Elliptic divisibility sequences and the elliptic curve discrete logarithm problem

Rachel Shipsey[1] and Christine Swart[2]

[1] University of London, Goldsmiths College, New Cross, London, SE14 6NW, map01rs@gold.ac.uk.
[2] University of Cape Town, Rondebosch, 7701, South Africa, christine.swart@uct.ac.za.

Abstract. We use properties of the division polynomials of an elliptic curve E over a finite field $\mathbb{F}_q$ together with a pure result about elliptic divisibility sequences from the 1940s to construct a very simple alternative to the Menezes-Okamoto-Vanstone algorithm for solving the elliptic curve discrete logarithm problem in the case where $\#E(\mathbb{F}_q) = q - 1$.

Keywords: elliptic divisibility sequences, elliptic curve cryptography, elliptic curve discrete logarithm problem.

1 Introduction

The use of elliptic curves in cryptography relies on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP):

> Let P be a point of order N on an elliptic curve E over a finite field $\mathbb{F}_q$. Given a point $Q = [k]P$ for some $k \in \{0, 1, \dots, N-1\}$, find k.

Given E, the number of points in the group $E(\mathbb{F}_q)$ can be computed in polynomial time using Schoof's algorithm. By Hasse's Theorem the order of the group is $q + 1 - t$, where $|t| \le 2\sqrt{q}$. The order N of P is usually assumed to be a large prime factor of $\#E(\mathbb{F}_q)$; this is because of the Pohlig-Hellman algorithm, which allows the ECDLP in each of the prime-order subgroups of $\langle P \rangle$ to be solved separately and then combined.

The discrete logarithm problem (DLP) in a finite field $\mathbb{F}_q$ is, given two elements a and $b = a^k$, to find k. If a cryptosystem is based on the DLP in $\mathbb{F}_q$ then the order q (and hence the keys of the cryptosystem) have to be large enough to prevent the Index Calculus attacks, which are subexponential in $\log q$. These methods do not work on elliptic curves; if E is chosen at random then the best algorithms known for solving the ECDLP are the exponential "square root" attacks (see, for example, [14]) which work in any finite group. So, in an elliptic curve cryptosystem over $\mathbb{F}_q$, q only has to be large enough to prevent these generic attacks, which have a running time proportional to $\sqrt{N}$ and hence $\sqrt{q}$. This is why elliptic curve cryptosystems can use smaller underlying fields than systems based on the DLP in a finite field, and achieve the same security using smaller keys. There are, however, some special cases of "weak curves" $E/\mathbb{F}_q$ that should not be used for cryptography because the discrete logarithm problem is no harder in them than in the underlying field. The first weak curves to be identified were those in which N divides $q^r - 1$ for small r, which are vulnerable to the "MOV attack" of Menezes, Okamoto and Vanstone [12], and to Frey and Rück's extension of it [13]. These attacks work by using the Weil-Tate pairing to give an isomorphism between $\langle P \rangle$ and the subgroup μ_N of N^{th} roots of unity in the extension field $\mathbb{F}_{q^r}$. This reduces the ECDLP in $E(\mathbb{F}_q)$ to a DLP in the field $\mathbb{F}_{q^r}^*$, which can be solved using Index Calculus methods if q^r is small enough. The attack works particularly well when $\#E(\mathbb{F}_q) = q \pm 1$.

The division polynomials of an elliptic curve $E/\mathbb{F}_q$, when evaluated at a point $P \in E(\mathbb{F}_q)$, yield a sequence of elements of $\mathbb{F}_q$ that satisfy the elliptic divisibility sequence (EDS) recurrence relation. Elliptic divisibility sequences were shown by Morgan Ward to have certain "symmetry" properties, which can be adapted to yield a symmetry formula satisfied by the division polynomials. Following an idea by Nelson Stephens we use this, together with well-known properties of the division polynomials, to give a simple alternative algorithm to solve the ECDLP in the case where $\#E(\mathbb{F}_q) = q - 1$. After some preliminary material on EDS and division polynomials in sections 2 and 3, we describe our ECDLP algorithm in section 4. In section 5 we comment briefly on the feasibility of extending our algorithm to the more general MOV setting, and make a brief remark describing how EDS can be used to elegantly reformulate Lenstra's elliptic curve factorisation method.

Finally, we note that the algorithm described here is the same underneath as the algorithm described in Shipsey's thesis [15], but using known properties of the division polynomials allows us to streamline it considerably. It is placed in a more general theoretical context of hard problems on EDS by Kate Stange and Kristin Lauter in [10].

2 Elliptic divisibility sequences

An *elliptic divisibility sequence* or *EDS* is a sequence (W_n) of integers satisfying the recurrence relation

$$W_{m+n}\, W_{m-n} = W_{m+1}\, W_{m-1}\, W_n^2 - W_{n+1}\, W_{n-1}\, W_m^2 \quad \text{for all } m, n \in \mathbb{Z}, \tag{1}$$

with the *divisibility property* that W_n divides W_m whenever n divides m. EDS were studied in some depth by Morgan Ward [22, 23]; they were interesting in being the first divisibility sequences to be defined by a non-linear recurrence.

It is easy to prove that all EDS have $W_0 = 0$, $W_1 = \pm 1$ and $W_{-n} = -W_n$ for all $n \in \mathbb{Z}$. Ward was interested in the properties of an EDS reduced modulo a prime. He showed that the multiples of most primes are regularly spaced in (W_n); the constant N is called the *gap* of p.

Theorem 1. *Let (W_n) be an EDS and p a prime not dividing W_2 or W_3. Then there exists a positive integer N such that*

$$W_n \equiv 0 \pmod{p} \quad \Longleftrightarrow \quad n \equiv 0 \pmod{N}.$$

Ward also found a "symmetry formula" satisfied by EDS. An elementary proof is given in [1]; we provide a sketch below.

Theorem 2. *Let (W_n) be an EDS, let p be a prime not dividing W_2 or W_3, and let p have gap N in (W_n). Then there exist constants c and d such that $d^2 \equiv c^N \pmod{p}$, and for all $s, t \in \mathbb{Z}$,*

$$W_{t+sN} \equiv c^{st}\, d^{s^2}\, W_t \pmod{p}.$$

Proof: Define the constants c and d by

$$c \equiv \frac{W_{N-1}}{W_{-1}} \cdot \frac{W_{-2}}{W_{N-2}} \bmod p \quad \text{and} \quad d \equiv \left(\frac{W_{N-1}}{W_{-1}}\right)^2 \frac{W_{-2}}{W_{N-2}} \bmod p.$$

We first prove the $s = 1$ case by induction on t. The formula holds trivially for $t = 0$ and holds for $t = -1$ and $t = -2$ by definition of c and d. The $t = -3$ case then follows because

$$W_{N-3}\, W_{N-1}\, W_2^2 - W_1\, W_3\, W_{N-2}^2 = W_{N-4}\, W_N \equiv 0 \pmod{p},$$

which supplies a relation between W_{N-3}, W_{N-2} and W_{N-1}. Now that we have the symmetry formula holding for four values of t, we can use the EDS formula with $n = 2$ to prove that it holds for the next value of t. Whenever we hit a value of t for which $W_{t-4} \equiv 0 \pmod{p}$ we use the EDS formula with $n = 3$ instead.

Now setting $t = -N + 1$ easily gives $d^2 \equiv c^N \pmod{p}$, and a brief induction on s completes the proof. □

There has recently been a surge of interest in the arithmetic properties of EDS; see for example [5, 7–9, 15, 17, 18, 20, 1].

3 Division polynomials of elliptic curves

Let $E/\mathbb{F}_q$ be an elliptic curve over a field $\mathbb{F}_q$ given by the Weierstrass equation

$$E : y^2 + a_1\, xy + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6. \tag{2}$$

The set of $\mathbb{F}_q$*-rational points*, denoted $E(\mathbb{F}_q)$, is the set of points both of whose coordinates lie in $\mathbb{F}_q$, together with an extra point $\mathcal{O}$ called the *point at infinity.* We write $E(\overline{\mathbb{F}_q}) = E$. Then there is a natural addition law under which $E(\mathbb{F}_q)$ forms an abelian group with $\mathcal{O}$ as the identity element. By Hasse's Theorem the order of the group is $q+1-t$, where $|t| \leq 2\sqrt{q}$. For background on elliptic curves and elliptic curve cryptography see [16], [24], [19] or [11]. For an elementary introduction to elliptic curves see [4].

The coordinates of the sum $P_1 + P_2$ of two points on an elliptic curve are rational functions of the coordinates of P_1 and P_2. By repeated application of the addition formulae it follows that the coordinates of the m^{th} multiple of the point (x, y) can be expressed as (albeit complicated) rational functions in x and y. In fact the following is true:

Theorem 3. *There exists a sequence of polynomials ψ_n, $n \in \mathbb{Z}$, such that for every point $(x, y) \in E$ and every integer m,*

$$\psi_m(x, y) = 0 \;\Leftrightarrow\; [m](x, y) = \mathcal{O},$$

and otherwise the x-coordinate of $[m](x, y)$ is given by

$$x - \frac{\psi_{m-1}(x, y)\ \psi_{m+1}(x, y)}{\psi_m(x, y)^2}.$$

The ψ_n are called the *division polynomials* of the curve $E/\mathbb{F}_q$. If $P = (x, y)$ is a point on E, then $\psi_n(x, y)$ is often denoted $\psi_n(P)$.

The ψ_n satisfy a recursion that makes it easy to calculate a given division polynomial evaluated at a given point; in fact we can evaluate $\psi_n(P)$ in $\mathrm{O}(\log n)$ operations in $\mathbb{F}_q$ using this "doubling" formula and an algorithm analogous to the square-and-multiply algorithm for exponentiation in which the basic objects are 6-tupels of consecutive terms of the EDS; see [15] for details.

Theorem 4. *Let $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$ be the usual quantities associated with a Weierstrass equation. Then the division polynomials of E satisfy*

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y + a_1x + a_3,\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8\\
\psi_4 &= \left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)\,x + b_4b_8 - b_6^2\right)\psi_2\\
\psi_{2k+1} &= \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3 \qquad \textit{for } k \geq 2,\\
\psi_{2k} &= \left(\frac{\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2}{\psi_2}\right)\psi_k \quad \textit{for } k \geq 3,\\
\psi_{-n} &= -\psi_n \quad \textit{for } n < 0.
\end{aligned}$$

It follows easily that the coefficients of each polynomial ψ_n are in the ring $\mathbb{Z}[a_i]$.

The nk^{th} division polynomial evaluated at a point P can be expressed in terms of the k^{th} division polynomial evaluated at P and the n^{th} division polynomial evaluated at $[k]P$. This is a reflection of the fact that $[nk]P = [n]\left([k]P\right)$, and can easily be proved by induction on n.

Theorem 5. *If $P \in E$ then the division polynomials satisfy*

$$\psi_{nk}(P) = \psi_k(P)^{n^2}\, \psi_n([k]P) \quad \text{for all } n, k \in \mathbb{Z},$$

as long as $[k]P \neq \mathcal{O}$.

In fact the division polynomials satisfy a more general recurrence relation than Theorem 4; this is proved in [4] using divisor theory, but an elementary proof may also be obtained by a straightforward adaptation of the main result in [21].

Theorem 6. *The division polynomials satisfy*

$$\psi_{m+n}\, \psi_{m-n} = \psi_{m+1}\, \psi_{m-1}\, \psi_n^2 - \psi_{n+1}\, \psi_{n-1}\, \psi_m^2 \quad \text{for } n, m \in \mathbb{Z}. \tag{3}$$

This is the same equation used to define elliptic divisibility sequences. Replacing (1) by (3) and $\mathbb{Q}$ by $\mathbb{F}_q$ in the proof of the EDS symmetry result Theorem 2 yields an additional property for division polynomials evaluated at a point of finite order.

Theorem 7. *Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field $\mathbb{F}_q$, and let P be a point of order $N \geq 4$. Then there exist constants $c, d \in \mathbb{F}_q$ such that $d^2 = c^N$ and for all $s, t \in \mathbb{Z}$,*

$$\psi_{t+sN}(P) = c^{st}\, d^{s^2}\, \psi_t(P) \text{ in } \mathbb{F}_q.$$

Since $\psi_n(P) = 0$ if and only if $[n]P = \mathcal{O}$ the zeroes in the sequence $\psi_n(P)$, $n \in \mathbb{Z}$ are regularly spaced distance N apart; so the order of P corresponds to the gap in an EDS.

4 The algorithm

Let E be an elliptic curve over $\mathbb{F}_q$ and let P and $Q = [k]P$ be points in $E(\mathbb{F}_q)$, where P has known order N. The elliptic curve discrete logarithm problem (ECDLP) is to find the integer k. We now explain how to use division polynomials and EDS to reduce this problem to a discrete logarithm problem in $\mathbb{F}_q^*$ in the special case where $\#E(\mathbb{F}_q) = q - 1$ and N is a large prime factor of $\#E(\mathbb{F}_q)$; say $q - 1 = \ell N$ with ℓ small.

We consider the sequence of division polynomials evaluated at P. By our symmetry result Theorem 7, it satisfies

$$\psi_{kq}(P) = \psi_{k+k\ell\, N}(P) = c^{k^2\, \ell}\, d^{k^2\, \ell^2}\, \psi_k(P)$$

and

$$\psi_{(k+1)q}(P) = \psi_{(k+1)+(k+1)\ell N}(P) = c^{(k+1)^2\, \ell}\, d^{(k+1)^2\, \ell^2}\, \psi_{k+1}(P)$$

in $\mathbb{F}_q$. Dividing and using the fact that $c^\ell\, d^{\ell^2} = \psi_{1+\ell N}(P) = \psi_q(P)$, we get

$$\psi_q(P)^{2k+1} = \frac{\psi_{q(k+1)}(P)}{\psi_{qk}(P)} \cdot \frac{\psi_k(P)}{\psi_{k+1}(P)}. \tag{4}$$

Since we do not know k, we cannot find $\psi_k(P)$ or the other terms on the right hand side directly. However, we can use Theorem 5 to write $\psi_{qk}(P)$ and $\psi_{q(k+1)}(P)$ in terms of the division polynomials of E evaluated at $[k]P$ and $[k+1]P$:

$$\psi_{qk}(P) = \psi_k(P)^{q^2}\, \psi_q([k]P)$$

and

$$\psi_{q(k+1)}(P) = \psi_{k+1}(P)^{q^2}\, \psi_q([k+1]P).$$

Since $[k]P = Q$ we can rewrite (4) as

$$\psi_q(P)^{2k+1} = \left(\frac{\psi_{k+1}(P)}{\psi_k(P)}\right)^{q^2-1} \cdot \frac{\psi_q(Q+P)}{\psi_q(Q)}. \tag{5}$$

We still don't know $\frac{\psi_{k+1}(P)}{\psi_k(P)}$, but we don't need to: since $\mathbb{F}_q^*$ has $q-1$ elements and $q-1 \mid q^2-1$, the first factor vanishes, leaving

$$\left(\psi_q(P)^2\right)^k = \frac{\psi_q(Q+P)}{\psi_q(P)\,\psi_q(Q)}. \tag{6}$$

The quantities on the right hand side can be calculated in $\mathrm{O}(\log q)$ operations in $\mathbb{F}_q$. We now have a discrete log problem $\alpha^k = \beta$ in $\mathbb{F}_q$, which can be solved for k modulo the order of $\psi_q(P)^2$ in $\mathbb{F}_q$ using the Index Calculus method, which takes subexponential time. Since $d^2 = c^N$ and ℓ is even, we have by Theorem 2

$$\psi_q(P) = \psi_{\ell N+1}(P) = d^{\ell^2}\, c^\ell = c^{(\ell N)\frac{\ell}{2}}\, c^\ell = \left(c^{q-1}\right)^{\frac{\ell}{2}}\, c^\ell = c^\ell.$$

Since $c^{\ell N} = c^{q-1} = 1$ in $\mathbb{F}_q$, the order of c^ℓ divides N. But N is prime, so either $\psi_q(P) = 1$ (in which case the algorithm fails, because $\langle P\rangle$ in $E(\mathbb{F}_q)$ has been mapped to $\langle 1\rangle$ in $\mathbb{F}_q$) or $\psi_q(P)$ has order N. Since ℓ is small, it seems unlikely that $c^\ell = 1$ in $\mathbb{F}_q$ (if c were a random element of $\mathbb{F}_q$ the probability would be $\frac{\ell}{q-1} = \frac{1}{N}$); this heuristic argument is in fact bourne out in experiments by Shipsey, and we state it as a conjecture:

Conjecture 1. If P is a point of order N on an elliptic curve $E/\mathbb{F}_q$ and $\#E(\mathbb{F}_q) = q-1 = \ell N$ where ℓ is even, then

$$\psi_q(P) \equiv 1 \pmod{p}$$

with probability $\frac{1}{N}$. (It is easy to show that this is equivalent to the condition that the period of the sequence $(\psi_n(P))$ divides ℓN.)

If this is true then with high probability $\psi_q(P)$ has order N, and we have succeeded in mapping the ECDLP to the DLP in $\mathbb{F}_q^*$.

Example

Let E be the elliptic curve

$$y^2 + xy + y = x^3 + x^2 + 21x$$

over the field $\mathbb{F}_{23}$, and P be the point $(0, 0)$. Then P has order $N = 11$, which divides $q - 1 = 22$. Let $Q = [k]P$ be the point $(18, 14) \in E(\mathbb{F}_q)$. We want to find k.

Using the elliptic curve addition formula we find $Q + P = (21, 0)$.

By Theorem 4 we have

$$\begin{aligned}
&\text{Sequence for } \psi_n(P) \bmod 23 = 0, 1, 1, 22, 2, \ldots \\
&\text{Sequence for } \psi_n(Q) \bmod 23 = 0, 1, 1, 20, 1, \ldots \\
&\text{Sequence for } \psi_n(Q+P) \bmod 23 = 0, 1, 22, 11, 18, \ldots
\end{aligned}$$

The q^{th} terms of these sequences are

$$\psi_{23}(P) = 2, \quad \psi_{23}(Q) = 9, \quad \psi_{23}(Q + P) = 6.$$

Equation (6) becomes

$$\left(2^2\right)^k = \frac{6}{2 \cdot 9} = 8.$$

Since $4^2 \not\equiv 1 \pmod{23}$ we know 4 has order 11 in $\mathbb{F}_{23}$. We now solve this DLP in $\mathbb{F}_{23}$ to find that $k \equiv 7 \pmod{11}$.

5 Final remarks

Remark 1. A slight variation on the above algorithm (using $\#E(\mathbb{F}_q) = N\ell$ instead of $q - 1$ in the initial symmetry equations) yields the following equation instead of (5):

$$\psi_{\ell N+1}(P)^{2k+1} = \left(\frac{\psi_{k+1}(P)}{\psi_k(P)}\right)^{\ell N(\ell N+2)} \cdot \frac{\psi_{\ell N+1}(Q+P)}{\psi_{\ell N+1}(Q)}. \tag{7}$$

This holds for any $\#E(\mathbb{F}_q)$, and so one might be tempted to try to use it for the case $\#E(\mathbb{F}_q) = q-3$, which would also get rid of the unknown factor $\left(\frac{\psi_{k+1}(P)}{\psi_k(P)}\right)$. But in this case

$$\psi_{\ell N+1}(P) = d^{\ell^2} c^\ell = c^{(\ell N)\frac{\ell}{2}} c^\ell = c^{(q-3)\frac{\ell}{2}} c^\ell = \left(c^{q-1}\right)^{\frac{\ell}{2}} = 1,$$

so $\psi_{\ell N+1}(P)^2$ has order 1 in $\mathbb{F}_q$, and the algorithm fails.

Remark 2. (Infeasibility of generalising to the other MOV cases using Somos sequences.)

The MOV algorithm reduces the ECDLP in $E(\mathbb{F}_q)$ to a DLP in the underlying field $\mathbb{F}^*_{q^r}$, where r is the smallest number for which N divides $q^r - 1$, as follows.

The algorithm chooses a random point T in $E[N]$, the set of points of E whose order divides n, and maps P to $\alpha = e_N(P,T)$ and $Q = [k]P$ to $\beta = e_N(Q,T)$, where e_N is the Weil pairing. Both α and β are in the subgroup μ_N of N^{th} roots of unity in the smallest extension field $\mathbb{F}_{q^r}$ containing $E[N]$ (see [11], page 68–72). Since the Weil pairing is bilinear, $\beta = e_N([k]P,T) = e_N(P,T)^k = \alpha^k$, and the algorithm succeeds if α has order N in μ_N. But the group $E[N]$ is isomorphic to $\mathbb{Z}_N \times \mathbb{Z}_N$ and hence consists of N cosets of $\langle P \rangle$. As T varies through the N cosets of $\langle P \rangle$ in $E[N]$, α varies through the N elements of μ_N (see [11] page 68, Lemma 5.4). So with $1 - \frac{1}{N}$ probability α has order N, and if it doesn't we can simply choose a different point T and try again.

Our algorithm as it stands does not have this randomisation built in — the homomorphism from $\langle P \rangle$ to a subgroup of $\mathbb{F}_q^*$ is always given by $P \mapsto \alpha = \psi_q(P)^2$ — which means, firstly, that if $\alpha = 1$ then the algorithm simply fails (and we have not proved that $\alpha = 1$ with probability $\frac{1}{N}$). Secondly, it means that our element α is always in the "small field" $\mathbb{F}_q$ instead of in the "big field" $\mathbb{F}_{q^r}$, and so our algorithm cannot cover the other cases of the MOV attack where $N \mid q^r - 1$ for some small r.

We thought it might be possible to solve these problems by using instead of the sequence $\psi_n(P)$ the Somos 4 sequence (A_n) associated with the sequence of points $T + [n]P$ for a random point T in $E[N]$ (see [20] or [2]). We hoped that as T varied through all N cosets of P in $E[N]$, $\alpha = \frac{A_{q^r}}{A_1}$ would vary through all N^{th} roots of unity of $\mathbb{F}_{q^r}$. However, it turns out that all these sequences have the same value of $\frac{A_{q^r}}{A_1}$.

Remark 3. (Factoring) We remark that Lenstra's elliptic curve factoring method [25] can be elegantly rewritten in terms of elliptic divisibility sequences. To factor an integer n, take a random EDS (W_n) and reduce it modulo n. Let $\mathbb{F}_q$ be be an appropriately chosen smooth number (perhaps $k!$ for some k) and find $W_K \bmod n$ (which takes $\mathrm{O}(\log K)$ operations modulo n using the doubling formula). If there is a prime factor p of n whose gap in (W_n) divides K, then p divides $\gcd(W_K \bmod n, n)$. If not, choose another EDS and repeat. (The analysis of the running time of the algorithm, however, still depends on elliptic curves.)

References

1. Mohamed Ayad: Points S-entiers des courbes elliptiques. Manuscripta Math. **76** (34) (1992) 305–324.
2. A. N. W. Hone: Elliptic curves and quadratic recurrence sequences. Bulletin of the London Mathematical Society **37** (2005) 161–171.
3. I. Blake, G. Seroussi, and N. Smart: Elliptic Curves in Cryptography. Cambridge University Press (1999).
4. L.S. Charlap and D.P. Robbins: An elementary introduction to elliptic curves. Technical Report **31**, Institute for Defense Analysis, Princeton (1988). Available at www.idaccr.org/reports/reports.html.
5. M. Einsiedler, G. Everest, and T. Ward: Primes in elliptic divisibility sequences. LMS Journal of Computation and Mathematics **4** (2001) 1–13.

6. G. Everest and V. Miller and N. Stephens: Primes generated by elliptic curves. Preprint (2003).
7. G. Everest and G. McLaren and T. Ward: Primitive divisors of elliptic divisibility sequences. Preprint (2004).
8. G. Everest and H. King: Prime powers in elliptic divisibility sequences. Preprint (2004).
9. G. Everest and I. Shparlinski: Prime divisors of sequences associated to elliptic curves. Preprint (2004).
10. K. Lauter and K. Stange: The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. To appear in Proceedings of Selected Areas in Cryptography SAC '08 (2008).
11. Alfred Menezes: Elliptic Curve Public Key Cryptosystems. Kluwer Academic Publishers (1997).
12. A. Menezes, T. Okamoto, and S. Vanstone: Reducing Elliptic Curve Logarithms to a Finite Field. IEEE Transaction on Information Theory **39** (1993) 1639–1646.
13. G. Frey and H.-G. Rück: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comp. **62**(206) (1994) 865–874.
14. Andrew Odlyzko: Discrete logarithms and their cryptographic significance. Advances in Cryptology – Eurocrypt '84. Lecture Notes in Computer Science **209** (1985) 224–314.
15. Rachel Shipsey: Elliptic Divisibility Sequences. PhD thesis, Goldsmiths, University of London (2001). Available at http://homepages.gold.ac.uk/rachel/.
16. J. Silverman and J. Tate: Rational Points on Elliptic Curves. Springer Undergraduate Texts in Mathematics (1992).
17. Joseph H Silverman: p-adic properties of division polynomials and elliptic divisibility sequences. Preprint (2004).
18. J. Silverman and N. Stephens: The sign of an elliptic divisibility sequence. Preprint (2004).
19. I. Blake, G. Seroussi and N. Smart: Elliptic Curves in Cryptography. Cambridge University Press (1999).
20. Christine Swart: Sequences related to elliptic curves. PhD thesis, Royal Holloway, University of London (2003).
21. C. Swart and A. van der Poorten: Recurrence relations for elliptic sequences: Every Somos 4 is a Somos k. Bulletin of the London Mathematical Society (accepted March 2004).
22. Morgan Ward: Memoir on Elliptic Divisibility Sequences. American Journal of Mathematics **70** (1948) 31–74.
23. Morgan Ward: The Law of Repetition of Primes in an Elliptic Divisibility Sequence. Duke Mathematical Journal **15** (1948) 941–946.
24. Lawrence C. Washington: Elliptic Curves: Number Theory and Cryptography. Chapman and Hall (2003).
25. H. W. Lenstra Jr.: Factoring integers with elliptic curves. Annals of Mathematics **2** (126) (1987) 649–673.