Explicit Formulas of Shallue & van de Woestijne Encoding

Armando Faz-Hernández

Cloudflare Inc.

Abstract

This document shows explicit formulas for the construction proposed by Andrew Shallue and Christiaan van de Woestijne (SW) [1]. We follow the Fouque-Tibouchi [2] approach for deriving formulas for SW map without loss of generality.

1 Definitions

Assume $\mathbb{F}$ is a finite field of characteristic larger than 5.

Let $E_{A,B}$ be an elliptic curve in short Weierstrass form:

$$E/\mathbb{F}\colon y^2 = f(x) = x^3 + Ax + B \tag{1}$$

where $4A^3 + 27B^2 \neq 0$.

Let $V_{A,B}$ be an algebraic threefold defined as:

$$V/\mathbb{F}\colon {x_4}^2 = f(x_1)f(x_2)f(x_3) \tag{2}$$

Let $S_{A,B}$ be a surface defined as:

$$S/\mathbb{F}\colon \lambda^2 h(u,v) = -f(u) \tag{3}$$

where $h(u,v) = u^2 + uv + v^2 + A$.

Let $C_{a,b,c}$ be a non-degenerate curve defined as:

$$C/\mathbb{F}\colon az^2 + bw^2 = c \tag{4}$$

such that $a, b, c \neq 0$. Given the point $(z_0 = \sqrt{\frac{c}{a}}, 0) \in C$, such that $\frac{c}{a}$ is a QR, the parametrization of the points on C on variable t is given as:

$$(z(t), w(t)) = \left(z_0 + tw(t), -\frac{2az_0t}{at^2+b}\right) \tag{5}$$

Proof on Appendix A.

1.1 Mappings

SW proved there exists a rational map that given a point in S obtains a point in V.

$$\begin{aligned}\psi\colon S &\to V \\ (u,v,\lambda) &\mapsto (x_1,x_2,x_3,x_4) = \left(v, -u-v, u+\lambda^2, \frac{f(u+\lambda^2)h(u,v)}{\lambda}\right)\end{aligned} \tag{6}$$

This map is proved for any point $(u, v, \lambda) \in S$ such that $f(u) \neq 0$, which implies that $\lambda \neq 0$ and $h(u, v) \neq 0$.

SW also showed how to construct a point in S by transforming S into a conic C for which, a parametrization on variable t is easy to find. Then,

$$\begin{aligned} \phi\colon \mathbb{F} &\to S \\ t &\mapsto (u, v(t), \lambda(t)) \end{aligned} \tag{7}$$

for some fixed u such that $f(u) \neq 0$.

2 Mathematical Construction

The mapping $\overbrace{\mathbb{F} \to C \to}^{\phi} S \xrightarrow{\psi} V$ gives a point in $t \mapsto \psi(\phi(t)) = (x_1, x_2, x_3, x_4) \in V$. Then, it is guaranteed that exists $i \in \{1, 2, 3\}$ such that $(x_i, y = \sqrt{f(x_i)}) \in E$ is a point on the elliptic curve.

Note 1. The composition of each rational map require some conditions to hold.

Note 2. There are different ways to convert S into $C_{a,b,c}$.

Note 3. The sign of y must be explicitly chosen.

3 Explicit Formulas

The purpose of this section is to obtain explicit formulas for $t \mapsto \psi(\phi(t)) = (x_1, x_2, x_3, x_4) \in V$. First, we need to determine a, b, c of a curve $C_{a,b,c}$ given S. Second, we will obtain the explicit parametrization of $(z(t), w(t)) \in C$. And finally, we will get formulas for $\psi(\phi(t)) \in V$.

We followed the same approach as Fouque-Tibouchi [2] (FT) for converting S into a conic C due to two reasons. It is expected that our derivation leads to the same formulas as the ones of FT when they are instantiated with a BN curve; and, the FT paper already includes a detailed analysis of the image size of the map and the proofs that this encoding is admissible, which is required to get indifferentiability.

3.1 Defining ϕ

Let S as above, and fix $u \in \mathbb{F}$ as a variable subject to some restrictions given in the course of this description. Let's manipulate S to transform it to a conic C.

$$\begin{aligned} \lambda^2(u^2 + uv + v^2 + A) &= -f(u) \\ \lambda^2\left(\frac{3}{4}u^2 + \left(v + \frac{u}{2}\right)^2\right) &= -f(u) - A\lambda^2 \end{aligned}$$

Define $z = v + \frac{u}{2}$ and $w = \frac{1}{\lambda}$, and replace them into the previous equation.

$$\begin{aligned} \lambda^2\left(\frac{3}{4}u^2 + z^2\right) &= -f(u) - A\lambda^2 \\ \frac{3}{4}u^2 + z^2 &= -\frac{f(u)}{\lambda^2} - A \\ z^2 + f(u)w^2 &= -\left(\tfrac{3}{4}u^2 + A\right) \end{aligned}$$

Hence, we have the shape of a curve C with coefficients $a = 1$, $b = f(u)$, and $c = -\left(\frac{3}{4}u^2 + A\right)$. We want that C be non-degenerated $(a, b, c \neq 0)$, so $f(u) \neq 0$ and $3u^2 + 4A \neq 0$.

At this point, we have an explicit conic C. Now, we want to derive a parametrization of their points. To do that, we know there exists a point $(z_0 = \sqrt{\frac{c}{a}}, 0) \in C$, iff $\frac{c}{a}$ is a QR. Thus, define $z_0 = \sqrt{-\left(\frac{3}{4}u^2 + A\right)} = \frac{1}{2}\sqrt{-(3u^2 + 4A)}$ and we must guarantee that there exists a u such that $-(3u^2 + 4A)$ is a QR.

The parametrization of C is given as: $(z(t), w(t)) = \left(z_0 + tw(t), -\frac{2az_0t}{at^2+b}\right)$, where

$$
\begin{aligned}
w(t) &= -\frac{2z_0t}{t^2 + f(u)} \\
z(t) &= z_0 - \frac{2z_0t^2}{t^2 + f(u)}
\end{aligned}
$$

Now, lets derive the explicit map ϕ, which sends $t \mapsto (u, v(t), \lambda(t))$ to a point in S. We know that $z = v + \frac{u}{2}$ and $w = \frac{1}{\lambda}$, lets solve these equations for $v(t)$ and $\lambda(t)$.

$$
\begin{aligned}
v(t) &= z(t) - \frac{u}{2} = z_0 - \frac{2z_0t^2}{t^2 + f(u)} - \frac{u}{2} = -\frac{u}{2} - z_0\left(\frac{t^2 - f(u)}{t^2 + f(u)}\right) \\
\lambda(t) &= \frac{1}{w(t)} = -\frac{t^2 + f(u)}{2z_0t}
\end{aligned}
$$

At this point, we require that both maps be defined, hence, we have:

- $v(t)$ is defined when $t^2 + f(u) \neq 0$.
- Since $t^2 + f(u) \neq 0$, then $\lambda(t) \neq 0$.
- $\lambda(t)$ is defined when $2z_0t \neq 0$: We already know $z_0 \neq 0$. So, we require $t \neq 0$.

3.2 Defining $\psi \circ \phi$

Now, lets derive the explicit map $\psi \circ \phi$, which sends $t \mapsto (x_1(t), x_2(t), x_3(t), x_4(t)) \in V$ to a point in the treefold.

$$
\begin{aligned}
x_1(t) &= -\frac{u}{2} - z_0\left(\frac{t^2 - f(u)}{t^2 + f(u)}\right) \\
x_2(t) &= -u - x_1 \\
x_3(t) &= u + \frac{1}{4{z_0}^2}\frac{\left(t^2 + f(u)\right)^2}{t^2}
\end{aligned}
\tag{8}
$$

These equations gives three candidates to be the x-coordinate of a point on E, where the unique restrictions in the parameter t are $t^2 + f(u) \neq 0$ and $t \neq 0$.

3.3 Solving the Map Exceptions

There exist some values t such that violates the blue restrictions. However, we want the hashing works for any $t \in \mathbb{F}$. To remedy that, we rely on the function

$$
\begin{aligned}
\texttt{inv0}\colon \mathbb{F} &\to \mathbb{F} \\
x &\mapsto 1/x \\
0 &\mapsto 0
\end{aligned}
\tag{9}
$$

Then, we can apply `inv0` on the calculation of x_i, and observe its behaviour under all combinations of blue restrictions:

$t^2 + f(u) = 0$	$t \neq 0$	$x_1(t) = x_2(t) = -\frac{u}{2}\,,\ x_3(t) = u$
$t^2 + f(u) \neq 0$	$t = 0$	$x_1(t) = -\frac{u}{2} + z_0\,,\ x_2(t) = -\frac{u}{2} - z_0\,,\ x_3(t) = u$
$t^2 + f(u) = 0$	$t = 0$	Can't happen, since $f(u) \neq 0$.

Also, it is easy to show that $f(-\frac{u}{2} + z_0) = f(u)$. Hence, by choosing u such that $f(u)$ is a QR, it always returns a point in the curve for any $t \in \mathbb{F}$.

4 SW Algorithm

4.1 Requirements

Given an elliptic curve $E_{A,B}/\mathbb{F}$, find u under the following restrictions:

- $f(u)$ is a non-zero QR.
- $-(3u^2 + 4A)$ is a non-zero QR.

4.2 Constants

Once such a u was found, precompute the following constants.

- $c_0 = -u/2$
- $c_1 = f(u) = u^3 + Au + B$
- $c_2 = -z_0 = -\frac{1}{2}\sqrt{-\left(3u^2 + 4A\right)}$
- $c_3 = \dfrac{1}{4{z_0}^2}$

4.3 Implementation

Assuming these are operations on $\mathbb{F}$:

- $\mathbf{M}$ = multipication
- $\mathbf{S}$ = squaring
- $\mathbf{A}$ = addition/subtraction
- $\mathbf{I}$ = Inverse
- $\mathbf{E}$ = Exponentiation
- $\mathbf{L}$ = Legendre symbol
- $\mathbf{R}$ = square-root

The implementation of SW map takes $1\mathbf{I}+2\mathbf{L}+1\mathbf{R}+10\mathbf{M}+5\mathbf{S}+9\mathbf{A}$ field operations, which is around $4\mathbf{E}$ field exponentiations.

Algorithm 1 SW Map

Ensure: $t \in \mathbb{F}$
Require: $(x, y) \in E_{A,B}/\mathbb{F}$

$t_0 \leftarrow t^2$
$t_1 \leftarrow t_0 + c_1$
$t_2 \leftarrow t_0 - c_1$
$t_3 \leftarrow t_0 \times t_1$
$t_4 \leftarrow \mathrm{inv0}(t_3)$
$x_1 \leftarrow c_0 + c_2 \times t_2 \times t_4 \times t_0$
$x_2 \leftarrow -u - x_1$
$x_3 \leftarrow u + c_3 \times {t_1}^2 \times t_4 \times t_1$
$f_1 \leftarrow x_1 \times ({x_1}^2 + A) + B$
$f_2 \leftarrow x_2 \times ({x_2}^2 + A) + B$
$f_3 \leftarrow x_3 \times ({x_3}^2 + A) + B$
$b_1 \leftarrow 0\,,\ b_2 \leftarrow 0\,,\ s \leftarrow 0$
if f_1 is QR **then**
  $b_1 \leftarrow 1$
end if
if f_2 is QR **then**
  $b_2 \leftarrow 1$
end if
$x \leftarrow \textsc{cmov}(x_3, x_2, b_2)$
$x \leftarrow \textsc{cmov}(x, x_1, b_1)$
$f \leftarrow \textsc{cmov}(f_3, f_2, b_2)$
$f \leftarrow \textsc{cmov}(f, f_1, b_1)$
$y \leftarrow \sqrt{f}$
if $\mathrm{sgn0}(t) \neq \mathrm{sgn0}(y)$ **then**
  $s \leftarrow 1$
end if
$y \leftarrow \textsc{cmov}(-y, y, s)$
return (x, y)

5 Examples

5.1 BN Curves

Setting $u = 1$ for BN curves leads to Fouque-Tibouchi [2] original formulas.

References

[1] A. Shallue and C. E. van de Woestijne, "Construction of rational points on elliptic curves over finite fields," in *Algorithmic Number Theory* (F. Hess, S. Pauli, and M. Pohst, eds.), (Berlin, Heidelberg), pp. 510–524, Springer Berlin Heidelberg, 2006.

[2] P.-A. Fouque and M. Tibouchi, "Indifferentiable hashing to barreto–naehrig curves," in *Progress in Cryptology – LATINCRYPT 2012* (A. Hevia and G. Neven, eds.), (Berlin, Heidelberg), pp. 1–17, Springer Berlin Heidelberg, 2012.

A Parametrizing a Conic

We want to find a parametrization of the points on C on variable t. To do that, we intersect a line passing through (z_0, w_0), this line has equation:

$$z = t(w - w_0) + z_0 \tag{10}$$

with the slope t. It is clear that $(z_0 = \sqrt{\frac{c}{a}}, 0) \in C$ is a point as long as $\frac{c}{a}$ be a QR. Then, the line equation passing through $(z_0, 0)$ is $z = z_0 + tw$.

Now, we substitute z into C equation as follows:

$$\begin{aligned} az^2 + bw^2 &= c \\ a(z_0 + tw)^2 + bw^2 - c &= 0 \\ az_0{}^2 + 2az_0tw + t^2w^2 + bw^2 - c &= 0 \end{aligned}$$

Solving this equation for w, we have:

$$\begin{aligned} az_0{}^2 + 2az_0tw + at^2w^2 + bw^2 - c &= 0 \\ w(at^2w + bw + 2az_0t) - c + az_0{}^2 &= 0 \\ w(at^2w + bw + 2az_0t) &= 0 \\ w(w(at^2 + b) + 2az_0t) &= 0 \end{aligned}$$

hence $w = 0$ or $w = -\dfrac{2atz_0}{at^2 + b}$. Finally, we have that

$$(z(t), w(t)) = \left(z_0 + tw(t), -\frac{2atz_0}{at^2 + b}\right) \in C \tag{11}$$

for $z_0 = \sqrt{\frac{c}{a}}$ be a QR.