Lifting Elliptic Curves and Solving the Elliptic Curve Discrete Logarithm Problem

Ming-Deh A. Huang, Ka Lam Kueh, and Ki-Seng Tan

[1] Department of Computer Science, University of Southern California, Los Angeles, CA 90089-0781
huang@pollux.usc.edu
[2] Institute of Mathematics, Acedemia Sinica, Taipei, Taiwan
maklk@ccvax.sinica.edu.tw
[3] Department of Mathematics, National Taiwan University, Taipei, Taiwan
tan@math.ntu.edu.tw

Abstract. Essentially all subexponential time algorithms for the discrete logarithm problem over finite fields are based on the index calculus idea. In proposing cryptosystems based on the elliptic curve discrete logarithm problem (ECDLP) Miller [6] also gave heuristic reasoning as to why the index calculus idea may not extend to solve the analogous problem on elliptic curves. A careful analysis by Silverman and Suzuki provides strong theoretical and numerical evidence in support of Miller's arguments. An alternative approach recently proposed by Silverman, dubbed 'xedni calculus', for attacking the ECDLP was also shown unlikely to work asymptotically by Silverman himself and others in a subsequent analysis. The results in this paper strengthen the observations of Miller, Silverman and others by deriving necessary but difficult-to-satisfy conditions for index-calculus type of methods to solve the ECDLP in subexponential time. Our analysis highlights the fundamental obstruction as being the necessity to lift an asymptotically increasing number of random points on an elliptic curve over a finite field to rational points of reasonably bounded height on an elliptic curve over $\mathbf{Q}$. This difficulty is underscored by the fact that a method that meets the requirement implies, by virtue of a theorem we prove, a method for constructing elliptic curves over $\mathbf{Q}$ of arbitrarily large rank.

1 Introduction

In the elliptic curve discrete logarithm problem (ECDLP), we are given an elliptic curve E over a finite field $\mathbf{F}_q$ and two points P and Q on the curve, and the problem is to find an integer n (if it exists) such that $Q = nP$. The ECDLP is an analog of the discrete logarithm problem over finite fields, which is the basis of many public key cryptosystems. Miller [6] and Koblitz [3] independently proposed public key cryptosystems based on the elliptic curve discrete logarithm problem. In proposing such cryptosystems Miller [6] also gave heuristic reasoning as to why the index calculus idea, which lies at the heart of all the subexponential algorithms for the discrete logarithm problem, may not extend to solve the elliptic curve discrete logarithm problem.

The classical index calculus method for the discrete logarithm problem works by lifting the problem from a finite field to the ring of integers, where there is much richer arithmetic structure to take advantage of. To extend this idea to work for the ECDLP, it is natural to consider lifting an elliptic curve $E/\mathbf{F}_p$ of interest to some elliptic curve $\mathcal{E}/\mathbf{Q}$ in order to possibly take advantage of the structure of $\mathcal{E}(\mathbf{Q})$. Miller pointed out the difficulty for such an approach is at least two fold: first in lifting the curve E to a curve $\mathcal{E}$ of sufficiently large rank over $\mathbf{Q}$, then in actually lifting points from E to rational points of reasonably bounded height on $\mathcal{E}$. A careful analysis by Silverman and Suzuki in [10] provides strong theoretical and numerical evidence in support of Miller's arguments.

Silverman [8] proposed an alternative approach, dubbed the 'xedni calculus', for attacking the ECDLP. The xedni idea 'turns the index calculus on its head' by first lifting a bounded number (nine) of points to $\mathbf{Q}$ then finding a lift $\mathcal{E}/\mathbf{Q}$ of E to fit the lifted points. This approach circumvents the difficulty of lifting points and does not require the lift $\mathcal{E}$ for E to have a large rank. In fact the success of this method depends on the lifted points being linearly dependent in $\mathcal{E}(\mathbf{Q})$. The probability for this to occur would presumably be low. To increase the probability Silverman imposed additional conditions on the lift based on some heuristic arguments involving the Birch-Swinnerton-Dyer Conjecture. However, a subsequent analysis by Silverman and Jacobson et al [2] shows that with the xedni algorithm the probability of success in finding a discrete logarithm on an elliptic curve over a finite field is in fact negligible asymptotically speaking.

The results in this paper strengthen the observations of Miller [6] and the analysis of Silverman et al [2, 10] by deriving necessary but difficult-to-satisfy conditions for any index-calculus type of method which involves the lifting idea to solve the ECDLP in subexponential time.

The center piece of our analysis is the following result concerning lifting an elliptic curve over a finite fields together with a finite set of points. Let E be an elliptic curve over a finite field $\mathbf{F}_p$. For $r \in \mathbf{Z}_{>0}$ and $h \in \mathbf{R}_{>0}$, let $n_E(r,h)$ denote the number of $(r+1)$-tuples $\lambda = (P_0, ..., P_r)$ with P_i in some cyclic subgroup of $E(\mathbf{F}_p)$ so that (E, λ) can be lifted to some $(\mathcal{E}_\lambda, \Lambda)$ over $\mathbf{Q}$ with the rank of $\mathcal{E}(\mathbf{Q})$ bounded by r and the canonical heights of the points in Λ bounded by h. We show that $n_E(r,h)$ is bounded by $2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}N^r$ where $N = |E(\mathbf{F}_p)|$.

From the theorem we deduce the following conclusions.

With the approach such as the index calculus method, where one lifts an elliptic curve $E/\mathbf{F}_p$ to an elliptic curve $\mathcal{E}/\mathbf{Q}$ before lifting random points (generated from the two points in question), in order to possibly achieve subexponential running time (such as $O(\exp(c(\log p)^{1/2}(\log\log p)^{1/2}))$, the rank of $\mathcal{E}$ needs to grow at least as fast as $(\log p)^{1/4}$ as p grows.

With the approach such as the xedni calculus method, where one lifts a set of random points (generated from the two points in question) then constructs a curve $\mathcal{E}$ to fit the lifted points, in order to possibly achieve subexponential running time (such as $O(\exp(c(\log p)^{1/2}(\log\log p)^{1/2}))$, the number of lifted points needs to grow at least as fast as $(\log p)^{1/4}$ as p grows. To underscore the difficulty in meeting this condition, we show that a method for lifting an asymptotically increasing number (such as $(\log p)^{1/4}$) of random points on an elliptic curve over $\mathbf{F}_p$ to rational points of canonical height bounded subexponential in $\log p$ on an elliptic curve over $\mathbf{Q}$ implies a method for constructing elliptic curves over $\mathbf{Q}$ of arbitrarily large rank. On the other hand, bounding the number of lifted points, as the xedni algorithm in [8], results in asymptotically negligible probability of success in solving the ECDLP.

Our analysis depends on a conjecture of Lang [4] that the canonical height of any nonzero rational point on an elliptic curve $\mathcal{E}$ over $\mathbf{Q}$ is bounded from below by $c \log |\Delta(\mathcal{E})|$ where c is a universal constant independent of $\mathcal{E}$ and $\Delta(\mathcal{E})$ is the minimal discriminant of $\mathcal{E}$. Lang's conjecture is the only unproven assumption needed throughout this paper. (The results in [2, 10] depend on Lang's conjecture as well as other heuristic assumptions.) It is worth mentioning that the conjecture has been proven to a large extent [1, 9].

It should be pointed out that our results are asymptotic in nature and they leave open the possibility for the index-calculus idea (including the xedni method) to successfully attack the ECDLP in the lower range of p.

The rest of this paper is organized as follows. In Section 2 we prove the theorem concerning the lifting problem and in Section 3 we relate the result to the elliptic curve discrete logarithm problem.

2 The lifting problem

Let E be an elliptic curve over a finite field $\mathbf{F}_p$ and $\lambda = (P_1, \ldots, P_m)$ with $P_i \in E(\mathbf{F}_p)$. Let $\mathcal{E}$ be an elliptic curve over $\mathbf{Q}$ and $\Lambda = (\mathcal{P}_1, \ldots, \mathcal{P}_m)$ with $\mathcal{P}_i \in \mathcal{E}(\mathbf{Q})$. We say that (E, λ) is lifted to $(\mathcal{E}, \Lambda)$ if E can be obtained as the reduction of $\mathcal{E}$ modulo p with P_i as the reduction of $\mathcal{P}_i$ modulo p for $i = 1, \ldots, m$. We say that λ is lifted with E with canonical height bounded by h if the canonical height of $\mathcal{P}_i$ is bounded by h for $i = 1, \ldots, m$.

Let $\hat{h}(\mathcal{P})$ denote the canonical height [7] of $\mathcal{P}$ for $\mathcal{P} \in \mathcal{E}(\mathbf{Q})$. Let

$$N(\mathcal{E}, b) = \#\{\mathcal{P} \in \mathcal{E}(\mathbf{Q}) : \hat{h}(\mathcal{P}) \leq b\}.$$

Let $r = r(\mathcal{E})$ be the rank of $\mathcal{E}(\mathbf{Q})$, T be the number of torsion points in $\mathcal{E}(\mathbf{Q})$, and R be the regulator of $\mathcal{E}$ over $\mathbf{Q}$. Then it is known [4] that

$$N(\mathcal{E}, b) \approx T \alpha_r \left(\frac{b}{R^{1/r}} \right)^{r/2},$$

where α_r is the volume of the unit r-ball. We assume Lang's conjecture [4] that

$$\hat{h}(\mathcal{P}) \geq c \log |\Delta(\mathcal{E})|$$

for some constant c independent of $\mathcal{E}$, where $\Delta(\mathcal{E})$ denotes the minimal discriminant of $\mathcal{E}$. Then from

$$R^{1/r} \geq \left(\frac{\sqrt{3}}{2} \right)^{r-1} \min \hat{h}(\mathcal{P})$$

where the minimum is over all nonzero $\mathcal{P} \in \mathcal{E}(\mathbf{Q})$ (see [4]), and

$$\alpha_r \approx \frac{1}{\sqrt{\pi r}} \left(\frac{2\pi e}{r}\right)^{r/2},$$

and that $T \leq 16$ (see [5]), it follows that for $r \geq 1$

$$N(\mathcal{E}, b) \leq 2^{c_1 r^2} \left(\frac{b}{\log|\Delta|}\right)^{r/2} \tag{1}$$

for some positive constant c_1 independent of $\mathcal{E}$.

Proposition 1. *There exists a positive constant c such that for all elliptic curves $\mathcal{E}$ defined over $\mathbf{Q}$, if the rank of $\mathcal{E}(\mathbf{Q})$ is no greater than r, then for any $\mathcal{P}_0$, ..., $\mathcal{P}_r$ in $\mathcal{E}(\mathbf{Q})$ with $\hat{h}(\mathcal{P}_i) \leq h$, there exist integers c_i with $|c_i| \leq 2^{cr^2}(\frac{h}{\log|\Delta|})^{r/2}$ such that $\sum_i c_i \mathcal{P}_i = 0$, where Δ is the minimal discriminant of $\mathcal{E}$.*

Proof For $\mathcal{P} \in \mathcal{E}(\mathbf{Q})$, let $||\mathcal{P}|| = \sqrt{\hat{h}(\mathcal{P})}$. For $a_i \in \{0, ..., m-1\}$,

$$||\sum_{i=0}^{r} a_i \mathcal{P}_i|| \leq \sum_{i=0}^{r} |a_i| ||\mathcal{P}_i|| \leq \sqrt{h} \sum_{i=0}^{r} |a_i| \leq m(r+1)\sqrt{h}.$$

So

$$\hat{h}(\sum_{i=0}^{r} a_i \mathcal{P}_i) \leq m^2 (r+1)^2 h.$$

Since the number of $(a_0, ..., a_r)$ with $a_i \in \{0, ..., m-1\}$ is m^{r+1}, if

$$N(\mathcal{E}, m^2(r+1)^2 h) < m^{r+1}, \tag{2}$$

then there must exist two distinct $(a_0, ..., a_r)$ and $(b_0, ..., b_r)$ with $a_i, b_i \in \{0, ..., m-1\}$ such that $\sum_i a_i \mathcal{P}_i = \sum_i b_i \mathcal{P}_i$, and hence $\sum_i c_i \mathcal{P}_i = 0$ with $c_i = a_i - b_i$, so $|c_i| < m$. From Eq. (1),

$$N(\mathcal{E}, m^2(r+1)^2 h) < 2^{c_1 r^2} \left(\frac{m^2(r+1)^2 h}{\log|\Delta|}\right)^{r/2}$$

for some constant c_1 independent of $\mathcal{E}$. Hence (2) holds if $m > 2^{cr^2}(h/\log|\Delta|)^{r/2}$ where c is a constant independent of $\mathcal{E}$.

Theorem 1. *Let E be an elliptic curve over a finite field $\mathbf{F}_p$. For $r \in \mathbf{Z}_{>0}$ and $h \in \mathbf{R}_{>0}$, let $n_E(r, h)$ denote the number of $\lambda = (P_0, ..., P_r)$ with P_i in some cyclic subgroup of $E(\mathbf{F}_p)$ so that (E, λ) can be lifted to some $(\mathcal{E}, \Lambda)$ over $\mathbf{Q}$ with the canonical heights of the points in Λ bounded by h and the rank of $\mathcal{E}(\mathbf{Q})$ bounded by r. Then $n_E(r, h)$ is bounded by $2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)} N^r$ where $N = |E(\mathbf{F}_p)|$ and Δ is the minimal discriminant of $\mathcal{E}$. .*

Proof Let $\lambda = (P_0, ..., P_r)$ with P_i in some cyclic subgroup of $E(\mathbf{F}_p)$ with a generator S. Suppose (E, λ) is lifted to some $(\mathcal{E}, \Lambda)$ with canonical height bounded by h. Suppose $\Lambda = (\mathcal{P}_0, ..., \mathcal{P}_r)$. If the rank of $\mathcal{E}(\mathbf{Q})$ is bounded by r, then from Proposition 1 it follows that there exist integers c_i such that

$$\sum_i c_i \mathcal{P}_i = 0,$$

where

$$|c_i| \leq 2^{cr^2} \left(\frac{h}{\log |\Delta|} \right)^{r/2}$$

and Δ is the minimal discriminant of $\mathcal{E}$.

Suppose $P_i = m_i S$. Then

$$0 = \sum_i c_i P_i = (\sum_i c_i m_i) S.$$

So

$$\sum_i c_i m_i \equiv 0 \pmod{N}$$

where N is the order of S. Now $n_E(r, h)$ is bounded by the number of $(m_0, ..., m_r)$ such that $\sum_i c_i m_i \equiv 0 \pmod{N}$ and $|c_i|$ is bounded by

$$M = 2^{cr^2} \left(\frac{h}{\log |\Delta|} \right)^{r/2}.$$

For each $c = (c_0, .., c_r)$, let n_c denote the number of $(m_0, ..., m_r)$ mod N such that

$$c_0 m_0 + ... + c_r m_r \equiv 0 \pmod{N}.$$

Suppose the g.c.d. of c_0, ..., c_r is g, then

$$n_c \leq g N^r \leq M N^r.$$

So

$$n_E(r, h) \leq (2M + 1)^{r+1} M N^r = 2^{O(r^3)} (h / \log |\Delta|)^{O(r^2)} N^r.$$

3 Analysis on the Index-calculus Approach to ECDLP

In the elliptic curve discrete logarithm problem we are given an elliptic curve E over a finite field $\mathbf{F}_p$, and two points $S, T \in E(\mathbf{F}_p)$, and the problem is to find an integer m (if it exists) so that $mS = T$.

A natural generalization of the index calculus method for the ECDLP can be outlined as follows.

1. Find an elliptic curve $\mathcal{E}$ defined over $\mathbf{Q}$ whose reduction mod p is E. Suppose $\mathcal{E}(\mathbf{Q})$ has rank r with a basis $\mathcal{P}_i$, $i = 1, ..., r$, and suppose $P_i \in E(\mathbf{F}_p)$ is the reduction of $\mathcal{P}_i$ mod p.

2. For random integer j, lift jS to some $S' \in \mathcal{E}(\mathbf{Q})$, and write S' in terms of $\mathcal{P}_i$ (up to a torsion point). Each S' yields a linear relation on the discrete logarithms of P_i. With r many linearly independent relations we can solve for the discrete logarithms $\log_S(P_i)$ of all P_i.
3. For random integer j, lift $T + jS$ to some $S' \in \mathcal{E}(\mathbf{Q})$, and write S' in terms of $\mathcal{P}_i$. Then $\log_S(T)$ can be determined.

For the method to work in subexponential time, $r+1$ random points in $E(\mathbf{F}_p)$ need to be lifted to points in $\mathcal{E}(\mathbf{Q})$ of canonical height bounded by some h which can be at most subexponential in $\log p$. The number of such $(r+1)$-tuples of points in $E(\mathbf{F}_p)$ cannot be greater than $n_E(r,h)$, which by Theorem 1 is bounded by $2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}N^r$. Hence the success probability is bounded by $\frac{2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}}{N}$. Since N can be in the order of p, for the success probability to be at least $1/exp[(\log p)^{1/2}(\log\log p)^{1/2}]$, say, it is necessary that $r^2 \log h > c' \log p$ for some constant c'. Since h can be at most $exp[O(1)(\log p)^{1/2}(\log\log p)^{1/2}]$, the number of lifted points $r+1$ needs to be at least in the order of $(\log p)^{1/4}$ as p grows.

The same conclusion can also be deduced from Proposition 1. Let h be an upper bound on $\hat{h}(\mathcal{P}_i)$ and $\hat{h}(S')$ where S' lifts a point P in $E(\mathbf{F}_p)$. Then from Proposition 1 it follows that there exist integers c_i with absolute values bounded by $2^{cr^2}(h/\log|\Delta|)^{r/2}$ such that

$$c_0 S' + c_1 \mathcal{P}_1 + \ldots + c_r \mathcal{P}_r = 0$$

so

$$c_0 P + c_1 P_1 + \ldots + c_r P_r = 0.$$

The number of $P \in E(\mathbf{F}_p)$ satisfying

$$c_0 P + c_1 P_1 + \ldots + c_r P_r = 0$$

with $|c_i| \le 2^{cr^2}(h/\log|\Delta|)^{r/2}$ is bounded by $2^{O(r^3)}h^{O(r^2)}$.

It follows that the probability that a random P can be lifted to some S' with height bounded by h is no greater than $\frac{2^{O(r^3)}h^{O(r^2)}}{p}$. For the probability to be at least $1/exp[(\log p)^{1/2}(\log\log p)^{1/2}]$, say, it is necessary that $r^2 \log h > c' \log p$ for some constant c'. Even if we allow the points to be lifted to subexponential canonical height so that h is about $exp[(\log p)^{1/2}(\log\log p)^{1/2}]$, the rank r of $\mathcal{E}$ still needs to be at least in the order of $(\log p)^{1/4}$.

Note that the observation above holds regardless of the method used to construct $\mathcal{E}$ and lift a point from E to $\mathcal{E}$. The fact that the rank of $\mathcal{E}$ needs to grow at least as fast as $(\log p)^{1/4}$ as p grows already poses a significant difficulty for the index calculus method to work.

Next we turn our attention to the xedni calculus method for the elliptic curve discrete logarithm problem. Below is a general outline for the method.

1. Generate random P_0, ..., P_r with $P_i = a_i S + b_i T$ where a_i, b_i are random integers.

2. Lift P_i to some $\mathcal{P}_i$ over $\mathbf{Q}$, then construct an elliptic curve $\mathcal{E}$ over $\mathbf{Q}$ so that the pair $\mathcal{E}$ and $(\mathcal{P}_0, ..., \mathcal{P}_r)$ is a lift of E and $(P_0, ..., P_r)$.
3. If the rank of $\mathcal{E}(\mathbf{Q})$ is no greater than r, then $\mathcal{P}_0$, ..., $\mathcal{P}_r$ are integrally dependent, so that
$$\sum_i c_i \mathcal{P}_i = 0$$
for some integers c_i, then upon reduction mod p we have
$$0 = \sum_i c_i(a_i S + b_i T) = (\sum_i c_i a_i)S + (\sum_i c_i b_i)T.$$
From this the discrete logarithm of T in terms of S can be obtained with high probability, since a_i and b_i are randomly chosen.

The xedni algorithm of Silverman is consistent with the outline above, with r set at 9, and as mentioned before, additional conditions imposed on $\mathcal{E}$.

For the method to work in subexponential time, $r + 1$ random points in $E(\mathbf{F}_p)$ need to be lifted to points of canonical height at most subexponential in $\log p$ on some $\mathcal{E}$ over $\mathbf{Q}$ of rank at most r. The number of random $(r + 1)$-tuples $\lambda = (P_0, ..., P_r)$ is bounded by N^{r+1}. For a λ to lead to a success in finding the discrete logarithm we need (E, λ) to be lifted to some $(\mathcal{E}, \Lambda)$ over $\mathbf{Q}$ with the canonical heights of the points in Λ bounded by h and the rank of $\mathcal{E}(\mathbf{Q})$ bounded by r. The number of such $(r + 1)$-tuples cannot be greater than $n_E(r, h)$, which by Theorem 1 is bounded by $2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}N^r$. Hence the success probability is bounded by $\frac{2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}}{N}$. Since N can be in the order of p, for the success probability to be at least $1/exp[(\log p)^{1/2}(\log\log p)^{1/2}]$, say, it is necessary that $r^2 \log h > c' \log p$ for some constant c'. Since h is at most $exp[O(1)(\log p)^{1/2}(\log\log p)^{1/2}]$, the number of lifted points $r + 1$ needs to be at least in the order of $(\log p)^{1/4}$ as p grows. This is true regardless of how the curve $\mathcal{E}$ is constructed for each $(r + 1)$-tuple of points in $E(\mathbf{F}_p)$. In particular, for bounded r (such as the case with the xedni method in [8]), the probability of success tends to zero asymptotically with p. Hence the xedni calculus method as described in [8] cannot work as a subexponential algorithm asymptotically.

To extend the scope of applicability of the xedni calculus idea, we would need to increase the the number of random points on an elliptic curve to be lifted to rational points of reasonably bounded canonical height on an elliptic curve over $\mathbf{Q}$. But the difficulty of such task is underscored by that of constructing elliptic curves of large rank over $\mathbf{Q}$ as reasoned below.

Let $m_E(r, h)$ denote the number of $\lambda = (P_0, ..., P_r)$ with P_i in $E(\mathbf{F}_p)$ so that (E, λ) can be lifted to some $(\mathcal{E}, \Lambda)$ over $\mathbf{Q}$ with the canonical heights of the points in Λ bounded by h. For any fixed r, suppose for elliptic curves E over $\mathbf{F}_p$, $m_E(r, h) \geq N^{r+1}/p^c$ where where c is a positive constant less than 1 and $\log h/\log p$ tends to 0 as p tends to infinity (say h is subexponential in $\log p$). Then by Theorem 1, $m_E(r, h) > n_E(r, h)$ for sufficiently large p and E with cyclic group $E(\mathbf{F}_p)$. It follows that for sufficiently large p, some elliptic curve over $\mathbf{Q}$ lifting some elliptic curve E over $\mathbf{F}_p$ together with some r-tuple of points on E must have rank at least r.

4 Acknowledgement

We would like to thank Joe Silverman for reading an earlier draft of this paper and for his valuable suggestions.

References

1. M. Hindry and J. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math., 93, (1988), 419-450.
2. M.J. Jacobson, N. Koblitz, J.H. Silverman, A. Stein, and E. Teske, Analysis of the Xedni Calculus Attack, Preprint.
3. N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, 48, pp. 203-209, 1987.
4. S. Lang, *Fundamental of Diophantine Geometry*, Springer-Verlag, 1983.
5. B. Mazur, Modular curves and Eisenstein ideal, *I.H.E.S. Publ. Math.* 47 (1977), 33-186.
6. V. Miller, The use of elliptic curves in cryptography. *Advances in Cryptography*, Ed. H.C. Williams, Springer-Verlag, 1986, 417-426.
7. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.
8. J.H. Silverman, The xedni calculus and the elliptic curve discrete logarithm problem, preprint.
9. J.H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J., 48 (1981), 633-648.
10. J.H. Silverman and J. Suzuki, Elliptic curve discrete logarithms and the index calculus, *Advances in Cryptology -Asiacrypt '98*, Springer-Verlag, 1998, 110-125.