ELLIPTIC CURVES SUITABLE FOR PAIRING BASED CRYPTOGRAPHY

FRIEDERIKE BREZING AND ANNEGRET WENG

Abstract. We give a method for constructing ordinary elliptic curves over finite prime field $\mathbb{F}_p$ with small security parameter k with respect to a prime ℓ dividing the group order $\#E(\mathbb{F}_p)$ such that $p << \ell^2$.

1. Introduction

Over the last few years there has been an increasing interest in pairing based cryptography. The primitives of pairing based crypto systems are two groups $(G, *)$ and $(H, \circ)$ in which the discrete logarithm problem is believed to be hard. Moreover, we require the existence of an efficiently computable, non-degenerate pairing $G \times G \to H$. This additional structure allows many interesting protocols for all kind of different applications [5, 7, 11, 14].
Well known examples of such a pairing are the Weil and the Tate pairing on an elliptic curve. Here, G is the group of points on an elliptic curve defined over a finite field $\mathbb{F}_q$ and H is equal to the multiplicative group of a field extension $\mathbb{F}_{q^k}^*$.

Definition 1.1. *Let E be an elliptic curve defined over $\mathbb{F}_q$ whose group order $\#E(\mathbb{F}_q)$ is divisible by a prime ℓ. Then E has* ***security parameter k*** *if k is the smallest integer such that ℓ divides $q^k - 1$.*

If E has security parameter $k > 1$ with respect to ℓ, the Weil pairing e_ℓ defines a non-degenerate pairing from the group of ℓ- torsion points in $E(\mathbb{F}_{q^k}^*)$ into $\mathbb{F}_{q^k}^*$. It can be evaluated in $\mathcal{O}(k^2 \log^3 q)$ bit operations. Supersingular elliptic curves have security parameter less than or equal to 6 [9, 13].
It is an interesting question whether there exist suitable elliptic curves with $k \geq 7$. Obviously, they can not be supersingular. But ordinary elliptic curves with such a small security parameter are very rare [2]. We are left with the problem to construct ordinary curves with relatively small security parameter (see e.g. [5, 8]).
Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$ and let ℓ be a prime dividing the group order $\#E(\mathbb{F}_q)$ such that E has security parameter k with respect to ℓ. We have

$$\#E(\mathbb{F}_q) = q + 1 - t \equiv 0 \mod \ell \text{ and} \tag{1}$$

$$q^k - 1 \equiv 0 \mod \ell. \tag{2}$$

Inserting equation (2) in (1) shows that $(t-1)$ must be a kth root of unity modulo ℓ. On the other hand, if E is an elliptic curve over $\mathbb{F}_q$ satisfying equation (1) and $t = \zeta_k + 1 \mod \ell$ for some primitive kth roots of unity modulo ℓ, E has security parameter k with respect to ℓ. This fact has first been discovered by Cocks and Pinch [6].
Since E is ordinary, it has complex multiplication by some order $\mathcal{O}$ of discriminant

Date: August 5, 2003.

dividing $t^2 - 4q$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$. Set

$$d = \begin{cases} \frac{D}{4} & \text{if } D \equiv 0 \mod 4 \\ D & \text{else.} \end{cases}$$

The Frobenius element $\pi_q : (x, y) \to (x^q, y^q)$ corresponds to an element $w = \frac{a+b\sqrt{D}}{2} \in \mathcal{O}$ such that $\mathrm{Norm}_{K/\mathbb{Q}}(w) = w\overline{w} = q$. We have $t = a$.
This observation leads to a simple algorithm. Given an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$. Take a prime ℓ with the properties that ℓ splits in $\mathcal{O}_K$ and $\ell \equiv 1 \mod k$ and determine a kth root of unity ζ_k modulo ℓ. Set $a = \zeta_k + 1 \mod \ell$ and $b = \pm\frac{a-2}{\delta} \mod \ell$ where δ is a square root of d modulo ℓ. Finally test whether $\mathrm{Norm}_{K/\mathbb{Q}}(w)$ is a prime p (or a prime power q). We find the corresponding elliptic curve defined over $\mathbb{F}_p$ (or $\mathbb{F}_q$) using the complex multiplication method (for the CM method see e.g. [1]).
The correctness of this method can easily be seen by the following lemma which summarizes the discussion above.

Lemma 1.2. *Let $E/\mathbb{F}_q$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{D})$ such that the Frobenius endomorphism corresponds to the imaginary quadratic integer $w = \frac{a+b\sqrt{D}}{2}$ with a, b constructed as above. Then $\#E(\mathbb{F}_q)$ is divisibly by ℓ and has security parameter k with respect to ℓ.*

Proof. By the choice of b, we find

$$\#E(\mathbb{F}_q) = \mathrm{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(w - 1) = \frac{1}{4}((a-2)^2 - Db^2) \equiv 0 \mod \ell.$$

Since the trace t of π_q is equal to $a = \zeta_k + 1 \mod \ell$, the security parameter of E with respect to ℓ is equal to k. $\square$

Note that the case that $\mathrm{Norm}_{K/\mathbb{Q}}(w)$ is not a prime but a prime power is very unlikely. Hence in the following we only consider the case where $\mathrm{Norm}_{K/\mathbb{Q}}(w)$ is prime.

The values a and b are solutions of equations modulo ℓ. Hence, they will in general be of size $O(\ell)$ leading to a prime of size $O(\ell^2)$. Desirable would be to have p of size $O(\ell)$.
It is still an open question to find an algorithm for the construction of ordinary elliptic curves with arbitrary security parameter k where p is significantly smaller than ℓ. Barreto, Lynn and Scott describe a method to derive a better relation between p and ℓ for the case where k is divisible by 3 [5]. In this paper we extend their idea using the fact described above to get more examples of curves with $p << \ell^2$.
Moreover we find examples where ℓ is a prime of low Hamming weight with respect to the basis 2. For such primes, the Weil resp. Tate pairing can efficiently be evaluated [4, 10].
Acknowledgements. The authors thank S. Galbraith and M. Scott for helpful comments on the paper. Especially, S. Galbraith suggested to look for examples where ℓ has small Hamming weight.
The necessary computations were done using Magma
(http://magma.maths.usyd.edu.au/magma/).

2. The main idea

We explain the main idea in the case where D is odd. Note that it can easily be modified for $D \equiv 0 \mod 4$.
Given k and a discriminant $D < 0$ which is not too large. We can consider the number field $M(\zeta_n, D)$. Suppose $M \simeq \mathbb{Q}[x]/(f(x))$ where f is a irreducible polynomial of degree d where $d = 2n$ or n depending on whether $\sqrt{D} \subseteq \mathbb{Q}(\zeta_n)$ or not.

Moreover we require that f represents primes.
Every element in M can be represented by a polynomial of degree $\leq d-1$. We can compute the polynomials $g_1, \ldots, g_{\varphi(k)}$ which represent the primitive kth roots of unity. Let $h_1, -h_1$ be the polynomials which represent $\sqrt{D}$. Suppose that g_i and h_i lie in $\mathbb{Z}[x]$.
We now set

$$a(x) = (g_i(x) + 1)$$

and

$$b'(x) = (a(x) - 2)h_j(x) \text{in } \mathbb{Q}[x]/(f(x)).$$

for some i, j.
We test if there exists some congruence class $x_0 \mod (-D)$ such that $b'(x_0) \equiv 0 \mod (-D)$. For all x_1, $x_0 \equiv x_1 \mod (-D)$, $b'(x_1)/D$ will be in $\mathbb{Z}$. We can now define

$$p(x) = \frac{1}{4}(a(x)^2 - \frac{b'(x)^2}{D}).$$

Now suppose the following conditions are satisfied:

- $p(x)$ is irreducible,
- $p(x)$ has integer values for $x_0 \mod (-D)$ and
- $f(Dy + x_0) \in \mathbb{Z}[y]$ is irreducible.

We can then try to find primes $\ell = f(x_1)$ for some $x_1 \equiv x_0 \mod D$ and test whether $p(x_1)$ is prime as well.
We easily check that if $a(x_1)$, $b'(x_1)$ are constructed as above, there exists an elliptic curve over the prime field $\mathbb{F}_{p(x_1)}$ with complex multiplication by the maximal order $\mathcal{O}_K$ in $\mathbb{Q}(\sqrt{D})$ such that the Frobenius endomorphism of E corresponds to the element

$$\frac{a(x_1) \pm \frac{b'(x_1)}{D}\sqrt{D}}{2} \in \mathcal{O}_K.$$

The order $\#E(\mathbb{F}_{p(x_1)})$ is equal to

$$\frac{(a(x_1) - 2)^2 - \frac{b'(x_1)^2}{D}}{2}$$

and will by construction be divisible by ℓ.
The degrees of $a(x)$ and $b'(x)$ are less than equal to $\deg(f) - 1 = d - 1$. Hence, ℓ will be of size $O(x_1^d)$ and p of size $O(x_1^{2d-2})$ which is significantly smaller than $O(\ell^2)$. In special cases, the relation between ℓ and p will be even better.
Note that the assumption that $a(x)$ and $b'(x) \in \mathbb{Z}[x]$ is very strong since only few number fields M have a power integer basis.

3. A better relation between ℓ and p

We demonstrate our idea presenting several examples. The first example has already been considered in [3]. It can easily be deduced from our general approach. In all our examples, the number field $M = \mathbb{Q}(\sqrt{D}, \zeta_n)$ is a cyclotomic field and therefore has a power integer basis.

1. Let $M = \mathbb{Q}(\zeta_9)$ and $K = \mathbb{Q}(\sqrt{-3})$. The 9th cyclotomic polynomial is given by $x^6 + x^3 + 1$. Suppose $\ell = x_0^6 + x_0^3 + 1$ for some integer x_0 and let $D = -3$. We would like to construct a suitable Frobenius element $\frac{a+b\sqrt{-3}}{2}$. The element a has to be equal to $\zeta_9 + 1$ where ζ_9 is a ninth root of unity. We set $a = x_0 + 1$. Moreover b should be equal to

$$\frac{\pm(a-2)}{\sqrt{-3}} = \frac{\pm\sqrt{-3}(a-2)}{3} = \frac{(x_0 - 1)(2x_0^3 + 1)}{3}.$$

We now choose $x_0 \equiv 1 \mod 3$. Then $a \equiv b \mod 2$ and $p = \mathrm{Norm}_{K/\mathbb{Q}}(\frac{a+b\sqrt{-3}}{2})$ is of size $O(\ell^{\frac{4}{3}})$.

2. Let $M = \mathbb{Q}(\zeta_{10}, \sqrt{-1})$ and $K = \mathbb{Q}(i)$. The number field M is generated by the polynomial $x^8 - x^6 + x^4 - x^2 + 1$. The primitive 10th roots of unity are represented by the polynomials
$$x^2, -x^4, -x^6 + x^4 - x^2 + 1, x^6$$
and the roots of -1 are given by the polynomials $\pm x^5$.
Suppose that ℓ is equal to $x_0^8 - x_0^6 + x_0^4 - x_0^2 + 1$ for some integer x_0. Set $a = (-x_0^6 + x_0^4 - x_0^2 + 2)$.. Then b should be equal to
$$\frac{\pm(a-2)}{\sqrt{-1}} = \frac{\pm(-x_0^6 + x_0^4 - x_0^2)}{x_0^5} \equiv \pm(-x_0^5 + x_0^3) \mod \ell.$$
We have to ensure that $\mathrm{Norm}_{K/\mathbb{Q}}(\frac{a+b\sqrt{-1}}{2})$ is prime.
We see that p is of order $O(\ell^{\frac{3}{2}})$.

3. $M = \mathbb{Q}(\zeta_{60})$. This field is generated by $f(x) = x^{16} + x^{14} - x^{10} - x^8 - x^6 + x^2 + 1$. We consider the cases $k = 10$, $k = 12$, $k = 15$, $k = 20$, $k = 30$ and $k = 60$ and $D = -3$.
We see that discriminant $D = -1$ is not possible because for all choice of $a(x)$ and $b'(x)$ there exist no x_1 such that $a_1(x_1) = b'(x_1) \equiv 0 \mod 2$. For $D = -3$ we collect from each case an example where the relation between p and ℓ is particularly good.
   (a) **k=10:** Thre exists no x_1 such that $b_1'(x_0) \equiv 0 \mod 3$.
   (b) **k=12:** Set $a = -x^5 + 1$ and $b = 2x^{15} + 2x^{10} - x^5 - 1$. Take $x \equiv 2 \mod 3$.
   (c) **k=15:** Set $a = x^8 + 1, b = -2x^{14} + 2x^{12} + 2x^{10} + x^8 + 2x^6 + 2x^4 - 3$. More examples are given by $a = x^{14} - x^{10} - x^8 + x^2 + 1, b = x^{14} + x^{10} - x^8 - 2x^6 + x^2$ and $a = x^{14} + x^{12} - x^8 - x^6 - x^4 + 2, b = x^{14} + x^{12} + 2x^{10} + x^8 - x^6 - x^4$. Take $x \equiv 1 \mod 3$.
   (d) **k=20:** One possible solution is given by $a = -x^{11} + x + 1$ and $b = x^{11} - 2x^{10} + x + 1$. Another possibity is $a = x^{11} - x + 1$ and $b = x^{11} + 2x^{10} + x - 1$. The element x has to be chosen $\equiv 1 \mod 3$.
   (e) **k=30:** One possible solution is given by $a = x^{12} - x^2 + 1$ and $x^{12} + 2x^{10} + x^2 - 1$. The element x has to be chosen $\equiv 1 \mod 3$.
   (f) **k=60:** Set e.g. $a = -x + 1$ and $b = 2x^{11} + 2x^{10} - x - 1$ where $x \equiv 2 \mod 3$.

4. Let q be a prime. Consider $M = \mathbb{Q}(\zeta_q, i)$ and $k = q$. In this case the minimal polynomial is given by
$$f(x) = x^{2q-2} - x^{2q-4} + x^{2q-6} - x^{2q-8} + \ldots + 1.$$
Note that $f(x)(x^2+1) = x^{2q} + 1$. Hence $x^{2q} = -1 \mod f(x)$, i.e. the element $\sqrt{-1}$ corresponds to $\pm x^q \mod f(x)$.
Moreover we have x^2 is a primitive $2q$th root of unity, i.e. $-x^2$ is a qth root of unity. We can set $a = -x^2 + 1$ and $b = (-x^2 - 1)x^q = -x^{q+2} - x^q$. The relation $\frac{\log(p)}{\log(\ell)}$ is approximately $\frac{q+2}{q-1}$.

5. Let q be a prime. Consider $M = \mathbb{Q}(\zeta_q, \zeta_3)$ and $k = q$. In this case the minimal polynomial is given by
$$f(x) = \frac{x^{2q} - x^q + 1}{x^2 - x + 1}.$$
We have $f(x)(x^3 + 1)\Phi(2q) = x^{3q} + 1$ and $f(x)(x^2 - x + 1) = x^{2q} - x^q + 1$. As above we see that $-x^3$ is a qth root of unity. We can choose $a = -x^3 + 1$. Now $(2x^q - 1)^2 + 3 = 4(x^{2q} - x^q + 1) \equiv 0 \mod f(x)$. So $(2x^q - 1)$ corresponds

to the element $\sqrt{-3}$ and we set $b = (-x^3 - 1)(2x^q + 1)$. The relation $\frac{\log(p)}{\log(\ell)}$ is approximately $\frac{q+3}{q-1}$.

4. Cryptographically interesting examples

4.1. **Curves with low Hamming weight.** Pairing based cryptography is very efficient if the prime ℓ is a prime of low signed Hamming weight (see [4, 10]). For the signed Hamming weight we allow the coefficients of the binary expansion to be $-1, 0, 1$.
Using the method in section 2 we find some particularly nice examples. To find these examples we run through all cylcotomic fields with discriminant divisible by 3 or 4. For each field, we determine the minimal polynomial $f(x)$ and test whether $f(x_0)$ is prime for some x_0 of low Hamming weight, say $x_0 = 2^i$, $x_0 = 2^i \pm 2^k$ or $x_0 = 3^i$. Next we choose a discriminant $D = -3, -4$, compute the corresponding polynomials $a(x)$ and $b'(x)$ and test whether $\frac{a(x_0)^2 - D(b(x_0)'/D)^2}{4}$ is prime, too.

1. Take $M = \mathbb{Q}(\zeta_{15})$, $k = 15$ and the imaginary quadratic field of discriminant $D = -3$.
   Let $x_0 = 2^{32}+1$ and $\ell = \Phi_{15}(x_0)$. The prime ℓ has 257 binary digits and signed Hamming weight 17. Set $a = x_0^4+1$ and $b = 2x_0^7-2x_0^6-2x_0^5+x_0^4-2x_0^3+2x_0^2-3$. The prime p is given by $\frac{1}{4}(a^2+3(\frac{b}{3})^2)$. It is of order $O(\ell^{\frac{7}{4}})$.
2. Take $M = \mathbb{Q}(\zeta_{20})$, $k = 10$ and the imaginary quadratic field of discriminant $D = -1$.
   Let $x_0 = 2^{23}+1$ and $\ell = \Phi_{20}(x_0)$. We have $\lfloor \log_2(\ell) \rfloor \sim 184$ and ℓ has signed Hamming weight 17. Set $a = x_0^2+1$ and $b = x_0^7 - x_0^5$. The prime $p = \frac{1}{4}(a^2+b^2)$ is of order $O(\ell^{\frac{7}{4}})$
3. Take $M = \mathbb{Q}(\zeta_{48})$, $k = 24$ and the imaginary quadratic field of discriminant $D = -3$.
   Let $x_0 = 2^{12}+2$ and $\ell = \Phi_{48}(x_0)$. The prime ℓ has 185 binary digits and sigend Hamming weight 24. Set $a = x_0^2+1$ and $b = -2x_0^{10}+2x_0^8+x_0^2-1$. The prime p is of order $O(\ell^{\frac{5}{4}})$.
   The prime p is given by $\frac{1}{4}(a^2+3(\frac{b}{3})^2)$.
4. Take $M = \mathbb{Q}(\zeta_{12})$, $k = 12$ and the imaginary quadratic field $D = -3$.
   Let $x_0 = 2^{39}+2^{11}+2^{10}$ and $\ell = \Phi_{12}(x_0)$. Then ℓ has 157 binary digits and signed Hamming weight 21. Set $a = -x_0^3+x_0+1$ and $x_0^3 - 2*x_0^2+x_0+1$. The prime p is of order $O(\ell^{\frac{3}{2}})$.

4.2. **Curves with fast addition chain.** There exist natural numbers whose Hamming weight is not particularly small but which still allow a fast scalar multiplication.

Lemma 4.1. *Let P be a point on an elliptic curve and let*

$$m = 2^{j_1} \pm 2^{j_2} \pm 2^{j_3}$$

where $0 \le j_3 < j_2 < j_1$. Then mP can be computed with j_1 doublings and two additions/subtractions.

Note that a subtraction has the same complexity as an addition, since taking the additive inverse on an elliptic curve is a free operation.

Proof. Set $Q_1 = 2^{j_3}P$, $Q_2 = 2^{j_2-j_3}Q_1$ and $Q_3 = 2^{j_1-j_2}Q_2$. We need j_1 doublings to compute Q_1, Q_2 and Q_3 and 2 additions/subtractions to compute $Q_3 \pm Q_2 \pm Q_1$. □

We can now consider the values of certain cyclotomic polynomials at m given as above.

Corollary 4.2. *Let f be a polynomial of degree s with coefficients in $\{0, \pm 1\}$ and t non-zero coefficients. Then $f(m)$ with m given as in Lemma 4.1 can be evaluted with sj_1 doublings and $2s + t - 1$ additions/subtractions.*

For the proof we just count the number of operations.

Example 4.3.

1. Take $m = 2^{22} + 2^{13} + 1$ and consider $M = \mathbb{Q}(\zeta_{24})$ with $k = 8$. We have $\Phi_{24} = x^8 - x^4 + 1$ and we realize $\ell = \Phi_{24}(m)$ and we can calculate ℓP with only $8 \cdot 22 = 176$ doublings and 18 additions. Note that the signed Hamming weight of $\Phi_{24}(m)$ is larger than 30.
   We have $\lfloor \log_2(\ell) \rfloor \sim 176$. Set $a = x_0^5 - x_0 + 1$ and $b = x_0^5 + 2x_0^4 + x_0 - 1$. The prime p is of order $O(\ell^{\frac{5}{4}})$.
   Alternatively, we can take $m = 2^{23} + 2^{17} + 2^6$. In this case, the evaluation takes $8 \cdot 23 = 184$ doublings and 18 additions. We set $a = -x_0^5 + x_0 + 1$ and $b = -x_0^5 + 2x_0^4 - x_0 - 1$. The prime is of order $O(\ell^{\frac{5}{4}})$.
   Or we take $m = 2^{22} - 2^{10} - 2^4$ and $-x_0^5 + x_0 + 1$ and $b = -x_0^5 + 2x_0^4 - x_0 - 1$. In all three cases, we find an elliptic curve over $\mathbb{F}_p$ with $p = \frac{1}{4}\left(a^2 + 3(\frac{b}{3})^2\right)$ with complex multiplication by $\mathbb{Z}[\zeta_3]$.
2. Take $\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$ and $m = 2^{20} + 2^{14} + 4$. Then $\ell = \Phi_{20}(m)$ can be computed using 160 doublings and 20 additions.
   Let $k = 10$ and set $a = -x_0^6 + x_0^4 - x_0^2 + 2$ and $b = 2x_0^5 - 2x_0^3$. We find an elliptic curve with complex multiplication by $\mathbb{Z}[i]$ over $\mathbb{F}_p$ with $p = \frac{1}{4}(a^2 + b^2)$ of order $O(\ell^{\frac{3}{2}})$.

References

[1] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61:29–68, 1993.

[2] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology*, 11(2):141–145, 1998.

[3] P. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. *Proceedings of the Third Workshop on Security in Communication Networks (SCN'2002), LNCS*, 2576, 2003.

[4] S.L.M. Barreto, H.Y. Kim, B. Lynn, and P. Scott. Efficient algorithms for pairing based cryptosystems. *Crypto 2002, LNCS*, 2442:354–368, 2002.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. *Asiacrypt '01, LNCS*, 2248:514–532, 2001.

[6] C. Cocks and R.G.E. Pinch. unpublished manuscript. 2002.

[7] M. Franklin D. Boneh. Identity-based encryption from the weil pairing. *Proceedings Crypto '01, LNCS*, 2139:213–229, 2001.

[8] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small mov degree over finite fields. preprint, 2002.

[9] G. Frey, M. Müller, and H.-G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory*, 45(5):1717–1718, 1999.

[10] S. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing. *ANTS IV, LNCS*, 2369:324–337, 2002.

[11] A. Joux. A one round protocol for tripartite diffie-hellman. *Proceedings of ANTS, LNCS*, 1838:385–393, 2000.

[12] A. Lenstra and E. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, 14:255–293, 2001.

[13] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[14] E. Verheul. Self-blindable credential certificates from the weil pairing. *Advances in Cryptology - Asiacrypt 2001, LNCS*, 2248:533–551, 2002.

Fachbereich Mathematik, Johann Wolfgang Goethe-Universität, Robert-Mayer-Str. 10, 60051 Frankfurt

Institut für Experimentelle Mathematik, Universität Essen-Duisburg, Ellernstr. 29, 45326 Essen, Germany

E-mail address: `brezing@stud.uni-frankfurt.de, weng@exp-math.uni-essen.de`