,x^8 + 3240\,x^6 \\
&\quad + 118098\,x^{19} - 1161297\,x^{17} + 59049\,x^{20} + 225\,x \\
&\quad - 1458\,x^{11} - 5103\,x^9 + 486\,x^4 - 360\,x^3 + 47385\,x^{12} \\
\lambda_4 &= -9 + 135\,x^2 + 11907\,x^{10} + 19683\,x^{18} \\
&\quad - 50301\,x^{13} - 162\,x^8 - 2349\,x^6 + 767637\,x^{19} \\
&\quad + 275562\,x^{17} + 59049\,x^{20} - 150903\,x^{15} - 75\,x \\
&\quad + 10206\,x^{11} + 3159\,x^9 + 162\,x^4 \\
\lambda_5 &= 9 - 27\,x^2 + 19683\,x^{18} + 1377\,x^8 + 216\,x^6 \\
&\quad + 59049\,x^{17} + 59049\,x^{20} + 39366\,x^{15} \\
&\quad - 4374\,x^{11} - 729\,x^9 - 243\,x^4 \\
\lambda_6 &= -3 + 19683\,x^{18} + 6561\,x^{13} + 189\,x^6 + 59049\,x^{20} \\
&\quad + 6561\,x^{15} + 2187\,x^{11} + 243\,x^9 + 90\,x^4 \\
\lambda_7 &= -3\,x^2 + 19683\,x^{18} + 59049\,x^{20} - 9\,x^4 \\
\lambda_8 &= 1 + 3\,x^2 + 19683\,x^{18} + 59049\,x^{20} \\
\lambda_9 &= -8 - 124659\,x^{16} + 57\,x^2 - 10206\,x^{10} \\
&\quad + 157464\,x^{18} + 3402\,x^8 - 162\,x^6 \\
&\quad - 189\,x^4 + 4374\,x^{12} + 45927\,x^{14} \\
\lambda_{10} &= 18954\,x^{10} - 13608\,x^8 + 2106\,x^6 + 41553\,x^{12} + 513\,x^4 \\
&\quad - 168399\,x^{14} - 231\,x^2 + 183708\,x^{16} + 28
\end{aligned}$$

$$\lambda_{11} = 6561\,x^{10} + 17496\,x^8 - 5832\,x^6 - 243\,x^4 - 96957\,x^{12} + 399\,x^2 + 122472\,x^{14} - 56$$
$$\lambda_{12} = -5589\,x^8 + 6480\,x^6 - 621\,x^4 - 28917\,x^{10} - 357\,x^2 + 51030\,x^{12} + 70$$
$$\lambda_{13} = -3969\,x^8 - 2835\,x^6 + 945\,x^4 + 147\,x^2 + 13608\,x^{10} - 56$$
$$\lambda_{14} = 27\,x^6 - 486\,x^4 + 3\,x^2 + 2268\,x^8 + 28$$
$$\lambda_{15} = 216\,x^6 + 72\,x^4 - 24\,x^2 - 8$$
$$\lambda_{16} = 9\,x^4 + 6\,x^2 + 1$$

Appendix C: Aurifeuillean Curves-54

The application $[c(x)]$ map $P \in \tilde{E}(\mathbb{F}_{p^9})$, to (5) which is $[\lambda_0]P + \sum_{i=1}^{10}[\lambda_i]\psi^i(P)$ an element of $\mathbb{G}_2$, where:

$$\lambda_0 = 17349\,x + 5944 + 166695327\,x^{18} + 330083910\,x^{19} - 8345592\,x^{14} + 9086985\,x^{13} + 19997928\,x^{16} - 1023516\,x^{15} - 42554646\,x^{17} - 5150385\,x^{12} + 773469\,x^{11} + 1486917\,x^9 + 43011\,x^7 - 61074\,x^8 - 2997\,x^5 - 17496\,x^6 + 12366\,x^4 - 10899\,x^3 + 5710014\,x^{10} + 4596\,x^2,$$
$$\lambda_1 = -55227\,x - 600055938\,x^{18} - 1028692629\,x^{19} + 33732288\,x^{14} - 32831244\,x^{13} - 59291757\,x^{16} - 5570289\,x^{15} + 144118926\,x^{17} + 17275842\,x^{12} - 1127763\,x^{11} - 5220126\,x^9 + 5508\,x^7 + 19764\,x^8 + 5346\,x^5 - 6048\,x^6 - 8550\,x^4 + 7290\,x^3 - 20055033\,x^{10} - 1353\,x^2 - 27143,$$
$$\lambda_2 = 32262 + 67812\,x + 673276698\,x^{18} + 1226979171\,x^{19} - 29570427\,x^{14} + 29445768\,x^{13} + 50152284\,x^{16} + 5701509\,x^{15} - 121011084\,x^{17} - 16585479\,x^{12} + 1471122\,x^{11} + 6693678\,x^9 - 48843\,x^7 - 21303\,x^8 - 28809\,x^5 + 51138\,x^6 + 13590\,x^4 - 3753\,x^3 + 21528828\,x^{10} - 5889\,x^2,$$
$$\lambda_3 = -3574 - 25539\,x - 134198694\,x^{18} - 350573913\,x^{19} + 3475143\,x^{14} - 9056367\,x^{13} - 32063607\,x^{16} + 10340136\,x^{15} + 48735108\,x^{17} + 9000234\,x^{12} - 4672161\,x^{11} - 1349379\,x^9 + 41877\,x^7 + 18954\,x^8 + 26271\,x^5 - 48195\,x^6 - 5967\,x^4 - 2853\,x^3 - 4537296\,x^{10} + 7638\,x^2,,$$
$$\lambda_4 = 166 + 10176\,x + 29170206\,x^{18} + 107528229\,x^{19} - 69984\,x^{14} + 981963\,x^{13} + 4737042\,x^{16} - 2191374\,x^{15} - 4979799\,x^{17} - 1458000\,x^{12} + 1346463\,x^{11} + 438615\,x^9 - 28998\,x^7 - 2754\,x^8 - 15822\,x^5 + 28917\,x^6 + 2088\,x^4 + 4104\,x^3 + 1054620\,x^{10} - 5037\,x^2,$$
$$\lambda_5 = 715 - 924\,x - 295245\,x^{18} - 1771470\,x^{19} - 166212\,x^{14} + 56862\,x^{13} - 583929\,x^{16} + 373977\,x^{15} + 492075\,x^{17} + 14580\,x^{12} - 183708\,x^{11} - 20412\,x^9 + 1458\,x^7 + 4617\,x^8 + 3078\,x^5 - 3780\,x^6 - 1359\,x^4 + 72\,x^3 + 177633\,x^{10} + 444\,x^2,$$
$$\lambda_6 = -155 + 501\,x + 2263545\,x^{18} + 3542940\,x^{19} - 190269\,x^{14} + 107163\,x^{13} + 262440\,x^{16} + 65610\,x^{15} - 393660\,x^{17} - 22599\,x^{12} - 26244\,x^{11} + 26730\,x^9 + 324\,x^7 - 1701\,x^8 - 1215\,x^5 + 1053\,x^6 + 594\,x^4 - 180\,x^3 + 69012\,x^{10} - 144\,x^2,$$
$$\lambda_7 = -30\,x - 590490\,x^{19} - 4374\,x^{14} - 56862\,x^{13} - 91854\,x^{16} + 131220\,x^{15} + 36450\,x^{12} - 7290\,x^{11} + 486\,x^7 - 810\,x^8 - 324\,x^5 + 432\,x^6 - 18\,x^4 + 90\,x^3 - 7290\,x^{10},$$
$$\lambda_8 = 59049\,x^{14} - 65610\,x^{16} - 14580\,x^{12} - 108\,x^4 - 90\,x^3 + 216\,x^6 - 810\,x^7 + 459\,x^5 - 2187\,x^{13} - 6561\,x^{15},$$
$$\lambda_9 = -10935\,x^{14} + 10935\,x^{13} - 32805\,x^{15} + 7290\,x^{12} - 135\,x^5 - 270\,x^6 + 135\,x^4 + 45\,x^3,$$
$$\lambda_{10} = -4374\,x^{14} - 4374\,x^{13} - 1458\,x^{12} - 27\,x^5 - 45\,x^4 - 9\,x^3.$$

References

1. Boneh D, Franklin MK. Identity-based encryption from the weil pairing. In: Advances in cryptology. 2001. p. 213–29. https://doi.org/10.1007/3-540-44647-8_13.
2. Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing. J Cryptol. 2004;17(4):297–319. https://doi.org/10.1007/s00145-004-0314-9.
3. Joux A. A one round protocol for tripartite Diffie–Hellman. In: Algorithmic number theory. 2000. p. 385–94. https://doi.org/10.1007/10722028_23.
4. Silvermann JH. The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106. New York: Springer; 1986.
5. Miller VS. The weil pairing, and its efficient calculation. J Cryptol. 2004;17(4):235–61. https://doi.org/10.1007/s00145-004-0315-8.
6. Blake IF, Murty VK, Xu G. Refinements of miller's algorithm for computing the weil/tate pairing. J Algorithms 2006;58(2):134–149 . https://doi.org/10.1016/j.jalgor.2005.01.009. http://www.sciencedirect.com/science/article/pii/S0196677405000271.
7. Hess F, Smart NP, Vercauteren F. The eta pairing revisited. IEEE Trans Inf Theory. 2006;52(10):4595–602.https://doi.org/10.1109/TIT.2006.881709.

8. Lee E, Lee H, Park C. Efficient and generalized pairing computation on abelian varieties. IEEE Trans Inf Theory. 2009;55(4):1793–803.
9. Scott M, Benger N, Charlemagne M, Dominguez LJ, Kachisa EJ. Fast hashing to $\mathbb{G}_2$ on pairing-friendly curves. In: Pairing-based cryptography—pairing. 2009. p. 102–13. https://doi.org/10.1007/978-3-642-03298-1_8.
10. Castañeda LF, Knapp E, Rodríguez-Henríquez F. Faster hashing to $\mathbb{G}_2$. In: Selected areas in cryptography. 2011. p. 412–30. https://doi.org/10.1007/978-3-642-28496-0_25.
11. Budroni A, Pintore F. Hashing to G2 on BLS pairing-friendly curves. ACM Commun Comput Algebra. 2018;52(3):63–6. https://doi.org/10.1145/3313880.3313884.
12. Scott M, Guillevic A. A new family of pairing-friendly elliptic curves. 2018. p. 43–57. https://doi.org/10.1007/978-3-030-05153-2_2.
13. Olivos J. On vectorial addition chains. J Algorithms. 1981;2:13–21.
14. Galbraith S, Scott M. Exponentiation in pairing-friendly groups using homomorphisms. In: Pairing-based cryptography—pairing. Berlin: Springer; 2008. p. 211–24.
15. Paulus S. Lattice basis reduction in function fields. In: Buhler JP, editor. Algorithmic number theory. Berlin: Springer; 1998. p. 567–75.
16. Mrabet NE, Joye M. Guide to pairing-based cryptography. Chapman and Hall/CRC cryptography and network security 2016.