Trace Zero Subvariety for Cryptosystems

Tanja Lange

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

Abstract

We present a kind of group suitable for cryptographic applications: the trace zero subvariety. The construction is based on Weil descent from curves of genus two over extension fields $\mathbb{F}_{p^n}$, $n = 3$.
On the Jacobian of the curve the group can be seen as a prime order subgroup, however, considering the construction as Weil descent we can argue that the security is equivalent to that of groups based on low-genus hyperelliptic curves over prime fields.
The advantage is that the complexity to compute scalar multiples is lower, as one can make use of the Frobenius endomorphism of the initial curve.
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 sensible messages 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 the group operation is fast, the group order can be computed efficiently, the discrete logarithm problem is hard, and 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 the fast arithmetic developed for finite fields 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 (for example is supersingular, or the group order is

divisible only by small primes, thus weak under Chinese remaindering). In his 1989 article Koblitz [17] suggests to take the ideal class group related to hyperelliptic curves as a group for cryptographic applications.
In the present state choosing random curves of genus ≥ 2 over prime fields is still infeasible. The best algorithm by Gaudry and Schost [12] needs about 1 week on one machine to compute a class number for a genus 2 curve over a prime field of 80 bits, and one needs a lot of tries to find a curve with a large prime order subgroup. Alternatives are to construct the curve via the CM-method (see Weng [37]), to choose Koblitz (subfield) curves (see Lange [19]) or to restrict to fields of small characteristic (see Kedlaya [16], Lauder and Wan [22], Vercauteren [36]).

In this article we propose a further kind of groups suitable for cryptographic applications as 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. The discrete logarithm problem is equivalent to that of low genus curves over prime fields. 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.
The construction we present was suggested by Frey in [5, 6]. It is based on the Weil restriction of a curve over $\mathbb{F}_{p^3}$ to $\mathbb{F}_p$. To obtain the fast arithmetic, we make use of an efficient arithmetic in the finite field $\mathbb{F}_{p^3}$ and of the Frobenius endomorphism.
In the genus 1 case these curves were studied by Naumann [28] and Blady [2]. The results presented here apply to that case as well and can easily be generalized to larger genera and to higher extension fields $\mathbb{F}_{p^n}, n > 3$. However, one should take into account the potential weakness of varieties of large dimension (see Gaudry [10]).
In their paper Rubin and Silverman [29] 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. However, our approach starts from an ordinary curve and was already given by the author in her thesis [19].

2 Background for the Construction

For a basic introduction to hyperelliptic curves see Menezes, Wu, and Zuccherato [25], more mathematical background can be found in Lorenzini [23] and Stichtenoth [34]. 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, i.e. the quotient group of the ideals modulo the principal ideals. In every nontrivial class there is exactly one ideal generated by a pair $u \in \mathbb{F}_{p^n}[x], \deg u \leq g$, u monic, and $y - v, v \in \mathbb{F}_{p^n}[x], \deg v < \deg u$. Cantor's algorithm [3, 17] 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 $\tilde{C}$. 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 $D = \sum_{i=1}^{r} P_i - r\infty$, *where* $P_i \neq \infty, P_i \neq -P_j$ *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 is defined over the integers and has the following form

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

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.

3 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 extension and small ground fields in a series of papers [18, 24, 31, 32, 30, 27, 13, 19] for elliptic and arbitrary genus curves. Here, we suggest to use very small extensions.
The starting point for our construction is a hyperelliptic curve of genus $g = 2$ defined over a prime field $\mathbb{F}_p$, where p is chosen such that p^4 is of the desired group size. This implies that $p > 5$ is odd. Furthermore, we assume that in the definition of the curve $f(x) = x^5 + f_3 x^3 + f_2 x^2 + f_1 x + f_0 \in \mathbb{F}_p[x]$, as this form can be achieved easily by replacing x with $x - f_4/5$ otherwise.
We consider the ideal class group over the finite field extension $\mathbb{F}_{p^3}$ and restrict the computations to the subgroup G defined by the property that its elements D are of trace zero, i.e. they satisfy $(\sigma^2 + \sigma + 1)(D) = 0$[1]. Obviously, σ is an automorphism of G. For short we denote the corresponding abelian variety by $\mathcal{G}$.
Let the characteristic polynomial of σ be given by $P(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 p T + p^2$. Then the group order of G is $|G| = |\mathrm{Cl}(C/\mathbb{F}_{p^3})| / |\mathrm{Cl}(C/\mathbb{F}_p)|$, explicitely

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

[1] In general, for a genus g curve considered over $\mathbb{F}_{p^n}$ the elements of trace zero form a subgroup as they are the kernel of a homomorphism and they can be interpreted as points on an abelian sub-variety of dimension $g(n-1)$ over $\mathbb{F}_p$.

4 Different Kinds 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 as for genus two curves explicit formulae [26, 35, 20] are more effective than Cantor's algorithm and we will show that less different cases of inputs need to be considered if we restrict the arithmetic to the trace zero subvariety. We make use of the intimate relation (Lemma 2.1) between the ideal class group and the divisor class group.

Recall that in the case of a genus two curve each divisor class $\bar{D}$ has a unique representative of the form $D = P_1 + P_2 - 2\infty$, $D = P_1 - \infty$ or $D = 0$. We now investigate these cases.
First of all the zero element satisfies the trace zero relation. This is also obvious from the fact that the relation defines a subgroup.
If the divisor class $\bar{D} \neq 0$ is defined over the ground field $\mathbb{F}_p$ (this is equivalent to $\sigma(\bar{D}) = \bar{D}$) then $\bar{D}$ has to be of order 3 to satisfy $\sigma^2(\bar{D}) + \sigma(\bar{D}) + \bar{D} = 0$. If $\sigma(\bar{D}) = -\bar{D}$ then $\sigma^2(\bar{D}) = \bar{D}$, thus $\bar{D} + \sigma(\bar{D}) + \sigma^2(\bar{D}) = \bar{D} \neq 0$.
From now on we assume $\sigma(\bar{D}) \neq \pm\bar{D}$. Let first $D = P_1 - \infty$, 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 $\bar{D} + \sigma(\bar{D})$ is represented by $[x^2 - (x_1 + \sigma(x_1))x + x_1\sigma(x_1), ((y_1 - \sigma(y_1))x + x_1\sigma(y_1) - \sigma(x_1)y_1)/(x_1 - \sigma(x_1))]$. The divisor class is in G iff this resulting class equals $-\sigma^2(\bar{D})$ which is represented by $[x - \sigma^2(x_1), -\sigma^2(y_1)]$. This cannot happen as the degrees are different. Via $P \mapsto P - \infty$ the curve is embedded into the divisor class group. Hence, this result shows that the curve lies completely outside the trace zero variety.
Let $D = P_1 + P_2 - 2\infty$, where $P_2 = \sigma(P_1)$. The trace zero relation means that $P_1 + \sigma(P_1) + \sigma(P_1 + \sigma(P_1)) + \sigma^2(P_1 + \sigma(P_1)) - 6\infty = 0$. Rearranging leads to $2(P_1 + \sigma(P_1) + \sigma^2(P_1) - 3\infty) = 0$. This can happen either if $P_1 + \sigma(P_1) + \sigma^2(P_1) - 3\infty = 0$ or if it is of order two. Similarly $D = 2P_1 - 2\infty$ can be in G only if $|\mathrm{Cl}(C/\mathbb{F}_{p^3})|$ is divisible by 2 or 3.
We have just shown:

Theorem 4.1. *Let* $2, 3 \not| |\mathrm{Cl}(C/\mathbb{F}_{p^3})|$. *Then the nontrivial elements of the trace zero variety are divisor classes represented by*

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

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

This implies that the routines to implement the arithmetic on G are doubling classes $[u, v]$ with $\deg u = 2$ and addition of two classes $[u_1, v_1], [u_2, v_2]$, $\deg u_1 = \deg u_2 = 2$, where one needs to distinguish $\gcd(u_1, u_2) = 1$ or of degree 1. This means that several subcases of the complete distinction (see Harley [14], Lange [20]) do not occur here.

5 Arithmetic in the Extension Field

To give estimates on the complexity of the arithmetic in G we briefly present the implementation of the finite field arithmetic in the extension of degree 3. 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 in the ground field 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 by 6s and 2m just like above. 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 that $y^3 - \alpha$ is irreducible we need to assure that α is no third power 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 adding. 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.

6 Arithmetic in 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 formula for genus 2. Nowadays the fastest algorithms can be found in [20] building upon [26] and [35]. 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 the above computations this equals 141 (194)m, 21 (20)s, and 1i in $\mathbb{F}_p$ for an addition. To double we need 141 (198)m, 33 (32)s, and 1i. The number in brackets refer to the case where no small α is available.
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 inherited from the larger variety and from the construction it also satisfies $T^2 + T + 1 = 0$. We propose the following alternative of computing multiples of the group elements: Instead of using an integer m as the secret number hidden in mD we take a tuple (r_0, r_1) of integers and compute $r_0D + r_1\sigma(D)$. 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 $s = -(p^2 - a_2 + a_1)/(a_1p - a_2 + 1) \bmod l$ we have $\sigma(D) = sD$ for all $D \in G'$. Therefore, there exists $0 \le r < l$ such that $r_0 + r_1s \equiv r \bmod l$ 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 6.1. *Let C be a hyperelliptic curve of genus two over $\mathbb{F}_p$, let $T^4 + a_1T^3 + a_2T^2 + a_1pT + p^2$ 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*

$$\mathbf{r} := \min\left\{\left\lfloor\frac{l}{m}\right\rfloor, \frac{p^2 - a_2 + a_1}{\gcd(p^2 - a_2 + a_1, a_1p - a_2 + 1)}\right\},$$

where $m = \max\{p^2 + a_1p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1p - 1\}$.
Then the $\mathbf{r}^2$ classes $r_0D + r_1\sigma(D)$, $0 \le r_i < \mathbf{r}$ 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

$$(a_1p - a_2 + 1)\sigma + p^2 - a_2 + a_1 = 0 \tag{2}$$

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 $a_1p - a_2 + 1$ and use (2)

$$(a_1p - a_2 + 1)(r_0 - r_0') - (p^2 - a_2 + a_1)(r_1 - r_1') = 0.$$

By the choice of $\mathbf{r}$ we have $|(a_1p-a_2+1)(r_0-r_0')-(p^2-a_2+a_1)(r_1-r_1')| < \max\{p^2+a_1p-2a_2+a_1+1, p^2+a_1-a_1p-1\}\cdot\mathbf{r} < l$ and therefore this equality not only holds modulo l but also in 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 $\mathbf{r}^2 \sim l \sim p^4$ and there are sufficiently many elements obtainable using this construction.

We now discuss the computation of (r_0, r_1)-folds. To compute $r_0D + r_1\sigma(D)$ from the binary representations $r_i = \sum_{j=0}^{\rho-1} r_{ij}2^j, r_{ij} \in \{0,1\}$ we use the Straus-Shamir trick together with the trace zero property $D + \sigma(D) = -\sigma^2(D)$.

Algorithm 6.2.
`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:` $H = r_0D + r_1\sigma(D)$;

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 $7/2\log_2 p$ compositions over $\mathbb{F}_{p^3}$. 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:

Result 6.3. *Let $\lambda = \log_2 p$. The computation of a scalar multiple in G' using Algorithm 6.2 needs*

$$3.5\lambda \textit{ inversions, } 97.5(94)\lambda \textit{ squarings, and } 501.5(695)\lambda \textit{ multiplications}$$

on average (number in brackets denote the costs for arbitrary α).

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 prove to be most efficient if one can allow to store a few, namely 3, precomputations. Solinas [33] proposes to use the joint sparse form (JSF) which is a generalization of a NAF to two multipliers, thus one allows $0, \pm 1$ 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 6.2. If enough storage is available we suggest to precompute all 'coefficients' $\sigma(D), -\sigma^2(D)$, and $D - \sigma(D)$. Then only table-look-ups and taking the negative are needed. Certainly like before one can use the trace zero relation and only precompute $D - \sigma(D)$.

Result 6.4. *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*

$$3\lambda \textit{ inversions, } 87(84)\lambda \textit{ squarings and } 423(590)\lambda \textit{ multiplications}$$

on average (number in brackets denote the costs for arbitrary α). The precomputations take 1 *inversion,* 21(20) *squarings, and* 157(210) *multiplications.*

Avanzi [1] gives a study of techniques to obtain even faster scalar multiplications allowing more precomputations. In our situation it would be optimal to precompute and 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, $81.75(79)\lambda$ squarings and $387.75(541.5)\lambda$ multiplications in $\mathbb{F}_p$.

7 Example

In this section we provide a curve for which the group G is suitable for cryptographic applications. Let $p = 75013447438681$ and $C : y^2 = x^5 + 34672227040499x^3 + 73462645749327x^2 +$

$2792938982291x + 22543037864275$.
Over the ground field $|\mathrm{Cl}(C/\mathbb{F}_p)| = 562701666049515642837890491 6$. Note that $2^{(p-1)/3} = 49604531110780$, i.e. 2 is not a third power in $\mathbb{F}_p$ and 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 the factorization
$|\mathrm{Cl}(C/\mathbb{F}_{p^3})| = |\mathrm{Cl}(C/\mathbb{F}_p)| \cdot 316633272362125514081735072073462983706551989479192937 21$,
hence the class number for the ground field times a prime with 184 binary digits, and we have that $|G|$ is itself prime.
The characteristic polynomial of the Frobenius endomorphism is
$T^4 - 8480356T^3 + 138416435415946T^2 - 636140739067303050436T + 562701729663575707925501976 1$.
Therefore
$\mathbf{r} = \min\{56270172966356905792721762 32, 56270172966356186628111234 59\}$
$\quad = 56270172966356186628111234 59$.
Hence, there are $\mathbf{r}^2 \sim 2^{184}$ different elements obtainable by the strategy described above, which means that $\mathbf{r}^2 \sim |G|$. A basepoint for G is
$D = [x^2 + (26211218157318\xi^2 + 45591290662272\xi + 33764365141175)x + 48541958828795\xi^2 + 45652287096075\xi + 61889907234993, (45212135336182\xi^2 + 18152382827206\xi + 44764837648723)x + 56934520250947\xi^2 + 49256703678444\xi + 68402135057553]$. 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.

8 Security and Comparison

Before being able to compare this group to other suitable ones we need to investigate the security parameters. To obtain $\mathcal{G}$ we started from a 2-dimensional abelian variety over $\mathbb{F}_{p^3}$. The restriction of scalars transforms this to a 6-dimensional variety over $\mathbb{F}_p$. Considering only the trace zero variety forces the dimension to drop down by two. Hence, we can view $\mathcal{G}$ as a four dimensional abelian variety defined over the prime field $\mathbb{F}_p$. Other varieties of dimension four are for example the Jacobians of hyperelliptic curves of genus four. Note, however, that by Diem [4], $\mathcal{G}$ is not principally polarized. Hence, it is not the Jacobian of a hyperelliptic curve. This shows, that the discrete logarithm problem in G cannot be attacked directly by Weil descent [8, 11, 7, 4]. To our best knowledge it is hard to find a curve of small genus such that the trace zero variety occurs as subvariety of its Jacobian.
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 which leads to a speed-up of Pollard's rho method by a factor of $\sqrt{3}$. As a countermeasure we choose slightly larger p to enlarge the group size by one bit. Gallant, Lambert, and Vanstone [9] 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 6.2. 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 [32]).

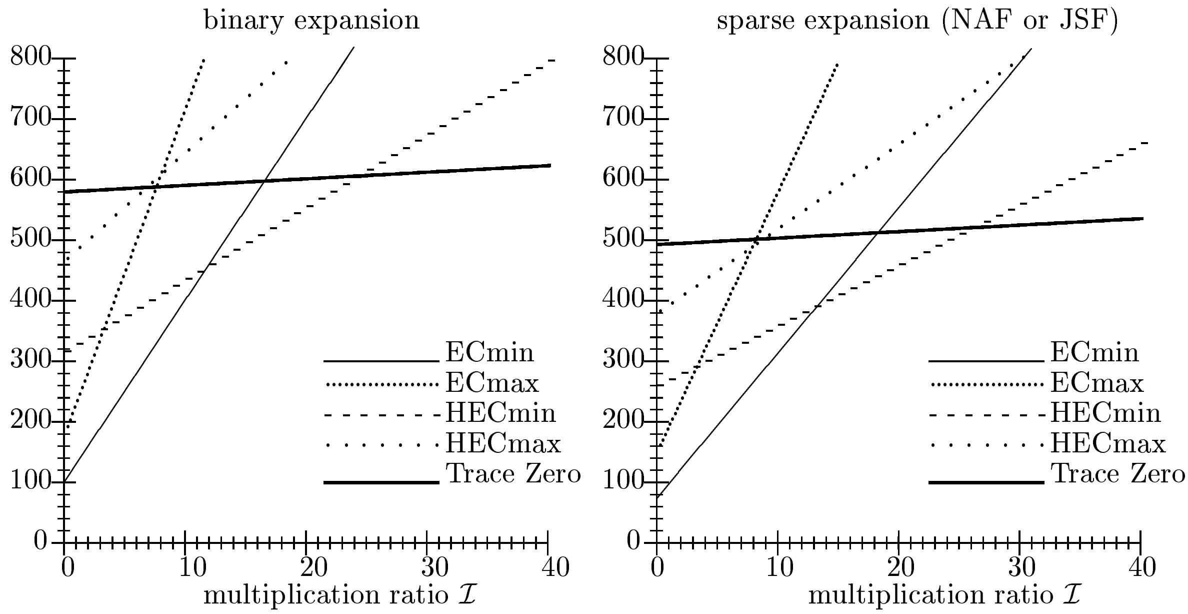
Like before we use affine representations. For a general addition on an *elliptic curve* $E: y^2 = x^3 + Ax + B$ we need 1 inversion, 1 squaring, and 2 multiplications in the finite field $\mathbb{F}_{p''}$, $p'' \sim p^4$ prime. To double a point we need one more squaring. For the *genus two curve* 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 school book method. Multiplying two numbers of w words each results in costs $O(w^2)$. A consequent use of Karatsuba's trick leads to an asymptotic behavior of $O(3^{\log_2 w})$. To play fair we assume the later for the comparison, as this is in favor of the arithmetic on the elliptic and hyperelliptic curves. Inversions are performed as extended greatest common divisor computations and thus they 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 ~ 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

To decide definitely 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 lower number of inversions the trace zero variety allows faster arithmetic compared to the other varieties with increase of $\mathcal{I}$. In the less probable cases of ECmin and HECmin $\mathcal{I}$ would need to be unusually large to give faster arithmetic, but on constrained environments like smart cards this situation might occur.

Note, that the diagrams are based on assumptions friendly towards the standard groups of elliptic and hyperelliptic curves. Implementations show that actually the trace zero variety is faster for normal group sizes on an ordinary PC. The experimental results will be published in an upcoming joint work with Roberto Avanzi.

9 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 the ElGamal cryptosystem one simply replaces the use of the secret integer in the range of the group order, i. e. the private key as well as the random nonce, by a tuple of the above kind $(r_0, r_1), 0 \leq r_i < \mathbf{r}$. s should be included in the public parameters as well. If all user agree on the same curve then s can as well be hard-coded.

In the protocol to produce electronic signatures one also needs to know 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 need to compute the corresponding integer $k \equiv k_0 + k_1 s \bmod l$ which amounts to one further multiplication and one addition modulo l. One also needs to know the private key as an integer and as a tuple. Thus, it is wise to store both (d_0, d_1) and $d = d_0 + d_1 s$ as private parameters.

10 Setting up the system

To set up a system based on the trace zero subvariety one chooses a prime of appropriate size and randomly takes a nonsingular curve C given by $y^2 = f(x), \deg f = 5, f_4 = 0$. Then one determines the characteristic polynomial of the Frobenius endomorphism from which one computes the group order of G by (1). If $|G|$ has no large prime factor one rejects the curve and starts with a different choice of f (and perhaps p). Alternatively, to save time one uses the CM-method.

If we assume that $|G| = l$ is prime, G is cyclic as a group and any element different from the zero element generates the whole group. To find an element of G one proceeds as follows: One randomly chooses an element D' from the ideal class group $\mathrm{Cl}(C/\mathbb{F}_{p^3})$ which is not defined over the ground field. Then one computes $D = D' - \sigma(D')$. Since $D' \neq \sigma(D')$ we have that $D \neq [1,0]$ and that D is in the trace zero subvariety. If the order of G is only almost prime $|G| = cl, l$ prime, one takes the same approach starting from D' and obtains D as $D = c(D' - \sigma(D'))$ and has to check additionally whether $D = [1,0]$. In this case D' is rejected and one starts with a further random choice of D'.

We suggest to start with a $D' = [u', v'], u'$ monic of degree 2 as we propose to implement arithmetic only for G (see Section 4). 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).

11 Compression of Elements from G

For applications it is necessary to store elements from G. Using a restricted device it might be wise to compress the representation of the elements if one has only low storage capacities on, say, a smart card. 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 [15]. However, again G is advantageous as we need to consider fewer cases like in Section 4.

Furthermore, 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.

Because all divisors D in G satisfy $D + \sigma(D) + \sigma^2(D) = 0$ we have that the sum equals a principal divisor $\mathrm{div}(F), F = F_1(x) + F_2(x)y \in \mathbb{F}_p(x,y)/(C)$. Put $D = [u,v]$. Then 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, $F_1 = x^3 + F_{12}x^2 + F_{11}x + F_{10}, F_2^2 = F_{20},\ F_{ij} \in \mathbb{F}_p$.

Sorting by 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 on the curve only 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}, and he 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.

Acknowledgment.
This work evolved from of my PhD thesis. I would like to thank my supervisor Gerhard Frey for useful and interesting discussions and friendly guidance. 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 multi-exponentiation in cryptography. Cryptology ePrint Archive, Report 2002/154, 2002.

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

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

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

[5] G. Frey. How to disguise an elliptic curve. Talk at Waterloo workshop on the ECDLP, 1998.

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

[7] S. D. Galbraith. Weil descent of Jacobians. In D. Augot and C. Carlet, editors, *WCC2001*, volume 6 of *Electronic Notes in Discrete Mathematics*. Elsevier Science Publishers, 2001.

[8] S. D. Galbraith and N. P. Smart. A Cryptographic Application of Weil Descent. In *Cryptography and Coding*, volume 1746 of *Lect. Notes Comput. Sci.*, pages 191–200. Springer, 1999.

[9] 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.

[10] 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.

[11] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15(1):19–46, 2002.

[12] P. Gaudry and E. Schost. announcement to NMBRTHRY@LISTSERV.NODAK.EDU, September, 24th 2002. see also `http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/papers/Japon.ps.gz`.

[13] 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.

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

[15] 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.

[16] K. S. Kedlaya. Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. *Journal of the Ramanujan Mathematical Society*, 16:323–338, 2001.

[17] N. Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.

[18] 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.

[19] T. Lange. *Efficient Arithmetic on Hyperelliptic Curves.* PhD thesis, Universität Gesamthochschule Essen, 2001.

[20] T. Lange. Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae. Cryptology ePrint Archive, Report 2002/121, 2002.

[21] T. Lange. Weighted Coordinates on Genus 2 Hyperelliptic Curves. Cryptology ePrint Archive, Report 2002/153, 2002.

[22] A. Lauder and D. Wan. Counting points on varieties over finite fields of small characteristic. submitted.

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

[24] 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.

[25] 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.

[26] 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.

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

[28] N. Naumann. Weil-Restriktion abelscher Varietäten. Master's thesis, Universität Gesamthochschule Essen, 1999.

[29] 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.

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

[31] 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.

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

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

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

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

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

[37] A. Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*. PhD thesis, Universität Gesamthochschule Essen, 2001.