Trace Zero Subvarieties of Genus 2 Curves for Cryptosystems

Tanja Lange

Information-Security and Cryptography,
Ruhr-University of Bochum,
Universitätsstr. 150,
D-44780 Bochum, Germany,
lange@itsc.ruhr-uni-bochum.de

Abstract

In this paper we present a kind of group suitable for cryptographic applications: the trace zero subvariety. We describe in detail the case of trace zero varieties constructed from genus 2 curves over prime fields. The curve is considered over an extension field of degree 3 and one performs Weil descent from its Jacobian to the prime field leading to a variety of dimension 6. The trace zero variety is a subvariety thereof. As a group it is isomorphic to a subgroup of the Jacobian of the original curve. For appropriately chosen parameters it is as secure as Jacobians of curves of genus $g \leq 3$.

Its main advantage is that the complexity of computing scalar multiplication is lower than on other curve based groups. This is achieved by making use of the Frobenius endomorphism.

Thus the trace zero subvariety can be used efficiently in protocols based on the discrete logarithm problem.

Keywords: Public key cryptography, discrete logarithm, hyperelliptic curves, abelian varieties, Frobenius endomorphism, fast arithmetic

1 Introduction

To allow secret transmission of sensitive data and to secure electronic commerce one needs to rely on protocols guaranteeing that messages cannot be read or altered by third parties and that a signing party cannot deny his signature. A widely used mathematical primitive in these protocols is the discrete logarithm problem: Given a cyclic group generated by D with a given group law and a scalar multiple Q of D, determine d such that $dD = Q$. A group is suitable for applications in cryptography if (i) the group operation is fast, (ii) the group order can be computed efficiently, (iii) the discrete logarithm problem is hard, and (iv) the representation is easy and compact.

Two common kinds of groups used in practice are the multiplicative group of a finite field and the group of points on an elliptic curve over a finite field. The first group comes equipped with a very fast arithmetic, but also with a subexponential algorithm for computing the discrete logarithm. Since this index calculus attack does not carry over to elliptic curves, only general techniques like Pollard's rho and kangaroo methods apply, unless the curve has a special structure (e. g. is supersingular, or the group order is divisible only by small primes, thus weak under Chinese remaindering). In his 1989 article, Koblitz [18] proposes to take

the Jacobian of a hyperelliptic curve as a group for cryptographic applications. If the genus $g \leq 3$ only generic attacks apply if the curve is cannot be attacked by the Frey-Rück [9, 10] or Rück [30] attack.
As of today, point counting on curves defined over large prime fields is still a problem. The best algorithm by Gaudry and Schost [13] needs about 1 week on one machine to compute the order of a genus 2 curve over a prime field of 80 bits. Still, many curves need to be counted before finding a curve with a large prime order subgroup. Alternatives are to construct the curve via the CM-method (see Weng [42]), to restrict to fields of small characteristic (see Kedlaya [17], Lauder and Wan [22], Vercauteren [40]), or to choose Koblitz (subfield) curves (see Lange [20]).

The trace zero varieties were suggested for cryptographic applications by Frey [7, 8]. The construction is based on the Weil restriction of a curve over $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. To obtain fast arithmetic in the group, one makes use of efficient arithmetic in the finite field $\mathbb{F}_{p^n}$ and of the Frobenius endomorphism. This way scalar multiplications in the group can be performed faster than on a Jacobian of same size.
In the genus 1 case these varieties were studied by Naumann [29] and Blady [3] for $n = 3$ and by Weimerskirch [41] for $n = 5$. In this article we investigate $g = 2$ and $n = 3$. The results presented here apply to the other cases as well. Several aspects of this study are new for those cases, too.
The results can easily be generalized to larger genera and to higher extension fields $\mathbb{F}_{p^n}$. However, we advice against using other instances as the resulting varieties are likely to be attacked: it might be possible to find curves of moderately large genus such that the trace zero variety is a subvariety of their Jacobians. Then an index calculus attack can solve discrete logarithm problem there. For Jacobians of hyperelliptic curves [12, 39] give details on index calculus attacks; for Jacobians of more general curves similar considerations hold. For the proposed parameters the security is equivalent to that of low genus curves over prime fields by [6].
In the trace zero variety the computation of scalar multiples – the main operation in the protocols – can be carried out efficiently, the group order can be determined and there are no known weaknesses. With a little effort the size of the representation can be reduced to be of the same bitlength as the group order plus a few bits. Our idea is especially interesting for low security applications where one requires a group size of only 128 bits. Since in our case the group order is p^4, one can choose p to fit in a 32-bit word, leading to an efficient arithmetic in the prime ground field.
The same implementational advantage was recently claimed for genus 4 curves. However, for the same field size the security of genus 4 curves is lower due to recent work by Thériault [39]. Hence, for this setting our proposal proves very useful.

We remark that XTR [23] and LUC [33] are based on a similar construction starting from an extension field and then taking a subgroup given by conditions on the norm of the elements, which corresponds to the trace in the additive setting. However, they can base the security on that of finite fields where there exist subexponential algorithms. Furthermore, they do not exploit the geometric background.
Rubin and Silverberg [31] consider supersingular elliptic curves for identity based cryptosystems. They independently suggest to use the trace zero subvariety of such curves to obtain short signatures keeping the same MOV exponent. This is different from our approach, which starts from an ordinary curve and was already given by the author in her thesis [20]. Our

methods for speeding up the computation of scalar multiples can be applied to their setting as well.

2 Mathematical Construction

2.1 Background Results

For a basic introduction to hyperelliptic curves see Menezes, Wu, and Zuccherato [26]. More mathematical background can be found in Lorenzini [24] and Stichtenoth [37]. We briefly state what is needed on general hyperelliptic curves in the sequel.

A hyperelliptic curve of genus g over a prime field of odd characteristic having at least one $\mathbb{F}_p$-rational Weierstraß point can be given by an equation of the form

$$C : y^2 = f(x), \ f \in \mathbb{F}_p[x],$$

f monic, $\deg f = 2g + 1$ and f has no multiple zeros. The group one uses is the ideal class group $\mathrm{Cl}(C/\mathbb{F}_{p^n})$ of the (affine) coordinate ring of C in $\mathbb{F}_{p^n}(x, y)$ which is a maximal order. The ideal class group is the quotient group of the ideals modulo the principal ideals. In every nontrivial class there is exactly one ideal generated by a pair $u(x), v(x) - y$ with $u, v \in \mathbb{F}_{p^n}[x], \deg u \leq g$, u monic, and $\deg v < \deg u$. One uses the ordered pair $[u, v]$ to represent that class. Cantor's algorithm [4, 18] describes the arithmetic in $\mathrm{Cl}(C/\mathbb{F}_{p^n})$. As the curve has only a single point at infinity, the ideal class group is isomorphic to the divisor class group of the set of points of the corresponding projective curve $\tilde{C}$. As f has odd degree, there is only a single non-affine point $\mathbb{P}_\infty$. The relation is given by

Lemma 2.1 (Mumford Representation).
Let the function field be given via the irreducible polynomial $y^2 - f(x)$, where $f \in \mathbb{F}_p[x]$, $\deg f = 2g + 1$, and f has no multiple zeros. Each nontrivial ideal class over $\mathbb{F}_{p^n}$ can be represented by a unique ideal generated by $u(x)$ and $y - v(x)$, $u, v \in \mathbb{F}_{p^n}[x]$, where

1. *u is monic,*
2. *$\deg v < \deg u \leq g$,*
3. *$u | v^2 - f$.*

Let $D = \sum_{i=1}^{r} P_i - rP_\infty$, where $P_i \neq P_\infty, P_i \neq -P_j$ for $i \neq j$ and $r \leq g$. Put $P_i = (x_i, y_i)$. Then the corresponding ideal class is represented by $u = \prod_{i=1}^{r}(x - x_i)$ and if P_i occurs n_i times then

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 - f(x)\right]_{|x=x_i} = 0, \ 0 \leq j \leq n_i - 1.$$

Finally, we mention that the divisor class group is isomorphic to the Jacobian of $\tilde{C}$, which is an abelian variety of dimension g.

The hyperelliptic involution ι maps $[u, v]$ to $[u, -v]$. A further endomorphism is the Frobenius endomorphism σ. It operates on the classes by $\sigma([u(x), v(x)]) = [u^p(x), v^p(x)]$ for $u, v \in \overline{\mathbb{F}}_p[x]$, where the exponentiation of the polynomials is understood coefficient-wise. The characteristic polynomial of the Frobenius endomorphism has the following form

$$P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + a_1 p^{g-1} T + p^g \in \mathbb{Z}[T].$$

Let $P(T) = \prod_{i=1}^{2g}(T - \tau_i)$ over $\mathbb{C}$. Via $|\mathrm{Cl}(C/\mathbb{F}_{p^n})| = \prod_{i=1}^{2g}(1 - \tau_i^n)$ the class numbers for all extension fields $\mathbb{F}_{p^n}$ depend only on the characteristic polynomial of σ.

2.2 The Trace Zero Subvariety

If we consider the curve over an extension field of the field of definition, using the Frobenius endomorphism σ of the curve is interesting to speed up the computation of scalar multiples. This has been studied for large extensions of small ground fields in a series of papers [19, 25, 34, 35, 32, 28, 14, 20] for elliptic and arbitrary genus curves. Here, we suggest to use very small extension degrees.

The starting point for our construction is a hyperelliptic curve of genus g defined over a prime field $\mathbb{F}_p$, where p is chosen such that p^{n-1} is of the desired group size. As one looks for group sizes of more than 100 bits and n is small, we can assume that $p > 5$. We consider the ideal class group over the finite field extension $\mathbb{F}_{p^n}$ and restrict the computations to the subgroup G defined by the property that its elements D are of trace zero, i. e.

$$G := \{\bar{D} \in \mathrm{Cl}(C/\mathbb{F}_{p^n}) | \bar{D} + \sigma(\bar{D}) + \cdots + \sigma^{n-1}(\bar{D}) = 0\}.$$

G is a subgroup of $\mathrm{Cl}(C/\mathbb{F}_{p^n})$ as it is the kernel of the trace map. Obviously, σ is a group automorphism of G.

Now we consider the construction from a geometric point of view. One starts with a g-dimensional abelian variety over $\mathbb{F}_{p^n}$. The restriction of scalars transforms this to a gn-dimensional variety over $\mathbb{F}_p$. Taking the subvariety of elements of trace zero leads to a $g(n-1)$-dimensional variety $\mathcal{G}$ over $\mathbb{F}_p$ which is isomorphic to G as group.

For the remainder of the paper we restrict our attention to the case $g = 2, n = 3$. We can assume $f(x) = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{F}_p[x]$, as this form can be achieved easily by replacing x by $x - f_4/5$ otherwise.

Let the characteristic polynomial of σ be given by $P(T) = T^4 + a_1T^3 + a_2T^2 + a_1pT + p^2$. Then the group order of G is $|G| = |\mathrm{Cl}(C/\mathbb{F}_{p^3})|/|\mathrm{Cl}(C/\mathbb{F}_p)|$, explicitly:

$$|G| = p^4 - a_1p^3 + (a_1^2 + 2a_1 - a_2 - 1)p^2 + (-a_1^2 - a_1a_2 + 2a_1)p + a_1^2 + a_2^2 - a_1a_2 - a_1 - a_2 + 1. \quad (1)$$

Due to security and implementation issues we require that $2 \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^3})|$ and $3 \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^6})|$. If $|G|$ is prime (the most interesting case for applications as the full group is used) one only needs to check that

$$2, 3 \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^2})| = p^4 + (a_1^2 - 2a_2 + 2)p^2 - 2a_1^2 + a_2^2 + a_1^2 - 2a_2 + 1 \quad (2)$$

to guarantee even $2, 3 \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^6})|$.

2.3 Different Types of Divisor Classes on Trace Zero Subvariety

In this section we investigate what the representatives of the classes in G look like. This is not only of theoretical interest but also of practical importance. For genus two curves explicit formulae [27, 38, 21] are more effective than Cantor's algorithm but several cases have to be considered according to some properties of the input divisors. We will show that less different cases need to be considered if we restrict the arithmetic to the trace zero subvariety. We make use of the relation (Lemma 2.1) between the ideal class group and the divisor class group.

Theorem 2.2. *Let $2, 3 \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^3})|$. The nontrivial elements of the trace zero variety are divisor classes represented by divisors of the form*

$$P_1 + P_2 - 2P_\infty \notin \mathrm{Div}(C/\mathbb{F}_p)^0,$$

where $P_1 \neq P_2, \sigma(P_2), \sigma^2(P_2)$.

Proof. Recall that in the case of a genus two curve each divisor class $\bar{D}$ has a unique representative of the form $D = P_1 + P_2 - 2P_\infty$, $D = P_1 - P_\infty$ or $D = 0$.
Obviously, the zero element satisfies the trace zero relation.
If the divisor class $\bar{D} \neq 0$ were defined over the ground field $\mathbb{F}_p$, then $\sigma(\bar{D}) = \bar{D}$, but $\sigma^2(\bar{D}) + \sigma(\bar{D}) + \bar{D} = 3\bar{D} \neq 0$ by assumption. If $\sigma(\bar{D}) = -\bar{D}$ then $\sigma^2(\bar{D}) = \bar{D}$, thus $\sigma^2(\bar{D}) + \sigma(\bar{D}) + \bar{D} = \bar{D} \neq 0$. Hence, such classes cannot be in G.
Therefore, $\sigma(\bar{D}) \neq \pm\bar{D}$. Let first $D = P_1 - P_\infty$, where $P_1 = (x_1, y_1) \in C(\mathbb{F}_{p^3}) \setminus C(\mathbb{F}_p)$, thus $x_1 \neq \sigma(x_1)$. Then the first polynomial representing $\bar{D} + \sigma(\bar{D})$ is given by $u = x^2 - (x_1 + \sigma(x_1))x + x_1\sigma(x_1)$. The divisor class is in G iff this resulting class equals $-\sigma^2(\bar{D})$. This cannot happen as $-\sigma^2(\bar{D})$ is represented by $[x - \sigma^2(x_1), -\sigma^2(y_1)]$ and the degrees of the first polynomials are different. Via $P \mapsto P - P_\infty$ the curve is embedded into the divisor class group. Hence, this result shows that the curve lies completely outside the trace zero variety.
Let $D = P_1 + P_2 - 2P_\infty$, where $P_2 = \sigma(P_1)$. The trace zero relation means that $P_1 + \sigma(P_1) + \sigma(P_1 + \sigma(P_1)) + \sigma^2(P_1 + \sigma(P_1)) - 6P_\infty$ equals a principal divisor div(F). Rearranging leads to $2(P_1 + \sigma(P_1) + \sigma^2(P_1) - 3P_\infty)$ =div(F). As above $P_1 + \sigma(P_1) + \sigma^2(P_1) - 3P_\infty$ does not equal a principal divisor and it must be of order 2 in contradiction to the assumption. Similarly $D = 2P_1 - 2P_\infty$ could be in G only if $|\mathrm{Cl}(C/\mathbb{F}_{p^3})|$ were divisible by 2 or 3. □

This result is interesting for the implementation of explicit formulae as it shows that several subcases of the complete case differentiation (see Harley [15], Lange [21]) do not occur here. For doubling only the general case is needed. In the addition of two classes $[u_1, v_1], [u_2, v_2]$ both $\deg u_i = 2$ and one only needs to distinguish if $\gcd(u_1, u_2) = 1$ or of degree 1. The first is the general case and the second can be transformed to it with a few operations.

3 Arithmetic

3.1 Arithmetic in the Extension Field

We sketch the implementation of the finite field arithmetic in extensions of degree 3. This will be used to give estimates on the complexity of the arithmetic in G. We assume the case of Kummer extensions, i. e. that $p \equiv 1 \bmod 3$. Hence, to construct $\mathbb{F}_{p^3} = \mathbb{F}_p[\xi]$ we use an irreducible binomial $y^3 - \alpha$. We abbreviate inversion, squaring, and multiplication in the extension field by capital letters, whereas those in $\mathbb{F}_p$ will be denoted by i, s, and m respectively.
Using Karatsuba multiplication we need 8m to compute 1M, as: $(b_2\xi^2 + b_1\xi + b_0)(c_2\xi^2 + c_1\xi + c_0) = (b_1c_1 + (b_0 + b_2)(c_0 + c_2) - b_0c_0 - b_2c_2)\xi^2 + ((b_0 + b_1)(c_0 + c_1) - b_0c_0 - b_1c_1 + b_2c_2\alpha)\xi + b_0c_0 + ((b_1 + b_2)(c_1 + c_2) - b_1c_1 - b_2c_2)\alpha$. 1S can be performed similarly by 6s and 2m or as $(b_2\xi^2 + b_1\xi + b_0)^2 = (b_1^2 + 2b_2b_0)\xi^2 + (2b_1b_0 - b_2^2\alpha)\xi + b_0^2 - 2b_2b_1\alpha$ by 3s and 5m using less additions.
To compute the inverse of $b \in \mathbb{F}_{p^3}$ we make use of Cramer's rule, i. e. use the resultant. Let $\Delta = b_2^3\alpha^2 + b_1^3\alpha + b_0^3 - 3b_0b_1b_2\alpha$. Then $(b_2\xi^2 + b_1\xi + b_0)^{-1} = ((b_1^2 - b_2b_0)\xi^2 + (b_2^2\alpha - b_1b_0)\xi + b_0^2 - b_2b_1\alpha)/\Delta$. In total this takes 1i, 2s and 12m in $\mathbb{F}_p$. Let η be a primitive third root of unity in $\mathbb{F}_p$; then $\sigma(b_2\xi^2 + b_1\xi + b_0) = b_2\eta^2\xi^2 + b_1\eta\xi + b_0$. For precomputed η^2 each of σ and σ^2 takes 2m.
To have $y^3 - \alpha$ irreducible we need to assure that α is no cube in $\mathbb{F}_p$. It is highly likely that there exists such an α of comparably small size that we need not count computing α times an element as a multiplication but perform it by repeated addition. E. g. if $\alpha = 2$ then a

multiplication by α can be realized by a cyclic shift and (perhaps) a modular reduction. By Chebotarev's density theorem the probability to have both $p \equiv 1 \bmod 3$ and $x^3 - 2$ irreducible is 1/3. When the field has been chosen to allow this, the costs reduce to S=6s, M=6m, and I=1i+3s+9m.

3.2 Arithmetic in the Group G

We now estimate the costs for computing in the trace zero subvariety. The following numbers are based on the assumption that the arithmetic in the ideal class group is performed using explicit formulae for genus 2. Nowadays the fastest algorithms can be found in [21] building upon [27] and [38]. As we have seen in the previous section, inversions in $\mathbb{F}_{p^3}$ can be broken down to one inversion and some multiplications in $\mathbb{F}_p$. Thus, inversions are comparably cheap and therefore we suggest to use affine coordinates. For implementations in more restricted environments we refer to the other algorithms in [21]. The methods presented in the sequel just carry through.

First we consider the arithmetic in the whole ideal class group $\mathrm{Cl}(C/\mathbb{F}_{p^3})$ and then show how to work in the subgroup. For hyperelliptic curves of genus two a general addition can be performed using 1I, 3S, and 22M whereas a doubling takes 1I, 5S, and 22M. By Section 3.1 this equals 141 (194)m, 21 (20)s, and 1i in $\mathbb{F}_p$ for an addition. The numbers in brackets refer to the case where no small α is available. To double we need 141 (198)m, 33 (32)s, and 1i.

The hardness of the discrete logarithm problem depends on the largest prime factor of the group order. As it is useful for the applications we now restrict our considerations to prime order subgroups of G. Let the prime l denote the order of this subgroup G'.

The Frobenius endomorphism in the trace zero subvariety satisfies its characteristic polynomial and, by construction, also $T^2 + T + 1 = 0$. We propose the following alternative of computing multiples of the group elements: Instead of using an integer m as the secret hidden in mD we take a tuple (r_0, r_1) of integers and compute $r_0 D + r_1 \sigma(D)$. Note, that in the subgroup under consideration the operation of the Frobenius endomorphism corresponds to the multiplication by an integer s modulo the group order l, i. e. for $s = -(p^2 - a_2 + a_1)/(a_1 p - a_2 + 1) \bmod l$ we have $\sigma(D) = sD$ for all $D \in G'$. Therefore, there exists an integer r with $0 \le r < l$ such that $r_0 + r_1 s \equiv r \bmod l$ and we see that choosing the tuple (r_0, r_1) is equivalent to choosing r as multiplier. To avoid collisions we use the following theorem to bound r_0 and r_1:

Theorem 3.1. *Let C be a hyperelliptic curve of genus two over $\mathbb{F}_p$, let $T^4 + a_1 T^3 + a_2 T^2 + a_1 p T + p^2$ be the characteristic polynomial of the Frobenius endomorphism and consider a base field extension of degree 3. Let D be a generator of a subgroup G' of prime order l of G. Put*

$$\mathbf{r} := \min\left\{ \left\lfloor \frac{l}{m} \right\rfloor, \frac{p^2 - a_2 + a_1}{\gcd(p^2 - a_2 + a_1, a_1 p - a_2 + 1)} \right\},$$

where $m = \max\{p^2 + a_1 p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1 p - 1\}$.
Then the $\mathbf{r}^2$ classes $r_0 D + r_1 \sigma(D)$, $0 \le r_i < \mathbf{r}$ are distinct.

Proof. For the elements of G the Frobenius endomorphism satisfies $T^2 + T + 1$ and its characteristic polynomial. We can combine these equations to obtain

$$(a_1 p - a_2 + 1)\sigma + p^2 - a_2 + a_1 = 0 \tag{3}$$

by inserting subsequently the trace zero relation.

Now assume that $r_0 + r_1 \sigma = r_0' + r_1' \sigma$ as endomorphisms in G'. Subtracting we obtain

$(r_0 - r_0') + (r_1 - r_1')\sigma = 0$, where by construction $|r_i - r_i'| < \mathbf{r}$. We multiply this equation by $a_1 p - a_2 + 1$ and use (3) to get

$$(a_1 p - a_2 + 1)(r_0 - r_0') - (p^2 - a_2 + a_1)(r_1 - r_1') = 0.$$

By the choice of $\mathbf{r}$ we have $|(a_1 p - a_2 + 1)(r_0 - r_0') - (p^2 - a_2 + a_1)(r_1 - r_1')| < \max\{p^2 + a_1 p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1 p - 1\} \cdot \mathbf{r} < l$ and therefore this equality not only holds modulo l but also over the integers. But again by the choice of $\mathbf{r}$ and as $p > 3$ this implies that $(r_0 - r_0') = (r_1 - r_1') = 0$. □

If the involved greatest common divisor is not too large and $|G|$ is almost prime we can hope for $\mathbf{r}^2 \sim l \sim p^4$ so that there are sufficiently many elements obtainable using this construction.

We now discuss the computation of (r_0, r_1)-folds. To compute $r_0 D + r_1 \sigma(D)$ from the binary representations $r_i = \sum_{j=0}^{\rho-1} r_{ij} 2^j, r_{ij} \in \{0, 1\}$ we follow Naumann and use the Straus-Shamir trick together with the trace zero property $D + \sigma(D) = -\sigma^2(D)$.

Algorithm 3.2.
INPUT: $D = [u, v], r_0, r_1, r_i = \sum_{j=0}^{\rho-1} r_{ij} 2^j, r_{ij} \in \{0, 1\}, r_{0\rho-1} + r_{1\rho-1} > 0$;
OUTPUT: $H = r_0 D + r_1 \sigma(D)$;

```
1. initialize
        if $r_{0\rho-1} = 1$ then
           if $r_{1\rho-1} = 0$ then $H = D$;
           else $H = -\sigma^2(D)$;
        else $H = \sigma(D)$;
2. for $j = \rho - 2$ to 0 do
   (a) $H = 2H$;
   (b) if $r_{0j} = 1$ then
              if $r_{1j} = 0$ then $H = H + D$;
              else $H = H - \sigma^2(D)$;
       else if $r_{1j} = 1$ then $H = H + \sigma(D)$;
3. output $(H)$.
```

Using this algorithm the computation of $r_0 D + r_1 \sigma(D)$ takes ρ doublings and asymptotically $3/4\rho$ additions, i. e. approximately $7/2 \log_2 p$ group operations. Although we do not use a normal basis here, the application of the Frobenius endomorphism is cheap compared to the costs of a usual group operation, as $\sigma(D)$ and $\sigma^2(D)$ need only 8 multiplications in $\mathbb{F}_p$ each for precomputed η^2. With probability of 1/2 we need to compute either $\sigma(D)$ or $\sigma^2(D)$. Summing up we have:

Theorem 3.3. *Let $\lambda = \log_2 p$. The computation of a scalar multiple in G' using Algorithm 3.2 needs*

$$3.5\lambda \textit{ inversions, } 94\lambda \textit{ squarings, and } 695\lambda \textit{ multiplications}$$

on average.
If a small α can be used only

$$3.5\lambda \textit{ inversions, } 97.5\lambda \textit{ squarings, and } 501.5\lambda \textit{ multiplications}$$

are needed on average

Note that we need the same number of operations if we use the right-to-left algorithm starting with the least significants bits. This avoids even the need to precompute the binary expansions. Likewise one can store $\sigma(D)$ and $\sigma^2(D)$ to save $\sim 8\lambda$ multiplications.
In the trace zero variety the negative of an element can be computed efficiently. To further speed up the computations one can allow signed expansions which are especially efficient if one can allow to store a few, namely 3, precomputations. Solinas [36] proposes the Joint Sparse Form (JSF) which is a generalization of a NAF to two multipliers allowing $0, \pm 1$ as coefficients. Important properties the JSF are that the density of the expansion, i. e. the number of non-zero columns divided by the total number of columns is 1/2, that the length is not increased, and that this density is minimal. Computing the JSF of two integers is easily accomplished. Having (r_0, r_1) in JSF we perform a left-to-right algorithm to compute the multiple like in Algorithm 3.2. If enough storage is available we suggest to precompute all "columns" $\sigma(D), -\sigma^2(D)$, and $D-\sigma(D)$. Then only table-look-ups and negations are needed. Plainly, like before, one can use the trace zero relation and only precompute $D - \sigma(D)$.

Theorem 3.4. *Let $\lambda = \log_2 p$. The computation of a scalar multiple in G' using JSF with precomputed $\sigma(D), -\sigma^2(D)$, and $D - \sigma(D)$ needs*

$$3\lambda \textit{ inversions, } 84\lambda \textit{ squarings and } 590\lambda \textit{ multiplications}$$

on average. The precomputations take 1 *inversion,* 20 *squarings, and* 210 *multiplications.*
If a small α can be used only

$$3\lambda \textit{ inversions, } 87\lambda \textit{ squarings and } 423\lambda \textit{ multiplications}$$

are needed on average. In this case the precomputations take 1 *inversion,* 21 *squarings, and* 157 *multiplications.*

Without the precomputations we need more field operations. The JSF is especially interesting if some storage is available. Avanzi [1] gives a study of techniques to obtain even faster scalar multiplications allowing more precomputations. In our situation the trade off between performance and on-line precomputations is optimal when we store all 10 occurring 'double-columns' and use a sliding window of width 2 to lower the number of additions. This reduces the number of group additions to $3/4\lambda$ leading to a total of 2.75λ inversions, 81.75λ squarings and 387.75λ multiplications in $\mathbb{F}_p$ if α is small, and to 2.75λ inversions, 79λ squarings and 541.5λ multiplications otherwise.

4 Example

In this section we provide a curve for which the group G is suitable for cryptographic applications. Let $p = 281474976710491$ and $C : y^2 = x^5 + 193146284752606x^3 + 201439328331345x^2 + 221507195424471x + 23552822732639$.
Over the ground field $|\mathrm{Cl}(C/\mathbb{F}_p)| = 79228161018801250124621690911$. Note that $2^{(p-1)/3} = 8833911861698$, i. e. 2 is not a third power in $\mathbb{F}_p$ so we can construct the extension field $\mathbb{F}_{p^3}$

by $y^3 - 2$, i.e. we are in the case where the field arithmetic is especially fast. Over $\mathbb{F}_{p^3}$ we have:

$$\frac{|\mathrm{Cl}(C/\mathbb{F}_{p^3})|}{|\mathrm{Cl}(C/\mathbb{F}_p)|} = |G| = 6277101853847397790150936843143247036285274358626659637071.$$

The number on the right hand side, is a 192 bit prime, thus, $|G|$ itself is prime.
The characteristic polynomial of the Frobenius endomorphism is
$T^4 - 5312621T^3 - 3284799370506639T^2 - 14953698722466654069 11T + 79228162514171450851229461081$.
Therefore
$\mathbf{r} = \min\{79228162514171807555090156430, 79228162514171779331161199099\}$
$\quad = 79228162514171779331161199099$.
Hence, there are $\mathbf{r}^2 \sim 2^{192}$ different elements obtainable by the strategy described above, which means that $\mathbf{r}^2 \sim |G|$. A basepoint for G is
$D = [x^2 + (190908433677287\xi^2 + 124971512810887\xi + 269332975121032)x + 56707541465516\xi^2 + 124248126629783\xi + 114802966638327, (208311975739313\xi^2 + 64280784374740\xi + 159345756325112)x + 12218460484198\xi^2 + 196610653413911\xi + 115774257113001]$. Further examples can be obtained by either taking random curves and computing their group order until a suitable one is found or via the CM method.

5 Security and Comparison

Before being able to compare this group to other suitable ones we need to investigate the security parameters. We recall that G is isomorphic to a four dimensional abelian variety $\mathcal{G}$ over the prime field $\mathbb{F}_p$. Other varieties of dimension four are e.g. the Jacobians of hyperelliptic curves of genus four for which there exist attacks [39] that, while still being exponential, have smaller asymptotic complexity than the square-root attacks. Note, however, that by Diem [5], $\mathcal{G}$ is in general not principally polarized. Hence, it is not the Jacobian of a hyperelliptic curve. In more detail Diem and Scholten [6] show that if $3 \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^2})$ then $\mathcal{G}$ is a subvariety of the Jacobian of a genus 6 curve and of no curve of smaller genus. For primes up to 45 bits Thériault's results imply that the generic attacks are still fastest.

From what was said above we can compare the arithmetic on G to that of the ideal class group of a genus two curve defined over a field $\mathbb{F}_q$, where $q = p'^2 \sim p^2$ or $q = p'$, p' a prime, and also to that of an elliptic curve defined over a field of size $\sim p^4$. This field can be assumed to be prime or of extension degree 2 or 4. The trace zero variety itself is defined over a prime field. Therefore we choose curves over prime fields for comparison. Certainly we need to be aware of the efficient-to-compute group endomorphism. It is of order 3 in G leading to a speed-up of Pollard's rho method by a factor of $\sqrt{3}$. As a countermeasure we choose slightly larger p to increase the group size by one bit. Gallant, Lambert, and Vanstone [11] propose to use curves over prime fields having efficient endomorphisms to speed up the scalar multiplication. We do not choose these curves for comparison as they are far more special.
Thus, we now compare the cost for arithmetic on elliptic and genus 2 curves over prime fields to that on the trace zero variety, all varieties having the same group order. We choose the double-and-add method to compute m-folds there if we compare to Algorithm 3.2. We also take into consideration the effects of using a NAF of the multiplier and 3 precomputations to compare with the effects of using a JSF. For both groups – the elliptic curve as well as the ideal class group of the genus two curve – the group-size is $\sim p^4$, therefore we assume that the binary

representation of the multiplier is on average of length $4\log_2 p$. In the double-and-add method we need $4\log_2 p$ doublings and $2\log_2 p$ additions. Using the NAF with 3 precomputations i. e. window width 4, we need $4/5\log_2 p$ additions and again $4\log_2 p$ doublings (cf. Solinas [35]).

Like before we use affine representations. For a general addition on an *elliptic curve* $E:\ y^2 = x^3+Ax+B$ we need 1 inversion, 1 squaring, and 2 multiplications in the finite field $\mathbb{F}_{p''}$, $p'' \sim p^4$ prime. To double a point we need one more squaring. For the *genus two curve* we again use the explicit formulae in $\mathbb{F}_{p'}, p' \sim p^2$.
For scalar multiples of size $m \sim p^4, p'' \sim p^4, p' \sim p^2, \lambda = \log_2 p$ this results in the following table. Note that the operations are given in the respective finite fields. From now on we assume that we are in the case that the α used to construct $\mathbb{F}_{p^3} \cong \mathbb{F}_p[y]/(y^3-\alpha)$ is small.

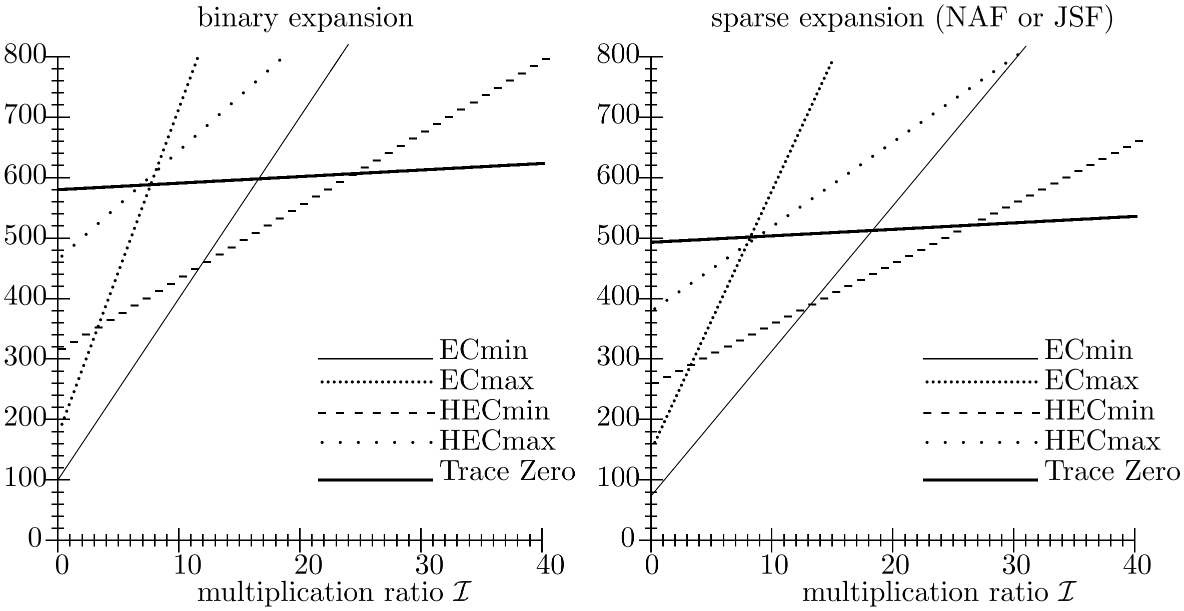
	Elliptic, Op. in $\mathbb{F}_{p''}$			**Genus 2, Op. in $\mathbb{F}_{p'}$**			**Trace zero, Op. in $\mathbb{F}_p$**		
	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.
Add.	1	1	2	1	3	22	1	21	141
Doub.	1	2	2	1	5	22	1	33	141
m-fold	6λ	10λ	12λ	6λ	26λ	132λ	3.5λ	97.5λ	501.5λ
NAF/JSF	4.8λ	8.8λ	9.6λ	4.8λ	22.4λ	105.6λ	3λ	87λ	423λ

To make a theoretical comparison we need to give ratios of the costs of operations in $\mathbb{F}_{p'}$ and $\mathbb{F}_{p''}$ to those in $\mathbb{F}_p$. For the relatively small kind of fields we consider, multiplications are usually performed by the schoolbook method. Multiplying two numbers of w words each has complexity $O(w^2)$. A consequent use of Karatsuba's trick leads to an asymptotic behavior of $O(w^{\log_2 3})$. To play fair we assume the later for the comparison, as this is in favor of the arithmetic on the elliptic and hyperelliptic curves[1]. Inversions are performed as extended greatest common divisor computations and thus their relative complexities behave like multiplications.
We consider group sizes between 120 and 300 bits. For 160 bit the situation is rather extreme – elements in $\mathbb{F}_{p''}$ need 5 words, those in $\mathbb{F}_{p'}$ 3 words and in $\mathbb{F}_p$ 2 words. This is the worst case for the trace zero variety as then a multiplication in $\mathbb{F}_p$ requires 3 multiplications of words, one in $\mathbb{F}_{p'}$ needs 6 and one in $\mathbb{F}_{p''}$ needs 15. The general case which also holds asymptotically is that assuming an element of $\mathbb{F}_p$ needs w words, one of $\mathbb{F}_{p'}$ needs $2w$ words and one in $\mathbb{F}_{p''}$ is four times as long, then the ratios are 3 and 9 respectively. This situation occurs for example in low security applications with group order $\sim$ 128 bits, then the elements of $\mathbb{F}_p$ fit in one word, and likewise for groups of more than 200 bits, especially 256 bits. We make the common assumption that one squaring needs ~ 0.8 multiplications in the respective field. The following table lists the approximate number of inversions and multiplications scaled down to $\mathbb{F}_p$ using the indicated ratios.

	Elliptic curve				**Genus 2 curve**				**Trace zero**	
	ECmin		ECmax		HECmin		HECmax			
ratio	5		9		2		3			
	Inv.	Mult.	Inv.	Mult.	Inv.	Mult.	Inv.	Mult.	Inv.	Mult.
m-fold	30λ	100λ	54λ	180λ	12λ	306λ	18λ	458λ	3.5λ	580λ
NAF/JSF	24λ	83λ	43λ	150λ	10λ	250λ	14λ	371λ	3λ	493λ

[1] However, for operands of the considered sizes the schoolbook method *is* fastest, so we are favoring the curves over the larger fields.

To decide which group is more suitable for a given environment, one needs to take into account the inversion-multiplication-ratio $\mathcal{I} = \frac{\text{cost of 1 inversion}}{\text{cost of 1 multiplication}}$. In general we have the following diagram which visualizes the costs of scalar multiplications depending on $\mathcal{I}$.



The pictures show that in the ordinary cases ECmax and HECmax the trace zero variety is advantageous to use for $\mathcal{I} \geq 8$ in the case of binary expansions and for $\mathcal{I} \geq 10$ for sparse expansions. Due to the much smaller contribution of inversions to the total running time, the trace zero variety allows faster arithmetic compared to the other varieties with increase of $\mathcal{I}$. In the less likely cases ECmin and HECmin, $\mathcal{I}$ would need to be unusually large to give faster arithmetic on trace zero varieties, but on constrained environments like smart cards this situation occurs frequently.

Note, that the diagrams are based on assumptions friendly towards the standard groups of elliptic and hyperelliptic curves. Experimental results, which will be published in a joint work with Roberto Avanzi [2], support our theoretical considerations: *In a software implementation over prime fields, the trace zero varieties of genus g curves are faster than the Jacobian varieties of curves of the same genus and of comparable group size.*

6 Practical Aspects

6.1 Protocols

As we changed the way of computing scalar multiples we now study the consequences for the cryptographic applications. In the Diffie-Hellman key-exchange and in the ElGamal cryptosystem, one simply replaces the secret integers in the range of the group order, i. e. the private key as well as the random nonce, by tuples of the above kind $(r_0, r_1), 0 \leq r_i < \mathbf{r}$. The integer s corresponding to the Frobenius should be included in the public parameters as well. If all users agree on the same curve then s can as well be hard-coded.

In electronic signature protocols we also need the multiplier as an integer modulo l. Thus if we choose the tuple (k_0, k_1) as the nonce in the signature scheme we also compute $k \equiv k_0 + k_1 s \bmod l$, which amounts to one further multiplication and one addition modulo l. Also the private key is needed as both integer and tuple. Thus, it is wise to store (d_0, d_1) and $d = d_0 + d_1 s$ as private parameters.

6.2 System Set-Up

To set up a system based on the trace zero subvariety one performs the following steps: First one chooses a prime p of appropriate size, then randomly picks a nonsingular curve C over $\mathbb{F}_p$ given by $y^2 = f(x), \deg f = 5, f_4 = 0$, then computes the characteristic polynomial of the Frobenius endomorphism, and thus obtains the group order by (1). If the group order is not good, i. e. $|G|$ has no large prime factor or (2) is not satisfied, then one discards the curve and tries with a new one. After some unsuccessful attempts one can also choose a new p.
An alternative approach would be to construct the curve by the CM-method.
If we assume that $|G| = l$ is prime, G is cyclic and any nonzero element generates the whole group. To find an element of G one proceeds as follows: pick a random element $\bar{D}' \in \mathrm{Cl}(C/\mathbb{F}_{p^3}) \setminus \mathrm{Cl}(C/\mathbb{F}_p)$, and compute $\bar{D} = \bar{D}' - \sigma(\bar{D}')$. Since $\bar{D}' \neq \sigma(\bar{D}')$ we have that $\bar{D}$ is nonzero and in the trace zero subvariety. If the order of G is almost prime, i. e. $|G| = cl, l$ prime and c small, one takes the same approach starting from $\bar{D}' \in \mathrm{Cl}(C/\mathbb{F}_{p^3}) \setminus \mathrm{Cl}(C/\mathbb{F}_p)$ and obtains $\bar{D}$ as $\bar{D} = c(\bar{D}' - \sigma(\bar{D}'))$ additionally checking whether $\bar{D} = [1, 0]$. In this extremely unlikely case $\bar{D}'$ is rejected and one starts with a further random choice of $\bar{D}'$.
We suggest to start with $[u', v'], u'$ monic of degree 2 as we propose to implement arithmetic only for G (see Section 2.3). It can be built by randomly choosing $X_1, X_2 \in \mathbb{F}_{p^3}$ until $f(X_1) = Y_1^2$ and $f(X_2) = Y_2^2$ are squares, thus $(X_1, Y_1), (X_2, Y_2) \in C(\mathbb{F}_{p^3})$. Then $u' = x^2 - (X_1 + X_2)x + X_1 X_2$ and $v' = ((Y_1 - Y_2)x + (X_1 Y_2 - X_2 Y_1))/(X_1 - X_2)$.
Depending on the chosen degree of compression it might be necessary to compute and include further equations in the set of parameters (see below).

6.3 Compression of Group Elements

For applications it is necessary to store elements from G. On a restricted device with limited storage capacities, such as a smart card, it might be wise to compress the representation of the elements. First of all, compression works like for general hyperelliptic curves in the sense that one can represent v by some cleverly chosen bits as given in [16]. However, again G is advantageous as we need to consider fewer cases like in Section 2.3.
Additionally, we can exploit that from the trace zero relation the $\mathbb{F}_p$-coefficients u_{ij} $(u_i = u_{i0} + u_{i_1}\xi + u_{i2}\xi^2)$ are related. On the cost of computing resultants and factoring a polynomial the number of such coefficients can be reduced from the remaining 6 to 4. We suggest to transmit only u_{12}, u_{11}, u_{10}, and u_{02} as this choice leads to equations of lowest degree.
Let the class of $\bar{D}$ be represented by the divisor D. For $[\bar{D} \in G$ we have that $D + \sigma(D) + \sigma^2(D)$ equals a principal divisor $\mathrm{div}(F), F = F_1(x) + F_2(x)y \in \mathbb{F}_p(x, y)/(C)$. For $D = [u, v]$ the product $u\sigma(u)\sigma^2(u)$ equals the norm of F. This leads to the identity

$$u\sigma(u)\sigma^2(u) = F_1^2 - F_2^2 f.$$

Since the left-hand-side is monic of degree 6, $\deg f = 5$, monic, we have that $\deg F_1 = 3$, monic and F_2 is constant. Hence, $F_1 = x^3 + F_{12}x^2 + F_{11}x + F_{10}, F_2^2 = F_{20},\ F_{ij} \in \mathbb{F}_p$.
Upon sorting with respect to the powers of x, this leads to the following 6 equations in the

10 variables u_{ij}, F_{ij}, where η denotes a primitive third root of unity:

$$\begin{aligned}
P_1 &= 3u_{10} - 2F_{12} + F_{20}, \\
P_2 &= 3(u_{00} + u_{10}^2 - \eta u_{11}u_{12}) - F_{12}^2 - 2F_{11}, \\
P_3 &= u_{12}^3\eta^2 + u_{11}^3\eta + u_{10}^3 - 3(u_{12}u_{11}u_{10}\eta + u_{12}u_{01}\eta + u_{11}u_{02}\eta - 2u_{10}u_{00}) - 2(F_{10} + F_{12}F_{11}) + f_3F_{20}, \\
P_4 &= 3(u_{12}^2u_{02}\eta^2 - \eta(u_{12}u_{11}u_{00} + u_{12}u_{10}u_{01} - u_{11}^2u_{01} + u_{11}u_{10}u_{02} + u_{02}u_{01}) + u_{10}^2u_{00} + u_{00}^2 + f_2F_{20}) \\
&\quad -2F_{12}F_{10} - F_{11}^2, \\
P_5 &= 3(u_{12}u_{02}^2\eta^2 - u_{12}u_{01}u_{00}\eta - u_{11}u_{02}u_{00}\eta + u_{11}u_{01}^2\eta - u_{10}u_{02}u_{01}\eta + u_{10}u_{00}^2) + f_1F_{20} - 2F_{11}F_{10}, \\
P_6 &= u_{02}^3\eta^2 + u_{01}^3\eta + u_{00}^3 - 3u_{02}u_{01}u_{00}\eta + f_0F_{20} - F_{10}^2.
\end{aligned}$$

For a given curve (thus fixed f_i, η, and p), using resultant computations or more powerful Groebner bases it is no problem to eliminate the additional variables F_{ij}. This leads to two equations – E_1 involving all remaining 6 variables u_{ij} and E_2 in which u_{01} does not occur. These equations depend only on the curve and can be computed once and for all at the setup of the system.

To compress a class the sender inserts the actual values of $u_{12}, u_{11}, u_{10}, u_{02}$ into E_2, solves for u_{00}, inserts $u_{12}, u_{11}, u_{10}, u_{02}, u_{00}$ into E_1, and solves for u_{01}. Then he transmits $\langle u_{12}, u_{11}, u_{10}, u_{02}, a, b\rangle$, where a (b) gives the place of the root of E_1 (E_2) coinciding with u_{01} (u_{00}) according to a fixed ordering of $\mathbb{F}_p$. The receiver recovers the missing values by first inserting into E_2, solving for u_{00} and finding the correct value using b. Then u_{01} is obtained from E_1 using $u_{12}, u_{11}, u_{10}, u_{02}, a$ and the value for u_{00} obtained before.

7 Conclusions

We have presented details on trace zero varieties of genus 2 curves over $\mathbb{F}_{p^3}$. First we considered mathematical aspects of the construction and detailed the arithmetic in $\mathbb{F}_{p^3}$ and in G. This was used to give a fair theoretical comparison between elliptic and genus 2 curves over prime fields and the trace zero group. Finally, we dealt with practical aspects to enable cryptographic applications of the trace zero varieties.

These considerations also hold true for other degrees of extension and other genera. A reference implementation taking into account trace zero varieties of elliptic curves over $\mathbb{F}_{p^3}$ and $\mathbb{F}_{p^5}$, too, shows that these groups indeed offer faster computations of scalar multiples. Therefore, these groups are really very interesting for cryptographic applications, especially on restricted devices.

Acknowledgment.

This work evolved from of my Ph.D. Thesis. I would like to express my deep gratitude towards my supervisor Gerhard Frey for interesting and intense discussions, his constant interest and permanent care.

Furthermore, I acknowledge fruitful discussions with Roberto Avanzi and Pierrick Gaudry. Work supported in part by DFG Graduiertenkolleg on Arithmetic Geometry and Cryptography.

References

[1] R. M. Avanzi. On the complexity of certain multi-exponentiation techniques in cryptography. to appear in J. Cryptology, see also Cryptology ePrint Archive, Report 2002/154.

[2] R. M. Avanzi and T. Lange. Cryptographic Applications of Trace Zero Varieties. Preprint, 2003.

[3] G. Blady. Die Weil-Restriktion elliptischer Kurven in der Kryptographie. Master's thesis, University Essen, 2002.

[4] D. G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48:95–101, 1987.

[5] C. Diem. *A Study on Theoretical and Practical Aspects of Weil-Restriction of Varieties.* PhD thesis, University Essen, 2001.

[6] C. Diem and J. Scholten. Cover Attacks – A report for the AREHCC project. see `http://www.arehcc.org`, 2003.

[7] G. Frey. How to disguise an elliptic curve. Talk at Waterloo workshop on the ECDLP, 1998. `http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`.

[8] G. Frey. Applications of arithmetical geometry to cryptographic constructions. In *Finite fields and applications (Augsburg, 1999)*, pages 128–161. Springer, Berlin, 2001.

[9] G. Frey and H. G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[10] S. D. Galbraith. Supersingular Curves in Cryptography. In *Advances in Cryptology – Asiacrypt 2001*, volume 2248 of *Lect. Notes Comput. Sci.*, pages 495–513. Springer, 2001.

[11] R. P. Gallant, J. L. Lambert, and S. A. Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In *Advances in Cryptology – Crypto'2001*, volume 2139 of *Lect. Notes Comput. Sci.*, pages 190–200. Springer, 2001.

[12] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology – Eurocrypt'2000*, Lect. Notes Comput. Sci., pages 19–34. Springer, 2000.

[13] P. Gaudry and E. Schost. Construction of Secure Random Curves of Genus 2 over Prime Fields, 2004. to appear in: Advances in Cryptology – Eurocrypt 2004.

[14] C. Günther, T. Lange, and A. Stein. Speeding up the Arithmetic on Koblitz Curves of Genus Two. In *Selected Areas in Cryptography – SAC 2000*, volume 2012 of *Lect. Notes Comput. Sci.*, pages 106–117. Springer, 2000.

[15] R. Harley. Fast arithmetic on genus 2 curves.
available at `http://cristal.inria.fr/~harley/hyper`, 2000.

[16] F. Hess, G. Seroussi, and N. P. Smart. Two topics in hyperelliptic cryptography. In *Selected Areas in Cryptography – SAC 2001*, volume 2259 of *Lect. Notes Comput. Sci.*, pages 181–189. Springer, 2001.

[17] K. S. Kedlaya. Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. *J. Ramanujan Math. Soc.*, 16:323–338, 2001.

[18] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1:139–150, 1989.

[19] N. Koblitz. CM-curves with good cryptographic properties. In *Advances in Cryptology–Crypto'91*, volume 576 of *Lect. Notes Comput. Sci.*, pages 279–287. Springer, 1992.

[20] T. Lange. *Efficient Arithmetic on Hyperelliptic Curves.* PhD thesis, University Essen, 2001.

[21] T. Lange. Formulae for Arithmetic on Genus 2 Hyperelliptic Curves. `http://www.itsc.ruhr-uni-bochum.de/tanja/preprints.html`, 2003. submitted.

[22] A. Lauder and D. Wan. Counting points on varieties over finite fields of small characteristic. To appear in MSRI Computational Number Theory Proceedings.

[23] A. K. Lenstra and E. R. Verheul. The XTR public key system. In *Proceedings Crypto 2000*, volume 1880 of *Lect. Notes Comput. Sci.*, pages 1–19, Berlin, 2000. Springer-Verlag.

[24] D. Lorenzini. *An Invitation to Arithmetic Geometry*, volume 9 of *Graduate studies in mathematics*. AMS, 1996.

[25] W. Meier and O. Staffelbach. Efficient Multiplication on Certain Nonsupersingular Elliptic Curves. In *Advances in Cryptology–Crypto'92*, volume 740 of *Lect. Notes Comput. Sci.*, pages 333–344. Springer, 1993.

[26] A. Menezes, Y.-H. Wu, and R. Zuccherato. An Elementary Introduction to Hyperelliptic Curves. In N. Koblitz, editor, *Algebraic Aspects of Cryptography*, pages 155–178. Springer, 1998.

[27] Y. Miyamoto, H. Doi, K. Matsuo, J. Chao, and S. Tsuji. A Fast Addition Algorithm of Genus Two Hyperelliptic Curve. In *Proc. of SCIS2002, IEICE Japan*, pages 497–502, 2002. in Japanese.

[28] V. Müller. Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two. *J. Cryptology*, 11:219–234, 1998.

[29] N. Naumann. Weil-Restriktion abelscher Varietäten. Master's thesis, University Essen, 1999.

[30] H.-G. Rück. On the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, 68:805–806, 1999.

[31] A. Silverberg and K. Rubin. Supersingular abelian varieties in cryptology. In *Advances in Cryptology - Crypto 2002*, volume 2442 of *Lect. Notes Comput. Sci.*, pages 336–353. Springer, 2002.

[32] N. P. Smart. Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic. *J. Cryptology*, 12:141–151, 1999.

[33] P. Smith and C. Skinner. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms. In *Proceedings Asiacrypt'94*, volume 917 of *Lecture Notes in Comput. Sci.*, pages 357–364. Springer-Verlag, 1995.

[34] J. Solinas. An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. In *Advances in cryptology – Crypto '97*, volume 1294 of *Lect. Notes Comput. Sci.*, pages 371–375. Springer, 1997.

[35] J. Solinas. Efficient arithmetic on Koblitz curves. *Designs, Codes and Cryptography*, 19:195–249, 2000.

[36] J. Solinas. Low-Weight Binary Representations for Pairs of Integers. Technical Report CORR 2001-41, Univertsity of Waterloo, 2001.

[37] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer, 1993.

[38] M. Takahashi. Improving Harley Algorithms for Jacobians of genus 2 Hyperelliptic Curves. In *Proc. of SCIS2002, IEICE Japan*, 2002. in Japanese.

[39] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In *Advances in cryptology – Asiacrypt 2003*, volume 2894 of *Lect. Notes Comput. Sci.*, pages 75–92. Springer, 2003.

[40] F. Vercauteren. Zeta Functions of Hyperelliptic Curves over Finite Fields of Characteristic 2. In *Advances in cryptology – Crypto 2002*, volume 2442 of *Lect. Notes Comput. Sci.*, pages 373–387. Springer, 2002.

[41] A. Weimerskirch. The Application of the Mordell-Weil Group to Cryptographic Systems. Master's thesis, Worchester polytechnic institute, 2001.

[42] A. Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation.* PhD thesis, University Essen, 2001.