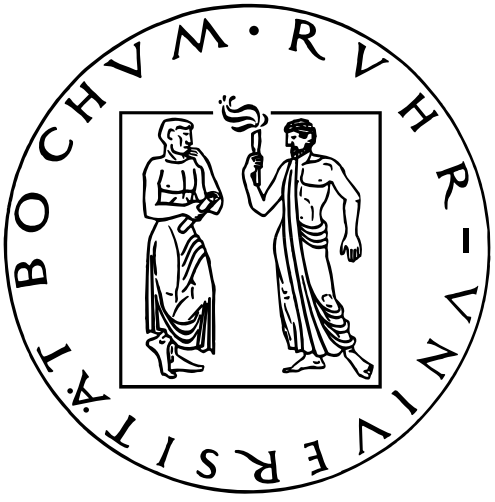
Cryptography on Trace-Zero Varieties

Malte Wienecke

February 17, 2008

Seminararbeit
Ruhr-Universität Bochum



Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

Contents

1 Introduction

To assure the security of public-key cryptography the algorithms are based on mathematical primitives, which cannot be broken easily. One of these primitives is the *Discrete Logarithm Problem* (DLP) in finite cyclic groups.

In the year 1985 Miller and Koblitz separately from each other suggested to use elliptic curves to establish the DPL. Four years later Koblitz proposed to take ideal class group related to hyper-elliptic curves as a group for cryptographic systems. In 1998 Fray had the idea to use trace zero varieties for building this applications.

Trace zero varieties have the advantage, that is possible to implement fast arithmetic, while the hardness of solving the DLP can be reduced to the hardness of the DLP of in practice used and well known groups.

In this paper I try to give a brief introduction in trace zero based cryptography. This includes a short description of the mathematical background and its arithmetic without the necessary proofs. After that the set up of a cryptographic system and a sample signature algorithm is mentioned. Last but not least the security of trace zero based cryptography is discussed.

2 Mathematical Background

To understand the functionality of trace zero based cryptography it is necessary to be aware of its mathematical background. In this paper this background is briefly presented without any proofs starting with the definition of hyper-elliptic curves. For further information see [FL05, Lan03, AC07].

A *hyper-elliptic curve* C of genus g over a prime field $\mathbb{F}_q$ where $q = p^n$ of odd characteristic is defined as:

$$C: \; y^2 + h(x)y = f(x), \qquad\qquad f \text{ monic}, \; \deg f = 2g+1, \; \deg h \leq g$$

The curve has at least one $\mathbb{F}_q$-rational Weierstraßpoint. An *elliptic curve* is a hyper-elliptic curve of genus 1.

The *Jacobian variety* $J_C(L)$ of C over L is for all finite extension $L/\mathbb{F}_q$ isomorphic to the ideal class group $\mathrm{Cl}(C/L)$. With the *Mumford's representation*, described in [Lan03], it is possible to represent the elements of $J_C(L)$ with a pair of polynomials $[u, v]$ where $u, v \in \mathbb{F}_{q^n}[x]$.

Another important operation is the *Frobenius endomorphism* σ. It is used on an element $[u, v]$ of $J_C(L)$ to raise the power of each coefficient of that element to q: $\sigma([u, v]) = [u^q(x), v^q(x)]$. The characteristic polynomial of this endomorphism has the following form:

$$\chi(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + a_1 q^{g-1} T + q^g, \qquad a_i \in \mathbb{Z}$$

With the *Hasse-Weil theorem* it is possible to receive the group order of any extension field $\mathbb{F}_{q^n}$ by using the complex roots τ_i of $\chi(T)$:

$$|J_C(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g} (1 - \tau_i^n)$$

After this little journey in the mathematical background of hyper-elliptic curves it is possible to create the trace zero subvariety. To simplify the entire procedure only trace zero varieties of genus 2 over binary fields are considered.

The starting point of this construction is a hyper-elliptic curve C of genus $g = 2$ over a finite prime field $\mathbb{F}_q$:

$$C: \; y^2 + xy = x^5 + f_3 X^3 + \epsilon x^2 + f_0, \qquad \epsilon \in \mathbb{F}_2, \quad f_0, f_3 \in \mathbb{F}_q$$

The Jacobian variety of C is $J_C(\mathbb{F}_{q^n})$ and D element of this variety. Now it is necessary to define an endomorphism of $J_C(\mathbb{F}_{q^n})$, the so called *trace of D*:

$$\mathrm{Tr}(D) = \sum_{i=0}^{n-1} \sigma^i(D) = D + \sigma(D) + \cdots + \sigma^{n-1}(D)$$

Based on this endomorphism one can reduce the Jacobian variety to a subgroup G with the property, that every element is of trace zero:

$$G = \{D \in J_C(\mathbb{F}_{q^n}) \mid \mathrm{Tr}(D) = \boldsymbol{0}\}, \qquad \boldsymbol{0} \text{ neutral element in } J_C(\mathbb{F}_{q^n})$$

G is the kernel of the trace endomorphism and thus G is a group, the so called *trace zero (sub)variety* (TZV) of $J_C(\mathbb{F}_{q^n})$.

The intersection of G and $J_C(\mathbb{F}_q)$ is produced by the n-torsion elements of $J_C(\mathbb{F}_q)$. If the greatest common divisor $gcd(n, |J_C(\mathbb{F}_q)|) = 1$ the intersection is empty and one can compute the group order of G:

$$|G| = \frac{|J_C(\mathbb{F}_{q^n})|}{|J_C(\mathbb{F}_q)|} = \frac{\prod_{i=1}^{2g}(1-\tau_i^n)}{\prod_{i=1}^{2g}(1-\tau_i)}$$

The other possibilities where $gcd(n, |J_C(\mathbb{F}_q)|) \neq 1$ are for this paper not necessary to discuss.

Based on the results of the papers [AC07, AL08] only the cases where the genus $g = 1$ and the degree of extension n equals 3 or 5 and where $g = 2$ and $n = 3$ are from security and practical interest. The group order of these cases are as followed:

$$\begin{aligned}
&|G| = p^2 - p(1+a_1) + a_1^2 - a_1 + 1 && \text{for } g=1,\ n=3,\\
&|G| = p^4 - (a_1+1)p^3 + (a_1+1)^2p^2 + \\
&\quad (5a_1 - (a_1+1)^3)p - (5a_1(a_1^2+a_1+1) - (a_1+1)^4) && \text{for } g=1,\ n=5,\\
&|G| = p^4 - a_1p^3 + (a_1^2 + 2a_1 - a_2 - 1)p^2 + \\
&\quad (-a_1^2 - a_1a_2 + 2a_1)p + a_1^2 + a_2^2 - a_1a_2 - a_1 - a_2 + 1 && \text{for } g=2,\ n=3
\end{aligned}$$

The integers $a_1,\ a_2$ are coefficients of the characteristic polynomial of the Frobenius endomorphism.

The actual group used in cryptographic applications is a subgroup G_0 of G of a large prime order ℓ. This group may be G itself.

3 Arithmetic in the Extension Field

The arithmetic used in the group G is based on the arithmetic of extension fields. These field extension are described as $\mathbb{F}_{p^n} = \mathbb{F}_p[\xi]$, where ξ is a root of an irreducible polynomial of the form $z^n - \alpha$. This representation is only possible if $p \equiv 1 \bmod n$, hence the polynomial $z^n - \alpha$ is irreducible whenever α is not a n^{th} power in $\mathbb{F}_p$. The roots of $z^n - \alpha$ are $\xi, \eta\xi, \ldots, \eta^{n-1}\xi$ where η is the n^{th}-root in $\mathbb{F}_p$.

In this context all elements of $\mathbb{F}_{p^3}$, respectively $\mathbb{F}_{p^5}$, shall be written as polynomials in ξ of degree at most 2, respectively 4, over $\mathbb{F}_p$. The addition of elements of $\mathbb{F}_{p^n}$ is made component-wise such as the subtraction and negation. The reduction modulo $z^n - \alpha$ can be ignored since α is short.

3.1 Multiplication and Squaring

The multiplication of elements of $\mathbb{F}_{p^n}$ is divided into two steps. The first step is the multiplication of the corresponding polynomials in ξ. The result is in the second step reduced exploiting the fact that $\xi^n = \alpha$.

For the actual multiplication the Karatsuba method is used. The multiplication of elements of degree 3 looks like this:

$$\begin{aligned}(a_0 + a_1\xi + a_2\xi^2)(b_0 + b_1\xi + b_2\xi^2) = \\ = a_0b_0 + ((a_0 + a_1)(b_0 + b_1) + a_0b_0 - a_1b_1)\xi \\ + ((a_0 + a_2)(b_0 + b_2) + a_0b_0 - a_2b_2 + a_1b_1)\xi^2 \\ + ((a_1 + a_2)(b_1 + b_2) + a_1b_1 - a_2b_2\xi^3 + (a_2b_2)\xi^4\end{aligned}$$

This method preforms the multiplication of two polynomials in 6 multiplications and 3 reductions. The so called schoolbook method would need for the same calculation 9 multiplications.

For squaring the schoolbook method is more efficient because the number of additions can be reduced significantly and because here the multiplication is not more expensive than squaring. To square elements in $\mathbb{F}_{p^3}$ only 3 squarings and 3 multiplications in $\mathbb{F}_p$ are needed, for $n = 5$ only 5 squarings and 10 multiplications. For the two cases the number of modular reductions are 3, respectively 5, as in the case of multiplication.

3.2 Frobenius Operation

Another used arithmetic method is the Frobenius automorphism in $\mathbb{F}_{p^n}$. For $a = a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0 \in \mathbb{F}_{p^n}$ there is $a^p = a_{n-1}\eta^{n-1}\xi^{n-1} + \cdots + a_1\eta\xi + a_0$ as the automorphism permutes the roots of $z^n - \alpha$. To compute higher powers of the Frobenius a similar method with $\eta^n = 1$ is applied. For each computation of a^{p^i}, where $1 \leq i < n$, $n-1$ multiplications in $\mathbb{F}_p$ are required, if the powers of η are pre-computed.

3.3 Inversion

To calculate the inverse of an element $a \in \mathbb{F}_{p^3}$ it is possible to consider the multiplication as a linear map and then compute a pre-image.

Assuming that $c = c_0 + c_1\xi + c_2\xi^2$ where $c_0, c_1, c_2 \in \mathbb{F}_p$ is the inverse of $a = a_0 + a_1\xi + a_2\xi^2 \in \mathbb{F}_{p^3}$ and $\xi^3 = \alpha$, the relation $ac = 1$ can be described as:

$$\begin{pmatrix} a_0 & a_2\alpha & a_1\alpha \\ a_1 & a_0 & a_2\alpha \\ a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Hence

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} a_0 & a_2\alpha & a_1\alpha \\ a_1 & a_0 & a_2\alpha \\ a_2 & a_1 & a_0 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = (a_0^3 + \alpha a_1^3 + \alpha^2 a_2^3 - 3\alpha a_0 a_1 a_2)^{-1} \begin{pmatrix} a_0^2 - \alpha a_1 a_2 \\ \alpha a_2^2 - a_0 a_1 \\ a_1^2 - a_0 a_2 \end{pmatrix}$$

This method allows inverting an element in $\mathbb{F}_{p^3}$ with just one inversion, 9 multiplications and 3 squarings in $\mathbb{F}_p$. It is often used for small field extensions.

4 Arithmetic in G

The arithmetic used in the TZV group G_0 based on the arithmetic for the whole group $J_C(\mathbb{F}_{q^n})$. The only difference is, that the *Frobenius endomorphism* σ is used to speed up the scalar multiplication. This can be archived if G_0 is generated by D of order ℓ then $\sigma(D) = sD$, for some integers s. For the given cases of TZV s can be computed as follows:

$$
\begin{aligned}
s &= \frac{q-1}{1-a_1} \bmod \ell && \text{for } g=1,\ n=3 \\
s &= \frac{q^2 - q - a_1^2 q + a_1 q + 1}{q - 2a_1 q + a_1^3 - a_1^2 + a_1 - 1} \bmod \ell && \text{for } g=1,\ n=5 \\
s &= -\frac{q^2 - a_2 + a_1}{a_1 q - a_2 + 1} \bmod \ell && \text{for } g=2,\ n=3
\end{aligned}
$$

Knowing this, it is possible to replace any scalar multiplication mD ($|m| \leq \ell/2$) with:

$$
m_0 D + m_1 \sigma(D) + \cdots + m_{n-1}\sigma^{n-1}(D), \qquad m_i = O(\ell^{1/(n-1)} = O(q^g))
$$

With this trick the multiple scalar product can be reduced to about $1/(n-1)^{\text{th}}$ of doublings necessary for calculating mD, if the implied constants are small enough.

Since in cryptographic algorithms m is normally random, there exist two approaches to obtain suitable m_i's. The first way splits the random m in opportune m_i's. The second approach generates the m_i values with suitable bounds on their size. Here it is necessary to avoid collisions, i. e. any two different sets of m_i's give different elements of G_0.

4.1 First approach: Scalar splitting

This way needs more time to generate suitable m_i's, but in some context (e. g. for digital signatures) it is the only possibility.

It starts with a given integer m with $|m| \leq \frac{\ell}{2} = \frac{|G_0|}{2}$ (w. l. o. g). The goal is to compute some m_i of bounded size, such that:

$$mD = m_0 D + m_1 \sigma(D) + \cdots + m_{n-1}\sigma^{n-1}(D)$$

The first step is to assume that $m = n_0 + k_1 q^g$, with $|n_0| \leq q^{g/2}$. In the next step we take advantage of the fact that the Frobenius operation σ in G_0 is equal to a multiplication by s and the following relations modulo the group size ℓ:

$$\chi(s) \equiv 0 \bmod \ell \quad \textit{and} \quad s^{n-1} + \cdots + s + 1 \equiv 0 \bmod \ell$$

Like that it is possible to expand m as desired, bounding each m_i to $O(q^g)$.

Theorem 4.1.1 *Considering the three mentioned cases , there exists an efficient technic to express a scalar m in form $m \equiv \sum_{i=0}^{n-2} m_i s^i \bmod \ell$ where $m_i = O(q^g)$. Then we have*

$$\begin{aligned} |m_i| &< 4q \textit{ if } k \geq 7 && \textit{for } g = 1 \textit{ and } n = 3, \\ |m_i| &< 2q \textit{ if } k \geq 17 && \textit{for } g = 1 \textit{ and } n = 5, \\ |m_i| &< 4q^2 \textit{ if } k \geq 23 && \textit{for } g = 2 \textit{ and } n = 3. \end{aligned}$$

For the proof see [AC07, AL08].

4.2 Second approach: Multi-scalar generation

The second approach is for the most cases faster than the first one and starts with $(n-1)$-tuples of scalars, instead of splitting them of a single scalar. Here it is necessary to avoid collisions. A collision is when two different tuples $(m_0, \ \ldots \ , m_{n-2})$ and $(m'_1, \ \ldots \ , m'_{n-2})$ generate the same element of G_0, i. e. $\sum_{i=0}^{n-2} m_i s^i \equiv \sum_{i=0}^{n-2} m'_i s^i \bmod \ell$. To ensure this the following theorem is used:

Theorem 4.2.1 *Let D be a generator of G_0. Then the r^{n-1} elements $r_0 D + \ \ldots \ + r_{n-2}\sigma^{n-2}(D)$ are pairwise distinct for $r_i < r$, where:*

For $g = 1$ and $n = 3$:

$$r := \min\left\{\frac{\ell}{q - a_1}, \ \frac{q-1}{\gcd(q-1, \ a_1 - 1)}\right\}$$

For $g = 1$ and $n = 5$:

$$r := \min\left\{\frac{\ell}{(1+q+|a_1|q)\mathcal{M}}, \ \frac{|q^2 - a_1^2 q + a_1 q - q + 1|}{\gamma}\right\}$$
$$\text{where } \mathcal{M} = \max\left\{|q^2 - a_1^2 q + 3a_1 q - 2q - a_1^3 + a_1^2 - a_1 + 2|, \right.$$
$$\left. \left|q^2 - a_1^2 q - a_1 q + a_1^3 - a_1^2 + a_1\right|\right\}$$
$$\gamma = \gcd(q^2 - a_1^2 q - q + 1, \ 2a_1 q - q - a_1^3 + a_1^2 - a_1 + 1)$$

For $g = 2$ and $n = 3$:

$$r := \min\left\{\frac{\ell}{\mathcal{M}}, \ \frac{q^2 - a_2 + a_1}{\gcd(q^2 - a_2 + a_1, \ a_1 q - a_2 + 1)}\right\}$$
$$\text{where } \mathcal{M} = \max\left\{|q^2 - a_1^q - 2a_2 + a_1 + 1|, \ |q^2 + a_1 - a_1 q - 1|\right\}$$

For the proof see [AC07, AL08].

After generating a 2-tuple or 4-tuple $(m_0, \ \ldots \ , m_{n-2})$ whose components are smaller than r, the scalar multiplication can be made by multi-exponentiation techniques. For cryptographic purpose r hast to be $O(q^g)$ with the implied constants as close to 1 as possible. This requirement involves more testing of curves. If the size of r is to small, not enough elements on the curves can be generated. That makes the generation of good cryptographic curves even more difficult.

5 Implementation

This chapter describes the cryptographic use of trace zero subvarieties and how to construct such a cryptographic system. After setting up this system a signature algorithm from [AL08] is introduced.

5.1 Set-Up

The first thing to do for the set-up of a cryptographic system is to generate the corresponding trace zero subvariety. There for one chooses a prime number of approbate size, such that $p = 1 \bmod n$ and $z^n - \alpha$ is irreducible for some small α, like $\alpha = 2$. After that a hyper-elliptic curve C of genus g over $\mathbb{F}_p$ is randomly generated. Here it is to consider, that it has the form $y^2 = x^{2g+1} + f_{2g-1}x^{2g-1} + \cdots + f_1 x + f_0 \in \mathbb{F}_p[x]$. Another point to keep in mind is, that the right hand polynomial has only simple roots in the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$. After that it is possible to calculate the characteristic polynomial of the Frobenius endomorphism, which allows computing the group order of G. If $|G|$ has no large prime factor, it is recommended to generate a new curve. After that one checks that:

$$\begin{aligned} &3 \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^6})| && \text{for } g = 2,\ n = 2, \\ &5 \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^{10}})| && \text{for } g = 1,\ n = 5. \end{aligned}$$

If $|G|$ has to be prime it satisfies to check $n \nmid |\mathrm{Cl}(C/\mathbb{F}_{p^2})|$. This means more concretely:

$$\begin{aligned} &3 \nmid p^4 + (a_1^2 - 2a_2 + 2)p^2 - 2a_1^2 + a_2^2 + a_1^2 - 2a_2 + 1 && \text{for } g = 2,\ n = 2, \\ &5 \nmid p^2 - 2p + a_1^2 + 2 && \text{for } g = 1,\ n = 5. \end{aligned}$$

Corresponding to the assumption that $|G| = \ell$ is prime, G is a cyclic group which is generated by any non-zero element. To find such an element, one chooses an element $D' \in \mathrm{Cl}(C/\mathbb{F}_{p^n})$, which is no element in the group field $D' \notin \mathrm{Cl}(C/\mathbb{F}_p)$. Taking advantage of the fact, that $D' \neq \sigma(D')$, it is possible to calculate $D = D' - \sigma(D')$ where $D \neq [1,\ 0]$ is. This D is in the trace zero subvariety.

If the order of G is almost prime $|G| = c\ell$, where ℓ prime, D can be obtained as $D = c(D' - \sigma(D'))$ where D' is calculated like before. If $D \neq [1,\ 0]$ D is element of the trace zero subvariety, otherwise D' should be discarded and newly chosen randomly.

5.2 Signature Algorithm

Here a signature algorithm, mentioned in [AL08], for the trace zero subgroup G, for $n = 3, g = 2$, is described and it uses the generated base point D. For other cases of G similar methods can be found. This one is based on the *P1363* standard algorithm for electronic signatures with the extension for hyper-elliptic curves. To prevent the inversion modulo the group size, this algorithm depends on ℓ. If the curve the method uses is fixed, then it is possible to precompute s, to speed up the calculations.

Assuming that the *Hash*-function transforms the message M into an integer modulo ℓ and the verification key $Q = d_0 + d_1$ has ben made public, the algorithm to generate a signature is as followed:

Algorithm 1. Signature Generation

INPUT: signing key $d = d_0 + d_1 s$, message M, base point D, parameter size r
OUTPUT: Signature (U, S)

1. **repeat**
2. Select random pair $(k_0, k_1), 1 \leq k_0, k_1 < r$;
3. $[u, v] := k_0 D + k_1 \sigma(D), u = x^v + \sum_{i=0}^{v-1} u_i$;
4. **until**
5. $U := \sum_{i=1}^{v-1} u_i p^i \bmod \ell$;
6. $k := (k_0 + k_1 s) \bmod \ell$;
7. $k' := k^{-1} \bmod \ell$;
8. $m := \mathrm{Hash}(M)$;
9. $S = k'(m + dU) \bmod \ell$;
10. **output** $(U,\ S)$.

To verify the signature his algorithm is used:

Algorithm 2. Signature Verification

INPUT: Signature $(U,\ S)$, message M, base point D, signers verification key Q
OUTPUT: True - Accept signature, False - Reject signature

1. $m := \mathrm{Hash}(M)$;
2. $w := S^{-1} \bmod \ell$;
3. $temp_1 := mw \bmod \ell$;
4. $temp_2 := Uw \bmod \ell$;
5. $[u', v'] := temp_1 D + temp_2 Q,\ u' = x^v + \sum_{i=0}^{v-1} u'_i$;

6. **if** $(u' == 1)$ **then output** False
7. **else**
8. $U' := \sum_{i=0}^{v-1} u'_i p^i \bmod \ell$;
9. **if** $(U' == U)$ **then output** True;
10. **else output** False;

That this signature algorithm works properly, it is possible to show its correctness with proofing the correctness of the verification as followed:

Proof of correctness of signature verification:
Let (U, S) be the signature of the message M, then

$$S = k^{-1}(m + (d_0 + d_1 s)U) \bmod \ell$$

if the signature was generated correctly.
Hence

$$\begin{aligned} k &\equiv S^{-1}(m + (d_0 + d_1 s)U) \\ &\equiv S^{-1}m + S^{-1}U(d_0 + d_1 s) \\ &\equiv wm + wU(d_0 + d_1 s) \\ &\equiv temp_1 + temp_2(d_0 + d_1 s) \bmod \ell \end{aligned}$$

Thus there is $temp_1 D + temp_2 Q = temp_1 + temp_2(d_0 + d_1 s) = kD$, from which it is possible to obtain $(U' == U)$ as required.

6 Security

The security of cryptographic systems based on trace zero subvarieties according of the results of the papers [Lan03, AC07, AL08] comparable to the security of hyper-elliptic curves of low genus g' over $\mathbb{F}_{p'}$, where $p' \sim (n-1)\frac{g}{g'}$ for $|G| \sim 128$ bits. This means that it is possible to use trace zero subvarieties for low security application.

For the cases where $n = 3, g = 2$ and $n = 5, g = 1$ it is possible to reduce the security for at most 6 bits, where $|G| \sim 2^{256}$, because one can not be sure that G is contained in a Jacobian of a curve of genus 6. The security of curves of genus 4 for similar fields are far less secure.

But there is also to stress that in [DS] a attack is described, which allows to reduce the bit length by $\frac{1}{6^{\text{th}}}$.

6.1 An attack on a trace zero crypto-system

The attack published in [DS] shows, that the DLP in trace zero groups of genus 2 over infinite fields of characteristic diverse than 2 or 3 and a field extension of degree 3 can be transformed into an DPL in a class group of degree 0 with genus of at most 6 over the base field. In this new class group the DPL can be attacked with the index calculus methods. This leads to a reduction of the bit length by $\frac{1}{6^{\text{th}}}$.

The basic idea behind this attack is finding smooth, projective curves $\mathcal{C}$ over $\mathbb{F}_p$ with non-constant morphisms, so called covers:

$$c: \ \mathcal{C}/\mathbb{F}_{p^3} \longrightarrow C/\mathbb{F}_{p^3} \tag{6.1}$$

This cover includes the homorphism

$$G_0 \hookrightarrow J_C(\mathbb{F}_{p^3}) \xrightarrow{c^*} J_{\mathcal{C}}(\mathbb{F}_{p^3}) \xrightarrow{N} J_{\mathcal{C}}(\mathbb{F}_p), \tag{6.2}$$

where G_0 is the trace zero group, c^* the pull-back homomorphism and N the norm-homomorphism (see [DS]).If the genus of $\mathcal{C}$ is small and the "transfer homomorphism" also it is possible to transfer the DPL in G_0 into $J_{\mathcal{C}}(\mathbb{F}_p)$. Considering the definition of c as a morphism over $\mathbb{F}_p$, it follows this diagram:

$$\begin{array}{ccccc} G_0 & \longrightarrow & J_C(\mathbb{F}_{p^3}) & \xrightarrow{c^*} & J_{\mathcal{C}}(\mathbb{F}_{p^3}) \\ & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} \\ & & J_C(\mathbb{F}_p) & \xrightarrow{c^*} & J_{\mathcal{C}}(\mathbb{F}_p) \end{array}$$

By defining G_0 as the kernel of $N: \ J_C(\mathbb{F}_{p^3}) \to J_C(\mathbb{F}_p)$ the homorphism 6.2 is trivial.

If it is now possible to create covers c such that $\mathcal{C}$ has an automorphism τ such that $c \circ \tau \neq c$, we can define C^τ and the corresponding isomorphism:

$$\phi: \ \mathcal{C}^\tau/\mathbb{F}_{p^3} \xrightarrow{\sim} \mathcal{C}/\mathbb{F}_{p^3}.$$

Instead of considering the original cover 6.1, one uses the new cover

$$c \circ \phi: \ \mathcal{C}^\tau/\mathbb{F}_{p^3} \longrightarrow C/\mathbb{F}_{p^3}$$

and the resulting transfer homomorphism

$$G_0 \hookrightarrow J_C(\mathbb{F}_{p^3}) \xrightarrow{c^*} J_{\mathcal{C}}(\mathbb{F}_{p^3}) \xrightarrow{\phi^*} J_{\mathcal{C}^\tau}(\mathbb{F}_{p^3}) \xrightarrow{N} J_{\mathcal{C}^\tau}(\mathbb{F}_p).$$

Based on this conclusions, it is possible to reduce $\frac{1}{6^{\text{th}}}$ of the bit length to solve the discrete logarithm problem in trace zero subvarieties.

For further information see [DS].

7 Résumé

After this little introduction into the trace zero based cryptography there are some aspects to keep in mind for the use of trace zero subvarieties.

The first advantage to mention is, that the trace zero varieties feature a better scalar multiplication performance than elliptic curves. This allows a fast arithmetic in this groups, which can speed up the calculations with a factor 3 compared with elliptic curves.

Also is it easily possible to construct of groups of cryptographic relevant size and the order of the group can simply be calculated using the characteristic polynomial of the Frobenius endomorphism.

However to represent an element of the trace zero variety more bit are needed compared with elements of elliptic or hyper-elliptic curves.

Another point to keep in mind, is the fact, that it is possible to reduce the security of the TZV of $1/6^{\text{th}}$ of the bit length using the described attack.

To sum up and make the point, the trace zero subvarieties are for the construction of cryptographic applications interesting groups if one considers the possible weaknesses.

Bibliography

[AC07] R. M. Avanzi and E. Cesena. Trace zero varieties over fields of characteristic 2 for cryptographic applications. Technical report, Faculty of Mathematics, Horst Görtz Institute for IT Security, Ruhr-University of Bochum - Germany and Dipartimento di Matematica, Università degli Studi RomaTRE, Rome - Italy, 2007.

[AL08] R. M. Avanzi and T. Lange. Cryptographic applications of trace zero varieties. Faculty of Mathematics, Horst Görtz Institute for IT Security, Ruhr-University of Bochum - Germany and Technical University of Denmark, Department of Mathematics - Denmark, 2008.

[DS] C. Diem and J. Scholten. An attack on a trace-zero cryptosystem. Institute for Experimental Mathematics, University of Duisburg-Essen - Germany and ESAT / COSIC, K.U. Leuven -Belgium.

[FL05] G. Frey and T. Lange. Mathematical background of public key cryptography. Technical report, Institute for Experimental Mathematics, University of Duisburg-Essen - Germany and Technical University of Denmark, Department of Mathematics - Denmark, 2005.

[Lan03] T. Lange. Trace zero subvariety for cryptosystems. Technical report, Information-Security and Cryptography - Ruhr-University of Bochum, 2003.