行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ 橢圓曲線密碼模組 ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☒個別型計畫 □整合型計畫
計畫編號：NSC 89－2115－M－032－001
執行期間： 88 年 08 月 01 日至 89 年 07 月 31 日

計畫主持人：陳燕美 淡江大學數學系
共同主持人：姚為成 新埔工學院共同科
計畫參與人員：兼任助理 趙惠菁 淡江大學數學系大學生
兼任助理 呂明杰 淡江大學數學系大學生

執行單位：淡江大學 數學系

中 華 民 國 89 年 10 月 02 日

一、中文摘要:

令 E/F_p 是定義在有限體的橢圓曲線, S 和 T 是曲線上的兩點, 橢圓曲線離散對數問題是想要找到整數 m 滿足 $T=mS$。在這份報告中我們將給一個解決此一問題的方法。我們將給定的曲線提升到定義在函數體一曲線, 其 Mordell-Weil 秩永遠小於或等於 3。對小的質數 p, 這個方法可以有效地解決我們的問題。

關鍵詞: 橢圓曲線, 有限體, 離散對數, 函數體, Mordell-Weil 秩。

二、英文摘要(Abstract):

Let E/F_p be an elliptic curve defined over a finite field of odd characteristic, and let S and T be points in $E(F_p)$. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is the problem to find an integer m satisfying $T=mS$. In this report, we give a method to solve ECDLP by lifting E over F_q to an elliptic curve E' over the function field $F_p(t)$ with Mordell-Weil rank less than or equal to 3. It has the advantage of working well for small values of prime p.

關鍵詞(Key Words): elliptic curves, finite field, discrete logarithms, function field, Mordell-Weil rank.

三、計畫緣由與目的:

The discrete logarithm problem(DLP) for the multiplicative group F_q^* has been studied extensively and it can be solved in subexponential time using the Index Calculus method ([Adl1]). This suggests that the public key system using the DLP for the multiplicative group F_q^* maybe not secure enough. Thus one is lead to the Elliptic Curve Cryptosystem, proposed independently by Miller and Koblitz in 1980's ([Mil1], [Kob1]). This ECDLP can be described as follows:

ECDLP: Let E/F_q be an elliptic curve over the finite field F_q, and let S and T be points on $E(F_q)$. To find an integer m(if exists) satisfying $T=mS$.

It seems very unlikely that there is an index calculus method for ECDLP ([Mil1], [Sil3]). So far, there is no subexponential algorithm for ECDLP in practice except for particular cases of curves having the Frobenius trace -2,0 and 1 ([Fre1], [Men1], [Sem1]). In 1998, Silverman proposed a new method, dubbed the Xedni Calculus ([Sil4]). Unfortunately, it has been proved that this Xedni Calculus is not practical ([Jac1]). In this project, we give yet anothermethod to solve ECDLP by lifting E over F_q to an elliptic curve E' over the function field F_q (t). All the curves E' which we use are elliptic curves with Birch-Swinnerton-Dyer conjecture already

proved ([Art1], [Mil2]).

四、計畫結果與討論:

In section 1, we describe how we lift an elliptic curve E over $\mathbb{F}_q$ together with three points to the projective plane over the function field $\mathbb{F}_q(t)$. In section 2, we show that the rank of the lifted curve in section 1 is always less than or equal to 3. In section 3, we estimate the canonical heights of the lifted points.

§1. Lifting curves over a finite field to curves over a function field

Let p be an odd rational prime (for the case $p = 2$, it can treated separately) and q a p-power, K the function field $\mathbb{F}_q(t)$, and R the polynomial ring $\mathbb{F}_q[t]$. Let $E/\mathbb{F}_q : y^2 = x^3 + ax^2 + bx$ be an elliptic curve over the finite field $\mathbb{F}_q$, and let $S, T \in E(\mathbb{F}_q)$. Choose three pairs of integers $(m_i, n_i), i \in \{1, 2, 3\}$ and let $P_1 = m_1S + n_1T, P_2 = m_2S + n_2T, P_3 = m_3S + n_3T$. Assume that $x_1x_2x_3(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \neq 0$(otherwise the ECDLP is almost solved). Observe that $(1, a, b)$ is the only solution of the following linear system over $\mathbb{F}_q$:

$$ux_1^3 + vx_1^2 + wx_1 = y_1^2$$
$$ux_2^3 + vx_2^2 + wx_2 = y_2^2$$
$$ux_3^3 + vx_3^2 + wx_3 = y_3^2$$

Choose u_1, u_2 and $u_3 \in \mathbb{F}$ so that $u_1^2 = x_1^2$, $u_2^2 = x_2^2$, $u_3^2 = x_3^2$. And then we define $d \in \mathbb{F}_q, f, g, h \in R$ as follows:

$$d = \det \begin{pmatrix} x_1^3 & x_1^2 & x_1 \\ x_2^3 & x_2^2 & x_2 \\ x_3^3 & x_3^2 & x_3 \end{pmatrix} = x_1x_2x_3(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \neq 0$$

$$f(t) = \det \begin{pmatrix} x_1^3 & (u_1t+y_1)^2 & x_1 \\ x_2^3 & (u_2t+y_2)^2 & x_2 \\ x_3^3 & (u_3t+y_3)^2 & x_3 \end{pmatrix}$$

$$g(t) = \det \begin{pmatrix} x_1^3 & x_1^2 & (u_1t+y_1)^2 \\ x_2^3 & x_2^2 & (u_2t+y_2)^2 \\ x_3^3 & x_3^2 & (u_3t+y_3)^2 \end{pmatrix}$$

$$h(t) = \det \begin{pmatrix} (u_1t+y_1)^2 & x_1^2 & x_1 \\ (u_2t+y_2)^2 & x_2^2 & x_2 \\ (u_3t+y_3)^2 & x_3^2 & x_3 \end{pmatrix}$$

Let $\mathcal{E}_1/K : y^2 = \frac{h}{d}x^3 + \frac{f}{d}x^2 + \frac{g}{d}x$ and let $\mathcal{P}_1 = (x_1, u_1t+y_1), \mathcal{P}_2 = (x_2, u_2t+y_2), \mathcal{P}_3 = (x_3, u_3t+y_3) \in \mathcal{E}_1(K)$. Then the reduction map modulo t: $\mathcal{E}_1/K \longrightarrow E/\mathbb{F}_q$ will map $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ to P_1, P_2, P_3 respectively. Let $\mathcal{E}/K : y^2 = x^3 + dfx^2 + d^2ghx$ and let $\mathcal{Q}_1 = (dhx_1, d^2h(u_1t+y_1)), \mathcal{Q}_2 = (dhx_2, d^2h(u_2t+y_2))$ and $\mathcal{Q}_3 = (dhx_3, d^2h(u_3t+y_3)) \in \mathcal{E}(K)$. Note that the map

$$\rho : \mathcal{E}_1 \to \mathcal{E}$$

$$(x, y) \mapsto (dhx, d^2hy)$$

is an isomorphism over K which maps $\mathcal{P}_i$ to $\mathcal{Q}_i$ for every $i \in \{1, 2, 3\}$. Then it is clear that $\deg(f) = 2, \ell(f) = d, \deg(g) \leq 1$ and $\deg(h) \leq 1$. Note that g and h won't be constant at the same time, that is $\deg(gh) \geq 1$(since $d \neq 0$ implied that the three vectors $(x_1, x_2, x_3), (x_1^2, x_2^2, x_3^2), (x_1^3, x_2^3, x_3^3)$ are $\mathbb{F}_q$-linearly independent). By routine computation, we have $\Delta(\mathcal{E}) = 16d^6g^2h^2(f^2 - 4gh)$.

§2. Bounding the Mordell-Weil rank

Consider an elliptic curve $\mathcal{E}$ defined over the rational function field K. Its conductor $N_\mathcal{E}$ can be regarded as a divisor

$$N_\mathcal{E} = \sum_{\nu \in M_K} f_\nu \nu$$

where f_ν are nonnegative integers(see [Sil5, Chapter 4, §10]), called the exponent of the conductor at ν. Denote $n_\mathcal{E}$ to be the sum $\sum_{\nu \in M_K} f_\nu \deg(\nu)$.

Then the Mordell-Weil rank of $\mathcal{E}(K)$ is bounded above by $n_{\mathcal{E}} - 4$(see [Bru1, Appendix]). By routine computation, we can show that for our lifted curves the inequality $n_{\mathcal{E}} \leq 7$ holds always. Therefore the following proposition follows immediately.

Proposition 2.1. *The rank of our lifted curve $\mathcal{E}(K)$ is less than or equal to 3.*

In order to solve the ECDLP, one had better lower the rank of the lifted curve to 2. Therefore we would like to study the 2-descent via 2-isogenies on elliptic curves over rational function fields which may help us to lower the rank. Now suppose that B and $A^2 - 4B$ are nonzero elements in R. Let $\mathcal{E}/K : y^2 = x^3 + Ax^2 + Bx$, $\mathcal{E}'/K : y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$ and let $\phi : \mathcal{E} \longrightarrow \mathcal{E}'$, $\hat{\phi} : \mathcal{E}' \longrightarrow \mathcal{E}$ be the dual isogenies of degree 2 defined as follows:

$$\phi((x,y)) = (\frac{y^2}{x^2}, \frac{y(B-x^2)}{x^2})$$
$$\hat{\phi}((x,y)) = (\frac{y^2}{4x^2}, \frac{y(A^2-4B-x^2)}{8x^2})$$

Notations:

$\Delta(\mathcal{E})$:= the discriminant of an elliptic curve $\mathcal{E}$.

$\ell(h)$:= the leading coefficient of h, for any $h \in R$.

$Ш(\mathcal{E}/K)$ = the Shafarevich-Tate group of $\mathcal{E}/K$.

$S^{(\phi)}(\mathcal{E}/K)$ = the ϕ-Selmer group of $\mathcal{E}/K$.

$S^{(\hat{\phi})}(\mathcal{E}'/K)$ = the $\hat{\phi}$-Selmer group of $\mathcal{E}'/K$.

M_K = the set of all places in K.

S = { finite places associated to prime divisors of $B(A^2-4B)$}$\cup${the infinite place}.

$K(S,2) = \{d \in K^*/K^{*2} : \mathrm{ord}_\nu(d) \equiv 0 \,(\mathrm{mod}\ 2)$ for every place in $S\}$.

α is a generator of $\mathbb{G}_m(\mathbb{F}_q)$.

r is the rank of the Mordell-Weil group $\mathcal{E}(K)$.

$s = \dim_{\mathbb{F}_2} S^{(\phi)}(\mathcal{E}/K)$.

$s' = \dim_{\mathbb{F}_2} S^{(\hat{\phi})}(\mathcal{E}'/K)$.

Fact. *(a)* $S^{(\phi)}(\mathcal{E}/K) \hookrightarrow K(S,2)$ *and given any* $d \in K(S,2)$, *the corresponding homogeneous space* C_d *can be given by*

$$C_d : dw^2 = d^2 - 2dAz^2 + (A^2 - 4B)z^4.$$

Similarly, $S^{(\hat{\phi})}(\mathcal{E}'/K) \hookrightarrow K(S,2)$ *and given any* $d \in K(S,2)$, *the corresponding homogeneous space* C'_d *can be given by*

$$C'_d : dw^2 = d^2 + dAz^2 + Bz^4.$$

(b) There is an exact sequence

$$0 \to \frac{\mathcal{E}'(K)}{\phi(\mathcal{E}(K))} \to S^{(\phi)}(\mathcal{E}/K) \to Ш(\mathcal{E}/K)[\phi] \to 0.$$

$$O \mapsto 1$$

$$(0,0) \mapsto A^2 - 4B$$

$$(x,y) \mapsto x \quad \text{if } x \neq 0$$

(See [Sil1, Chapter 10, Theorem 4.2 and Proposition 4.9].)

Lemma 2.2.

$$s \leq \#\{\text{prime divisors of } (A^2 - 4B)\} + 1,$$

$$s' \leq \#\{\text{prime divisors of } B\} + 1.$$

Observe the following commutative diagram of exact sequence of $\mathbb{F}_2$-vector

spaces:

$$\begin{array}{ccccc}
 & & 0 & & 0 \\
 & & \downarrow & & \downarrow \\
 & & \dfrac{\mathcal{E}'(K)[\hat{\phi}]}{\phi(\mathcal{E}(K)[2])} & (\mathbb{Z}/2\mathbb{Z})^{2-\epsilon} & 0 \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & \dfrac{\mathcal{E}'(K)}{\phi(\mathcal{E}(K))} & \to S^{(\phi)}(\mathcal{E}/K) \to & Ш(\mathcal{E}/K)[\phi] \to 0 \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & \dfrac{\mathcal{E}(K)}{2\mathcal{E}(K)} & \to S^{(2)}(\mathcal{E}/K) \to & Ш(\mathcal{E}/K)[2] \to 0 \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & \dfrac{\mathcal{E}(K)}{\hat{\phi}(\mathcal{E}'(K))} & \to S^{(\hat{\phi})}(\mathcal{E}'/K) \to & Ш(\mathcal{E}'/K)[\hat{\phi}] \to 0 \\
 & & \downarrow & & \\
 & & 0 & &
\end{array}$$

where $\varepsilon = \dim_{\mathbb{F}_2} \mathcal{E}(K)[2]$. From the diagram, one can obtain

$$r + \varepsilon \leq \dim_{\mathbb{F}_2} S^{(2)}(\mathcal{E}/K) \leq s + s' - (2 - \varepsilon)$$

and thus one has the inequality

$$r \leq s + s' - 2. \qquad (2.3)$$

The following proposition follows immediately from Lemma 2.2 and (2.3).

Proposition 2.4.

$$r \leq \#\{\text{prime divisors of } B\} + \#\{\text{prime divisors of } (A^2 - 4B)\}.$$

Proposition 2.5. *Suppose B and $A^2 - 4B$ are not perfect square in R with $\deg(A) \leq 2, \deg(B) \leq 2$. Then either $r = s + s' - 2$ or $r \leq s + s' - 4$.*

Proof. From (2.3), we have that $r \neq s+s'-3$ if and only if either $r = s+s'-2$ or $r \leq s + s' - 4$. Suppose that $r = s + s' - 3$. Taking $\mathbb{F}_2$-dimension to each

term in the above big diagram:

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & s & \to & s & \to & 0 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & s+s'-2 & \to & s+s'-2 & \to & 0 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & s'-1 & \to & s' & \to & 1 & \to & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}
$$

(Recall that the Shafarevich-Tate groups of our curves $\mathcal{E}/K$ and $\mathcal{E}'/K$ are both finite and thus the $\mathbb{F}_2$-dimension of their 2-parts are even(See [Mil2]).)

Now consider the dual diagram of the previous one, we have

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & s'-1 & \to & s' & \to & 1 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & s+s'-2 & \to & s+s'-2 & \to & 0 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & s & \to & s & \to & 0 & \to & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}
$$

Observe that there is a contradiction which occurs at the last vertical exact sequence of the last diagram. Therefore $r \neq s + s' - 3$. $\square$

The following theorem will help us to compute the difference of s and s'.

Theorem 2.6. *(Duality Theorem) Let $\phi : \mathcal{E}/K \to \mathcal{E}'/K$ and $\hat{\phi} : \mathcal{E}'/K \to \mathcal{E}/K$ be dual isogenies of elliptic curves over K. For any place $\nu \in M_K$, let c_ν, c'_ν be the numbers of components of the fiber of the Neron model over ν of E, E' respectively. Then*

$$\frac{|S^{(\phi)}(E/K)|}{|S^{(\hat{\phi})}(E'/K)|} = \frac{|\mathcal{E}_{tors}(K)|}{|\mathcal{E}'_{tors}(K)|} \prod_{\nu \in M_K} \frac{c'_\nu}{c_\nu}.$$

(See [Cas1].)

Lemma 2.7. *Let $\mathcal{E}/K : y^2 = x^3 + Ax^2 + Bx$ and $\mathcal{E}'/K : y^2 = x^3 - 2Ax^2 + (A^2 - 4B)$. Let $\phi : \mathcal{E}/K \to \mathcal{E}'/K$ and $\hat{\phi} : \mathcal{E}'/K \to \mathcal{E}/K$ be dual isogenies of degree 2. Suppose that $\deg(A) = 2, 1 \leq \deg(B) \leq 2$ and $\ell(A) \in \mathbb{F}_q^{*2}$. Suppose further that both B and $A^2 - 4B$ are squarefree in A. Then*

$$s - s' = \#\{\text{prime divisors of } B^2 - 4A\} - \#\{\text{prime divisors of } B\} - 1.$$

Proposition 2.8. *The rank of our lifted curve is strictly less than 3 except g, h are associated to different finite places in M_K and either $f^2 - 4gh$ factors as $\wp_1\wp_2$ where $\wp_1, \wp_2$ are irreducible, quadratic, and associated to different finite places in M_K or $f^2 - 4gh$ factors as $\wp_1\wp_2\wp_3\wp_4$ where $\wp_1, \wp_2, \wp_3, \wp_4$ are irreducible, linear, and associated to different finite places in M_K.*

Now we give two lemmas which will be used to prove Proposition 2.8.

Lemma A. *(a) $C_\alpha \notin S^{(\phi)}(\mathcal{E}/K)$.*

(b) If $f^2 - 4gh$ has a linear factor, then $C'_\alpha \notin S^{(\hat{\phi})}(\mathcal{E}'/K)$.

Lemma B. *If $\wp$ is a linear factor $f^2 - 4gh$, then $C_\wp \notin S^{(\phi)}(\mathcal{E}/K)$.*

In those two exceptional case, we will show that either their rank is equal to 3 or ≤ 1, the latter one is extremely impossible to happen according to our lifting experience.

Proposition 2.9. *Suppose that g, h are associated to different finite places in M_K and $f^2 - 4gh$ factors as $\wp_1\wp_2$ where $\wp_1, \wp_2$ are irreducible, quadratic, and associated to different finite places in M_K. Then either $r = 3$ or $r \leq 1$.*

Proposition 2.10. *Suppose g, h are associated to different finite places in M_K and $f^2 - 4gh$ factors as $\wp_1\wp_2\wp_3\wp_4$ where $\wp_1, \wp_2, \wp_3, \wp_4$ are irreducible, linear, and associated to different finite places in M_K. Then either $r = 3$ or $r \leq 1$.*

§3. Computing The Canonical Heights

Let K be the function field $\mathbb{F}_q(t)$ and let $\mathcal{E}/K$ be an elliptic curve over K. Recall that the canonical height on $\mathcal{E}/K$ is a function $\hat{h} : \mathcal{E}(\bar{K}) \longrightarrow \mathbb{Q}$ which can be decomposed into sum of local heights

$$\hat{h}(\mathcal{P}) = \sum_{\nu \in M_K} \hat{\lambda}_\nu(\mathcal{P}) \tag{3.1}$$

where $\hat{\lambda}_\nu$ is the local height function at the place ν.

Theorem 3.2. *(Local height at nonarchimedean valuations) Let $\mathcal{E}/K$ be an elliptic curve given by a Weierstrass equation*

$$\mathcal{E}/K : y^2 = x^3 + Ax^2 + Bx$$

which is minimal at the place ν, and let $\mathcal{P} = (x, y) \in E(K_\nu)$.

$$a = 3x^2 + 2Ax + B,\ b = 2y,\ c = 3x^4 + 4Ax^3 + 6Bx^2 - B^2,$$

$$c_4 = 16(A^2 - 3B),\ \Delta(\mathcal{E}) = 16B^2(A^2 - 4B),$$

$$N = ord_\nu(\Delta(\mathcal{E})),\ n = min\{ord_\nu(b), \frac{1}{2}N\},\ d = \deg(\nu).$$

(a) If $ord_\nu(a) \leq 0$ *or* $ord_\nu(b) \leq 0$, *then* $\hat{\lambda}(\mathcal{P}) = max\{0, -\frac{1}{2}ord_\nu(x)d\} + \frac{1}{12}Nd$.

(b) Otherwise, if $ord_\nu(c_4) = 0$, *then* $\hat{\lambda}(\mathcal{P}) = -\frac{n(N-n)}{2N}d + \frac{1}{12}Nd$.

(c) Otherwise, if $ord_\nu(c) \geq 3ord_\nu(b)$, *then* $\hat{\lambda}(\mathcal{P}) = -\frac{1}{3}ord_\nu(b)d + \frac{1}{12}Nd$.

(d) Otherwise, $\hat{\lambda}(\mathcal{P}) = -\frac{1}{8}ord_\nu(c)d + \frac{1}{12}Nd$.

(See [Sil2].)

Now we turn back to consider our lifted curve $\mathcal{E} : y^2 = x^3 + dfx^2 + d^2ghx$ over the function field K. Recall that $1 \leq \deg(g) + \deg(h) \leq 2$ and $\deg(f) = 2$. By routine computation, we have

$$c_4 = 16d^2(f^2 - 3gh),\ \Delta(\mathcal{E}) = 16d^6g^2h^2(f^2 - 4gh)$$

and $\deg(\Delta(\mathcal{E})) = 6$ or 8, then it is clear that the Weierstrass equation given as above is minimal at every finite place in K(See [Sil1, Chapter 7, Remark 1.1]). The following proposition gives bounds for the heights of $Q_i, i \in \{1, 2, 3\}$.

Proposition 3.3. *For every* $i \in \{1, 2, 3\}$, $-\frac{13}{24} \leq \hat{h}(Q_i) \leq \frac{3}{8}$.

Corollary 3.4. *For every* $i \in \{1, 2, 3\}$, $\hat{h}(Q_i) \in \dfrac{\mathbb{Z}}{840}$.

Proposition 3.5. *Given any* $P_1, P_2, P_3 \in E(\mathbb{F}_q)$, *the computation of the canoniacl height of the three lifted points* Q_1, Q_2, Q_3 *can be done in a probabilistic algorithm with* $O(\log q)$ *operations in* $\mathbb{F}_q$.

五、計畫成果自評:

Proposition 2.8 tells that the rank of the lifted curve is less than or equal to the number of lifted points. Proposition 3.3 gives explicit bounds of the canonical heights of the lifted points. So we can life the given curve to a curve defined over a global field with small rank and hence it is highly possible that the lifted points are linearly

depedent. Once they are depedent, one can obtain a relation and solve the ECDLP.

六、參考文獻:

[Adl1] L. Adleman, *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, Proc. 20th IEEE Found. Comp. Sci. Symp., 1979, pp. 55-60.

[Art1] M. Artin and H.P.F. Swinnerton-Dyer, *The Shafarevich-Tate Conjecture for Pencils of Elliptic Curves on K3 Surfaces*, Invention Math. 20, 249-266(1973).

[Bru1] A. Brumer, *The Average Rank of Elliptic Curves I*, Invent. Math. 109, 445-472(1992).

[Cas1] J.W.S. Cassels, *Arithmetic on curve of genus 1*,VIII J. reign Angew. Math., 217, pp. 180-199, 1965.

[Che1] Yen-Mei J. Chen, *The Selmer Groups and the Ambiguous Ideal Class Groups of Cubic Fields*, Bull. Austral. Math. Soc., Vol(54) 267-274, 1996.

[Che2] Yen-Mei J. Chen, *The Selmer Groups of Elliptic Curves and the Ideal Class Groups of Quadratic Fields*, Communications in Algebra, 25(7) 2157-2167, 1997.

[Cox1] David Cox and Walter R. Parry, *Torsion in Elliptic Curves over k(t)*, Compositio Mathmetica, Vol. 41, Fasc. 3, 1980, pp. 337-354.

[Evd1] S. Evdokimov, *Factorization of Polynomials over Finite Fields in Subexponential Time under GRH*, Lecture Notes in Computer Science, Vol. 877, 1994, pp. 209-219.

[Fre1] G. Frey and H.-G. Guck, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. 62(1994), 865-874.

[Kol1] N. Koblitz, *Elliptic curve cryptosystem*, Mathematics of Computation 48 (1987), 203-209.

[Jac1] M. Jacobson, N. Koblitz, J. Silverman, A. Stein, E. Teske, *Analysis of the Xedni Calcu;us Attack*, preprint, 1999.

[Men1] A. Menezes, T. Okamoto and S.A. Vanstone, *Reducing elliptic curves logarithms to logarithm in a finite field*, IEEE Trans. Info. Theory, 39, (1993) 1639-1646.

[Mil1] V.S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology CRYPTO'85, Springer-Verlag, 1986, pp. 417-426.

[Mil2] J.S. Milne, *On a conjecture of Artin and Tate*, Annals of Mathematics, 102(1975), 517-533.

[Rab1] M.O. Rabin, *Probabilistic Algorithms in Finite Fields*, SIAM. J. Comput., Vol 9, No 2, 1980, 273-280.

[Sem] I. Semaev, *Evaluation of Discrete Logarithms in a Group of p-torsion Points of an Elliptic Curve in characteristic p*, Math. of Comp. 67(1998), 353-356.

[Sil1] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer--Verlag, 1985.

[Sil2] J. Silverman, *Computing Heights on Elliptic Curves*, Math. Comp., vol 51,

1988, pp. 339-358.
[Sil3] J. Silverman, J. Suzuki, *Elliptic curve discrete logarithms and the index calculus*, ASIACRYPT'98, to appear.
[Sil4] J. Silverman, *The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem*, preprint, 1998.
[Sil5] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer Verlag, 1994.
[Tat1] J. Tate, *Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil*, Lect. Notes Math., Vol. 476, pp. 33-52, 1975.