Endomorphisms for faster elliptic curve cryptography on general curves

Steven D. Galbraith*, Xibin Lin**, and Michael Scott* * *

[1] Mathematics Department,
Royal Holloway, University of London,
Egham, Surrey, TW20 0EX,
United Kingdom.
steven.galbraith@rhul.ac.uk

[2] School of Mathematics and Computational Science
Sun-Yat Sen University Guangzhou, 510275, P.R.China
linxibin@mail2.sysu.edu.cn

[3] School of Computing, Dublin City University.
Ballymun, Dublin 9, Ireland.
mike@computing.dcu.ie

Abstract. We present efficiently computable homomorphisms for general elliptic curves by working over quadratic extensions. This allows point multiplication to be accelerated using the Gallant-Lambert-Vanstone method. Our preliminary results give up to a 74 percent speedup for elliptic curve cryptography using general curves. Further speedups are possible when using special curves.

Keywords: elliptic curves, point multiplication, GLV method, isogenies.

1 Introduction

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and let $P \in E(\mathbb{F}_q)$ have order r. The fundamental operation in elliptic and hyperelliptic curve cryptography is point multiplication $[n]P$ where $n \in \mathbb{Z}$. There is a vast literature on efficient methods for computing $[n]P$ (a good reference is [2]).

The Gallant-Lambert-Vanstone method [8] is an important tool for speeding up point multiplication. The basic idea is as follows. If the elliptic curve E has a efficiently computable endomorphism ψ (other than a standard multiplication by n map) such that $\psi(P) \in \langle P \rangle$ then one can replace the computation $[n]P$ by the multiexponentiation $[n_0]P + [n_1]\psi(P)$ where $|n_0|, |n_1| \approx \sqrt{r}$. In principle this makes the computation $[n]P$ nearly twice as fast. In practice the speedup is not 100 percent, but is still very significant. Some examples allow higher degree decompositions such as $[n_0] + [n_1]\psi(P) + \cdots + [n_{m-1}]\psi^{m-1}(P)$ where $|n_i| \approx r^{1/m}$ which gives further speedups (though, for technical reasons such as the lack of an m-dimensional joint sparse form, one does not expect it to be m-times faster than the other best methods). We call the latter approach the m-dimensional GLV method.

Unfortunately, suitable efficiently computable endomorphisms have only been known in two cases, namely subfield curves (i.e., groups $E(\mathbb{F}_{q^m})$ where E is defined over $\mathbb{F}_q$; these do not have

* This work supported by EPSRC grant EP/D069904/1.

** This author thanks the Chinese Scholarship Council.

* * * This author acknowledges support from the Science Foundation Ireland under Grant No. 06/MI/006

prime or nearly prime order unless q is very small) and curves with special endomorphism structure (essentially, that the endomorphism ring has small class number). Hence, if one is using randomly chosen prime-order elliptic curves over finite fields for cryptography then the GLV method is not usually available.

This paper presents a new construction for efficiently computable endomorphisms which are suitable for the GLV method. Our technique applies to all elliptic curves and can be used with curves of prime order. The idea is somewhat analogous to subfield curves: We take elliptic curves E with $j(E) \in \mathbb{F}_q$ and consider the group $E(\mathbb{F}_{q^m})$. However a crucial difference is that E is defined over $\mathbb{F}_{q^m}$, not $\mathbb{F}_q$. This means it is possible to obtain curves of prime order and so there is no need to restrict attention to q being small. Our method can be used with any primes p and any elliptic curves E and always gives rise to a GLV method of dimension at least 2. Hence, it is not too misleading to say that our technique nearly doubles the speed of elliptic curve cryptosystems in large characteristic.

To put our results in perspective let us compare our contribution with the recent and very significant research of Bernstein and Lange on Edwards curves [4, 5]. The main contributions of Edwards curves are mathematical elegance and group operations which are particularly suitable for side-channel resistant implementation. From the narrower point of view of computational efficiency the contribution of Edwards (and variants such as twisted and inverted Edwards) coordinates is a speedup of (at best) 15 percent over previous methods, at the cost of a restriction to curves whose group order is divisible by 4. This restriction to non-prime order groups is serious: in many cryptographic applications it is essential for security that group elements lie in the correct prime order subgroup; testing subgroup membership can lead to a significant computational overhead in some applications (for more details see Section 4.3 of [11], [12]). Furthermore the need to test for small sub-group membership leaves open a door for mistakes by the non-expert implementor. Hence, for many applications it is clearly better to use elliptic curves of prime order.

In contrast, our results give up to a 74 percent speedup over previous implementations and can be applied to elliptic curves of prime order. For these reasons we believe that our results are a major breakthrough. Note however that our techniques can also be implemented on curves in Edwards form, and exploit their benefits.

We now give an outline of the paper. First we describe our new homomorphism and explain how it leads to a 2-dimensional GLV method for any elliptic curve. Section 3 gives a specific key generation algorithm which may be convenient for some applications. Section 4 shows how to get a 4-dimensional GLV method for $y^2 = x^3 + B$ over $\mathbb{F}_{p^2}$. Section 5 shows that our homomorphisms can also be used for curves written in Edwards form. Section 6 discusses the generalisation of our methods to higher genus curves. The proof of the pudding is the timings in Section 7. Section 8 discusses known security threats from using our construction and explains how to avoid them.

2 The homomorphism

We consider elliptic curves defined over any field $\mathbb{F}_q$ with point at infinity ∞. Recall that if E is an elliptic curve over $\mathbb{F}_q$ with $q + 1 - t$ points then one can compute the number of points $\#E(\mathbb{F}_{q^m})$ efficiently. For example, $\#E(\mathbb{F}_{q^2}) = q^2 + 1 - (t^2 - 2q) = (q + 1)^2 - t^2$. As usual we define

$$E(\mathbb{F}_{q^m})[r] = \{P \in E(\mathbb{F}_{q^m}) : [r]P = \infty\}.$$

When we say that a curve or mapping is 'defined over $\mathbb{F}_{q^k}$' we mean that the coefficients of the polynomials are all in $\mathbb{F}_{q^k}$. The implicit assumption throughout the paper is that when we say an object is defined over a field $\mathbb{F}_{q^k}$ then it is not defined over any smaller field, unless explicitly mentioned.

The following result gives our main construction. Novices can replace the word 'isogeny' with 'isomorphism', set $d = 1$ and replace $\hat{\phi}$ by ϕ^{-1} without any significant loss of functionality.

Theorem 1. *Let E be an elliptic curve defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = q + 1 - t$ and let $\phi : E \to E'$ be a separable isogeny of degree d defined over $\mathbb{F}_{q^k}$ where E' is an elliptic curve defined over $\mathbb{F}_{q^m}$ with $m \mid k$. Let $r \mid \#E'(\mathbb{F}_{q^m})$ be a prime such that $r > d$ and such that $r \| \#E'(\mathbb{F}_{q^k})$. Let π be the q-power Frobenius map on E and $\hat{\phi} : E' \to E$ be the dual isogeny of ϕ. Let*

$$\psi = \phi\pi\hat{\phi}.$$

Then

1. *$\psi \in End(E')$ (i.e., ψ is a group homomorphism).*
2. *For all $P \in E'(\mathbb{F}_{q^k})$ we have $\psi^k(P) - [d^k]P = \infty$ and $\psi^2(P) - [dt]\psi(P) + [d^2q]P = \infty$.*
3. *There is some $\lambda \in \mathbb{Z}$ such that $\lambda^k - d^k \equiv 0 \pmod{r}$ and $\lambda^2 - dt\lambda + d^2q \equiv 0 \pmod{r}$ such that $\psi(P) = [\lambda]P$ for all $P \in E'(\mathbb{F}_{q^m})[r]$.*

Proof. First note that $\hat{\phi}$ is an isogeny from E' to E and is defined over $\mathbb{F}_{q^k}$, that π is an isogeny from E to itself defined over $\mathbb{F}_q$, and that ψ is an isogeny from E to E' defined over $\mathbb{F}_{q^k}$. Hence ψ is an isogeny of E' to itself, and is defined over $\mathbb{F}_{q^k}$ (or a subfield). Therefore, ψ is a group homomorphism.

Since $\phi\hat{\phi} = d$ on E' it follows that

$$\psi^2 = \phi\pi\hat{\phi}\phi\pi\hat{\phi} = \phi\pi d\pi\hat{\phi} = d\phi\pi^2\hat{\phi}$$

and, by induction, $\psi^k = d^{k-1}\phi\pi^k\hat{\phi}$. For $P \in E'(\mathbb{F}_{q^k})$ we have $\hat{\phi}(P) \in E(\mathbb{F}_{q^k})$ and so $\pi^k(\hat{\phi}(P)) = \hat{\phi}(P)$. Hence $\psi^k(P) = [d^k]P$.

Similarly, writing $Q = \hat{\phi}(P)$ we have $\pi^2(Q) - [t]\pi(Q) + [q]Q = \infty$ and so $[d]\phi(\pi^2 - [t]\pi + [q])\hat{\phi}(P) = \infty$. Using the previous algebra, this implies

$$(\psi^2 - [dt]\psi + [qd^2])P = \infty.$$

Finally, let $P \in E'(\mathbb{F}_{q^m})$ have order r. Since $\psi(P) \in E'(\mathbb{F}_{q^k})$ also has order r and $r \| \#E'(\mathbb{F}_{q^k})$ it follows that $\psi(P) = [\lambda]P$ for some $\lambda \in \mathbb{Z}$. Clearly, $\psi([a]P) = [a]\psi(P) = [\lambda]([a]P)$ for all $a \in \mathbb{Z}$. Since $\psi^k(P) - [d^k]P = [\lambda^k]P - [d^k]P = \infty$ it follows that $\lambda^k - d^k \equiv 0 \pmod{r}$. Similarly, $\lambda^2 - dt\lambda + d^2q \equiv 0 \pmod{r}$. □

2.1 Special case of quadratic twists

We now give our general result, which applies to elliptic curves over $\mathbb{F}_p$. Our construction can of course be used for elliptic curves over fields of small characteristic, but it seems more natural to use subfield curves and Frobenius expansions in that case. Hence, for the remainder of the paper we focus on the case of characteristic $p > 3$.

Corollary 1. *Let $p > 3$ be a prime and let E be an elliptic curve over $\mathbb{F}_p$ with $p + 1 - t$ points. Let E' over $\mathbb{F}_{p^2}$ be the quadratic twist of $E(\mathbb{F}_{p^2})$, so that $\#E'(\mathbb{F}_{p^2}) = (p-1)^2 + t^2$. Write $\phi : E \to E'$ for the twisting isomorphism defined over $\mathbb{F}_{p^4}$. Let $r \mid \#E'(\mathbb{F}_{p^2})$ be a prime such that $r > 2p$ Let $\psi = \phi\pi\phi^{-1}$. For $P \in E'(\mathbb{F}_{p^2})[r]$ we have $\psi^2(P) + P = \infty$.*

Proof. Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_p$. We have $\#E(\mathbb{F}_{p^2}) = p^2 + 1 - (t^2 - 2p)$. Let $u \in \mathbb{F}_{p^2}$ be a non-square in $\mathbb{F}_{p^2}$, define $A' = u^2 A, B' = u^3 B$ and $E' : y^2 = x^3 + A'x + B'$. Then $\#E'(\mathbb{F}_{p^2}) = p^2 + 1 + (t^2 - 2p) = (p-1)^2 + t^2$. The isomorphism $\phi : E \to E'$ is defined by

$$\phi(x, y) = (ux, \sqrt{u}^3 y)$$

and is defined over $\mathbb{F}_{p^4}$.

If $r \mid \#E'(\mathbb{F}_{p^2})$ is prime such that $r > 2p$ then $r \nmid \#E(\mathbb{F}_{p^2})$ and so $r \| \#E'(\mathbb{F}_{p^4}) = \#E(\mathbb{F}_{p^2}) \#E'(\mathbb{F}_{p^2})$. Hence we may apply Theorem 1 to get that ψ is a group homomorphism such that $\psi(P) = \lambda P$ such that $\lambda^4 - 1 \equiv 0 \pmod{r}$ for $P \in E'(\mathbb{F}_{p^2})[r]$. We now show that, in fact, $\lambda^2 + 1 \equiv 0 \pmod{r}$.

By definition, $\psi(x, y) = (ux^p/u^p, \sqrt{u}^3 y^p / \sqrt{u}^{3p})$ where $u \in \mathbb{F}_{p^2}$ (i.e., $u^{p^2} = u$) and $\sqrt{u} \notin \mathbb{F}_{p^2}$ (and so, $\sqrt{u}^{p^2} = -\sqrt{u}$). If $P = (x, y) \in E'(\mathbb{F}_{p^2})$ then $x^{p^2} = x, y^{p^2} = y$ and so

$$\begin{aligned} \psi^2(x, y) &= (ux^{p^2}/u^{p^2}, \sqrt{u}^3 y^{p^2} / \sqrt{u}^{3p^2}) \\ &= (x, (-1)^3 y) \\ &= -P. \end{aligned}$$

This completes the proof. □

The above result applies to any elliptic curve over $\mathbb{F}_p$ (with $p > 3$) and shows that the 2-dimensional GLV method can be applied. Note that it is possible for $\#E'(\mathbb{F}_{p^2})$ to be prime, since E' is not defined over $\mathbb{F}_p$. One feature of this construction is that, since p is now half the size compared with using elliptic curves over prime fields, point counting is much faster than usual. Since we are dealing with elliptic curves over $\mathbb{F}_{p^2}$ where p is prime then Weil descent attacks are not a threat (see Section 8).

Corollary 2. *Let $p \equiv 5 \pmod{8}$ be a prime. Let notation be as in the previous corollary. Then one may choose*

$$\psi(x, y) = (-x^p, iy^p)$$

where $i \in \mathbb{F}_p$ satisfies $i^2 = -1$.

Proof. We have $4 \| (p-1)$ and $2 \| (p+1)$. Since 2 is not a square in $\mathbb{F}_p$ one can define $\mathbb{F}_{p^2} = \mathbb{F}_p(u)$ where $u = \sqrt{2}$. Note that $u^p = -u$ and that $u^{p-1} \equiv 2^{(p-1)/2} \equiv -1 \pmod{p}$. It follows that $u^{(p^2-1)/2} = -1$ and so u is not a square in $\mathbb{F}_{p^2}$.

Since -1 is a square in $\mathbb{F}_p$ the equation $x^4 = 1$ has solutions $x = 1, -1, i, -i \in \mathbb{F}_p$. Let $w \in \mathbb{F}_{p^4}$ satisfy $w^2 = u$. Note that $(w/w^p)^4 = 1$ and so $w^p = \pm iw$.

Finally, our homomorphism ψ is defined to be

$$\psi(x, y) = (ux^p/u^p, w^3 y^p / w^{3p}) = (-x^p, \pm iy^p).$$

Renaming i if necessary gives the result. □

An exercise for the reader is to show that if E is an elliptic curve over $\mathbb{F}_p$ and if E' over $\mathbb{F}_p$ is the quadratic twist of E then the map ψ of our construction satisfies $\psi(P) = -P$ for all $P \in E'(\mathbb{F}_p)$. Our homomorphism is therefore useless for the GLV method in this case.

2.2 Higher dimension decompositions

The GLV method can be generalised to m-dimensional decompositions $[n]P = [n_0]P + [n_1]\psi(P) + \cdots + [n_{m-1}]\psi^{m-1}(P)$ (for examples with $m = 4$ and $m = 8$ see [6]). Such a setting gives improved performance. As we have found 2-dimensional expansions using $E'(\mathbb{F}_{p^2})$ it is natural to try to get an m-dimensional decomposition using $E'(\mathbb{F}_{p^m})$.

In general, to obtain an m-dimensional decomposition it is required that ψ does not satisfy any polynomial equation on $E'(\mathbb{F}_{p^m})[r]$ of degree $< m$ with small integer coefficients. Note that ψ always satisfies a quadratic polynomial equation but that the coefficients are not necessarily small modulo r.

The following result gives a partial explanation of the behaviour of ψ on $E'(\mathbb{F}_{p^m})$.

Corollary 3. *Let $p > 3$ be a prime and let E be an elliptic curve over $\mathbb{F}_p$. Let E' over $\mathbb{F}_{p^m}$ be the quadratic twist of $E(\mathbb{F}_{p^m})$. Write $\phi : E \to E'$ for the twisting isomorphism defined over $\mathbb{F}_{p^{2m}}$. Let $r \mid \#E'(\mathbb{F}_{p^m})$ be a prime such that $r > 2p^{m/2}$ Let $\psi = \phi\pi\phi^{-1}$. For $P \in E'(\mathbb{F}_{p^m})[r]$ we have $\psi^m(P) + P = \infty$.*

Proof. As in Corollary 1, we have $r \| \#E'(\mathbb{F}_{p^{2m}}) = \#E'(\mathbb{F}_{p^m})\#E(\mathbb{F}_{p^m})$. Also, using the same method as the proof of Corollary 1 we have

$$\begin{aligned}\psi^m(x,y) &= (ux^{p^m}/u^{p^m}, \sqrt{u}^3 y^{p^m}/\sqrt{u}^{3p^m}) \\ &= -P.\end{aligned}$$

□

The problem is that the polynomial $x^m + 1$ is not usually irreducible, and it is possible that ψ satisfies a smaller degree polynomial. For example, in the case $m = 3$ one sees that $\#E'(\mathbb{F}_{p^3})$ cannot be prime as it is divisible by $N = \#E(\mathbb{F}_{p^2})/\#E(\mathbb{F}_p)$. If $r \mid \#E'(\mathbb{F}_{p^3})/N$ then $\psi^2(P) - \psi(P) + 1 = \infty$ for $P \in E'(\mathbb{F}_{p^3})[r]$. Hence one only gets a 2-dimensional decomposition in the case $m = 3$.

Indeed, the interesting case is when m is a power of 2, in which case $x^m + 1$ is irreducible and one can obtain an m-dimensional GLV decomposition. Indeed, Nogami and Morikawa [14] already proposed exactly this key generation method (choosing E over $\mathbb{F}_p$ and then using a quadratic twist over $\mathbb{F}_{p^{2^c}}$) as a method to generate curves of prime order. Note that [14] does not consider the GLV method.

Therefore, the next useful case is $m = 4$, giving a 4-dimensional GLV method. On the downside, this case is potentially vulnerable to Weil descent attacks (see Section 8) and so the prime p must be larger than we would ideally like.

The other way to get higher dimension decompositions is to have maps ϕ defined over larger fields than a quadratic extension. An example of this is given in Section 4.

3 Key generation

Let $p > 3$ be prime. We present a key generation algorithm for the construction based on quadratic twists. Our algorithm is designed so that the resulting curve $E' : y^2 = x^3 + A'x + B'$ over $\mathbb{F}_{p^2}$ has coefficient $A' = -3$, which is convenient for efficient implementation when using Jacobian coordinates (see Section 13.2 of [2]).

We follow the conditions of Corollary 2, which give a particularly simple map ψ. It should be clear that the algorithm can be used in more general cases.

1. Choose a prime $p = 5 \pmod 8$. Note that p can be a special prime, such as NIST prime (see Section 2.2.6 of [11]).
2. Set $u = \sqrt{2} \in \mathbb{F}_{p^2}$.
3. Set $A' = -3$ and $A = A'/2 \in \mathbb{F}_p$.
4. Repeat
   - Choose random $B \in \mathbb{F}_p$ and let $E : y^2 = x^3 + Ax + B$.
   - Compute $t = p + 1 - \#E(\mathbb{F}_p)$.
5. Until $(p-1)^2 + t^2 = hr$ where r is prime and $h = 1$ (or maybe $h < H$ for some bound H on the cofactor).
6. Set $B' = Bu^3 \in \mathbb{F}_{p^2}$ and $E' : y^2 = x^3 + A'x + B'$.
7. Compute $\lambda \in \mathbb{Z}$ such that $\lambda^2 + 1 \equiv 0 \pmod r$.
8. Compute $i \in \mathbb{F}_p$ so that $i^4 = 1$. Then $\psi(x, y) = (-x^p, iy^p)$.

One can directly verify that $(B')^p = -B'$ and so ψ clearly maps $E'(\mathbb{F}_{p^2})$ to itself. As in Corollary 1, the homomorphism ψ is can be used for a 2-dimensional GLV method, since $\psi(P) = \lambda P$ for $P \in E'(\mathbb{F}_{p^2})[r]$.

AS remarked earlier, key generation is fast compared with standard ECC, since the point counting for $\#E(\mathbb{F}_p)$ is over a field half the usual size (this is precisely the point of the paper [14]).

4 Using special curves

We have seen that one can obtain a 2-dimensional GLV method for any elliptic curve over $\mathbb{F}_p$. However, 2-dimensional GLV methods were already known for some special curves (i.e., those with a non-trivial automorphism or endomorphism of low degree). We now show how one can get higher-dimensional expansions using elliptic curves E over $\mathbb{F}_{p^2}$ with $\#\mathrm{Aut}(E) > 2$.

The two examples of interest are $E : y^2 = x^3 + B$ and $y^2 = x^3 + Ax$. We give the details in the former case. The latter is analogous.

Let $p \equiv 1 \pmod 6$ and let $B \in \mathbb{F}_p$. Define $E : y^2 = x^3 + B$. Choose $u \in \mathbb{F}_{p^{12}}$ such that $u^6 \in \mathbb{F}_{p^2}$ and define $E' : Y^2 = X^3 + u^6 B$ over $\mathbb{F}_{p^2}$. Repeat the construction (choosing p, B, u) until $\#E'(\mathbb{F}_{p^2})$ is prime (or nearly prime). Note that there are 6 possible group orders for $y^2 = x^3 + B'$ over $\mathbb{F}_{p^2}$ and three of them are never prime as they correspond to group orders of curves defined over $\mathbb{F}_p$.

The isomorphism $\phi : E \to E'$ is given by $\phi(x, y) = (u^2 x, u^3 y)$ and is defined over $\mathbb{F}_{p^{12}}$. The homomorphism $\psi = \phi\pi\phi^{-1}$, where π is the p-power Frobenius on E, is defined over $\mathbb{F}_{p^2}$ and satisfies the characteristic equation

$$\psi^4 - \psi^2 + 1 = 0.$$

Hence one obtains a 4-dimensional GLV method for these curves. This leads, once again, to a nearly doubling of the speed of these curves compared with previous techniques.

5 Using Edwards curves

In this section we explain how to write our homomorphism in terms of the Edwards equation for an elliptic curve, under the assumption that our original curve E has a point of order 4 and a unique point of order 2 (these conditions imply that E can be written in Edwards form). This means that the multiexponentiation can be performed using the Edwards formulae for elliptic curve additions and doublings. We closely follow Section 2 of [4].

Let E be an elliptic curve $E/\mathbb{F}_{p^2} : y^2 = x^3 + Ax + B$ with a point $P = (r_1, s_1)$ of order 4 and a unique point $Q = [2]P = (r_2, 0)$ of order 2. Suppose we have an efficiently computable homomorphism $\psi : E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^2})$ of the form $\psi : (x, y) = (c_1 x^p, c_2 y^p)$, where $c_1, c_2 \in \mathbb{F}_{p^2}$ are constants. We assume that $\psi(P) = \lambda P$ for $P \in E(\mathbb{F}_{p^2})$ for some $\lambda \in \mathbb{Z}$. We will transform E to an Edwards elliptic curve E_e with an efficiently computable homomorphism ψ_e on it, such that $\psi_e(P) = [\lambda]P$ for $P \in E_e(\mathbb{F}_{p^2})$.

We first move Q to $(0, 0)$ using the standard transformation $\chi_1(x, y) = (x - r_2, y)$ which maps to $E_1 : y^2 = X^3 + a_2 X^2 + a_4 X$, where $a_2 = 3r_2$ and $a_4 = 3r_2^2 + A$ are defined over $\mathbb{F}_{p^2}$.

As in [4], let $d = 1 - \frac{4r_1^3}{s_1^2} \in \mathbb{F}_{p^2}$ and consider the elliptic curve $E_e : \bar{x}^2 + \bar{y}^2 = 1 + d\bar{x}^2\bar{y}^2$ in Edwards form. We now present the explicit birational map from $E_1 \to E_e$ given in [4].

Let $t_1 = \sqrt{\frac{r_1}{1-d}} = \pm\frac{s_1}{2r_1}$. Define $E_2 : (\frac{r_1}{1-d})y^2 = x^3 + a_2 x^2 + a_4 x$. Then there is an isomorphism χ_2 from $E_1 \to E_2$ by $\chi_2(x, y) = (x, y/t_1)$. As explained in [4], we know that $a_4 = r_1^2$ and $a_2 = 2r_1(1+d)/(1-d)$. Let $E_3 : (\frac{1}{1-d})y^2 = x^3 + 2((1+d)/(1-d))x^2 + x$. The isomorphism χ_3 from E_2 to E_3 is given by $\chi_3(x, y) = (x/r_1, y/r_1)$. Finally, E_3 is birationally equivalent to E_e by the birational map $\chi_4(x, y) = (2x/y, (x - 1)/(x + 1))$.

To summarize the above, there is a birational map ρ from E to E_e given by

$$\rho(x, y) = \left(\frac{2t_1(x - r_2)}{y}, \frac{x - r_2 - r_1}{x - r_2 + r_1}\right) = (\bar{x}, \bar{y}).$$

The birational map ρ^{-1} from E_e to E is given by $\rho^{-1}(\bar{x}, \bar{y}) = (\frac{(r_2-r_1)\bar{y}-(r_1+r_2)}{\bar{y}-1}, \frac{-2r_1 t_1(\bar{y}+1)}{\bar{x}(\bar{y}-1)})$.

We may now define the homomorphism $\psi_e = \rho\psi\rho^{-1}$. We will compute an explicit form for ψ_e. Let $a = r_1 + r_2$ and $b = r_2 - r_1$. Then

$$\begin{aligned}
\psi_e(\bar{x}, \bar{y}) &= \rho\psi\rho^{-1}(\bar{x}, \bar{y}) \\
&= \rho\left(\frac{c_1(b\bar{y} - a)^p}{(\bar{y} - 1)^p}, \frac{c_2(-2r_1 t_1(\bar{y} + 1))^p}{(\bar{x}(\bar{y} - 1))^p}\right) \\
&= \left(\frac{2t_1(c_1(\frac{b\bar{y}-a}{\bar{y}-1})^p - r_2)}{c_2(\frac{-2r_1 t_1(\bar{y}+1)}{\bar{x}(\bar{y}-1)})^p}, \frac{c_1(\frac{b\bar{y}-a}{\bar{y}-1})^p - a}{c_1(\frac{b\bar{y}-a}{\bar{y}-1})^p - b}\right) \\
&= \left(\frac{\bar{x}^p(m_1 - m_2\bar{y}^p)}{m_3(\bar{y}^p + 1)}, \frac{m_4\bar{y}^p - m_5}{m_6\bar{y}^p - m_7}\right)
\end{aligned}$$

where $m_1 = c_1 a^p - r_2$, $m_2 = c_1 b^p - r_2$, $m_3 = c_2 r_1^p t_1^{p-1}$, $m_4 = c_1 b^p - a$, $m_5 = c_1 a^p - a$, $m_6 = c_1 b^p - b$, and $m_7 = c_1 a^p - b$ are constants in $\mathbb{F}_{p^2}$ which may be precomputed.

It follows that ψ_e can be computed naively using two Frobenius computations, 5 multiplications and two inversions. We can also use the Montgomery method to replace two inversion with one inversion and one multiplication. So the homomorphism ψ_e is certainly efficiently computable.

6 Hyperelliptic curves

Afficionados will have noticed that Theorem 1 holds (with minor modifications to the second part of property (2)) for arbitrary abelian varieties. We now present an analogue of Corollary 1 for hyperelliptic curves.

Let $C : y^2 = x^{2g+1} + f_{2g}x^{2g} + \cdots + f_1x + f_0$ be a genus g curve over $\mathbb{F}_q$ with a single point at infinity. Consider the Jacobian of C over $\mathbb{F}_{q^m}$ and take a quadratic twist $C' : y^2 = x^{2g+1} + uf_{2g}x^{2g} + \cdots + u^{2g}x + u^{2g+1}f_0$ where $u \in \mathbb{F}_{q^m}$ is a non-square. The isomorphism $\psi : C \to C'$ is given by

$$\phi(x, y) = (ux, \sqrt{u}^{2g+1}y)$$

This map induces an isomorphism $\phi : \mathrm{Jac}(C) \to \mathrm{Jac}(C')$ over $\mathbb{F}_{q^{2m}}$ which can be explicitly calculated on the Mumford representation.

Our construction leads to the homomorphism $\psi = \phi\pi\phi^{-1}$ satisfying $\psi^m(D) + D = 0$ for $D \in \mathrm{Jac}(C')(\mathbb{F}_{q^m})$ and therefore, when m is a power of 2, one obtains an m-dimensional GLV method.

In this case, the speedup for key generation is crucial: counting the number of points on random Jacobians of cryptographic size in large characteristic is currently impractical, however our new approach is certainly feasible in practice.

On the other hand, Weil descent attacks are much more successful in higher genus. Indeed, as discussed in Section 8, even the case $m = 2$ is potentially vulnerable to Weil descent attacks. Hence one needs to increase the size of q to attain the required security level and so the benefit of our ideas in this setting is unclear.

7 Experimental results

Consider an elliptic curve implementation which is to provide security at the standard AES-128 bit level. In this case, from an implementation point of view, it is hard to resist the obvious attractions of the Mersenne prime $p = 2^{127} - 1$, which is also used in Bernstein's `surface1271` genus 2 implementation [3]. This prime supports a very fast modular reduction algorithm. Over this prime field we will use the elliptic curve

$$y^2 = x^3 + x + 214$$

defined over the field $\mathbb{F}_p$, whose quadratic twist over $\mathbb{F}_{p^2}$ has $\#E'(\mathbb{F}_{p^2}) = p + 1 + t^2 - 2p$ points on it, where

$$\#E'(\mathbb{F}_{p^2}) = 3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE072951F72CD97D8E9DE1C16A098F87AD$$

is a prime. The curve was quickly found using a modified version of Schoof's algorithm.

For comparison purposes we use an existing implementation of an NIST standard elliptic curve P-256 which provides the same level of security[11], and we compare times for a full point multiplication. Our implementation will use standard Jacobian coordinates, as specified in the IEEE-1363 standard. Whereas improved parameterisations and formulae have since become available, we point out that these would benefit both implementations more or less equally. (Having said that, when the point doubling and addition formulae are implemented over $\mathbb{F}_{p^2}$ we note that field squarings are now fully 50% faster than field multiplications, and that field inversions are not quite as bad as they would be over $\mathbb{F}_p$, for a double-length p, and hence implementations based on affine coordinates may be of interest in very space constrained environments.)

First, a short analysis of the speed-up to be expected using the new idea. When implementing $\mathbb{F}_{p^2}$ arithmetic, extension field multiplication using Karatsuba costs $3m$, where m is the cost of an $\mathbb{F}_p$ multiplication. Also, using an obvious trick, a field squaring costs $2m$. Since $\mathbb{F}_p$ squarings do not arise in these calculations, we ignore them. When implementing the double-multiplication algorithm using a Joint Sparse Form [11], the cost of the calculation for each bit of the multiplier is 1 point doubling, plus 0.5 ”mixed” point additions. Substituting the costs of point doubling and mixed point addition using standard Jacobian coordinates and IEEE-1363 formulae, gives a total cost of $(3(3m) + 6(2m) + (8(3m) + 3(2m))/2 = 36m$ per bit. For the 128 bit size of the multipliers required for the GLV method, this amounts to $128.36m = 4608m$ for the whole calculation.

For the NIST curve, the cost of a point multiplication depends on the windowing method used. Here we use a standard wNAF method, with a window size of 4. The expected cost per bit will then be approximately $(4M + 4S) + 0.2(8M + 3S)$, where M is the cost of an $\mathbb{F}_p$ multiplication and S the cost of an $\mathbb{F}_p$ squaring. For simplicity we will assume that $M = S$, and so the total cost for a 256-bit point multiplication works out as roughly $2585.6M$.

In our implementations we averaged the cost over 10^5 point multiplications, and the results are presented in Table 1. We also include in the table the often neglected costs of field additions and subtractions. Note that when implementing $\mathbb{F}_{p^2}$ arithmetic, each multiplication using Karatsuba also requires at least 5 $\mathbb{F}_p$ additions/subtractions, so the number of these operations increases dramatically.

Table 1. Point multiplication operation counts NIST-256 vs New Method

	$\mathbb{F}_p$ muls	$\mathbb{F}_p$ adds/subs
NIST (256-bit p)	2729	3825
Our Method (128-bit p)	4662	15148

It has been observed by Avanzi [1], that software implementations over smaller prime fields (as required by our proposed method) suffer disproportionally when implemented using general purpose multi-precision libraries, and this “Avanzi effect” will work against us here, as we are using the general purpose MIRACL library [15]. However we are confident that special purpose libraries like the mpFq library [10] which generate field-specific code, and implementations which work hard to squeeze out overheads, such as Bernsteins implementation’s [3] can do a lot better than the results presented here.

For comparison purposes we have implemented both methods on two widely differing platforms, a 3GHz 32-bit Pentium 4 (Prescott) with SSE2 instruction set extensions, and on an 8-bit 4MHz Atmel Atmega128 chip (which is a popular choice for Wireless Sensor Network nodes). See Table 2

Table 2. Point multiplication timings – NIST-256 vs New Method

	Pentium IV (ms)	Atmega128 (s)
NIST (256-bit p)	1.90	7.68
Our Method (128-bit p)	1.64	4.41

While one might expect that timings would be dominated by the $O(n^2)$ base field multiplication operations, for small values of n the $O(n)$ component of base field additions and subtractions becomes significant. Observe that on the 32-bit processor a 128-bit field element requires $n = 4$, and so it is perhaps not surprising that the speed-up is less than might have been anticipated. However on the 8-bit processor $n = 16$, and so $O(n^2)$ operations dominate, and we observe a gratifying 74% speed-up. And whereas ECC is already "fast enough" on desktop computers, it is on the resource constrained devices that a faster ECC method will be most appreciated.

8 Security implications

Our homomorphisms (at least, in the case when ϕ is an isomorphism) define equivalence classes of points in $E'(\mathbb{F}_{p^m})$ of size $2m$ by $[P] = \{\pm\psi^i(P) : 0 \leq i < m\}$. By the methods of Gallant-Lambert-Vanstone [7] and Wiener-Zuccherato [17] one can perform the Pollard algorithms for the discrete logarithm problem on these equivalence classes. This speeds up the solution of the discrete logarithm problem by a factor of $\sqrt{m}$ over previous techniques.

A more serious threat to our proposal comes from the Weil descent philosophy, and in particular the work of Gaudry [9]. Gaudry gives an algorithm for the discrete logarithm problem in $E'(\mathbb{F}_{p^n})$ requiring time $O(p^{2-4/(2n+1)})$ (with bad constants) which, in principle, beats the Pollard methods for $n \geq 3$. Gaudry's method also applies to abelian varieties: if A is an abelian varitey of dimension d over $\mathbb{F}_{p^n}$ then the algorithm has complexity $O(p^{2-4/(2dn+1)})$. Hence, for Jacobians of genus 2 curves over $\mathbb{F}_{p^2}$ one has an algorithm running in time $O(p^{1.55})$, rather than the Pollard complexity of $O(p^2)$.

Gaudry's method is still exponential time and so one can secure against it by increasing the parameters. For example, to achieve 128-bit security level using our construction with genus 2 curves over $\mathbb{F}_{p^2}$ (or elliptic curves over $\mathbb{F}_{p^4}$) one should take p to be approximately 80 bits rather than the desired 64 bits.

References

1. R. Avanzi, Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementations, CHES 2004, Springer LNCS 3156 (2004), 148–162
2. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, Handbook of elliptic and hyperelliptic cryptography, Chapman and Hall/CRC, 2006.
3. D. J. Bernstein, Elliptic vs. hyperelliptic, part 1 ECC 2006, Toronto, Canada http://www.cacr.math.uwaterloo.ca/conferences/2006/ecc2006/slides.html
4. D. J. Bernstein and T. Lange, Faster addition and doubling on elliptic curves, in K. Kurosawa (ed), Asiacrypt 2007, Springer LNCS 4833 (2007) 29–50.
5. D. J. Bernstein and T. Lange, Inverted Edwards coordinates, in S. Boztas and H.-F. Lu (eds.), AAECC 2007, Springer LNCS 4851 (2007) 20–27.
6. S. D. Galbraith and M. Scott, Exponentiation in pairing-friendly groups using homomorphisms, preprint 2008. http://eprint.iacr.org/2008/117
7. R. P. Gallant, R. J. Lambert and S. A. Vanstone, Improving the parallelized Pollard lambda search on anomalous binary curves, *Math. Comp.*, **69** (2000), 1699-1705.
8. R. P. Gallant, R. J. Lambert and S. A. Vanstone, Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In J. Kilian (Ed.), CRYPTO 2001, Springer LNCS 2139 (2001), 190–200.
9. P. Gaudry, Index calculus for abelian varieties and the elliptic curve discrete logarithm problem, to appear in *J. Symbolic Comput.*
10. P. Gaudry and E. Thome, The mpFq library and implementing curve-based key exchanges. SPEED workshop presentation, Amsterdam, June 2007
11. D. Hankerson, A. J. Menezes and S. Vanstone, Guide to elliptic curve cryptography, Springer (2004).

12. A. J. Menezes, Another look at HMQV, *J. Mathematical Cryptology*, 1 (2007), 47-64.
13. B. Möller, Algorithms for multi-exponentiation. In S. Vaudenay and A. M. Youssef (Eds.), SAC 2001, Springer LNCS 2259 (2001), 165–180.
14. Y. Nogami and Y. Morikawa, Fast generation of elliptic curves with prime order over $\mathbb{F}_{p^{2^c}}$, in Proceedings International Symposium on Information Theory 2003.
15. M.Scott, MIRACL – Multiprecision Integer and Rational Arithmetic C/C++ Library, http://ftp.computing.dcu.ie/pub/crypto/miracl.zip, 2008
16. J. H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106. Springer-Verlag, 1986.
17. M. J. Wiener and R. J. Zuccherato, Faster Attacks on Elliptic Curve Cryptosystems. In S. Tavares and H. Meijer (Eds.), SAC 1998, Springer LNCS 1556 (1999), 190–200.