

# An explicit, generic parameterization for the Shallue–van de Woestijne map

Riad S. Wahby

Stanford University  
[rsw@cs.stanford.edu](mailto:rsw@cs.stanford.edu)

## 1 Introduction

In this note, we derive an explicit mapping based on the work of Shallue and van de Woestijne [SvdW06] that can be applied to essentially any elliptic curve whose base field has odd characteristic. Our derivation is similar to the one described by Fouque and Tibouchi [FT10], but applies more generally. In particular, because the work of Fouque and Tibouchi focuses only on pairing-friendly curves in the Barreto-Naehrig family [BN06], it is restricted to curves  $E(\mathbb{F}_p) : y^2 = x^3 + b$  satisfying  $p \equiv 1 \pmod{3}$ . In contrast, the mapping given in this note applies to essentially any curve  $E(\mathbb{F}) : y^2 = x^3 + ax + b$  that is non-singular (i.e.,  $4a^3 + 27b^2 \neq 0 \in \mathbb{F}$ ) and whose base field  $\mathbb{F}$  satisfies  $\#\mathbb{F} > 5$ .

This note owes a textual debt to [WB19], particularly in the description of the background and notation. For a brief survey of related work, see Section 1.1 of that paper.

## 2 Background

**Notation.** We write  $E(\mathbb{F})$  for the group (in multiplicative notation) of rational points on elliptic curve  $E$  over field  $\mathbb{F}$ ; this group’s order is  $\#E(\mathbb{F})$ .

$\text{Inv}_0(\alpha)$  returns 0 if  $\alpha = 0$ , else it returns  $\alpha^{-1} \in \mathbb{F}$ .

$\text{Sgn}_0(\beta)$  is a function that returns the “sign” of  $\beta$ . For  $\beta \in \mathbb{F}_p$ , let  $\text{Sgn}_0(\beta) = -1$  if  $\beta > (p-1)/2$ , and 1 otherwise. For extensions of  $\mathbb{F}_p$ ,  $\text{Sgn}_0$  generalizes in a natural way.

We regard the square root in  $\mathbb{F}$  as a function, so we fix a canonical representation, namely,  $\beta \triangleq \sqrt{\alpha} \in \mathbb{F}$  such that  $\text{Sgn}_0(\beta) = 1$ .

### 2.1 The Shallue–van de Woestijne map

For any elliptic curve  $E(\mathbb{F}) : y^2 = f(x) = x^3 + ax + b$ ,  $\#\mathbb{F} > 5$ , Shallue and van de Woestijne give a map from  $L \subseteq \mathbb{F}$  to the curve  $E(\mathbb{F})$  [SvdW06]. They observe, generalizing and simplifying the result of Skalba [Ska05], that for any rational point on the threefold

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

such that  $x_4 \neq 0$ , at least one of  $f(x_j), j \in \{1, 2, 3\}$  must be a square. This implies that one of the  $x_j$  is the  $x$ -coordinate of a rational point on  $E(\mathbb{F})$ .

To construct a rational point on  $V(\mathbb{F})$ , the authors define the surface  $S(\mathbb{F})$  and the rational map  $\phi_1 : S(\mathbb{F}) \mapsto V(\mathbb{F})$ , which is invertible on its image [SvdW06, Lemma 6]:

$$S(\mathbb{F}) : y^2(u^2 + uv + v^2 + a) = -f(u)$$

$$\phi_1 : (u, v, y) \mapsto \left( v, -u - v, u + y^2, f(u + y^2) \cdot \frac{y^2 + uv + v^2 + a}{y} \right).$$

Next, the authors observe [SvdW06, Lemma 7] that fixing  $u = u_0$  satisfying  $f(u_0) \neq 0$  and  $3u_0^2 + 4a \neq 0$  specializes  $S(\mathbb{F})$  to a curve that is birational to a conic with a rational parameterization. This gives a rational map  $\phi_2 : \mathbb{A}^1 \mapsto S(\mathbb{F})$  that is invertible on its image.

Putting it all together, define  $L = \{t \in \mathbb{F} : \phi_1(\phi_2(t)) \text{ is defined}\}$ . Then, to map  $t \in L$  to  $E(\mathbb{F})$ , first compute  $\phi_1(\phi_2(t))$ , which is a rational point  $(x_1, x_2, x_3, x_4)$  on  $V(\mathbb{F})$ , so at least one  $f(x_j), j \in \{1, 2, 3\}$  is square. Choose the smallest  $j$  where this is the case, compute the corresponding  $y$ -coordinate, and return  $(x_j, y)$ .

### 3 A generic parameterization

We now give a generic Shallue–van de Woestijne mapping (§2.1) for the elliptic curve  $E(\mathbb{F}) : y^2 = f(x) = x^3 + ax + b$ . To begin, we work with  $S(\mathbb{F})$  generically in terms of  $u = u_0$ ; we discuss how to choose  $u_0$  below. Rewriting as in [SvdW06, Lemma 7]:

$$y^2 \left( \frac{3}{4}u_0^2 + \left(v + \frac{u_0}{2}\right)^2 \right) = -f(u_0) - ay^2$$

$$\frac{z^2}{f(u_0)} + w^2 = -\frac{3u_0^2 + 4a}{4f(u_0)} \quad \text{where } z = v + \frac{u_0}{2}, \quad w = \frac{1}{y}$$

If  $u_0$  is chosen such that the RHS is square, a solution to the above equation is given by  $(z_0, w_0) \triangleq (0, \sqrt{-(3u_0^2 + 4a)/(4f(u_0))})$ . Setting  $w = w_0 + tz$  and substituting yields

$$2tw_0f(u_0) + (1 + t^2f(u_0))z = 0 \quad z \neq 0$$

$$z = -\frac{2tw_0f(u_0)}{1 + t^2f(u_0)}$$

$$w = w_0 + tz = w_0 \frac{1 - t^2f(u_0)}{1 + t^2f(u_0)}$$

Solving for  $y$  and  $v$ ,

$$y = \frac{1}{w} = \frac{1}{w_0} \cdot \frac{1 + t^2f(u_0)}{1 - t^2f(u_0)}$$

$$v = z - \frac{u_0}{2} = -\frac{u_0}{2} - \frac{2tw_0f(u_0)}{1 + t^2f(u_0)}$$

Finally, from the map  $\phi_1$  (§2.1), we have

$$x_1 = v = -\frac{u_0}{2} - \frac{2tw_0f(u_0)}{1 + t^2f(u_0)}$$

$$x_2 = -u_0 - v = -\frac{u_0}{2} + \frac{2tw_0f(u_0)}{1 + t^2f(u_0)}$$

$$x_3 = u_0 + y^2 = u_0 + \left( \frac{1}{w_0} \cdot \frac{1 + t^2f(u_0)}{1 - t^2f(u_0)} \right)^2$$

This map is undefined when  $t^2f(u_0) = \pm 1$ . To handle this case, we start by applying Montgomery's trick [Mon87], i.e., evaluating the above map in one inversion by computing  $\alpha = \text{Inv}_0((1 + t^2f(u_0))(1 - t^2f(u_0)))$ ; then  $1/(1 \pm t^2f(u_0)) = \alpha(1 \mp t^2f(u_0))$ . In the exceptional cases both inverses are 0, so  $x_1 = x_2 = -u_0/2$  and  $x_3 = u_0$ . Thus, if  $u_0$  is chosen such that  $f(u_0)$  or  $f(-u_0/2)$  is square in  $\mathbb{F}$ , the map will be exception-free, i.e., it will return a point on the curve for any  $t \in \mathbb{F}$ .

**Putting it all together.** Fix  $u_0$  such that  $f(u_0) \neq 0 \in \mathbb{F}$ ,  $-(3u_0^2 + 4a)/(4f(u_0))$  is a nonzero square in  $\mathbb{F}$ , and  $f(u_0)$  or  $f(-u_0/2)$  is square in  $\mathbb{F}$ . On input  $t \in \mathbb{F}$ , evaluate the  $x_j$  with Montgomery's trick and  $\text{Inv}_0(\cdot)$ . Finally, compute the result as follows:

$$(x, y) = \begin{cases} \left( x_1, \sqrt{f(x_1)} \cdot \text{Sgn}_0(t) \right) & \text{if } f(x_1) \text{ is square } \in \mathbb{F}; \text{ else} \\ \left( x_2, \sqrt{f(x_2)} \cdot \text{Sgn}_0(t) \right) & \text{if } f(x_2) \text{ is square } \in \mathbb{F}; \text{ else} \\ \left( x_3, \sqrt{f(x_3)} \cdot \text{Sgn}_0(t) \right) & \text{otherwise} \end{cases}$$

Note that by the definition of  $\sqrt{\cdot}$  in Section 2, the above ensures that  $\text{Sgn}_0(y) = \text{Sgn}_0(t)$ .

**Does a suitable  $u_0$  exist?** We show that, under a seemingly mild assumption, a suitable  $u_0$  exists with overwhelming probability for any curve of cryptographic interest.

Consider that case that  $a \neq 0$ . Then  $u_0$  meets all requirements if  $f(u_0)$  and  $-3u_0^2 - 4a$  are nonzero squares. Consider the sets  $U \triangleq \{u_0 : f(u_0) \text{ is a nonzero square } \in \mathbb{F}\}$  and  $V \triangleq \{-3u_0^2 - 4a : u_0 \in U\}$ . Because  $f(\cdot)$  has degree 3,  $|U|$  is a constant fraction of  $\#\mathbb{F}$ ; similarly, by the definition of  $V$ ,  $|V|$  is a constant fraction of  $|U|$ , and thus of  $\#\mathbb{F}$ . If any element of  $V$  is a nonzero square in  $\mathbb{F}$ , the corresponding value of  $u_0$  is suitable by construction. Under the assumption that  $\Pr[-3u_0^2 - 4a \text{ is square } \in \mathbb{F}]$  is independent of  $\Pr[f(u_0) \text{ is square } \in \mathbb{F}]$ , with overwhelming probability a suitable  $u_0$  exists: half of the elements of  $\mathbb{F}$  are square, and thus the probability that  $V$  does not contain a square is  $2^{-|V|}$ , which is at worst polynomially smaller than  $2^{-\#\mathbb{F}}$ .

Next, consider the case that  $a = 0$  and  $\mathbb{F} \triangleq \mathbb{F}_p, p \equiv 2 \pmod{3}$ . The condition on  $p$  guarantees that  $-3$  is nonsquare in  $\mathbb{F}_p$ , so  $u_0$  must be chosen such that  $f(u_0)$  is nonzero and nonsquare in  $\mathbb{F}_p$  in order to satisfy the condition that  $-3u_0^2/4f(u_0)$  is square in  $\mathbb{F}_p$ . Consider the sets  $S \triangleq \{u_0 : f(u_0) \text{ is a nonzero nonsquare } \in \mathbb{F}_p\}$  and  $T \triangleq \{f(-u_0/2) : u_0 \in S\}$ . By an argument similar to the above,  $|T|$  is a constant fraction of  $\#\mathbb{F}_p$ . If any element of  $T$  is a nonzero square in  $\mathbb{F}_p$ , the corresponding value of  $u_0$  is suitable by construction. Under the assumption that  $\Pr[f(-u_0/2) \text{ is square } \in \mathbb{F}_p]$  is independent of  $\Pr[f(u_0) \text{ is nonsquare } \in \mathbb{F}_p]$ , with overwhelming probability a suitable  $u_0$  exists.

Finally, consider the case that  $a = 0$  and  $\mathbb{F} \triangleq \mathbb{F}_p, p \equiv 1 \pmod{3}$ . The condition on  $p$  guarantees that  $-3$  is square in  $\mathbb{F}_p$ , so any  $u_0$  such that  $f(u_0)$  is square in  $\mathbb{F}_p$  is suitable.

We note that the assumptions stated above appear to be true in practice, but to our knowledge they are not easily proved.

## Acknowledgments

We thank Armando Faz-Hernández for helpful comments.

## References

- [BN06] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *SAC 2005*, volume 3897 of *LNCS*, pages 319–331. Springer, Heidelberg, August 2006.
- [FT10] Pierre-Alain Fouque and Mehdi Tibouchi. Estimating the size of the image of deterministic hash functions to elliptic curves. In Michel Abdalla and Paulo S. L. M. Barreto, editors, *LATINCRYPT 2010*, volume 6212 of *LNCS*, pages 81–91. Springer, Heidelberg, August 2010.
- [Mon87] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, 48(177):243–264, 1987.

- [Ska05] Mariusz Skalba. Points on elliptic curves over finite fields. *Acta Arithmetica*, 117(3):293–301, 2005.
- [SvdW06] Andrew Shallue and Christiaan E. van de Woestijne. Construction of rational points on elliptic curves over finite fields. In *Algorithmic Number Theory Symposium*, July 2006.
- [WB19] Riad S. Wahby and Dan Boneh. Fast and simple constant-time hashing to the BLS12-381 elliptic curve. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(4), 2019. Preprint: <https://ia.cr/2019/403>.