Reducing Elliptic Curve Logarithm to Logarithm in a Finite Field $\mathbb{F}_q$ for Some Orders *

Wei Yu[1], Kunpeng Wang[2], Bao Li[2]

1. Department of Information Security, University of Science and Technology of China, Hefei, 230026
2. State Key Laboratory of Information Security, Beijing, 100049, China

Abstract. We change elliptic curve discrete logarithm problem to discrete logarithm problem of $\mathbb{F}_q$ using elliptic divisibility sequences. And the method works for the situation $\#E(\mathbb{F}_q) = q-1, q\pm\sqrt{q}, q\pm\sqrt{2q-1}, q\pm\sqrt{3q-2}, q+\sqrt{4q-3}$.

Key words: elliptic curve discrete logarithm problem, discrete logarithm problem, elliptic divisibility sequences.

1 Introduction

The discrete logarithm problem (DLP) in a finite field $\mathbb{F}_q$ can be stated as follows: given $a, b \in \mathbb{F}_q$, find an integer x such that $b = a^x$. Since the Index Calculus methods for computing logarithms in a finite field runs in subexponential time. Hence, converting elliptic curve discrete logarithm problem (ECDLP) to discrete logarithm problem DLP in $\mathbb{F}_q$ is effective.

Elliptic curve cryptography relies on the difficulty of solving the elliptic curve discrete logarithm problem(ECDLP). ECDLP can be stated as follows: an elliptic curve E over $\mathbb{F}_q$,denoted $E(\mathbb{F}_q)$, $P \in E(\mathbb{F}_q)$,where P is a point of order N on $E(\mathbb{F}_q)$, given $Q = [k]P, Q \in E(\mathbb{F}_q)$, find k.

The best known algorithms for solving ECDLP are Pollard's ρ algorithm [1] and its parallel variants [2]. They are generic algorithms, and work in any finite group and run in $O(\log N)$ where N is the order of P. P. Gaudry [3] solves ECDLP defined over small extension fields faster than Pollard's ρ algorithm. Index calculus methods can not be extended to elliptic curve groups [4–6]. Xedni algorithm [7–9] attempted to lift ECDLP to $\mathbb{Q}$, and [10] attempted to lift ECDLP to a local field. None of them proved to be feasible. In all, the best attack on ECDLP takes exponential time when elliptic curve E is general.

* Supported by the National Research Foundation of China under Grant No.60970153, and National Basic Research Program of China under Grant No.2007CB311201(973).

Let r satisfy the following conditions: the order N divides $q^r - 1$ where r is the smallest integer answering for the equation $N|q^r - 1$. MOV[11] attack using Weil pairing and FR[12] attack using Tate pairing give an isomorphism between $< P >$ and the μ_N (N^{th} roots of unity in $\mathbb{F}_{q^r}$). These attacks reduce the ECDLP in $E(\mathbb{F}_q)$ to DLP over $\mathbb{F}_{q^r}^*$. If k is small, then MOV attack and FR attack work efficiently.

N.Smart's attack [13] can solve $\#E(\mathbb{F}_q) = q$ which are anomalous elliptic curves. R. Shipsey and C. Swart [14] use elliptic divisibility sequences to solve ECDLP in the case where $\#E(\mathbb{F}_q) = q - 1$. We generalize the algorithm of [14]. We use elliptic divisibility sequences(EDS) to convert ECDLP to DLP of $\mathbb{F}_q$ in cases where $\#E(\mathbb{F}_q) = q-1, q \pm \sqrt{q}, q \pm \sqrt{2q-1}, q \pm \sqrt{3q-2}, q + \sqrt{4q-3}$. That is to say, we change exponential time to subexponential time. The process is all elementary level and without burden in theory.

The paper is organized as follows: In Section 2, we recall some basic facts about EDS and introduce the properties of EDS. In Section 3, we introduce the division polynomials of elliptic curves. In Section 4, we introduce our algorithm. In Section 5, we point out the cases where we can solve ECDLP to DLP of $\mathbb{F}_q$. The cases are $\#E(\mathbb{F}_q) = q-1, q \pm \sqrt{q}, q \pm \sqrt{2q-1}, q \pm \sqrt{3q-2}, q + \sqrt{4q-3}$. In Section 6, we give an example. Finally, we point out some conclusions.

2 Elliptic Divisibility Sequences

Elliptic divisibility sequences(EDS) are described in detail in Morgan Ward's paper [15]. The properties of EDS can be found in his paper which is published in the same year[16]. Elliptic curves sequences are the sequences satisfying the nonlinear recurrence relation

$$W_{m+n}W_{m-n} = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2. \tag{1}$$

The EDS have the divisibility property that $n|m$ imply $W_n|W_m$. If we let $m = n = 0$, then $W_0 = 0$, and if $m = 1, m + n = 0$, then $W_1^2 = 1$.

Fibonacci sequence is the oldest example of a divisibility sequence, and it satisfies the EDS equation (1).

Theorem 1 *[17] Let W_n be an EDS, and $p \nmid W_2, p \nmid W_3$. Then there exists a positive integer N satisfying*

$$W_n \equiv 0(\mod p) \Leftrightarrow n \equiv 0(\mod N).$$

Theorem 2 *[14] Let W_n be an EDS, and $p \nmid W_2, p \nmid W_3$. and let p have gap N in (W_n). Then there exist constants c and d such that $d^2 = c^N$ $(\mathrm{mod} p)$, then for all $s, t \in \mathbb{Z}$,*

$$W_{t+sN} \equiv c^{st} d^{s^2} W_t (\mathrm{mod} p), \tag{2}$$

with $c \equiv \frac{W_{N-1}}{W_{-1}} \frac{W_{-2}}{W_{N-2}} (\mathrm{mod} p)$, $d \equiv \left(\frac{W_{N-1}}{W_{-1}}\right)^2 \frac{W_{-2}}{W_{N-2}} (\mathrm{mod} p)$.

For more properties of EDS, please refer to [18–24].

3 Division polynomials of elliptic curves

Let $E/\mathbb{F}_q$ be an elliptic curve E defined over $\mathbb{F}_q$, its Weierstrass equation is

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

By Hasse's Theorem, $\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$.

Theorem 3 *There exists a sequence of polynomials $\psi_n, n \in \mathbb{Z}$,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

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

Then ψ_n are called the division polynomials of the curve $E/\mathbb{F}_q$. If P=(x,y), we denote $\psi_n(x, y)$ by $\psi_n(P)$.

Theorem 4 *Let $b_2 = a_1^2 + 4a_2$,$b_4 = a_1 a_3 + 2a_4$,$b_6 = a_3^2 + 4a_6$,$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_6 + a_2 a_3^2 - a_4^2$ be the quantities associated with elliptic curve defined by equation (3). Then the division polynomials of*

E, ψ_n satisfy

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

ψ_n satisfy a recursion easy to calculate for a given point. We can evaluate $\psi_n(P)$ in $O(\log n)$ operations.

Theorem 5 *[25] Given an elliptic divisibility sequence W together with a set of consecutive terms $< W_k >$ and integer l, the term W_{lk} can be found in logarithmic time.*

Theorem 6 *[14] If $P \in E$, then the division polynomials satisfy*

$$\psi_{nk}(P) = \psi_k(P)^{n^2}\psi_n([k]P),$$

for all $n, k \in \mathbb{Z}$.

The theorem can be found in [14],which is proved by L.S. Charlap and D.P. Robbins [26] using divisor theory. we can also find this theorem in [27]'s Theorem 6 and can be obtained by a straightforward adaptation of the main result in [23].

Theorem 7 *The division polynomials satisfy*

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2, \ \textit{for all } m, n \in \mathbb{Z}.$$

Division polynomials of elliptic curves is an EDS, which is easily checked. Look the equation (1), if $m = k+1, n = k$, then we get the equation calculating ψ_{2k+1}, and if $m = k+1, n = k-1$, then we get the equation calculating ψ_{2k}.

Theorem 8 *[14] Elliptic curve $E/\mathbb{F}_q$, and let P be a point of order $N \geqslant 4$, there exist constants $c, d \in \mathbb{F}_q$ such that $d^2 = c^N$, and for all $s, t \in \mathbb{Z}$,*

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

Because $\psi_n(P) = 0$ if and only if $[n]P = \mathcal{O}$. The zeros in the sequence $\psi_n(P)$ are regularly spaced distance N apart, where $n \in Z$. Then the order of P corresponds to the gap in EDS.

4 The algorithm

By Hasse's Theorem, the order of Elliptic curve $E/\mathbb{F}_q$ is $\#E(F_q) = q + 1 - t, where - 2\sqrt{q} \leq t \leq 2\sqrt{q}$. Let $x = t - 1$, then the order can be represented as $q - x, where - 2\sqrt{q} - 1 \leq x \leq 2\sqrt{q} - 1$. Let $q - x = lN$, N is the large prime factor of $\#E(F_q)$. At present, we start changing ECDLP to DLP as follows:

By Thoerem 8,

$$\psi_{kq}(P) = \psi_{kx+klN}(P) = c^{k^2lx} d^{k^2l^2} \psi_{kx}(P),$$

$$\psi_{(k+1)q}(P) = \psi_{(k+1)x+(k+1)lN}(P) = c^{(k+1)^2lx} d^{(k+1)^2l^2} \psi_{(k+1)x}(P).$$

Thus, we get

$$\frac{\psi_{(k+1)q}(P)}{\psi_{kq}(P)} = (c^{lx} d^{l^2})^{2k+1} \frac{\psi_{(k+1)x}(P)}{\psi_{kx}(P)}, \tag{5}$$

and because

$$\psi_q(P) = \psi_{x+lN}(P) = c^{lx} d^{l^2} \psi_x(P), \tag{6}$$

then

$$\frac{\psi_{(k+1)q}(P)}{\psi_{kq}(P)} = \left(\frac{\psi_q(P)}{\psi_x(P)} \right)^{2k+1} \frac{\psi_{(k+1)x}(P)}{\psi_{kx}(P)}. \tag{7}$$

By theorem 6,

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

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

so

$$\frac{\psi_{(k+1)q}(P)}{\psi_{kq}(P)} = \left(\frac{\psi_{(k+1)}(P)}{\psi_k(P)} \right)^{q^2} \frac{\psi_q([k+1]P)}{\psi_q([k]P)}, \tag{8}$$

and also by theorem 6

$$\psi_{xk}(P) = \psi_k(P)^{x^2} \psi_x([k]P),$$

$$\psi_{x(k+1)}(P) = \psi_{(k+1)}(P)^{x^2}\psi_x([k+1]P),$$

there is

$$\frac{\psi_{(k+1)x}(P)}{\psi_{kx}(P)} = \left(\frac{\psi_{(k+1)}(P)}{\psi_k(P)}\right)^{x^2}\frac{\psi_x([k+1]P)}{\psi_x([k]P)}. \tag{9}$$

From equation (7,8,9), we get

$$\left(\frac{\psi_{(k+1)}(P)}{\psi_k(P)}\right)^{q^2}\frac{\psi_q([k+1]P)}{\psi_q([k]P)} = \left(\frac{\psi_q(P)}{\psi_x(P)}\right)^{2k+1}\left(\frac{\psi_{(k+1)}(P)}{\psi_k(P)}\right)^{x^2}\frac{\psi_x([k+1]P)}{\psi_x([k]P)},$$

rearrange it as

$$\left(\frac{\psi_{(k+1)}(P)}{\psi_k(P)}\right)^{q^2-x^2}\frac{\psi_q([k+1]P)}{\psi_q([k]P)}\frac{\psi_x([k]P)}{\psi_x([k+1]P)} = \left(\frac{\psi_q(P)}{\psi_x(P)}\right)^{2k+1}. \tag{10}$$

Since $Q=[k]P$, we can write the equation (10) as

$$\left(\frac{\psi_q(P)}{\psi_x(P)}\right)^{2k+1} = \left(\frac{\psi_{(k+1)}(P)}{\psi_k(P)}\right)^{q^2-x^2}\frac{\psi_q(P+Q)}{\psi_q(Q)}\frac{\psi_x(Q)}{\psi_x(P+Q)},$$

rearrange it as

$$\left[\left(\frac{\psi_q(P)}{\psi_x(P)}\right)^2\right]^k = \left(\frac{\psi_{(k+1)}(P)}{\psi_k(P)}\right)^{q^2-x^2}\frac{\psi_q(P+Q)}{\psi_q(Q)}\frac{\psi_x(Q)}{\psi_x(P+Q)}\frac{\psi_x(P)}{\psi_q(P)}. \tag{11}$$

Since F_q^* has $q-1$ elements, if $(q-1)|(q^2-x^2)$, then we have

$$\left(\frac{\psi_{(k+1)}(P)}{\psi_k(P)}\right)^{q^2-x^2} = 1,$$

so

$$\left[\left(\frac{\psi_q(P)}{\psi_x(P)}\right)^2\right]^k = \frac{\psi_q(P+Q)}{\psi_q(Q)}\frac{\psi_x(Q)}{\psi_x(P+Q)}\frac{\psi_x(P)}{\psi_q(P)}. \tag{12}$$

Since we can compute $\psi_q(P), \psi_x(P), \psi_q(Q), \psi_x(Q), \psi_q(P+Q), \psi_x(P+Q)$ in logarithmic time(Theorem 5), we successfully change ECDLP to DLP in $\mathbb{F}_q$. Then we discuss when $(q-1)$ divides (q^2-x^2).

From theorem 8 then we get

$$\left(\frac{\psi_q(P)}{\psi_x(P)}\right)^2 = c^{2lx}d^{2l^2} = c^{2lx}c^{l^2N} = c^{2lx+l(q-x)} = c^{l(q+x)} = c^{l(x+1)} = c^{lt}. \tag{13}$$

Thus, from equation (13), if $lt \equiv 0(\text{mod} q-1)$, then the algorithm fails.

5 When the algorithm works

When $(q-1)$ divides (q^2-x^2), where $-2\sqrt{q}-1 \leq x \leq 2\sqrt{q}-1$, we can get $(q^2-x^2) = q(q-1)+y(q-1)$, then $x^2 = y+(1-y)q$. We consider the different values of y.

case 1: $y = 1, \Longrightarrow x^2 = 1, \Longrightarrow x = \pm 1$. In this case, $\#E(\mathbb{F}_q) = q \pm 1$. when $\#E(\mathbb{F}_q) = q-1$,[11, 12, 14] all can convert ECDLP to DLP in $\mathbb{F}_q$.when $\#E(\mathbb{F}_q) = q+1$,[11, 12] can convert ECDLP to DLP in $\mathbb{F}_{q^2}$. in this case, t=0,then our algorithms fail.

case 2: $y = 0, \Longrightarrow x^2 = q, \Longrightarrow x = \pm\sqrt{q}$. In this case, $\#E(\mathbb{F}_q) = q\pm\sqrt{q} = \sqrt{q}(\sqrt{q}\pm 1)$, which is not security curve. We change these cases to DLP in $\mathbb{F}_q$.

case 3: $y = -1, \Longrightarrow x^2 = 2q-1, \Longrightarrow x = \pm\sqrt{2q-1}$. In this case, $\#E(\mathbb{F}_q) = q \pm \sqrt{2q-1}$, which is not security curve. We change these cases to DLP in $\mathbb{F}_q$.

case 4: $y = -2, \Longrightarrow x^2 = 3q-2, \Longrightarrow x = \pm\sqrt{3q-2}$. In this case, $\#E(\mathbb{F}_q) = q \pm \sqrt{3q-2}$, which is security curve. We change these cases to DLP in $\mathbb{F}_q$.

case 5: $y = -3, \Longrightarrow x^2 = 4q-3, \Longrightarrow x = -\sqrt{4q-3}$. In this case, $\#E(\mathbb{F}_q) = q + \sqrt{4q-3}$, which is security curve. We change these cases to DLP in $\mathbb{F}_q$.

If $y > 1$, then $x^2 < 0$ which is not possible. And if $y \leqslant -4$, then x can't satisfy $-2\sqrt{q}-1 \leq x \leq 2\sqrt{q}-1$.

When $(q-1)|(q^2-x^2)$, we get equation (12). We compute $\psi_q(P), \psi_x(P)$, $\psi_q(Q), \psi_x(Q), \psi_q(P+Q), \psi_x(P+Q)$ in logarithmic time(Theorem 5).

When $\#E(\mathbb{F}_q) = \begin{cases} q-1 \\ q \pm \sqrt{q} \\ q \pm \sqrt{2q-1} \\ q \pm \sqrt{3q-2} \\ q + \sqrt{4q-3} \end{cases}$, we change ECDLP to DLP in logarithmic time.

6 Example

An example of the order $\#E(\mathbb{F}_q) = q-1$ can be found in [14]. Let us consider $\#E(\mathbb{F}_{457}) = q-x = 494$, where $q = 45$, $x = -37$, $t = -36$. Its weierstrass equation is

$$y^2 = x^3 + x + 94, q = 457. \tag{14}$$

Let $P=(4,194)$, the order of P is 19.

$[1]P=(4,194),[2]P=(452,197),[3]P=(255,42),[4]P=(173,54),$ $[5]P=(314,125),[6]P=(376,163),[7]P=(150,199),[8]P=(115,62),$ $[9]P=(284,386),[10]P=(284,71),[11]P=(115,395),[12]P=(150,$ $258),[13]P=(376,294),[14]P=(314,332),[15]P=(173,403),[16]P=$ $(255,415),[17]P=(452,260),[18]P=(4,263),[19]P=\mathcal{O}$.

If $Q=(150,258)$, then $P+Q=(376,294)$.

According to Theorem 4,

$\psi(P)$ mod 457 = 0, 1, 388, 348, 407, 304, 84, 193, 32, 389, 213, 250, 443, 412, 77, 222, 69, 169, 427, 0, 11 ...

$\psi(Q)$ mod 457 = 0, 1, 59, 366, 129, 208, 6, 163, 139, 453, 454, 280, 331, 385, 424, 160, 351, 431, 175, 0, 357 ...

$\psi(P+Q)$ mod 457 = 0, 1, 131, 284, 207, 327, 88, 126, 250, 80, 447, 37, 384, 113, 191, 226, 142, 76, 336, 0, 423...

Using algorithm of [25] compute $\psi_{-x}(P)$ =50, $\psi_q(P)$ =200, $\psi_{-x}(Q)=$ 110, $\psi_q(P)$ =407, $\psi_{-x}(P+Q)$ =17, $\psi_q(P)$ =256. Then

$$\left(\frac{\psi_q(P)}{\psi_x(P)}\right)^2=16, \tag{15}$$

$$\frac{\psi_q(P+Q)}{\psi_q(Q)}\frac{\psi_x(Q)}{\psi_x(P+Q)}\frac{\psi_x(P)}{\psi_q(P)}=347. \tag{16}$$

and by equation (12), we get $16^k=347\mathrm{mod}457$. At last, compute $k=12$ using Index Calculus method.

7 Conclusion

We have successfully reduced ECDLP of the order in cases where $\#E(\mathbb{F}_q)$ $=q-1,q\pm\sqrt{q},q\pm\sqrt{2q-1},q\pm\sqrt{3q-2},q-\sqrt{4q-3}$ to DLP based on the principle of EDS. In fact, our algorithm can do something more. The algorithm can solve $N|q^2-x^2$, where $q-1|q^2-x^2$.

References

1. J. M. Pollard. Monte Carlo methods for index computation mod p. Math. Comp., 32(143):918-924, 1978.
2. P. C. van Oorschot and M. J. Wiener. Parallel collision search with cryptanalytic applications. J. of Cryptology, 12:1-28, 1999.
3. P. Gaudry. Some remarks on the elliptic curve discrete logarithm. Unpublished manuscript, 2004.

4. V. Miller, Uses of elliptic curves in cryptography, in Advances in CryptologyArypto 85 (Lecture Notes in Computer Sciences), vol. 218. New York Springer-Verlag, 1986, pp. 417-426.
5. A. Odlyzko, Discrete logarithms and their cryptographic significance, in Advances in Cryptology4urocrypt'84. Lecture Notes in Computer Science, vol. 209. 1985, 224-314.
6. D. Coppersmith, Fast evaluation of logarithms in fields of characteristic two, IEEE Trans. Inform Theory, vol. IT-30, pp. 587-594, 1984.
7. M.-D Huang, K. Kueh, and K.-S. Tan. Lifting elliptic curves and solving the elliptic curve discrete logarithm problem. In L. Adleman and M.-D. Huang, editors, ANTS, volume 877 of Lecture Notes in Comput. Sci., pp. 377-384. SpringerCVerlag, 2000.
8. M. Jacobson, N. Koblitz, J. Silverman, A. Stein, and E. Teske. Analysis of the Xedni calculus attack. Des. Codes Cryptogr., 20:41-64, 2000.
9. J. Silverman. The Xedni calculus and the elliptic curve discrete logarithm problem. Des. Codes Cryptogr., 20:5-40, 2000.
10. P. Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. Cryptography ePrint Archive,Report 2004/073.
11. A. Menezes, T. Okamoto, and S. Vanstone: Reducing Elliptic Curve Logarithms to a Finite Field. IEEE Transaction on Information Theory 39, 1993, 1639-1646.
12. G. Frey and H.-G. R*ü*ck: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comp. 62(206), 1994, 865-874.
13. N. Smart, The discrete logarithm problem on elliptic curves of trace one", Journal of Cryp- tology, 12, 1999, 193-196.
14. Rachel Shipsey and Christine Swart, Elliptic divisibility sequences and the elliptic curve discrete logarithm problem. http://eprint.iacr.org/2008/444.pdf.
15. Morgan Ward: Memoir on Elliptic Divisibility Sequences. American Journal of Mathematics 70, 1948, 31-74.
16. Morgan Ward: The Law of Repetition of Primes in an Elliptic Divisibility Sequence. Duke Mathematical Journal 15, 1948, 941-946.
17. Mohamed Ayad: Points S-entiers des courbes elliptiques. Manuscripta Math. 76 (34), 1992, 305-324.
18. M. Ayad, Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques. Ann. Inst. Fourier (Grenoble) 43(3), 1993, 585-618.
19. M. Einsiedler, G. Everest, and T. Ward: Primes in elliptic divisibility sequences. LMS Journal of Computation and Mathematics 4, 2001, 1-13.
20. C.Swart, Elliptic curves and related sequences. PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.
21. J.H. Silverman, Common divisors of elliptic divisibility sequences over function fields. Manuscripta Math. 114(4), 2004, 431-446.
22. J.H. Silverman, p-adic properties of division polynomials and elliptic divisibility sequences. Math. Ann. 332(2), 2005, 443-471.
23. 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, 2004.
24. G. Everest, A.v.d. Poorten, I. Shparlinski, T. Ward, Elliptic Divisibility Sequences. In: Recurrence Sequences. American Mathematical Society, Providence, 2003, 163-175.
25. Rachel Shipsey: Elliptic Divisibility Sequences. PhD thesis, Goldsmiths, University of London, 2001. Available at http://homepages.gold.ac.uk/rachel/.

26. 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.
27. 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.