Comparing Various Elliptic Curve Addition Optimization Techniques Using Endomorphisms

Skyler Bistarkey-Rez
sdb@ucsb.edu

12 June 2018

Abstract

The scalar point multiplication is the central operation used in Elliptic Curve cryptography, and consists of several chained point additions or doublings. Considering that a point addition is a fairly costly operation, when aiming for efficiency, it is the goal to reduce either the number of additions required for a multiplication, the cost of a single addition, or both. This paper will survey and briefly compare various endomorphism-based techniques used to optimize point multiplication by reducing the total number of point operations required.

1 Introduction

When discussing Elliptic Curves, endomorphisms are functions that map from one point on an elliptic curve to another point on the same curve in a deterministic fashion [1]. The endomorphisms that will be examined in this paper will take the form $\phi : E \to E$, to represent a mapping from a curve definition to the same curve definition. While the described endomorphisms will vary based on the properties of the curves and fields over which the curves are defined, they all have the common effect of transforming a given point in a predictable fashion such that the number of total point additions required for a point multiplication is greatly reduced.

While there are many different representations of Ellipitic Curves, this paper will focus on three specific ones: Koblitz curves, Twisted Edwards curves, and Short Weierstrass curves. The first representation that will be discussed, *Koblitz curves*, were originally introduced by Neil Koblitz as anomalous binary curves [2]. Koblitz curves take the form

$$E : y^2 + xy = x^3 + ax^2 + 1$$

and, unlike the other curves that will be discussed in this paper, will be defined over the field $GF(2^k)$ for some integer k rather than $GF(p)$ for some prime p. This requires representing elements in polynomial basis or normal basis rather than integer basis, which can make arithmetic slightly more complex [8].

The second representation of elliptic curves for which endomorphisms will be discussed are known as Edwards curves, namely *Twisted Edwards curves*. An Edwards curve is a curve of the form

$$E : ax^2 + y^2 = 1 + dx^2y^2$$

and it becomes a twisted Edwards curve when $ad(a - d) \neq 0$ [3]. These curves will be defined over the field $GF(p)$ for some large prime number p, allowing the use of traditional arithmetic instructions when performing operations on elements.

The final representation of Elliptic Curves that will be discussed are known as *Short Weierstrass* curves. These curves have the form

$$E : y^2 = x^3 + ax + b$$

and the only constraint on the above equation is that the characteristic is not 2 or 3 [7]. This opens the above equation up to a wide variety of a and b values, many of which have now been standardized. Much like the Twisted Edwards curves above, these will be defined over the field $GF(p)$ for some large prime number p, simplifying arithmetic instructions slightly.

2 Koblitz Curves and the Frobenius Endomorphism

Koblitz describes his class of curves as the curves over $GF(q)$ such that the map $\tau : (x, y) \rightarrow (x^q, y^q)$ (known as the Frobenius endomorphism) satisfies the characteristic equation $T^2 - T + q = 0$ [2]. Koblitz focuses on the case in which $q = 2^k$, as this allows the Frobenius endomorphism to now become $\tau : (x, y) \rightarrow (x^{2^k}, y^{2^k})$. The reason that this is important is that curve points over $GF(2^k)$ can be represented in normal basis form with the binary vectors $\overrightarrow{x}$, $\overrightarrow{y}$.

From there, a squaring a point in $GF(2^k)$ just becomes a rotation of the bits to the left [8]. Therefore, computing $\tau(P)$ is as simple as performing a k-bit left rotation for each binary vector $\overrightarrow{x}$, $\overrightarrow{y}$ that make up P. Since any Koblitz curve E over $GF(2^k)$ satisfies the characteristic equation $T^2 - T + 2^k = 0$, this makes it simple to compute $[2^k]P$ for any point P on E with the following equation:

$$[2^k]P = \tau(P) - \tau^2(P)$$

Meaning that $[2^k]P$ can now be computed with only two bit rotations and one point addition. However, this method by itself is not immediately useful for computing $[n]P$ for any generic n.

This is where *τ-adic expansion* comes into play. Koblitz mentions that for the Frobenius map $\tau : (x, y) \rightarrow (x^2, y^2)$, τ can be represented as $\tau = (1 + \sqrt{-7}/2)$ [2]. From this, any natural number n can then be represented in τ base as follows:

$$n = \sum c_i \tau^i$$

Where $c_i \in \{0, 1\}$. Using this, any $[n]P$ can now instead be computed as $\sum c_i \tau^i(P)$, which potentially reduces the amount of overall additions required for a single multiplication. The specific amount will be analyzed in more detail in the subsequent section.

2.1 Advantage of the Frobenius Endomorphism and τ-adic Expansions

Koblitz initially presents his method in comparison to the generic binary method in order to demonstrate the issues present with the plain τ-adic method. Namely, he points to the curve $E : y^2 + xy = x^3 + x^2 + 1$ over the field $GF(8)$ and tries to perform the point multiplication for $[10]P$. Since this is equivalent to $[2][5]P$, the binary method would compute this as $2[P \oplus [4]P]$, which requires three additions. 5 is represented in τ-adic notation as $\tau^5 + \tau^2 + 1$, meaning that $[10]P = \tau^5(2P) \oplus \tau^2(2P) \oplus 2P$, also requiring three additions, demonstrating how the basic Frobenius endomorphism addition method is not necessarily more advantageous than the basic binary method [2].

However, Jerome Solinas examined this problem in an effort to improve efficiency of Frobenius endomorphism-based point multiplication chains. He demonstrated that not only does every n have a τ-adic form, but it also has a τ-adic NAF form [6], meaning that any n can be represented in the form:

$$n = \sum c_i' \tau^i$$

where now $c_i' \in \{-1, 0, 1\}$. As the amount of additions done for this point multiplication is directly equal to the amount of non-zero terms in the τ-adic form, it is important to consider the amount of non-zero terms that can be expected in both the original τ-adic representation and the τ-adic NAF representation.

Solinas points out that the non-zero τ-adic NAF density is directly related to the non-zero density of a normal NAF representation, meaning that the average density for τ-adic representations is approximately $\frac{1}{3}$ of the overall τ-adic NAF representation length [6]. Ideally, this would make τ-adic NAF much more efficient than normal NAF, as now doubling no longer needs to occur on terms with zero as a coefficient. However, τ-adic NAF tends to be twice as long as normal NAF, doubling the total number of additions and greatly reducing the benefit introduced by the Frobenius Endomophism with τ-adic NAF [6].

In order to remedy this loss of efficieny, Solinas proposed the reduced τ-adic NAF (RTNAF), which uses algorithm 1 to generate a number ρ for n such that, for any point P, $[\rho]P = [n]P$ under the τ-adic NAF based multiplication algorithm and ρ's τ-adic NAF representation is roughly half the length of n's.

Algorithm 1 Breaking n into Reduced τ-adic NAF

procedure RTNAF(n, k, τ) ▷ k is defined as the parameter used for $GF(2^k)$
  $\delta \leftarrow (\tau^k - 1)/(\tau - 1)$
  Return $\rho \leftarrow n \bmod \delta$.
end procedure

With this new form, the length of the τ-adic NAF returns to levels nearly equivalent to that of the normal NAF. Thus, the Frobenius endomorphism over Koblitz curves, when used with the reduced τ-adic NAF representation of an integer n of length m, can complete the point multiplication in only $m/3$ point additions on average [6].

3 Endomorphisms Over Twisted Edwards Curves

The endomorphism that will be used to improve efficiency on arithmetic over Twisted Edwards Curves is actually comprised of three endomorphisms chained together. The first endomorphism is valid over short Weierstrass curves of the form $E_s : y^2 = x^3 + a_s x + b_s$, and is as follows:

$$\phi(x, y) = \Big(\phi^{-2}\frac{f(x)}{g(x)}, y\phi^{-3}(\frac{f(x)}{g(x)})'\Big)$$

where ϕ is a complex number and f and g are polynomial functions that map from $\mathbb{Q}(\phi) \to \mathbb{Q}$ [3]. While this endomorphism initially does not seem applicable to Twisted Edwards curves, Liu *et al.* then present two more homomorphisms, no longer mapping between curves of the same type [3]. Instead, the first of these homomorphisms maps a point on a Twisted Edwards curve to a point on a Weierstrass curve, and the second maps a point on a Weierstrass curve to a point on a Twisted Edwards curves. The two homomorphisms are as follows, where $E_{a,d}$ represents a Twisted Edwards curve and E_s represents a short Weierstrass curve:

$$\begin{aligned}
\psi :& E_{a,d} \to E_s, \\
& (x_t, y_t) \to (x_s, y_s) = \Big(\frac{c_1(1+y_t)}{1-y_t} + c_2, \frac{c_1(1+y_t)}{x_t(1-y_t)}\Big) \\
\psi^{-1} :& E_s \to E_{a,d}, \\
& (x_t, y_t) \to (x_s, y_s) = \Big(\frac{x_s - c_2}{y_s}, \frac{x_s - c_3}{x_s + c_4}\Big)
\end{aligned}$$

where $c_1 = (a-d)/4$, $c_2 = (a+d)/6)$, $c_3 = (5a-d)/12$, and $c_4 = (a-5d)/12$ [3].

The above three homomorphisms can then be combined to be implemented as an endomorphism over Twisted Edwards curves ϕ_t defined as:

$$\phi_t : E_{a,d} \to E_{a,d}, (x_t, y_t) \to \psi^{-1}(\phi(\psi(x_t, y_t)))$$

While this may seem like a large amount of computation to do in order to perform one endomorphism, Liu *et al.* highlight the fact that choosing curve parameters intelligently (i.e., $a = -1, d = 1$) allows $\phi_t(x, y)$ to be reduced to

$$\phi_t(x, y) = (\alpha x, 1/y)$$

where α is the integer that satisfies $\alpha^2 + 1 = 0 \bmod p$, and p is the prime used for $GF(p)$ over which the curve is defined [3]. Now that the efficient endomorphism over a Twisted Edwards curve has been defined, the point multiplication $[k]P$ can be transformed into $[k_1]P \oplus [k_2]\phi_t(P)$, with each of k_1 and k_2 being approximately half the length of the original k.

The above is possible because the endomorphism $\phi_t(P)$ is equivalent to $[\lambda]P$, where λ satisfies a constraint based on the order of the curve over $GF(p)$. Specifically, λ can be evaluated as the value that satisfies $\lambda^2 + 1 = 0 \bmod r$, where r is the (prime) order of the point P being multiplied.

3.1 Computing k_1 and k_2

While the method above has the advantageous property that it can halve the number of point additions required, it also requires the computation of integers k_1, k_2 such that $k_1 + \lambda \cdot k_2 = k$, where both k_1 and k_2 are "short" compared to k. It is only then that the point multiplication $[k]P$ can be broken down into $[k_1]P + [k_2]\phi_t(P)$. These values can be computed with algorithm 2 presented by Gallant, Lambert, and Vanstone [4]. The reason the algorithm works is that it involves first finding two

Algorithm 2 Evenly Splitting k

procedure k-SPLIT(n, k, λ) ▷ Return k_1, k_2 such that $k_1 + k_2 \cdot \lambda = k \bmod n$
  Run $EEA(n, \lambda)$
  Receive from EEA a series of equations $s_i \cdot n + t_i \cdot \lambda = r_i$
  Find the greatest index m such that $r_m \geq \sqrt{n}$
  $v_1 \leftarrow (r_{m+1}, -t_{m+1})$
  if $|(r_m, -t_m)| < |(r_{m+2}, -t_{m+2})|$ **then**
    $v_2 \leftarrow (r_m, -t_m)$
  else
    $v_2 \leftarrow (r_{m+2}, -t_{m+2})$
  end if
  Solve for β_1, β_2 such that $(k, 0) = \beta_1 v_1 + \beta_2 v_2$
  $b_1 \leftarrow \lceil \beta_1 \rfloor, b_2 \leftarrow \lceil \beta_2 \rfloor$
  $(u_x, u_y) \leftarrow b_1 v_1 + b_2 v_2$
  return $k_1 \leftarrow u_x, k_2 \leftarrow u_y$
end procedure

vectors $v_1 = (v_x, v_y), v_2 = (w_x, w_y)$ such that $(v_x + \lambda v_y) = 0 \bmod n$ and $(w_x + \lambda w_y) = 0 \bmod n$. Since both of these vectors are obtained from the EEA at a maximal position, they are both guaranteed to be short. Then, using those to find a vector that is equal to $(k, 0)$ provides an x and y coordinate that are both shorter than k, and produce $x + \lambda y = 0 \bmod n$ [4].

4 Endomorphisms Over Short Weierstrass Curves

The endomorphisms over Short Weierstrass Curves, though much simpler than the chain of endomorphisms presented in section 3, are nevertheless employed in a very similar way. There are two in particular that are presented by Gallart, Lambert, and Vanstone that seem promising for improving efficiency of point multiplications, and act on different curves.

Firstly, consider the curve

$$E_1 : y^2 = x^3 + ax$$

defined the field $GF(p)$ for some large prime p. Then, select an element $\alpha \in GF(p)$ such that $\text{Order}(\alpha) = 4$. Then, for any point $P \in E_1$ (defined over $GF(p)$) of prime

order r, the following endomorphism holds:

$$\phi_1 : (x, y) \rightarrow (-x, \alpha y)$$

and is equivalent to computing the point multiplication $[\lambda]P$, where λ satisfies the equation $\lambda^2 + 1 = 0 \bmod r$ [4]. Note that although it is not explicitly stated, this is likely the same constraint on λ identified in [3].

However, should the short Weierstrass Curve have the form

$$E_2 : y^2 = x^3 + b$$

instead, then an element $\beta \in GF(p)$ can be selected such that Order$(\beta) = 3$. Then, for any point $P \in E_2$ (defined over $GF(p)$) of prime order r, the following endomorphism holds:

$$\phi_2 : (x, y) \rightarrow (\beta x, y)$$

and is equivalent to computing the point multiplication $[\lambda]P$, where λ satisfies the equation $\lambda^2 + \lambda + 1 = 0 \bmod r$ [4].

Since the parameters α and β are chosen based on the field over which the curve is defined, those elements can be included in the curve definition and as such would not need to be recomputed every time. Additionally, if the point P is held constant, or points with the same prime order r are chosen, then λ can be precomputed as well and incur no additional cost to point multiplication.

5 Efficiency Comparison

The efficiency of each endomorphism-based technique must be evaluated not only on the number of reduced point additions that results, but also how easy the endomorphism is to compute, as well as how many times it must be computed in performing a single point multiplication. Additionally, once the endomorphism is applied, it may or may not be eligible to apply other techniques on the remaining point addition chains, such as the w-width sliding window point addition algorithm.

For Koblitz curves, the initial τ-adic NAF representation of an integer k of length m does not offer many advantages from a normal NAF representation of k, since it doubles the length of k on average [6]. However, with Solinas' proposed reduced τ-adic NAF representation, the length of the τ-adic NAF becomes comparable to that of the normal NAF representation. Since it also is expected to contain approximately $m/3$ non-zero terms, and only has to perform point additions for non-zero terms, this method of point multiplication only has to perform $m/3$ additions on average, making it extremely efficient. One downside to Koblitz curves is that the normal basis representation complicates multiplication [8]. However, it greatly simplifies addition into a single bitwise XOR operation, and the multiplication algorithm is still order $O(n^2)$, meaning a low amount of efficiency is lost due to this [8].

For Twisted Edwards Curves, since α and λ are determined from curve parameters, these two integers can be precomputed and distributed with the curve, resulting in no additional overhead. The only overhead associated with the endomorphism is finding

k_1, k_2 for any integer k of length m, which involves a variety of steps (see algorithm 2), the longest of which is the Extended Euclidean Algorithm, which runs in $O(m)$ time [9]. Therefore, this method does not incur significant extra cost from computing k_1 and k_2. However, even efficient methods for performing the computation $[k_1]P+[k_2]Q$ using signed w-width NAF represetations of k_1 and k_2 and performing the addition in parallel [5] [4] would still require $m/2$ point doublings and $m/4$ point additions when combined with the double addition algorithm.

For Weierstrass curves, the same arguments hold for the Twisted Edwards Curves. However, though α and β are based on the curve for which the endomorphisms are defined, λ is based instead on the point of prime order on which the endomorphism is being performed. Since Liu *et al.* identify λ under similar constraints as Gallant, Lambert, and Vanstone, it is likely that both the Twisted Edwards endomorphism technique and the Short Weierstrass endomorphism techniques suffer from requiring a point of prime order, somewhat complicating the process of finding a suitable point [3] [4].

5.1 Comparison to Traditional Methods

Two of the best non-endomorphism-based algorithms for performing a point multiplication are the w-width NAF point multiplication, and the w-width sliding window algorithm. The w-width sliding window algorithm is expected to take $m - w$ point doublings and $(1-2^{-w})(m-w)/w$ point multiplications, while the w-width NAF point multiplication algorithm is expected to take $1+m$ doublings and $2^{w-2}-1+m/(w+1)$ point additions [7].

Therefore, while those two methods both allow for greatly reduced exponentiation over the basic binary method, they still end up with a total of well over m point operations. Meanwhile, the Koblitz Curve endomorphism technique is only expected to take $m/3$ point additions, and both the Twisted Edwards Curve and Weierstrass Curve endomorphisms are expected to take $3m/4$ total point operations. Thus, a large gain is seen in the case of Koblitz curves, and a still significant gain is seen for both Twisted Edwards Curves and Short Weierstrass Curves.

6 Conclusion

I have surveyed a total of three different categories of Elliptic Curves, each with their own endomorphisms. Of the techniques surveyed, the Frobenius Endomorphism applied to Koblitz Curve points over $GF(2^k)$ using reduced τ-adic NAF representation produces the most significant improvement. However, this requires normal basis conversion of points and may suffer from unoptimized hardware implementations. Endomorphisms applied to points on Twisted Edwards Curves over $GF(p)$ prove to simplify arithmetic, at the cost of many more point multiplications. The same can be said for Endomorphims applied to Short Weierstrass Curves over $GF(p)$. Considering the widespread use of Short Weierstrass Curves in Elliptic Curves Cryptography, such endomorphisms could be valuable to improve efficiency of preexisting cryptosystems.

References

[1] Pete Clark. Lectures on Shimura Curves 1: Endomorphisms of Elliptic Curves. `http://math.uga.edu/~pete/SC5-AlgebraicGroups.pdf`. University of Georgia.

[2] Neal Koblitz. CM-Curves with Good Cryptographic Properties. *Advances in Cryptology - Crypto '91*. Springer-Verlag (1992).

[3] Zhe Liu, Johann Großschädl, Zhi Hu, Kimmo Järvinen, Husen Wang, Ingrid Verbauwhede. Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things. *IEEE Transactions on Computers, Vol. 66, No. 5*. May 2017.

[4] Robert Gallant, Robert Lambert, Scott Vanstone. Faster point Multiplication on Elliptic Curves with Efficient Endomorphisms. *Advances in Cryptology - Crypto 2001*. 2001.

[5] Atsuko Miyaji, Takatoshi Ono, Henri Cohen. Efficient Elliptic Curve Exponentiation. *Information and Communications Security*. 1997.

[6] Jerome Solinas. Efficient Arithmetic on Koblitz Curves. *Designs, Codes and Cryptography, 19*. 2000.

[7] Çetin Kaya Koç. Lecture Slides on Cryptographic Engineering. `https://koclab.cs.ucsb.edu/teaching/cren/docx/` University of California, Santa Barbara. 2018.

[8] Chang Shu. Implementation of the Optimal Normal Basis Operations in Elliptic Curve Cryptography in VIVA.

[9] Amotz Bar-Noy. Finding the GCD. `http://www.sci.brooklyn.cuny.edu/~amotz/BC-ALGORITHMS/PRESENTATIONS/gcd.pdf`. City University of New York. 2012.