

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang
Scribe: Iftikhar A Burhanuddin
burhanud@usc.edu
Class #6 - February 12, 2002

Administrivia: Scribe notes for class #5 are online at the course webpage:
<http://www-rcf.usc.edu/~mdhuang/cs599>

Today's class: Attacks on ECDLP continued

1. Classical Index Calculus for DL/\mathbf{F}_p^*
2. Index Calculus type attack for ECDLP
3. Xedni calculus method for ECDLP

Assignment: Mail Bilal Shaw (bilalsha@usc.edu) about interesting websites and links to papers which can be displayed at the course webpage

Remark: Peter Shor's paper [2] outlines how DLP and factoring can be done in quantum polynomial time using a quantum computer. The flavour of the algorithm is different from conventional methods and it talks about quantum Fourier analysis. So a possible project is the study of the use of Quantum computers to solve hard cryptographic problems.

I. Index Calculus method for DL/\mathbf{F}_p^*

Discrete Logarithm Problem: Given $\mathbf{F}_p^* = \langle g \rangle$ and $a \in \mathbf{F}_p^*$ to compute t such that $a = g^t \pmod p$

Notation: $t = \log_g a$. Please don't confuse with the logarithm function. But notice that the usual logarithm rule applies even in this scenario: $\log_g ab = \log_g a + \log_g b$. We'll drop the base g in the discussion which follows.

This method relies on smoothness of numbers to compute discrete logarithms in finite fields in sub exponential time. The idea is to lift elements of \mathbf{F}_p to \mathbf{Z} using the *trivial* lift: regards the elements as numbers in \mathbf{Z} . We try to linearize the problem and then rely on simple Linear Algebra to give us the solution.

Suppose $c \equiv \prod_i p_i^{e_i} \pmod p \Rightarrow \log c \equiv \sum_i e_i \log p_i \pmod{p-1}$

Say our factor base contains some k primes, $F = \{2, 3, \dots, p_k\}$, and $p_k \leq b$, for some suitable bound b . We call a number which factors into primes in F as being b -smooth.

Pick random number x and compute $a.g^x \pmod p = g^{x+t} \pmod p$. Suppose in the map $x \mapsto g^{x+t}$, x is uniformly distributed over $\{1, 2, \dots, p-1\}$ and t

being a fixed number, then g^{x+t} is a random element in \mathbf{F}_p^* . a itself may not be b -smooth and the purpose of the randomization is to hope that the element generated is sufficiently smooth. Regarding $a.g^x \bmod p$ as an integer instead of being an element in a finite field is called we previously termed a *lift*.

Suppose $a.g^x \bmod p$ factors smoothly over our factor base,
 $\Rightarrow a.g^x \bmod p = \prod_i p_i^{e_i} \Rightarrow t + x \equiv \sum_i e_i \log p_i \bmod p - 1$
 t and the $\log p_i$'s are the unknowns in the above congruence.
 (Notice that the modulus is $p - 1$ this is because
 $g^{LHS} = g^{RHS} \Rightarrow g^{LHS-RHS} = 1 \Rightarrow LHS \equiv RHS \bmod \text{ord}(g)$)

So the # unknowns = $1 + \#p_i = 1 + \#F$

Therefore we need $1 + \#F$ b -smooth numbers to solve the linear system to get t and the $\log p_i$'s which comes along as a bonus. Actually we need more than $1 + \#F$ many congruences since some of them may be linearly dependent.

Remark: We skimmed over some details like solving linear systems modulo a composite number and in practice sieving techniques instead of generating random x 's.

Now what is the probability of success?
 b should be big enough to guarantee that the probability of success is substantial or atleast non-negligible.

It turns out that if b -smooth $\approx e^{O(\sqrt{\log p \log \log p})}$ then the probability for a random number $\in \{1, 2, \dots, p - 1\}$ to be b -smooth $\approx \frac{1}{e^{O(c_1 \sqrt{\log p \log \log p})}}$, where $c_1 = f(c)$. We'll disregard constants from now on as $L[\alpha, c'] * L[\alpha, c''] = L[\alpha, c' + c'']$, the constants add up in the exponent.

Hence the expected # of random x 's before $a.g^x$ is b -smooth is

$$\begin{aligned} &\approx e^{O(\sqrt{\log p \log \log p})} \\ \#F < b &\approx e^{O(\sqrt{\log p \log \log p})} \\ \Rightarrow \text{total } \# \text{ trials} &\approx e^{O(\sqrt{\log p \log \log p})} \end{aligned}$$

We didn't solve DL/\mathbf{F}_p^* in \mathbf{F}_p^* but we lifted the elements to \mathbf{Z} and took the discrete logarithm in \mathbf{F}_p^* and then looked as the linear congruences modulo a composite number. \mathbf{Z} is just one of the possibilities to the where we want to lift \mathbf{F}_p^* to. Other choices are $\mathbf{F}_p[x]$, ring of integers over a number field, function field, etc. And these fancier algorithms move the running time from $L[\frac{1}{2}]$ to $L[\frac{1}{3}]$.

II. Index Calculus type attack for ECDLP

Victor Miller's paper [3] which talks about using Elliptic Curve to do Cryptography also hints at the seeming inapplicability of an index calculus type attack

(which succeeds in the DL/ \mathbf{F}_p^*) to ECDLP

Elliptic Curve Discrete Logarithm Problem: Given $E : y^2 = x^3 + ax + b$, $a, b \in \mathbf{F}_p$ and $S \in E(\mathbf{F}_p)$ and $\text{ord}(S) = N$ and $T \in \langle S \rangle$ to compute m such that $T = mS$

Inspired by the Index Calculus method let's try lifting $S \in E(\mathbf{F}_p)$ to $\tilde{E}(\mathbf{F}_p)$, $\tilde{E} : y^2 = x^3 + ax + b$, $a, b \in \mathbf{Z}$.

Say $S = (x_0, y_0)$. We know that $S \in E(\mathbf{F}_p) \subset \mathbf{F}_p[X]/\mathbf{F}_p$ and $y_0^2 = x_0^3 + ax_0 + b$ holds in \mathbf{F}_p . So as integers $y_0^2 \equiv x_0^3 + ax_0 + b \pmod{p}$. Then is $(x_0, y_0) \in \tilde{E}(\mathbf{F}_p) \subset \mathbf{Z}[X]/\mathbf{Z}$? We see that $\exists d, y_0^2 = x_0^3 + ax_0 + b + dp$. But this is another curve, lets call it $\tilde{E} : y^2 = x^3 + ax + (b + dp)$ and we see that $(x_0, y_0) \in \tilde{E}(\mathbf{Z})$. Also d is fixed by (x_0, y_0) and so for a different point we get a different d . Hence the difficulty of using an index calculus type attack for ECDLP is that lifting points is *tricky*. How to efficiently lift even two points to the same curve is not well understood.

Remark:

1. In theory if you fix d then $S = (x_0, y_0) \in E(\mathbf{F}_p)$ has a lift to $\tilde{S} = (x_0, y_0) \in \tilde{E}(\mathbf{Z})$. Now consider $m.\tilde{S} \in \tilde{E}(\mathbf{Z})$ and if we reduce this point modulo p (co-ordinate wise) we get $m.S \in E(\mathbf{F}_p)$ and this is equal to T . So now we have two points lifted to the same curve but this lift requires computing the EC discrete log to obtain m .
2. The number of bits to write down the points grows exponentially as illustrated on Page 143 of Koblitz's book [4].

III. Xedni Calculus method for ECDLP

Silverman's idea [5] was to lift a set of points from the given curve defined over a finite field to a plane curve over the rationals (= integers in projective coordinates) that fits these points.

More about Xedni and Index techniques in Lecture # 7

Bibliography:

1. Neal Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, Vol. 48, No. 177, 1987, 203-209.
2. P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), 124-134.

3. V. Miller, Uses of elliptic curves in cryptography, Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, volume 218, Springer-Verlag, pages 417-426, 1986.
4. Neal I. Koblitz, Algebraic Aspects of Cryptography (Algorithms and Computation in Mathematics, Vol 3), Springer-Verlag, 1998.
5. J.H. Silverman: The Xedni calculus and the elliptic curve discrete logarithm problem. Design Codes Cryptography 20(2000), 5-40
6. Lifting Elliptic Curves and Solving the Elliptic Curve Discrete Logarithm Problem, by Ming-Deh A. Huang, Ka-Lam Kueh, and Ki-Sing Tan, Mar 31, 2000. ANTS-IV, Algorithmic Number Theory (Ed.: Wieb Bosma), Lecture Notes in Computer Science 1838, pp. 377-384.

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang
 Scribe: Iftikhar A Burhanuddin
 burhanud@usc.edu
 Classes #7 - February 19, 2002

Today's class: Attacks on ECDLP continued

1. Index Calculus type attacks for ECDLP - General Idea
2. Index Calculus attack for ECDLP
3. Xedni Calculus attack for ECDLP

Elliptic Curve Discrete Logarithm Problem: Given $E : y^2 = x^3 + ax + b$, $a, b \in \mathbf{F}_p$ and $S \in E(\mathbf{F}_p)$ and $\text{ord}(S) = N \sim p$, a big prime and $T \in \langle S \rangle$ to compute m such that $T = mS$

I. Index Calculus type attacks for ECDLP - General Idea

1. (A) Lift E/\mathbf{F}_p to \tilde{E}/\mathbf{Q}
 (B) Lift points $a_i S + T$ with random a_i to $P_i \in \tilde{E}(\mathbf{Q})$, for some \tilde{E} (which reduces mod p to E), $i = 0, 1, \dots, r$, where r is the rank of the latter curve which will talk about later.
Note: If we do (A) and then (B) we get Victor Miller's Index Calculus attack [1] and instead if we do (B) and then (A) we get the Xedni Calculus attack [2].

2. Hopefully, the P_i 's are linearly dependent in $\tilde{E}(\mathbf{Q})$ i.e.,

$$\exists \lambda_i \in \mathbf{Z}, \lambda_0 P_0 + \lambda_1 P_1 + \dots + \lambda_r P_r = 0$$

Now with λ_i computed the discrete logarithm m can be extracted:

$$\begin{aligned} \sum_{i=0}^r \lambda_i P_i &= 0 \text{ on } \tilde{E} \\ \Downarrow \text{reduction mod } p & \\ \sum_{i=0}^r \lambda_i \overline{P_i} &= 0 \text{ on } E \\ \Rightarrow \sum_{i=0}^r \lambda_i (a_i S + T) &= 0 \text{ on } E \\ \Rightarrow \sum_{i=0}^r \lambda_i (a_i + m) S &= 0 \text{ on } E \\ \Rightarrow (\sum_{i=0}^r \lambda_i a_i) + m (\sum_{i=0}^r \lambda_i) &\equiv 0 \text{ mod } N \text{ on } E \quad (**) \end{aligned}$$

We can invert $\sum_{i=0}^r \lambda_i$ and find m modulo N unless we are unlucky and $\sum_{i=0}^r \lambda_i$ turns out to be 0 mod N in which case we patiently start all over again

II. Index Calculus attack for ECDLP

1. Lift E/\mathbf{F}_p to some \tilde{E}/\mathbf{Q}
2. Then lift random points $a_i S + T$ to $P_i \in \tilde{E}(\mathbf{Q})$ (and this is very difficult to do)

The structure of $\tilde{E}(\mathbf{Q})$ contains copies of \mathbf{Z} which represents the non-torsion part and the torsion part is denoted by $\tilde{E}(\mathbf{Q})_{\text{tor}}$, which is a subgroup of $\tilde{E}(\mathbf{Q})$ and contains points on the curve which are killed by a finite number.

$$\begin{aligned} \tilde{E}(\mathbf{Q}) &\cong \mathbf{Z} \oplus \dots \oplus \mathbf{Z} \oplus \tilde{E}(\mathbf{Q})_{\text{tor}} \\ \tilde{E}(\mathbf{Q})_{\text{tor}} &= \{P \in \tilde{E}(\mathbf{Q}) \mid n.P = 0 \text{ for some } n \in \mathbf{Z}\} \\ |\tilde{E}(\mathbf{Q})_{\text{tor}}| &\leq 16 \end{aligned}$$

The number of copies of \mathbf{Z} in $\tilde{E}(\mathbf{Q})$ is called the Mordell Weil rank and is denoted by r . $\mathbf{Z} \oplus \dots \oplus \mathbf{Z}$ can be viewed as a r -dimensional vector space and so if the P_i 's have to be dependent we need to lift atleast r points...a heuristically sound argument.

The Mordell Weil Theorem says that $\tilde{E}(\mathbf{Q})$ is a finitely generated group, that is the rank r is finite. Hence once we choose an elliptic curve, the rank is bounded and therefore the number of independent points we can choose is bounded. This puts a constraint on the size of our factor base and makes it difficult to apply Index Calculus to ECDLP which worked very well in the DLP scenario, one reason being that in the latter case we had an infinite supply of primes for our factor base.

Remark: If \mathbf{K} is a number field (a finite extension of \mathbf{Q}) then $\tilde{E}(\mathbf{K})$ is finite.

III. Xedni Calculus for ECDLP

1. Lift random points $a_i S + T$ to P_i over \mathbf{Q}
2. Then find a curve \tilde{E}/\mathbf{Q} fitting P_i and $\tilde{E} \bmod p = E$

Any curve $F(x, y) = a_0 x^3 + a_1 x^2 y + a_2 x y^2 + a_3 y^3 + a_4 x^2 + a_5 x y + a_6 y^6 + a_7 x + a_8 y + a_9$ is defined by a vector $a = (a_0, a_1, \dots, a_9)$. The vectors a and λa , where λ is a scalar represent the same curve. We have 9 degrees of freedom in choosing a . Say $P_i = (x_i, y_i)$, such that $F(x_i, y_i) = 0, i = 1, \dots, 9$

$$\begin{pmatrix} x_1^3 & x_1^2 y_1 & y_1^3 & \dots & y_1 & 1 \\ x_2^3 & x_2^2 y_2 & y_2^3 & \dots & y_2 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_9^3 & x_9^2 y_9 & y_9^3 & \dots & y_9 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_9 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

$$A_{9 \times 10} a_{10 \times 1} = 0$$

If A has a rank of 9, then a is uniquely determined upto a constant factor. Say $\bar{A} = A \bmod p$, that is each entry of A is reduced modulo p . If \bar{A} also has full rank (=9) over \mathbf{F}_p then $\bar{A}\bar{a} = 0$ also has a unique solution upto constant factor.

Say $\tilde{E} : F_a(x, y) = 0$ and $F_a(x_i, y_i) = 0, \Rightarrow \bar{F}_{\bar{a}}(x_i, y_i) = 0, i = 1, \dots, 9$. But there is only one curve satisfying these relations hence $\bar{F}_{\bar{a}} = 0$ is our original curve E , that is $\tilde{E} \bmod p = E$

Some definitions and facts:

Say $t = \frac{p}{q} \in \mathbf{Q}$, height of rational number t , $H(t) = \max(|p|, |q|)$ and logarithmic height $h(t) = \log(H(t))$, which is the length of t , that is the number of bits to write down t .

Say $P = (x, y)$, $h(P) := h(x(P))$, where $x(p)$ denotes the x-coordinate of point P. The height depends on the model and mathematicians came up with the canonical height of a point which does not depend on the model, which is defined as:

$$P \in \tilde{E}(\mathbf{Q}), \hat{h}(P) = \frac{1}{2} \lim_{n \rightarrow \infty} 4^{-n} h(2^n P)$$

$$\hat{h}(mP) = m^2 \hat{h}(P) \text{ and } \hat{h}(0) = 0$$

$$\Rightarrow \text{if } mP = 0 \text{ then } \hat{h}(P) = 0$$

$$\hat{h}(P) = \frac{1}{2} h(P) + o(1),$$

where the error term depends on the elliptic curve \tilde{E}

Canonical height defines a *metric* on $\tilde{E}(\mathbf{Q})$ and is a way to measure rational non-torsion points as it annihilates the torsion part of the curve.

The inner product of points P, Q on the curve $\tilde{E}(\mathbf{Q})$ is a positive definite quadratic form and defined as follows:

$$\langle P, Q \rangle := \frac{1}{2} [\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)]$$

$$\|P\|^2 = \langle P, P \rangle = \frac{1}{2} [\hat{h}(2P) - 2\hat{h}(P)]$$

$$= \frac{1}{2} [4\hat{h}(P) - 2\hat{h}(P)] = \hat{h}(P)$$

When $r = 1$, $\tilde{E}(\mathbf{Q}) = \mathbf{Z}P \oplus \tilde{E}(\mathbf{Q})_{\text{tor}}$ and the whole group becomes a 1-dimensional lattice, where the length of the basis element P is given by $\|P\|$.

When $r = 2$, $\tilde{E}(\mathbf{Q}) = \mathbf{Z}P_1 \oplus \mathbf{Z}P_2 \oplus \tilde{E}(\mathbf{Q})_{\text{tor}}$ and $\tilde{E}(\mathbf{Q})$ can be thought of as a 2-dimensional lattice and the angle between the basis vectors is given by $\frac{\langle P_1, P_2 \rangle}{\|P_1\| \|P_2\|}$

The kernel of the homomorphism from $\tilde{E}(\mathbf{Q})$ to $\mathbf{Z}P_1 \oplus \mathbf{Z}P_2$ is $\tilde{E}(\mathbf{Q})_{\text{tor}}$ hence $\tilde{E}(\mathbf{Q})/\tilde{E}(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}P_1 \oplus \mathbf{Z}P_2$.

We show that the number of lattice points on curve \tilde{E} of rank r and the canonical height bounded by b , $N(\tilde{E}, b)$ has the following upper bound

$$N(\tilde{E}, b) = \#\{P \in \tilde{E}(\mathbf{Q}) \mid \hat{h}(P) \leq b\} \leq 2^{c_1 r^2} \left(\frac{b}{\log \Delta(\tilde{E})}\right)^{\frac{r}{2}}$$

where $\Delta(\tilde{E})$ is the discriminant of \tilde{E} and c_1 is a constant

Proof: A good approximation to $N(\tilde{E}, b)$ is:

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

where $T = |\tilde{E}(\mathbf{Q})_{\text{tor}}|$ and $\alpha_r = \frac{1}{\sqrt{\pi r}} \left(\frac{2\pi e}{r}\right)^{\frac{r}{2}}$ and $R = \det \langle P_i, P_j \rangle, 1 \leq i, j \leq r$ is the volume of the (parallelepiped) fundamental region determined by the basis. This volume is called the regulator of the curve and is independent of the choice of basis and an invariant of the curve.

Based on a conjecture by Serge Lang the canonical height can be lower bounded:

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

Then using $T \leq 16$ and

$$R^{1/r} \geq \left(\frac{\sqrt{3}}{2}\right)^{r-1} \min_{P \in \tilde{E}(\mathbf{Q})/\tilde{E}(\mathbf{Q})_{\text{tor}}} \hat{h}(P)$$

we obtain

$$N(\tilde{E}, b) \leq 2^{c_1 r^2} \left(\frac{b}{\log \Delta(\tilde{E})}\right)^{\frac{r}{2}} \leq 2^{O(r^2)} b^{\frac{r}{2}} \quad (***)$$

The last inequality is a very loose bound but can be used to bound $|\lambda_i|$'s such that $\sum_i \lambda_i P_i = 0$ that is when the P_i 's are dependent. For example $\|3P_1 + 2P_2\| \leq (3+2) \max\{\|P_1\|, \|P_2\|\}$

Say $P_i \in \tilde{E}(\mathbf{Q})$ and suppose $\max_i a_i = m$ and $\max_i \|P_i\| = \sqrt{h}$ that is $\max_i \hat{h}(P_i) = h$

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

Hence

$$\hat{h}(\sum_{i=0}^r a_i P_i) \leq hm^2(r+1)^2$$

And using (***) with $b = hm^2(r+1)^2$, we get

$$N(\tilde{E}, hm^2(r+1)^2) \leq 2^{O(r^2)}(hm^2(r+1)^2)^{\frac{r}{2}}$$

Since the number of (a_0, \dots, a_r) with $a_i \in \{0, 1, \dots, m\} = (m+1)^{r+1}$ by the pigeon-hole principle

$$\begin{aligned} & \text{If } (m+1)^{r+1} > 2^{O(r^2)}(hm^2(r+1)^2)^{\frac{r}{2}} \text{ then } \exists (a_0, \dots, a_r) \neq (b_0, \dots, b_r), \\ & a_i, b_i \in \{0, \dots, m\} \text{ such that } \sum_i a_i P_i = \sum_i b_i P_i \\ & \Rightarrow \sum (a_i - b_i) P_i = 0 \text{ with } |a_i - b_i| \leq m \end{aligned}$$

And the bound on the coefficients of the P_i 's holds when $(m+1)^{r+1} > 2^{O(r^2)}(hm^2(r+1)^2)^{\frac{r}{2}} \Rightarrow m \leq 2^{O(r^2)} h^{\frac{r}{2}}$ loose bound

Lemma: If rank of $(\tilde{E}) = r$ then P_0, \dots, P_r has a linear dependency of the form $\sum_{i=0}^r \lambda_i P_i = 0$, where $|\lambda_i| \leq 2^{O(r^2)} h^{\frac{r}{2}}$ with $h = \max_{\{i=0, \dots, r\}} \hat{h}(P_i)$

$$(E/\mathbf{F}_q; a_0 S + T, \dots, a_r S + T) \xrightarrow{\text{lift}} (E/\mathbf{F}_q; P_0, \dots, P_r)$$

1. $\hat{h}(P_i) = O(e^{\sqrt{\log p \log \log p}}) = h$ We want the maximum canonical height to be exponentially bounded as we are shooting for a sub exponential ECDLP algorithm
2. We hope the P_i 's are dependent

If [1] and [2] are satisfied, we have a *good lift*. [2] and *Lemma* tell us that

$$\exists \lambda_i \sum \lambda_i P_i = 0 \text{ and } |\lambda_i| = 2^{O(r^2)} h^{\frac{r}{2}}$$

Reducing modulo p , we obtain

$$\sum \lambda_i (a_i S + T) = 0 \Rightarrow \sum \lambda_i (a_i + m) S = 0 \Rightarrow \sum \lambda_i b_i \equiv 0 \pmod{N}$$

So not only do the P_i 's have small dependency but so do the b_i 's. For each choice of non-zero λ_i , $\#(b_i) = N^r$ and

$$\#(\lambda_i) \leq (2^{O(r^2)} h^{\frac{r}{2}})^{r+1} \approx 2^{O(r^3)} h^{O(r^2)}$$

Hence the total $\#$ of b_i 's, that is, total $\#$ of points that give rise to a good lift is $\leq 2^{O(r^3)} h^{O(r^2)} N^r$
Each good lift is a choice of b_i . Hence the grand total of $\#(b_i) = N^{r+1}$

Therefore fraction of *good* b_i 's is

$$\leq \frac{2^{O(r^3)} h^{O(r^2)} N^r}{N^{r+1}} = \frac{2^{O(r^3)} h^{O(r^2)}}{N}$$

For this to be reasonable we need the fraction to be at most sub exponentially small ($\frac{1}{e^{\sqrt{\log p \log \log p}}}$). Hence we need $N \leq 2^{O(r^3)} h^{O(r^2)} e^{\sqrt{\log p \log \log p}}$. We assumed that $N \sim p$, and solving for the rank we see that we need r to be increasing with $(\log p)^{\frac{1}{3}}$.

Bibliography:

1. Lifting Elliptic Curves and Solving the Elliptic Curve Discrete Logarithm Problem, by Ming-Deh A. Huang, Ka-Lam Kueh, and Ki-Sing Tan, Mar 31, 2000. ANTS-IV, Algorithmic Number Theory (Ed.: Wieb Bosma), Lecture Notes in Computer Science 1838, pp. 377-384.
2. Neal Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, Vol. 48, No. 177, 1987, 203-209.