On The Discrete Logarithm Problem in Finite Fields
(有限体上の離散対数問題について)

張　祺智

On The Discrete Logarithm Problem in Finite Fields

Qizhi Zhang

January 6, 2012

Contents

1 Introduction

Let G be a cyclic group of order n with a generator g, and b be an element of G. The problem to compute x from the equation $g^x = b$ is called discrete logarithm problem.

In several cases, including the case where G is the multiplicative group of a finite field, or the group of rational points of an elliptic curve over a finite field, we do not know any algorithm that can solve the discrete logarithm problem in G in polynomial time in $\log n$. Based on this fact, the discrete logarithm problem in such a group G is extensively applied in cryptography. It is an important and difficult problem to estimate the greatest lower bound for the complexity of solving the discrete logarithm problem.

There is a natural algorithm to solve the discrete logarithm problem by using the Chinese remainder theorem for any cyclic group. If the order of the group does not have a big prime divisor, this algorithm is effective. We recall this algorithm in section 2.1. For a general cyclic group, there is an algorithm with time and space complexity $O(\sqrt{n})$, which is proposed by [Shanks 1971]. We recall it in section 2.2. There is also an algorithm with time complexity $O(\sqrt{n})$ and space complexity $O(1)$, which is proposed by [Pollard 1978]. We recall it in section 2.3.

In the case where the group is the multiplicative group of a finite field, there are some sub-exponential algorithms for the discrete logarithm problem in such a group. The index calculus algorithm is discovered by Kraitchik [Kraitchik 1922] in 1922. After the discrete logarithm problem became important in crypto-system, Pohlig [Pohlig 1977] rediscovered the idea. Adleman [Adleman 1979] optimized the algorithm and presented it in the form we know it today. We recall it in section 3.1. The nmber field sieve is proposed for factoring integers originally (See, for example, [Buhler 1993], [Lenstra-Lenstra 1993]), and transplanted for the discrete logarithm problem (See, for example, [Gordon 1993] [Schirokauer 1993] [Schirokauer 2008]). We recall it in section 3.2. The function field sieve is proposed in [Adleman 1994]. We recall a modification of the simpler and improved version in section 3.3 which is presented in [Adleman and Huang 1999].

Alternatively, we can estimate the greatest lower bound by studying an equivalent problem of a discrete logarithm problem. Let p be an prime number. In [Huang-Raskind 2009], they lifted the discrete logarithm problem in $\mathbb{F}_p^\times$ to a real quadratic field. They defined the "ramification signature" for the real quadratic field and proved that the discrete logarithm problem in $\mathbb{F}_p^\times$ is random polynomial time equivalent to computing the ramification signature of the real quadratic field under two heuristic assumptions, namely, an assumption on the class number and an assumption on a global unit of the real quadratic field. We recall this work in section 4.

In section 5, we generalize the term "ramification signature" of a real quadratic field. In [Huang-Raskind 2009], it is defined in the case where "p and l split". We generalize it to the case where "p is unramified and l splits". We then lift the discrete logarithm problem in $k^\times$ (for $k = \mathbb{F}_p$ or $\mathbb{F}_{p^2}$) to a real quadratic field and prove that the discrete logarithm problem in $k^\times$ is random polynomial time equivalent to computing the ramification signature of the real quadratic field , with one heuristic assumption on the class number. We also show that in the proof of the equivalence in [Huang-Raskind 2009] one can remove the assumption on the global unit. More precisely, we give an improvement (Step 4 in section 5.3 below) on the construction of real quadratic field and global unit that makes the condition (2), (3) in proposition 2 in section 4.1 in [Huang-Raskind 2009] be satisfied automatically.

2 Algorithms of the discrete logarithm problem in general cyclic group

2.1 Reduction

There is a natural algorithm to solve the discrete logarithm problem by Chinese remainder theorem for any cyclic group of small order. Let G be a cyclic group of order n. Let g be a generator of G and b be an element in G. Suppose that all the prime divisors of n are small. We describe this algorithm to compute an integer x such that $g^x = b$ in the following:

Suppose that $n = n_1 n_2$ where $(n_1, n_2) = 1$. If we can solve x_1, x_2 from the equations $(g^{n_2})^{x_1} = b^{n_2}$ and $(g^{n_1})^{x_2} = b^{n_1}$, we then can compute x from

$$\begin{cases} x \equiv x_1 & \mod n_1, \\ x \equiv x_2 & \mod n_2. \end{cases}$$

Clearly, this x is a solution of the equation $g^x = b$.

Suppose that n has the prime decomposition $n = p_1^{e_1} \cdots p_m^{e_m}$. There is a decomposition

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_m,$$

where G_i is a cyclic group of order $p_i^{e_i}$ for $i = 1, 2, \cdots m$.

The assumption that all the prime divisors of n are small implies that we can reduce the discrete logarithm problem in G to the discrete logarithm problem in G_i for $i = 1, 2, \cdots, m$.

Now suppose that G is a cyclic group of degree p^e where p is a small prime number, g is a generator of G and b is an element in G. We want to find the solution x of the equation $g^x = b$. We know that x can be written as $x = x_0 + x_1 p + \cdots + x_{e-1} p^{e-1}$ where $x_0, x_1, \cdots, x_{e-1} \in \{0, 1, \cdots p-1\}$. We compute $x_0, x_1, \cdots, x_{e-1}$ inductively.

Let us compute x_0 firstly. The fact $p^{e-1} x \equiv p^{e-1} x_0 \pmod{p^e}$ implies that

$$(g^{p^{e-1}})^{x_0} = g^{p^{e-1} x}.$$

Therefore, the fact that $g^x = b$ implies that

$$(g^{p^{e-1}})^{x_0} = b^{p^{e-1}}.$$

The both sides of the last equation above are in $G^{p^{e-1}}$, which is a cyclic group of order p. The assumption that p is a small prime implies that we can solve this equation to get x_0 easily.

Secondly, suppose that we have computed $x_0, \cdots, x_{k-1}$, we compute x_k now.

The fact that $(x - x_0 - x_1 p - \cdots - x_{k-1} p^{k-1}) p^{e-k-1} \equiv x_k p^{e-1} \pmod{p^e}$ implies that

$$(g^{p^{e-1}})^{x_k} = g^{(x - x_0 - x_1 p - \cdots - x_{k-1} p^{k-1}) p^{e-k-1}}.$$

Therefore, the fact that $g^x = b$ implies that

$$(g^{p^{e-1}})^{x_k} = (b g^{-x_0 - x_1 p - \cdots - x_{k-1} p^{k-1}})^{p^{e-k-1}}.$$

The both sides of the congruence above are in $G^{p^{e-1}}$, which is a cyclic group of order p. The assumption that p is a small prime implies that we can solve this equation to get x_k easily.

Hence, by induction, we can compute x.

2.2 Baby-step giant-step

Baby-step giant-step algorithm is proposed in [Shanks 1971]. It works for any cyclic group. Given a cyclic group G of order n, a generator g of the G and an element b in G, the problem is to find an integer a such that $g^a = b$. The baby-step giant-step algorithm is based on rewriting a as $a = im+j$, with m the minimal integer that is greater than $\sqrt{n}$ and $0 \leq i < m$ and $0 \leq j < m$. Therefore, we have:

$$b(g^{-m})^i = g^j.$$

We describe the algorithm as follows:

1. Let m be the minimal integer greater than $\sqrt{n}$. Let f be a Hash function that maps any element in G to a memory address.

2. Compute g^j for $0 \leq j < m$, and save the pairs (j, g^j) in the memory address $f(g^j)$.

3. For $0 \leq i < m$, compute bg^{-mi} and compare it with the second coordinate in the memory address $f(bg^{-mi})$. If they are the same when $i = i_0$, denote the first coordinate in the memory address $f(bg^{-mi})$ by j_0, and return $i_0 m + j_0$.

The running time of the algorithm and the space complexity is $O(\sqrt{n})$, much better than the $O(n)$ running time of the naive brute force calculation.

2.3 Pollard's rho algorithm

The Pollard's rho algorithm is proposed by Pollard [Pollard 1978]. Given a cyclic group G of order n, a generator α of the group and a group element β, we state the Pollard's rho algorithm to find an integer x such that $\alpha^x = \beta$.

1. Divide G into three subset $G_0 \amalg G_1 \amalg G_2$ of approximately equal size. Define $f : G \longrightarrow G$ by

$$f(g) = \begin{cases} \alpha\gamma & \text{if } \gamma \in G_0, \\ \gamma^2 & \text{if } \gamma \in G_1, \\ \gamma\beta & \text{if } \gamma \in G_2. \end{cases}$$

and define $g : G \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ and $h : G \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ by

$$g(\gamma, a) = \begin{cases} a & \text{if } \gamma \in G_0, \\ 2a & \text{if } \gamma \in G_1, \\ a+1 & \text{if } \gamma \in G_2. \end{cases} \quad \text{and} \quad h(\gamma, b) = \begin{cases} b+1 & \text{if } \gamma \in G_0, \\ 2b & \text{if } \gamma \in G_1, \\ b & \text{if } \gamma \in G_2. \end{cases}$$

respectively.

2. Let $a_0 = 0$, $b_0 = 0$, $\gamma_0 = 1 \in G$, $i = 1$;

3. Compute $\gamma_i := f(\gamma_{i-1})$, $a_i := g(\gamma_{i-1}, a_{i-1})$, $b_i := h(\gamma_{i-1}, b_{i-1})$;

3. Compute $\gamma_{2i} := f(f(\gamma_{2i-2}))$, $a_{2i} := g(f(\gamma_{2i-2}), g(\gamma_{2i-2}, a_{2i-2}))$, $b_{2i} := h(f(\gamma_{2i-2}), h(\gamma_{2i-2}, b_{2i-2}))$;

4. If $\gamma_i = \gamma_{2i}$ and $\gcd(b_i - b_{2i}, n) = 1$ then return $(b_i - b_{2i})^{-1}(a_i - a_{2i}) \mod n$.

5. If $\gamma_i \neq \gamma_{2i}$ then $i \leftarrow i + 1$, and go to step 2.

Proof. Because $\gamma_i = \alpha^{a_i}\beta^{b_i}$. ∎

The running time of Pollard's rho algorithm is approximately $O(\sqrt{n})$.

3 Algorithms of the discrete logarithm problem in the multiplicative group of finite fields

3.1 Index calculus algorithm

The index calculus algorithm is discovered by Kraitchik [Kraitchik 1922] in 1922. After the discrete logarithm problem became important in crypto-system, Pohlig [Pohlig 1977] rediscovered the idea. Adleman [Adleman 1979] optimized the algorithm and presented it in the form we know it today.

Let p be an big prime number, g and b be two positive integers that do not divided by p. We describe the index calculus algorithm to solve x from the equation $g^x \equiv b \pmod p$:

1. Take a bound $B > 0$, Let S be the set consisting of all the prime numbers less than B and q be the maximal number in S.

2. For $n = 1, 2, \cdots$, compute $(g^n \mod p)$. If it is B-smooth (i.e. all the prime divisors of n are bounded by B), we can write it by $(g^n \mod p) = 2^{e_n^2} 3^{e_n^3} 5^{e_n^5} \cdots q^{e_n^q}$. We can compute e_n^l by division. Hence, we get a system of linear equations:

$$e_n^2 \log_g 2 + e_n^3 \log_g 3 + \cdots + e_n^q \log_g q = n \text{ for } n \text{ where } (g^n \mod p) \text{ is } B\text{-smooth},$$

where $\log_g$ is the discrete logarithm in $\mathbb{F}_p^\times$.

We can solve $\log_g 2, \log_g 3, \cdots \log_g q$ from this system of linear equations as long as we have enough equations.

3. For $k = 1, 2, \cdots$, compute $(g^k b \mod p)$ and test that whether it is B-smooth. If it is, write it as

$$g^k b \equiv 2^{f_2} 3^{f_3} 5^{f_5} \cdots q^{f_q} \mod p.$$

Hence, we have

$$k + \log_g b = f_2 \log_g 2 + f_3 \log_g 3 + \cdots f_q \log_g g.$$

We can compute $\log_g b$ from this formula.

Assuming an optimal selection of the smooth bound B, the expected running time of the index-calculus algorithm is $exp(c(\log p)^{\frac{1}{2}}(\log\log p)^{\frac{1}{2}})$ for some positive constant c.

3.2 Number field sieve

The nmber field sieve is proposed for factoring integers originally (See, for example, [Buhler 1993], [Lenstra-Lenstra 1993]), and transplanted for the discrete logarithm problem (See, for example, [Gordon 1993] [Schirokauer 1993] [Schirokauer 2008]).

Given a big prime p_0, a big odd prime divisor l of $p_0 - 1$, a positive integer g such that $g \mod p$ is a generator of $\mathbb{F}_{p_0}^\times$ and a positive integer v, we describe the general number field sieve to compute $\log_t v \mod l$.

1. Let d be the minimal integer that is greater than $3^{\frac{1}{3}}(\log p_0)^{\frac{1}{3}}(\log\log p_0)^{-\frac{1}{3}}$. Take $u = O(exp((\frac{9}{8})^{\frac{1}{3}}(\log p_0)^{\frac{1}{3}}(\log\log p_0)^{\frac{2}{3}})$ and $y = O(exp((\frac{9}{8})^{\frac{1}{3}}(\log p_0)^{\frac{1}{3}}(\log\log p_0)^{\frac{2}{3}})$.

2. Let m be the maximal integer that is less than $p_0^{\frac{1}{d}}$. We then write p_0 by m-adic represent:

$$p_0 = m^d + a_1 m^{d-1} + \cdots + a_d,$$

where $a_i = 0, 1, \cdots, m-1$.

3. Let $f(x) := x^d + a_1 x^{d-1} + \cdots + a_d$, and $K := \mathbb{Q}[x]/(f(x))$, then $(p_0, x-m)$ is a point in $Spec\frac{Z[x]}{f(x)}$. We assume that the discriminant of f is not divided by l.

4. Let $T := \{(a,b) \in \mathbb{Z} \times \mathbb{Z}; |a| \leq u, 0 < b \leq u, a - bm$ and $Nm(a-bx)$ is y-smooth $\}$.

5. Let B be the set of the prime ideals of $\mathbb{Z}$ which correspond to prime numbers bounded by y. Let B' be the set of the closed points in $Spec\mathcal{O}_K$ which are over the points in B.

6. The assumption that the discriminant of f is not divided by l implies that $Spec\mathbb{Z}[x]/(f(x))$ and $\mathcal{O}_K$ are unramified at l. Therefore, we have

$$\mathcal{O}_K \otimes \mathbb{Z}/l\mathbb{Z} = \mathbb{F}_{l^{t_1}} \oplus \cdots \oplus \mathbb{F}_{l^{t_k}},$$

where $t_1, \cdots, t_k$ are positive integers. Let t be the least common multiple of $t_1, \cdots, t_k$. Let $\epsilon := \gamma^t - 1$ and $\Gamma := \{\gamma \in \mathcal{O}_K; Nm(\gamma) \not\equiv 0 \mod l\}$, we then have the following commutative diagram:

$$\begin{array}{ccccc}
\otimes_{i=1}^k \mathbb{W}(\mathbb{F}_{l^{t_i}}) & \xrightarrow{\hat{\epsilon}} & \oplus_{i=1}^k U^{(1)}(\mathbb{F}_{l^{t_i}}) & \xrightarrow{-1} & \oplus_{i=1}^k l\mathbb{W}(\mathbb{F}_{l^{t_i}})/l^2\mathbb{W}(\mathbb{F}_{l^{t_i}}) \\
\sim\uparrow & & & & \sim\uparrow \\
(\mathcal{O}_K \otimes \mathbb{Z}_l) & & & & l\mathcal{O}_K/l^2\mathcal{O}_K \\
\uparrow & & & & \sim\uparrow \\
\Gamma & & \xrightarrow{\lambda} & & l\frac{\mathbb{Z}[x]}{f(x)}/l^2\frac{\mathbb{Z}[x]}{f(x)}
\end{array}$$

For any $\gamma \in \Gamma$, the image of γ under the homomorphism λ can be written as $l(\lambda_0(\gamma) + \lambda_1(\gamma)x + \cdots + \lambda_{d-1}x^{d-1})$, where $\lambda_0(\gamma), \cdots, \lambda_{d-1}(\gamma) \in \mathbb{F}_l$. Therefore, we get the homomorphisms

$$\begin{array}{rccll}
\lambda_i: & \Gamma & \longrightarrow & \mathbb{F}_l & \\
 & \gamma & \mapsto & \lambda_i(\gamma) & i = 0.1, \cdots, d-1
\end{array}$$

7. If g and v are y-smooth, consider the map:

$$\begin{array}{ccccc}
T \cup \{g, v\} & \longrightarrow & \mathbb{F}_l^{\sharp B} \oplus & \mathbb{F}_l^{\sharp B'} \oplus & \mathbb{F}_l^d \\
(a,b) \in T & \mapsto & \{v_p(a-bm)\}_{p \in B}, & \{v_\beta(a-bx)\}_{\beta \in B'}, & \{\lambda_i(a-bx)\}_{i=0}^{d-1}, \\
g & \mapsto & \{v_p(g)\}_{p \in B}, & 0, & 0, \\
v & \mapsto & \{v_p(v)\}_{p \in B}, & 0, & 0,
\end{array}$$

Increase the smoothness bound y if necessary, there exist integers $k_{a,b}$ (for $(a,b) \in T$) and k_g such that

$$\begin{array}{lll}
\sum_{(a,b)\in T} k_{(a,b)} v_p(a-bm) + k_g v_p(g) + v_p(v) \equiv 0 \mod l & \text{for } p \in B, \\
\sum_{(a,b)\in T} k_{(a,b)} b_\beta(a-bx) \equiv 0 \mod l & \text{for } \beta \in B', \\
\sum_{(a,b)\in T} k_{(a,b)} \lambda_i(a-bx) \equiv 0 \mod l & \text{for } i = 0, 1, \cdots, d-1.
\end{array}$$

We solve $k_{(a,b)}$ for $(a,b) \in T$ and k_g from this system of linear equations. Then we have $\log_g v \equiv -k_g \mod l$ with probability greater than $1 - 2l^{-2}$.

7'. If g is y-smooth but v is not y-smooth, we take a y-smooth element $v' \in \mathbb{Z}[x]/(f(x))$

such that $v' \equiv v \mod (p, x-m)$. Consider the map:

$$\begin{array}{ccccc} T \cup \{g, v\} & \longrightarrow & \mathbb{F}_l^{\sharp B} \oplus & \mathbb{F}_l^{\sharp B'} \oplus & \mathbb{F}_l^d \\ (a,b) \in T & \mapsto & \{v_p(a-bm)\}_{p \in B}, & \{v_\beta(a-bx)\}_{\beta \in B'}, & \{\lambda_i(a-bx)\}_{i=0}^{d-1}, \\ g & \mapsto & \{v_p(g)\}_{p \in B}, & 0, & 0, \\ v' & \mapsto & 0, & \{v_\beta(v')\}_{\beta \in B'}, & \{\lambda_i(v')\}_{i=0}^{d-1}. \end{array}$$

Increase the smoothness bound y if necessary, there exist integers $k_{a,b}$ (for $(a,b) \in T$) and k_g such that

$$\begin{array}{lll} \sum_{(a,b)\in T} k_{(a,b)} v_p(a-bm) + k_g v_p(g) & \equiv 0 \mod l & \text{for } p \in B, \\ \sum_{(a,b)\in T} k_{(a,b)} b_\beta(a-bx) + v_\beta(v') & \equiv 0 \mod l & \text{for } \beta \in B', \\ \sum_{(a,b)\in T} k_{(a,b)} \lambda_i(a-bx) + \lambda_i(v') & \equiv 0 \mod l & \text{for } i = 0, 1, \cdots, d-1. \end{array}$$

We solve $k_{(a,b)}$ for $(a,b) \in T$ and k_g from this system of linear equations. Then we have $\log_g v \equiv k_g \mod l$ with probability greater than $1 - 2l^{-2}$.

$7''$. If v is y-smooth but g is not y-smooth, we take a y-smooth element $g' \in \mathbb{Z}[x]/(f(x))$ such that $g' \equiv g \mod (p, x-m)$. Consider the map:

$$\begin{array}{ccccc} T \cup \{g, v\} & \longrightarrow & \mathbb{F}_l^{\sharp B} \oplus & \mathbb{F}_l^{\sharp B'} \oplus & \mathbb{F}_l^d \\ (a,b) \in T & \mapsto & \{v_p(a-bm)\}_{p \in B}, & \{v_\beta(a-bx)\}_{\beta \in B'}, & \{\lambda_i(a-bx)\}_{i=0}^{d-1}, \\ g' & \mapsto & 0, & \{v_\beta(g')\}_{\beta \in B'}, & \{\lambda_i(g')\}_{i=0}^{d-1}, \\ v & \mapsto & \{v_p(v)\}_{p \in B}, & 0, & 0. \end{array}$$

Increase the smoothness bound y if necessary, there exist integers $k_{a,b}$ (for $(a,b) \in T$) and k_g such that

$$\begin{array}{lll} \sum_{(a,b)\in T} k_{(a,b)} v_p(a-bm) + v_p(v) & \equiv 0 \mod l & \text{for } p \in B, \\ \sum_{(a,b)\in T} k_{(a,b)} b_\beta(a-bx) + k_g v_\beta(g') & \equiv 0 \mod l & \text{for } \beta \in B', \\ \sum_{(a,b)\in T} k_{(a,b)} \lambda_i(a-bx) + \lambda_i(g') & \equiv 0 \mod l & \text{for } i = 0, 1, \cdots, d-1. \end{array}$$

We solve $k_{(a,b)}$ for $(a,b) \in T$ and k_g from this system of linear equations. Then we have $\log_g v \equiv k_g \mod l$ with probability greater than $1 - 2l^{-2}$.

$7'''$. If both g and v are not y-smooth, we take a y-smooth element $g' \in \mathbb{Z}[x]/(f(x))$ such that $g' \equiv g \mod (p, x-m)$ and an y-smooth element $v' \in \mathbb{Z}[x]/(f(x))$ such that $v' \equiv v \mod (p, x-m)$. Consider the map:

$$\begin{array}{ccccc} T \cup \{g, v\} & \longrightarrow & \mathbb{F}_l^{\sharp B} \oplus & \mathbb{F}_l^{\sharp B'} \oplus & \mathbb{F}_l^d \\ (a,b) \in T & \mapsto & \{v_p(a-bm)\}_{p \in B}, & \{v_\beta(a-bx)\}_{\beta \in B'}, & \{\lambda_i(a-bx)\}_{i=0}^{d-1}, \\ g' & \mapsto & 0 & \{v_\beta(g')\}_{\beta \in B'}, & \{\lambda_i(g')\}_{i=0}^{d-1}, \\ v' & \mapsto & 0 & \{v_\beta(v')\}_{\beta \in B'}, & \{\lambda_i(v')\}_{i=0}^{d-1}. \end{array}$$

Increase the smoothness bound y if necessary, there exist integers $k_{a,b}$ (for $(a,b) \in T$) and k_g such that

$$\begin{array}{lll} \sum_{(a,b)\in T} k_{(a,b)} v_p(a-bm) & \equiv 0 \mod l & \text{for } p \in B, \\ \sum_{(a,b)\in T} k_{(a,b)} b_\beta(a-bx) + k_g v_\beta(g') + v_\beta(v') & \equiv 0 \mod l & \text{for } \beta \in B', \\ \sum_{(a,b)\in T} k_{(a,b)} \lambda_i(a-bx) + k_g \lambda_i(g') + \lambda_i(v') & \equiv 0 \mod l & \text{for } i = 0, 1, \cdots, d-1. \end{array}$$

We solve $k_{(a,b)}$ for $(a,b) \in T$ and k_g from this system of linear equations. Then we have $\log_g v \equiv -k_g \mod l$ with probability greater than $1 - 2l^{-2}$.

Proof. We give the proof of step 7 only. The proof of step $7', 7''$ and $7'''$ is similar. By the algorithm, we have

$$f'(m)^l \prod_{(a,b)\in T} (a-bm)^{k_{a,b}} g^{k_g} v \in (\mathbb{Z}\setminus 0)^l \longrightarrow \mathbb{F}_p^{\times l} \mod p.$$

The proposition 3.1 below shows that we have

$$f'(x)^l \prod_{(a,b)\in T} (a-bx)^{k_{a,b}} \in (\frac{\mathbb{Z}[x]}{f(x)})^l$$

with probability greater than $1-2l^{-2}$. We have $x \equiv m \mod (p, x-m)$. Therefore, we have

$$f'(m)^l \prod_{(a,b)\in T} (a-bm)^{k_{a,b}} \in \mathbb{F}_p^{\times l}$$

with probability greater than $1-2l^{-2}$. Hence, we have $g^{k_g} v \in \mathbb{F}_p^{\times l}$, and $\log_g v \equiv -k_g \mod l$ with probability greater than $1-2l^{-2}$.

Proposition 3.1. *Assume that the class number is not divided by l and g, v are y-smooth. Then:*

1. $\prod_{(a,b)\in T}(a-bm)^{k_{(a,b)}} t^{k_t} v \in (\mathbb{Z}\setminus 0)^l$.

2. $\prod_{(a,b)\in T}(a-bx)^{k_{a,b}} \in (\mathcal{O}_K \setminus 0)^l$ *and* $f'(x)^l \prod_{(a,b)\in T}(a-bx)^{k_{a,b}} \in (\frac{\mathbb{Z}[x]}{f(x)})^l$ *with probability greater than* $1-2l^{-2}$.

Proof.

1. Clearly.

2. We have $v_\beta(\prod_{(a,b)\in T}(a-bx)^{k_{a,b}}) \equiv 0 \mod l$ for any $\beta \in Spec\mathcal{O}_K$. Hence $(\prod_{(a,b)\in T}(a-bx)^{k_{a,b}}) = I^l$ for some ideal I of $\mathcal{O}_K$. The assumption that the class number of K is not divided by l implies that

$$I = h\mathcal{O}_K \quad \text{for some } h \in \mathcal{O}_K.$$

Therefore,

$$\prod_{(a,b)\in T} (a-bx)^{k_{a,b}} = h^l \mu \quad \text{for some } \mu \in \mathcal{O}_K^\times.$$

We will show that μ is in $\mathcal{O}_K^{\times l}$ with probability greater than $1-2l^{-2}$:

The fact that $\sum_{(a,b)\in T} k_{a,b}\lambda_i(a-bx) \equiv 0 \mod l$ implies that

$$\lambda(\prod_{(a,b)\in T} (a-bx)^{k_{a,b}}) = 0.$$

We have also $\lambda(g^l) = 0$. Hence $\lambda(\mu) = 0$. It means that

$$\lambda_0(\mu) = \cdots = \lambda_{d-1}(\mu) = 0.$$

Regard $\lambda_0, \lambda_1, \cdots \lambda_{d-1}$ as linear maps from $\mathcal{O}_K^\times/\mathcal{O}_K^{\times l}$ to $\mathbb{F}_l$. The Dirichlet's unit theorem implies that $\dim_{\mathbb{F}_l}(\mathcal{O}_K^\times/\mathcal{O}_K^{\times l}) \leq d-1$. Hence $\dim_{\mathbb{F}_l} Hom(\mathcal{O}_K^\times/\mathcal{O}_K^{\times l}, \mathbb{F}_l) \leq d-1$. The lemma

3.2 below shows that $\lambda_0, \lambda_1, \cdots, \lambda_{d-1}$ generate $Hom_{\mathbb{F}_l}(\mathcal{O}_K^\times/\mathcal{O}_K^{\times l}, \mathbb{F}_l)$ with probability greater than $1-2l^{-2}$. Therefore, $\mu \in \mathcal{O}_K^{\times l}$ with probability greater than $1-2l^{-2}$. Therefore,

$$\prod_{(a,b)\in T}(a-bx)^{k_{a,b}} \in (\mathcal{O}_K \setminus 0)^l \quad \text{and} \quad f'(x)^l \prod_{(a,b)\in T}(a-bx)^{k_{a,b}} \in (\frac{\mathbb{Z}[x]}{(f(x))} \setminus 0)^l$$

with probability greater $1-2l^{-2}$. ■

Lemma 3.2. *Let k and r be two positive integers. Let V be a linear space of dimension k over $\mathbb{F}_l$. Take $v_1, v_2, \cdots, v_{k+r}$ from V random and independent, then the probability that $v_1, v_2, \cdots, v_{k+r}$ generate V is greater than $1-2l^{-r-1}$.*

■

Remark 3.3. For the computation of the valuation $v_\beta(a-bx)$, there are two cases:

1. For prime number $p \in \mathbb{Z}$, if all the points in $\mathbb{Z}[x]/(f(x))$ over p are regular, the points in $Spec\mathcal{O}_K$ over p are same as the points in $Spec\mathbb{Z}[x]/(f(x))$ over p. Therefore, every point in them is represented by the term $(p, r(x))$, where $r(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$ which is a decomposition term of $f(x) \mod p$. For any $a-bx \in \mathbb{Z}[x]/(f(x))$, there is at most one point β over p such that the valuation $v_\beta(a-bx)$ is positive. Hence, we can compute it by $v_p(Nm(a-bx))$.

2. For prime number $p \in \mathbb{Z}$, if there exists a point in $Spec\mathbb{Z}[x]/(f(x))$ over p which is non-regular, we have to resolve the singularity to get the points in $Spec\mathcal{O}_K$ over p. In this case, we have to use more complex representation.

We represent an order in K, or an ideal of an order in K by basis of the form $a_{0,0}, a_{1,0}+a_{1,1}x, \cdots, a_{d-1,0}+\cdots+a_{d-1,d-1}x^{d-1}$ ($a_{i,j} \in \mathbb{Q}$) as a $\mathbb{Z}$-module. Given an order $\mathcal{O}$ in K and a prime number p, let $I_p := \cap_{\beta \in Spec\mathcal{O}, p\in\beta}\beta = \Pi_{\beta\in Spec\mathcal{O},p\in\beta}\beta$ be the p-radical of $\mathcal{O}$. The following proposition tells us how to compute I_p:

Proposition 3.4. *With the notation as above, then*

1. *$I_p/p\mathcal{O}$ is the nilradical of $\mathcal{O}/p\mathcal{O}$.*
2. *If k is a positive integer such that $p^k \geq dim_{\mathbb{F}_p}(\mathcal{O}/p\mathcal{O})$, then*

$$\frac{I_p}{p\mathcal{O}} = \ker(Fr_p^k : \frac{\mathcal{O}}{p\mathcal{O}} \longrightarrow \frac{\mathcal{O}}{p\mathcal{O}})$$

■

Define $O_p := \{h \in \mathcal{O}_K; p^k h \in \mathbb{Z}[x]/(f(x)) \text{ for some } k \in \mathbb{N}\}$, then we have $O_p \otimes \mathbb{Z}_{(p)} = \mathcal{O}_K \otimes \mathbb{Z}_{(p)}$, where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at the prime ideal (p). To compute O_p, we use the following theorem:

Theorem 3.5. *Let $\mathcal{O}$ be an order in a number field K and let p be a prime number. Set*

$$\mathcal{O}' = \{h \in K; hI_p \subset I_p\}$$

Then either $\mathcal{O}' = \mathcal{O}$, in which case all the points in $\mathcal{O}$ over p are regular, or $\mathcal{O} \subsetneq \mathcal{O}' \subset \mathcal{O}_K$ and $p \mid [\mathcal{O}' : \mathcal{O}] \mid p^d$, where d is the degree of the extension $K/\mathbb{Q}$.

Proof See [Cohen 1993], Theorem 6.1.3. ■

Clearly, we have $\mathcal{O}' \subset \frac{1}{p}\mathcal{O}$. Hence, we only need to compute the subspace $\mathcal{O}'/\mathcal{O}$ of the $\mathbb{F}_p$-linear space $\frac{1}{p}\mathcal{O}/\mathcal{O}$. In fact, we have the following proposition:

Proposition 3.6. *With the above notation, we have*

$$\mathcal{O}'/\mathcal{O} = \ker(\frac{1}{p}\mathcal{O}/\mathcal{O} \longrightarrow Hom(I_p/pI_p, \frac{1}{p}I_p/I_p)).$$

■

Using this proposition, we can compute $\mathcal{O}'$ by linear algebra over $\mathbb{F}_p$.

We call the process that compute $\mathcal{O}'$ from $\mathcal{O}$ "solve singularity of O at p".

Using the Theorem 3.5, we can compute O_p from $\mathbb{Z}[x]/(f(x))$ iteratively. To be specific, we solve the singularity of $\mathcal{O} = \mathbb{Z}[x]/(f(x))$ at p to get $\mathcal{O}'$, then we solve the singularity of $\mathcal{O}'$ at p to get $\mathcal{O}''$, and repeat this process until we get a ring $\mathcal{O}^\sim$ satisfying that the solving singularity of $\mathcal{O}^\sim$ at p is itself. By Theorem 3.5, we have $O_p = \mathcal{O}^\sim$.

After computing $\mathcal{O}_p$, we can compute the decomposition of (p) in $\mathcal{O}_K$ in the same way as the decomposition of (p) in O_p. For the algorithm, we refer to [Cohen 1993] section 6.2.2 - section 6.2.5.

We then compute the valuation $v_\beta(h)$ for a given $\beta \in Spec\mathcal{O}_p$ over p and a $h \in K$ through the following proposition:

Proposition 3.7. *Let $\mathcal{O}$ be an order in K, β be an invertible prime ideal of $\mathcal{O}$ and a be an element in $\beta \setminus \mathcal{O}$. Then we have:*

For any $h \in \mathcal{O}$, $v_\beta(h)$ is the largest integer v such that $a^v h \in \mathcal{O}$.

Proof. It is similar to [Cohen 1993], Lemma 4.8.16. ■

To compute the valuation $v_\beta(h)$, we take an element $a \in \beta^{-1} \setminus \mathcal{O}$ by

$$p\beta^{-1}/p\mathcal{O} = \ker(\mathcal{O}/p\mathcal{O} \longrightarrow End(\beta/p\mathcal{O})).$$

Then we can compute the valuation by Proposition 3.7.

If we make the assumption that for $-u \leq a \leq u, 0 < b \leq u$, $(a - bm)Nm(a - bx)$ is random and has a uniform distribution in $[0, 2du^{d+1}p^{\frac{2}{d}}]$, the running time of number theory sieve is $exp((\frac{64}{9} + o(1))(\log p)^{\frac{1}{3}}(\log\log p)^{\frac{2}{3}})$.

3.3 Function field sieve

The function field sieve is proposed in [Adleman 1994]. We describe a modification of a simpler and improved version which is presented in [Adleman and Huang 1999].

Let p be a small prime number, $B \geq 1$ be a real number. A polynomial in $\mathbb{F}_p$ is said to be B-smooth if its every irreducible divisor has degree at most B. Let $g(x)$ be a polynomial in $\mathbb{F}_p[x]$ of minimal degree such that $f(x) := x^n + g(x)$ is irreducible. Let $q = p^n$ and $r := \frac{q-1}{p-1}$. we use $\mathbb{F}[x]/(f(x))$ as a model of $\mathbb{F}_q$. Given two elements $t, u \in \mathbb{F}_q^\times$ satisfying $u \in \langle t \rangle$ represented by two B-smooth elements $t(x), u(x) \in \mathbb{F}_q[x]$ respectively, and two integral parameters $C \geq 0$ and $d \geq 1$, we describe the function field sieve to compute $\log_t u$.

Let $k := d \times \lceil \frac{n}{d} \rceil$, where $\lceil x \rceil$ means the minimal integer that not less than x. We have $n \leq k < n + d$ and

$$x^{k-n}f(x) = x^k + x^{k-n}g(x) = m(x)^d + x^{k-n}g(x)$$

where $m(x) = x^{\lceil \frac{n}{d} \rceil}$. Let $H(x,y) = y^d + x^{k-n}g(x) \in \mathbb{F}_q[x,y]$. Let $X := Spec\mathbb{F}_p[x]$ and Y be the complete regular curve defined by $H(x,y) = 0$. There is a point $P = (f(x), y - m(x))$ with residue field $\mathbb{F}_q$ in Y. Let K be the rational function field of Y, and $\mathcal{O}_K$ be the integral closure of $\mathbb{F}_p[x]$ in K. We assume that the class number of K is co-prime to r.

Let

$$M_X := \{A \in X; [\mathbb{F}_p(A) : \mathbb{F}_p] \leq B\}$$
$$M_Y := \{Q \in Y; Q \text{ is over a point in } M_X\}$$

An element $h \in \mathcal{O}_K$ is called B-smooth, if its norm is B-smooth. Let

$$S := \{(a(x), b(x)) \in \mathbb{F}_p[x] \oplus \mathbb{F}_p[x]; (a(x), b(x)) = 1, \deg a(x) \leq C, \deg b(x) \leq C, \\ a(x) - b(x)m(x) \text{ and } a(x) - b(x)y \text{ are } B\text{-smooth}\}.$$

We consider the map

$$\begin{array}{ccccc} S \cup \{u(x), v(x)\} & \longrightarrow & (\mathbb{Z}/r\mathbb{Z})^{\sharp M_X} & \oplus & (\mathbb{Z}/r\mathbb{Z})^{\sharp M_Y} \\ (a(x), b(x)) \in S & \mapsto & \{v_A(a(x) - b(x)m(x)) \mod r\}_A, & & \{v_Q(a(x) - b(x)y) \mod r\}_Q, \\ u(x) & \mapsto & \{v_A(u(x)) \mod r\}_A, & & \{0\}_Q, \\ t(x) & \mapsto & \{v_A(t(x)) \mod r\}_A, & & \{0\}_Q, \end{array}$$

Increase the smooth bound B if necessary, there are non-negative integers $\{k_{a,b}\}_{(a,b)\in S}$ and k_t such that

$$\begin{array}{lll} \sum_{(a,b)\in S} k_{a,b} v_A(a(x) - b(x)m(x)) + v_A(u(x)) + k_t v_A(t(x)) & \equiv 0 \mod r & \text{for } A \in M_x, \\ \sum_{a,b\in S} k_{a,b} v_Q(a(x) - b(x)y) & \equiv 0 \mod r & \text{for } Q \in M_Y. \end{array}$$

Solve $\{k_{a,b}\}_{(a,b)\in S}$ and k_u from this system of linear equations. Then

$$\prod_{(a,b)\in S}(a(x) - b(x)m(x))^k_{a,b} u t^{k_t} \in (\mathbb{F}_p[x] \setminus 0)^r,$$
$$(\prod_{(a,b)\in S}(a(x) - b(x)y)^{k_{(a,b)}}) = I^r \text{ for some ideal } I \text{ of } \mathcal{O}_K.$$

There is a $g \in \mathcal{O}_K$ such that $I = (g)$, because the class number of K is co-prime to r. Hence there is a $\mu \in \mathcal{O}_K^\times = \mathbb{F}_p^\times$ such that

$$\prod_{(a,b)\in S} (a(x) - b(x)y)^{k_{a,b}} = g^r \mu.$$

Module $(f(x), y - m(x))$, we have

$$\prod_{(a,b)\in S} (a(x) - b(x)m(x))^{k_{a,b}} = \bar{g}^r \mu$$

Notice that $\bar{g}^r \in \mathbb{F}_q^{\times r} = \mathbb{F}_p^\times$ and $\mu \in \mathbb{F}_p^\times$. Hence we have

$$\prod_{(a,b)\in S} (a(x) - b(x)m(x))^{k_{a,b}} \in \mathbb{F}_p^\times.$$

We also have

$$(\prod_{(a,b)\in S} (a(x) - b(x)m(x))^{k_{a,b}} u t^{k_t} \mod (f(x))) \in (\frac{\mathbb{F}_p[x]}{f(x)})^{\times r} = \mathbb{F}_q^{\times r} = \mathbb{F}_p^\times$$

Therefore, we have

$$u t^{k_t} \in \mathbb{F}_q^\times.$$

Let $t' := t^r$ and $\eta = ut^{k_t}$. Solve the discrete logarithm problem $t'^e = \eta$ in $\mathbb{F}_p^\times$ and get e. Science $ut^{k_t} = t^{re}$, we can compute

$$log_t u = re - k_t.$$

If we make the assumption that for $\deg a(x) \leq C$ and $\deg b(x) \leq C$, $(a(x)-b(x)m(x))Nm(a(x)-b(x)y)$ is random and has a uniform distribution in $\{h(x) \in \mathbb{F}_p[x]; \deg h \leq d+k+c+n-1\}$, and $n \leq (\log q/\log\log q)^e$ for $q \to \infty$, the running time of function field sieve is $exp(O(1)(\log q)^{\max\{\frac{1}{3},1-e\}}(\log\log p)^{\min\{\frac{2}{3},e\}})$.

4 Ramification signature for prime fields

In [Huang-Raskind 2009], the authors lifted the discrete logarithm problem in $\mathbb{F}_p^\times$ to a real quadratic field. They defined the "ramification signature" for the real quadratic field and proved that the discrete logarithm problem in $\mathbb{F}_p^\times$ is random polynomial time equivalent to computing the ramification signature of the real quadric field under two heuristic assumptions, namely, an assumption on the class number and an assumption on a global unit of the real quadratic field. Let us recall this work.

4.1 Definition

Let p, l be two prime integers with $p \equiv 1(\mod l)$ and $l > 2$. Let K be a real quadratic field where p and l split. Let α be a global unit of K. For any place u of K let P_u denote the prime ideal corresponding to u. For any finite set S of places of K, let G_S denote the Galois group of a maximal extension of K that is unramified outside of S.

Proposition 4.1. *Let S be the set consisting of one place u over l, one place v over p, and both archimedean places. Suppose that*

(1) $l \nmid h_K$ where h_K is the class number of K;

(2) $\alpha^{l-1} \not\equiv 1(\mod P_\omega^2)$ for all places $\omega \mid l$;

(3) $\alpha^{\frac{p-1}{l}} \not\equiv 1(\mod P_v)$.

Then the $\mathbb{F}_l$-dimension of $H^1(G_S, \mathbb{Z}/l\mathbb{Z})$ is one. If χ is any nonzero element of this group, then χ is ramified at u and v.

Proof. See [Huang-Raskind 2009], section4.2, proposition 2. ∎

Remark 4.2. If χ is any nonzero element of $H^1(G_S, \mathbb{Z}/l\mathbb{Z})$, it satisfies

$$\langle \chi_u, \alpha_u \rangle + \langle \chi_v, \alpha_v \rangle = 0 \qquad (A)$$

Denote the integral ring $\mathcal{O}_K$ in K by A_K, its completion at u by A_u, its completion at v by A_v. Through the natural isomorphism $A_u^\times/A_u^{\times l} \cong (\mathbb{Z}/l^2\mathbb{Z})^\times/(\mathbb{Z}/l^2\mathbb{Z})^{\times l}$, $A_u^\times/A_u^{\times l}$ is generated by $1+l$. For any generator g of $\mathbb{F}_p^\times/\mathbb{F}_p^{\times l}$, it is regarded as a generator of $A_v^\times/A_v^{\times l}$ through the natural isomorphism $A_v^\times/A_v^{\times l} \cong k(v)^\times/k(v)^{\times l}$. Clearly, $\langle 1+l, \chi_u \rangle^{-1}\langle g, \chi_v \rangle$ is independent of the choice of $\chi \neq 0 \in Hom(\pi_1(U), \mathbb{Z}/l\mathbb{Z})$. This term is called the **ramification signature** , with respect to $1+l$ and g, of the cyclic extension of degree l over K which is ramified at u, v and unramified elsewhere.

4.2 Reduction from signature computation problem to discrete logarithm problem

Suppose given p, l, $K = \mathbb{Q}(\sqrt{D})$, U, u, v, α, g, as in Proposition 4.1. Then the computation of the ramification signature, with respect to $1+l$ and g, of the cyclic extension of degree l over K which is ramified at u, v and unramified elsewhere can be reduced to a discrete logarithm problem in $\mathbb{F}_p^\times$ as follows:

Let us consider the following commutative diagram:

$$\begin{array}{ccccccc} A_K^\times & \longrightarrow & A_u^\times & \xrightarrow{\sim} & \mathbb{Z}_l^\times & \longrightarrow & \mathbb{Z}_l^\times/\mathbb{Z}_l^{\times l} \\ & & & & \downarrow & & \downarrow \\ & & & & (\mathbb{Z}/l^2\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/l^2\mathbb{Z})^\times/(\mathbb{Z}/l^2\mathbb{Z})^{\times l}. \end{array}$$

If the image in $(\mathbb{Z}/l^2\mathbb{Z})^\times$ of α equals $\xi(1+l)^y$, where ξ is an $(l-1)$-st root of unity, then its image in $(\mathbb{Z}/l^2\mathbb{Z})^\times/(\mathbb{Z}/l^2\mathbb{Z})^{\times l}$ will be equal to $(1+l)^y$. We can easily compute ξ, y and consequently the first term in (A) $\langle \alpha_u, \chi \rangle = y\langle 1+l, \chi \rangle$.

For the second term in (A), if the image of α under the morphism $A_K^\times \longrightarrow A_v^\times/A_v^{\times l} \cong \mathbb{F}_p^\times/\mathbb{F}_p^{\times l}$ is $a = g^m$, then $\langle \alpha_v, \chi_v \rangle = m\langle g, \chi_v \rangle$.

Therefore, if one can compute m from $a = g^m$, then one can compute

$$\langle 1+l, \chi_u \rangle^{-1} \langle g, \chi_v \rangle = -m^{-1}y \quad \in \mathbb{Z}/l\mathbb{Z}.$$

4.3 Reduction from discrete logarithm problem in prime fields to signature computation problem

Let g be a generator of $\mathbb{F}_p^\times$, $a \in \mathbb{F}_p^\times$ and l be a prime dividing $p-1$. We show the computation of discrete logarithm $\log_g a \mod l$ can then be reduced to computing the ramification signature of a real quadratic field as follows.

If $a^{\frac{p-1}{l}} = 1$, then $m \equiv 0 \pmod{l}$. Thus suppose $a^{\frac{p-1}{l}} \neq 1$. We will lift a to some unit α of a real quadratic field K such that $\alpha \equiv a \mod v$ for some place v of K over p, $\alpha^{l-1} \neq 1 \mod I_u^2$, and $\alpha^{l-1} \neq 1 \mod I_{u'}^2$ for the two places u and u' of K over l. We do it as follows:

1. Compute $b \in \mathbb{F}_p^\times$ such that $ab = 1$ in $\mathbb{F}_p^\times$.

2. Put $c := \frac{a+b}{2}$, $d := \frac{a-b}{2}$. Note that $c^2 - d^2 = 1$ and $a = c + d$. We can assume $d \neq 0$; otherwise, $a^2 = 1$ and $m = \frac{p-1}{2}$ or $p-1$.

3. Lift d to an integer. We have $(\frac{1+d^2}{p}) = (\frac{c^2}{p}) = 1$. We choose $k \in \{0, 1, ..., l-1\}$ randomly until $(\frac{(d+kp)^2+1}{l}) = 1$. Let $x = d + kp$.

4. Let $K := \mathbb{Q}(\sqrt{x^2+1})$, $v = (p, \sqrt{x^2+1} - c)$, $v' = (p, \sqrt{x^2+1} + c)$, u be any point of $Spec A_K$ over l.

5. Let $\alpha := x + \sqrt{x^2+1}$. Thus, $\alpha \equiv d + c \equiv \tilde{a} \mod v$, $\alpha \equiv d - c \equiv -\tilde{b} \mod v'$. Note that $Nm(\alpha) = 1$, so α is a unit of K.

Let $U := Spec A_K \setminus \{u, v\}$. We assume that it is likely for K to satisfy the condition in Proposition 4.1. Then $\langle \alpha_u, \chi \rangle + \langle \alpha_v, \chi \rangle = 0$, for any $\chi \neq 0 \in Hom(\pi_1(U), \mathbb{Z}/l\mathbb{Z})$. Let $(1+l)^y$ be the image of α under the morphism

$$A_K^\times \longrightarrow A_u^\times \cong \mathbb{Z}_l^\times \longrightarrow (\mathbb{Z}/l^2\mathbb{Z})^\times/(\mathbb{Z}/l^2\mathbb{Z})^{\times l}.$$

For the first term in (A), we have $\langle \alpha_u, \chi \rangle = y\langle 1+l, \chi \rangle$. For the second term in (A), we have $\langle \alpha_v, \chi \rangle = m\langle \tilde{g}, \chi \rangle$. Hence we obtain

$$y\langle 1+l, \chi \rangle + m\langle \tilde{g}, \chi \rangle = 0.$$

Therefore, if we can compute the ramification signature $\langle \chi, 1+l \rangle^{-1} \langle \chi, g \rangle$ of U with respect to g, then we can compute $m = -y\langle \chi, 1+l \rangle^{-1} \langle \chi, g \rangle$.

Therefore, we conclude that the discrete logarithm problems in $\mathbb{F}_p^\times$ are random polynomial time equivalent to some signature computation problem with the assumptions (1), (2), and (3) in proposition 4.1.

5 Main result

In this section, we generalize the proposition 2 in section 4.1 in [Huang-Raskind 2009] (proposition 4.1 in previous section), where they considered the case where "p and l split". We consider the more general case where "p is unramified and l splits" here.

We then generalize the definition of "ramification signature" of a real quadratic field to the situation "p is unramified and l splits". The definition in [Huang-Raskind 2009] is the specialization of our definition in the situation "p and l split".

We then lift the discrete logarithm problem in $k^\times$ (for $k = \mathbb{F}_p$ or $\mathbb{F}_{p^2}$) to a real quadratic field and prove that the discrete logarithm problem in $k^\times$ is random polynomial time equivalent to computing the ramification signature of the real quadratic field with one heuristic assumption on the class number. We also show that in the proof of the equivalence in [Huang-Raskind 2009] one can remove the assumption on the global unit. More precisely, we give an improvement (Step 4 in section 5.3 below) on the construction of real quadratic field and global unit that makes the condition (2), (3) in proposition 2 in section 4.1 in [Huang-Raskind 2009] be satisfied automatically.

In subsection 1, we redefine the ramification signature for a real quadratic field. In subsection 2, we prove the reduction from the computation of a ramification signature of a real quadratic field to the discrete logarithm problem. In subsection 3, we prove the reduction from the discrete logarithm problem in prime field to the computation of a ramification signature of a real quadratic field. In subsection 4, we prove the reduction from the discrete logarithm problem in finite fields of order square of prime number to the computation of a ramification signature of a real quadratic field.

5.1 Definition

To define the ramification signature for a real quadratic field, we need a proposition.

Proposition 5.1. *Let l and p be two distinct odd prime numbers, and $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field that splits over l and unramified over p. We denote the ring of integers in K by A_K, a point over l by u and a (the) point over p in $SpecA_K$ by v. Let I_u and I_v be the prime ideals of A_K corresponding to u and v, respectively. Let $Z := \{u, v\}$, and $U := SpecA_K \setminus Z$. Let A_u and A_v be the completions of A_K at u and v respectively. Denote $k(v)$ be the residue field of A at v, it is isomorphic to $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.*

Suppose that the order $n(v)$ of the multiplicative group $k(v)^\times$ is divisible by l, the class

number of K is not divisible by l, and there is a unit $\alpha \in A_K^\times$, such that

$$\alpha^{l-1} \neq 1 \mod I_u^2, \quad \alpha^{\frac{n(v)}{l}} \neq 1 \mod I_v.$$

Then we have the following:

a. *There is an exact sequence*

$$1 \longrightarrow A_K^\times/A_K^{\times l} \xrightarrow{i} A_u^\times/A_u^{\times l} \oplus A_v^\times/A_v^{\times l} \xrightarrow{j} \pi_1(U)^{ab}/\pi_1(U)^{ab^l} \longrightarrow 1\,. \qquad (A)$$

b. $\dim_{\mathbb{Z}/l\mathbb{Z}} \pi_1(U)^{ab}/\pi_1(U)^{ab^l} = 1$;

c. *For any nontrivial character $\chi : \pi_1(U) \longrightarrow \mathbb{Z}/l\mathbb{Z}$, χ is ramified at both u and v.*

Proof.

a. Let us consider the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1 & \longrightarrow & K^\times & \xrightarrow{\sim} & K^\times & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \{\pm 1\}^{\oplus 2} \oplus A_u^\times/A_u^{\times l} \oplus A_v^\times/A_v^{\times l} & \longrightarrow & \{\pm 1\}^{\oplus 2} \oplus K_u^\times/A_u^{\times l} \oplus K_v^\times/A_v^{\times l} \oplus \oplus_{x\neq u,v}\mathbb{Z} & \longrightarrow & Div(K) & \longrightarrow & 0. \end{array}$$

Through the snake lemma and class field theory, we have the following exact sequence:

$$A_K^\times \longrightarrow \{\pm 1\}^{\oplus 2} \oplus A_u^\times/A_u^{\times l} \oplus A_v^\times/A_v^{\times l} \longrightarrow \pi_1(U)^{ab}/Im(A_u^{\times l} \oplus A_v^{\times l}) \longrightarrow Cl(K) \longrightarrow 1\,.$$

where the term $Im(A_u^{\times l} \oplus A_v^{\times l})$ is the image of $A_u^{\times l} \oplus A_v^{\times l}$ under the reciprocity map

$$K_u^\times \oplus K_v^\times \longrightarrow \mathrm{Gal}(K_u^{ab}/K) \oplus \mathrm{Gal}(K_v^{ab}/K) \longrightarrow \pi_1(U)^{ab}$$

As the class number of K is assumed indivisible by l, a diagram chasing shows an exact sequence

$$A_K^\times/A_K^{\times l} \longrightarrow A_u^\times/A_u^{\times l} \oplus A_v^\times/A_v^{\times l} \longrightarrow \pi_1(U)^{ab}/\pi_1(U)^{ab^l} \longrightarrow 1.$$

The hypothesis on the existence of the global unit shows that the left morphism is nonzero. Thus it is injective, since $A_K^\times/A_K^{\times l}$ is an $\mathbb{Z}/l\mathbb{Z}$- linear space of dimension 1. Therefore, we obtain the exact sequence (A).

b. The complete discrete valuation rings A_u and A_v are isomorphic to $\mathbb{Z}/l\mathbb{Z}$ and $W(k(v))$ (the witt ring over $k(v)$) respectively. Therefore, the middle term in the sequence (A) is isomorphic to $(\mathbb{Z}/l^2\mathbb{Z})^\times/(\mathbb{Z}/l^2\mathbb{Z})^{\times l} \oplus k(v)^\times/k(v)^{\times l}$, and is of $\mathbb{Z}/l\mathbb{Z}$-dimension 2. The left term in (A) has $\mathbb{Z}/l\mathbb{Z}$-dimension 1 since K is a real quadratic field, and l is odd. Thus, the right term in (A) has $\mathbb{Z}/l\mathbb{Z}$-dimension 1.

c. We consider the dual sequence

$$0 \longrightarrow Hom(\pi_1(U)^{ab}, \mathbb{Z}/l\mathbb{Z}) \xrightarrow{j^*} Hom(A_u^\times/A_u^{\times l} \oplus A_v^\times/A_v^{\times l}, \mathbb{Z}/l\mathbb{Z}) \longrightarrow Hom(A_K^\times/A_K^{\times l}, \mathbb{Z}/l\mathbb{Z}) \longrightarrow 0 \qquad (B)$$

of (A). Denote the image of α under the morphism i by (α_u, α_v). For any $\chi \neq 0 \in Hom(\pi_1(U)^{ab}, \mathbb{Z}/l\mathbb{Z})$, we have

$$\langle \alpha_u, \chi \rangle + \langle \alpha_v, \chi \rangle = 0 \qquad (C)$$

by (B). Therefore, the following four conditions are equivalent:

(i). χ is ramified at u,

(ii). $\langle \alpha_u, \chi \rangle \neq 0$,

(iii). $\langle \alpha_v, \chi \rangle \neq 0$,

(iv). χ is ramified at v.

The map $j^\star$ is injective, indicating that there is not non-trivial character $\chi : \pi_1(U) \longrightarrow \mathbb{Z}/l\mathbb{Z}$ such that it is unramified at both points u and v. Therefore, for any non-trivial $\chi \in Hom(\pi_1(U), \mathbb{Z}/l\mathbb{Z})$, χ must be ramified at both u and v. ■

The following corollary is proved in the proof of Proposition 5.1.

Corollary 5.2. *Under the conditions in proposition 5.1, we have the following:*

(i) $< \alpha_u, \chi > \neq 0$,

(ii) $< \alpha_v, \chi > \neq 0$,

(iii) $< \alpha_u, \chi > + < \alpha_v, \chi > = 0$.

for any non-trivial character $\chi : \pi_1(U) \longrightarrow \mathbb{Z}/l\mathbb{Z}$.

■

Through the natural isomorphism $A_u^\times / A_u^{\times l} \cong (\mathbb{Z}/l^2\mathbb{Z})^\times / (\mathbb{Z}/l^2\mathbb{Z})^{\times l}$, $A_u^\times / A_u^{\times l}$ is generated by $1 + l$. For any generator g of $k(v)^\times / k(v)^{\times l}$, we regard it as a generator of $A_v^\times / A_v^{\times l}$ through the natural isomorphism $A_v^\times / A_v^{\times l} \cong k(v)^\times / k(v)^{\times l}$. Clearly, $\langle 1 + l, \chi_u \rangle^{-1} \langle g, \chi_v \rangle$ is independent of the choice of $\chi \neq 0 \in Hom(\pi_1(U), \mathbb{Z}/l\mathbb{Z})$. We call this term the **ramification signature of U with respect to g.**

5.2 Reduction from signature computation problem to discrete logarithm problem

Suppose given p, l, $K = \mathbb{Q}(\sqrt{D})$, U, u, v, α, g, as in Proposition 5.1. Then the computation of the ramification signature of U with respect to g can be reduced to a discrete logarithm problem in $k(v)$ as follows by using Corollary 5.2.

Let us consider the following commutative diagram:

$$\begin{array}{ccccccc} A_K^\times & \longrightarrow & A_u^\times & \xrightarrow{\sim} & \mathbb{Z}_l^\times & \longrightarrow & \mathbb{Z}_l^\times / \mathbb{Z}_l^{\times l} \\ & & & & \downarrow & & \downarrow \\ & & & & (\mathbb{Z}/l^2\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/l^2\mathbb{Z})^\times / (\mathbb{Z}/l^2\mathbb{Z})^{\times l}. \end{array}$$

If the image in $(\mathbb{Z}/l^2\mathbb{Z})^\times$ of α equals $\xi(1 + l)^y$, where ξ is an$(l - 1)$-st root of unity, then its image in $(\mathbb{Z}/l^2\mathbb{Z})^\times / (\mathbb{Z}/l^2\mathbb{Z})^{\times l}$ will be equal to $(1 + l)^y$. We can easily compute ξ, y and consequently the first term in (C) $\langle \alpha_u, \chi \rangle = y\langle 1 + l, \chi \rangle$.

For the second term in (C), if the image of α under the morphism $A_K^\times \longrightarrow A_v^\times / A_v^{\times l} \cong k(v)^\times / k(v)^{\times l}$ is $a = g^m$, then $\langle \alpha_v, \chi_v \rangle = m\langle g, \chi_v \rangle$.

By Corollary 5.2, if we can compute m from $a = g^m$, then we can compute

$$\langle 1+l, \chi_u \rangle^{-1} \langle g, \chi_v \rangle = -m^{-1}y \quad \in \mathbb{Z}/l\mathbb{Z}.$$

5.3 Reduction from discrete logarithm problem in prime fields to signature computation problem

Let k be an finite field. Let g be a generator of $k^\times$, $a \in k^\times$ and l be a prime dividing the order of $k^\times$. In the case $k = \mathbb{F}_p$, the construction in previous section gives us a real quadratic field and a global unit in the field that enable us to reduce the computation of m satisfying $a = g^m$ to the signature computation problem of the real quadratic field. However, the construction requires some conditions on the class number of the field and the unit (the condition (1),(2) and (3) in proposition 4.1) to be satisfied. We give an improvement in Step 4 below on the construction recalled below. With the improvement, the condition (2) and (3) in Proposition 4.1 is satisfied automatically.

We show the computation of discrete logarithm $\log_g a \mod l$ can then be reduced to computing the ramification signature of a real quadratic field as follows, by using Corollary 5.2.

If $a^{\frac{p-1}{l}} = 1$, then $m \equiv 0 \pmod{l}$. Thus suppose $a^{\frac{p-1}{l}} \neq 1$. We will lift a to some unit α of a real quadratic field K such that $\alpha \equiv a \mod v$ for some place v of K over p, $\alpha^{l-1} \neq 1 \mod I_u^2$, and $\alpha^{l-1} \neq 1 \mod I_{u'}^2$ for the two places u and u' of K over l. We do it as follows:

1. Compute $b \in \mathbb{F}_p^\times$ such that $ab = 1$ in $\mathbb{F}_p^\times$.

2. Put $c := \frac{a+b}{2}$, $d := \frac{a-b}{2}$. Note that $c^2 - d^2 = 1$ and $a = c + d$. We can assume $d \neq 0$; otherwise, $a^2 = 1$ and $m = \frac{p-1}{2}$ or $p-1$.

3. Lift d to an integer. We have $(\frac{1+d^2}{p}) = (\frac{c^2}{p}) = 1$. We choose $k \in \{0, 1, ..., l-1\}$ randomly until $(\frac{(d+kp)^2+1}{l}) = 1$. Lemma 5.3 below for $c = -1$ shows that we can obtain such k with probability of about 50% each time.

4. If we find such k, let $d_1 := d + kp \in \mathbb{Z}_l^\times$. We may take $\sqrt{d_1^2+1} \in \mathbb{Z}_l^\times$ since $(\frac{d_1^2+1}{l}) = 1$. If $(d_1 + \sqrt{d_1^2+1})^{l-1} \equiv 1 \mod l^2$, let $x = d_1$; otherwise let $x = d_1 + pl$. Lemma 5.4 below for $c = -1$ shows that $(x + \sqrt{x^2+1})^{l-1} \not\equiv 1 \mod l^2$, $(x - \sqrt{x^2+1})^{l-1} \not\equiv 1 \mod l^2$.

5. Let $\alpha := x + \sqrt{x^2+1}$. Thus, $\alpha \equiv d + c \equiv \tilde{a} \mod v$, $\alpha \equiv d - c \equiv -\tilde{b} \mod v'$, $\alpha^{l-1} \neq 1 \mod I_u^2$ and $\alpha^{l-1} \neq 1 \mod I_{u'}^2$.

6. Let $K := \mathbb{Q}(\sqrt{x^2+1})$. Note that $Nm(\alpha) = 1$, so α is a unit of K.

Let $U := Spec A_K \setminus \{u, v\}$. We assume that $l \nmid h_K$, which is likely to be satisfied. Corollary 5.2 then shows $\langle \alpha_u, \chi \rangle + \langle \alpha_v, \chi \rangle = 0$, for any $\chi \neq 0 \in Hom(\pi_1(U), \mathbb{Z}/l\mathbb{Z})$. Let $(1+l)^y$ be the image of α under the morphism

$$A_K^\times \longrightarrow A_u^\times \cong \mathbb{Z}_l^\times \longrightarrow (\mathbb{Z}/l^2\mathbb{Z})^\times / (\mathbb{Z}/l^2\mathbb{Z})^{\times l}.$$

For the first term in (C), we have $\langle \alpha_u, \chi \rangle = y\langle 1+l, \chi \rangle$. For the second term in (C), we have $\langle \alpha_v, \chi \rangle = m\langle \tilde{g}, \chi \rangle$. Hence, we obtain

$$y\langle 1+l, \chi \rangle + m\langle \tilde{g}, \chi \rangle = 0.$$

Therefore, if we can compute the ramification signature $\langle \chi, 1+l \rangle^{-1} \langle \chi, g \rangle$ of U with respect to g, then we can compute $m = -y\langle \chi, 1+l \rangle^{-1} \langle \chi, g \rangle$.

Therefore, we conclude that the discrete logarithm problems in $\mathbb{F}_p^\times$ are random polynomial time equivalent to some signature computation problem with only one assumption, namely, that on the class number.

The following are the statements and proofs of lemma 5.3 and lemma 5.4.

Lemma 5.3. *Let l be an odd prime, $c \in \mathbb{F}_l^\times$. Define a map $f : \mathbb{Z}/l\mathbb{Z} \longrightarrow \{0, 1, -1\}$ by $a \mapsto (\frac{a^2-c}{l})$. Then, we have*

$$|f^{-1}(0)| = 2, \quad |f^{-1}(1)| = (l-3)/2, \quad |f^{-1}(-1)| = (l-1)/2 \quad \text{if } (\frac{c}{l}) = 1,$$

$$|f^{-1}(0)| = 0, \quad |f^{-1}(1)| = (l-1)/2, \quad |f^{-1}(-1)| = (l+1)/2 \quad \text{if } (\frac{c}{l}) = -1.$$

Proof. Let X be the curve defined by $y^2 = x^2 - c$ over $\mathbb{F}_l$. For any $a \in \mathbb{F}_l$, the cardinality of the set $\{$ $\mathbb{F}_l$-rational point of X that has first coordinate a $\}$ is $f(a) + 1$. Therefore, the following holds:

$$\sum_{a \in \mathbb{F}_l} (f(a) + 1) = |X(\mathbb{F}_l)|.$$

The curve X is isomorphic to the affine scheme defined by $z\omega = 1$ over $\mathbb{F}_l$, which implies $|X(\mathbb{F}_l)| = l - 1$, and $\sum_{a \in \mathbb{F}_l} f(a) = |X(\mathbb{F}_l)| - l = -1$. Clearly,

$$\begin{array}{ll} f^{-1}(0) = \{\sqrt{c}, -\sqrt{c}\} & \text{if } (\frac{c}{l} = 1), \\ f^{-1}(0) = \phi & \text{if } (\frac{c}{l} = -1). \end{array}$$

which completes the proof. ∎

Lemma 5.4. *Let p and l be two distinct odd prime numbers. Let c be an integer such that $c^{l-1} \equiv 1 \mod l^2$ and a be an integer such that $(\frac{a^2-c}{l}) = 1$. We denote a square root of $a^2 - c$ in $\mathbb{Z}_l^\times$ by $\sqrt{a^2 - c}$. If $(a+\sqrt{a^2-c})^{l-1} \in 1 + l^2\mathbb{Z}_l$, then we have $((a+pl)+\sqrt{(a+pl)^2-c})^{l-1} \notin 1 + l^2\mathbb{Z}_l$ and $((a+pl) - \sqrt{(a+pl)^2-c})^{l-1} \notin 1 + l^2\mathbb{Z}_l$.*

Proof. By Hensel's lemma, there is a unique square root $\sqrt{(a+x)^2 - c}$ of $(a+x)^2 - c$ in $\mathbb{Z}_l[[x]]$ such that it's image under the morphism $x \mapsto 0 : \mathbb{Z}_l[[x]] \longrightarrow \mathbb{Z}_l$ is $\sqrt{a^2 - c}$. Let $h(x) := (a+x) + \sqrt{(a+x)^2 - c}$, we then have

$$h(pl) \equiv h(0) + h'(0)pl \mod l^2,$$

where $h'(0) = 1 + \frac{a}{\sqrt{a^2-c}} = \frac{h(0)}{\sqrt{a^2-c}}$. Therefore, we have

$$h(pl) \equiv h(0)(1 + \frac{p}{\sqrt{a^2 - c}}l) \mod l^2.$$

The term $\frac{p}{\sqrt{a^2-c}}$ is not divided by l, which implies $h(pl)^{l-1} \not\equiv h(0)^{l-1} \mod l^2$. Hence, we have

$$\begin{array}{lll} & ((a+pl) + \sqrt{(a+pl)^2 - c})^{l-1} & \\ \not\equiv & (a + \sqrt{a^2 - c})^{l-1} & \mod l^2 \\ \equiv & 1 & \mod l^2. \end{array}$$

The fact that $((a+pl) + \sqrt{(a+pl)^2 - c})^{l-1}((a+pl) - \sqrt{(a+pl)^2 - c})^{l-1} = c^{l-1} \equiv 1 \mod l^2$ shows

$((a+pl) - \sqrt{(a+pl)^2 - c})^{l-1} \not\equiv 1 \mod l^2$. ∎

5.4 Reduction from discrete logarithm problem in finite fields of order square of prime number to signature computation problem

Let k be an finite field. Let g be a generator of $k^\times$, $a \in k^\times$ and l be a prime dividing the order of $k^\times$. In the case $k = \mathbb{F}_p$, we have showed the computation of discrete logarithm $\log_g a \mod l$ can be reduced to computing the ramification signature of a real quadratic field in previous subsection. We also show it in the case $k = \mathbb{F}_{p^2}$ as follows, by using Corollary 5.2.

If $a \in \mathbb{F}_{p^2}^{\times l}$, then we have $m \equiv 0 \mod l$. Thus we can suppose $a \notin \mathbb{F}_{p^2}^{\times l}$.

a. If $l \nmid p-1$, we must have $l | p+1$. Let $\tilde{a} := a^{p-1}, \tilde{g} := g^{p-1}$. We then have

$$\tilde{a} = \tilde{g}^m, \quad Nm(\tilde{a}) = Nm(\tilde{g}) = 1, \quad \tilde{a} \notin \mathbb{F}_{p^2}^{\times l}.$$

We take $t \in \mathbb{F}_p$ such that $(\frac{t}{p}) = -1$. We have $\mathbb{F}_{p^2} = \mathbb{F}(\sqrt{t})$. We put $\tilde{a} = a_0 + b_0\sqrt{t}$, where $a_0, b_0 \in \mathbb{F}_p$. We can assume $b_0 \neq 0$; otherwise, $\tilde{a}^2 = 1$ and $m = \frac{p+1}{2}$ or $p+1$.

We have $a_0^2 - b_0^2 t = Nm(\tilde{a}) \equiv 1 \mod p$. Hence, for any $k \in \mathbb{Z}$, the following holds:

$$(\frac{(a_0+kp)^2-1}{p}) = (\frac{a_0^2-1}{p}) = (\frac{b_0^2 t}{p}) = (\frac{t}{p}) = -1.$$

We choose $k \in \{0, 1, \cdots, l-1\}$ randomly, until $(\frac{(a_0+kp)^2-1}{l}) = 1$. Lemma 5.3 for $c = 1$ shows that we can obtain such k with probability about 50% each time.

If we find such k, let $a_1 := a_0 + kp \in \mathbb{Z}^\times$. We have $\sqrt{a_1^2-1} \in \mathbb{Z}_l$ because $(\frac{a_1^2-1}{l}) = 1$. If $(a_1 + \sqrt{a_1^2-1})^{l-1} \not\equiv 1 \mod l^2$, let $x = a_1$. Else, let $x = a_1 + pl$. Lemma 5.4 for $c = 1$ shows that $(x + \sqrt{x^2-1})^{l-1} \not\equiv 1 \mod l^2$.

Let $K := \mathbb{Q}(\sqrt{x^2-1})$. Then, K inerts over p and splits over l because $(\frac{x^2-1}{p}) = -1$, and $(\frac{x^2-1}{l}) = 1$. Let $v \in SpecA_K$ be the point over p and $u \in SpecA_K$ be a point over l. Let $\alpha := x + \sqrt{x^2-1} \in A_K$. We then have $\alpha^{l-1} \not\equiv 1 \mod I_v^2$ and

$$\alpha \equiv a_0 + \sqrt{a_0^2-1} \equiv a_0 + b_0\sqrt{t} \equiv \tilde{a} \equiv \tilde{g}^m \mod v$$

implying that $\alpha^{\frac{p^2-1}{l}} \not\equiv 1 \mod I_v$ as $\tilde{a} \notin \mathbb{F}_{p^2}^{\times l}$. As $\alpha := x + \sqrt{x^2-1} \in A_K$ and $Nm(\alpha) = x^2 - (x^2-1) = 1$, we have $\alpha \in A_K^\times$.

Let $U := SpecA_K \setminus \{u, v\}$. We assume that $l \nmid h_K$, which is likely to be satisfied. Corollary 5.2 then shows $\langle \alpha_u, \chi \rangle + \langle \alpha_v, \chi \rangle = 0$, for any $\chi \neq 0 \in Hom(\pi_1(U), \mathbb{Z}/l\mathbb{Z})$. Let $(1+l)^y$ be the image of α under the morphism

$$A_K^\times \longrightarrow A_u^\times \cong \mathbb{Z}_l^\times \longrightarrow (\mathbb{Z}/l^2\mathbb{Z})^\times / (\mathbb{Z}/l^2\mathbb{Z})^{\times l}.$$

For the first term in (C), we have $\langle \alpha_u, \chi \rangle = y\langle 1+l, \chi \rangle$. For the second term in (C), we have $\langle \alpha_v, \chi \rangle = m\langle \tilde{g}, \chi \rangle$. Hence, we obtain

$$y\langle 1+l, \chi \rangle + m\langle \tilde{g}, \chi \rangle = 0.$$

Therefore, if we can compute the ramification signature $\langle \chi, 1+l \rangle^{-1} \langle \chi, g \rangle$ of U with respect to g, then we can compute $m = -y\langle \chi, 1+l \rangle^{-1} \langle \chi, g \rangle$.

b. If $l|p-1$, we have $Nm(a) = Nm(g)^m$ as elements in $\mathbb{F}_p$. We can reduce the computation of m satisfying $Nm(a) = Nm(g)^m$ to the signature computation problem of the real quadratic field using the algorithm in previous section.

Acknowledgments. I would like to thank professor Takeshi Saito for giving me valuable advice.

References

[Adleman 1979] L. Adleman, A subexponential algorithm for the discrete logarithm problem with applications to cryptography,In Foundations of Computer Science, 1979., 20th Annual Symposium on , 2008,

[Adleman 1994] L.M. Adleman, The function field sieve, Algorithmic number theory, ANTS-I (eds. L.M. Adleman, M.-D. Huang), Lecture Notes in Comput. Sci., vol. 877, Springer-Verlag, Berlin, 1994, pp. 108-121.

[Adleman and Huang 1999] L.M. Adleman, M.-D. Huang, Function field method for discrete logarithms over finite fields, Inform. and Comput. 151:1-2 (1999), 5-16.

[Buhler 1993] J.P. Buhler, H.W. Lenstra, Jr., C. Pomerance, Factoring Integers with the Number Field Sieve, in A.K. Lenstra and H.W. Lenstra, Jr. (eds), The Development of the Number Field Sieve, Lecture Notes in Mathematics 1554, Springer-Verlag, New York, 1993, pp. 50-94

[Cohen 1993] H. Cohen, A course in computational algebraic number theory, Graduate Text in Mathematics 138, Springer, Berlin, 1993.

[Gordon 1993] D.M.Gordon, "Discrete logarithms in GF(p) using the number field sieve", SIAM J. Discrete Math. 6:1 (1993), 124-138

[Hellman-Reyneri 1983] M.E. Hellman and J.M. Reyneri, Fast computation of discrete logarithms in GF (q),Advances in Cryptology–Proceedings of Crypto, 1983,

[Huang-Raskind 2009] Ming-Deh Huang and Wayne Raskind , Global Duality, Signature Calculus and the Discrete Logarithm Problem, LMS Journal of Computation and Mathematics , Volume 12 , Jan 2009 , pp 228-263.

[Joux-Lercier 2003] A. Joux, R. Lercier, Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the Gaussian integer method. Math. Comp. 72 (2003), no. 242, 953967 (electronic).

[Kraitchik 1922] M. Kraitchik, Thorie des nombres, Gauthier–Villards, 1922

[Lenstra-Lenstra 1993] A. K. Lenstra and J. H. W. Lenstra, The development of the number field sieve, Lecture Notes in Mathematics 1554, Springer, Berlin, 1993.

[Milne 1980] J. S. Milne, Etale Cohomology. Princeton Mathematical Series, 1980

[MOV 1993] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inform. Theory, 39(5):1639-1646,1993.

[Pohlig 1977] S.C.Pohlig, Algebraic and Combinatoric Aspects of Cryptograhy, Thechnical report Stanford University, 1977,

[Pollard 1978] Pollard, J. M. (1978). "Monte Carlo methods for index computation (mod p)". Mathematics of Computation 32 (143): 918924. JSTOR 2006496.

[Schirokauer 1993] O. Schirokauer, Discrete logarithms and local units, Theory and applications of numbers without large prime factors (ed. R.C. Vaughan), Philos. Trans. Roy. Soc. London Ser. A, vol. 345, The Royal Society, London, 1993, pp. 409-423.

[Schirokauer 2000] O. Schirokauer, Using number fields to compute logarithms in finite fields, Math. Comp. 69:231 (2000), 1267-1283.

[Schirokauer 2008] O. Schirokauer, The impact of the number field sieve on the discrete logarithm problem in finite fields. Algorithmic number theory: lattices, number fields, curves and cryptography, 397420, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.

[Shanks 1971] D. Shanks. Class number, a theory of factorization and genera. In Proc. Symp. Pure Math. 20, pages 415440. AMS, Providence, R.I., 1971.

[Stevenhagen 2008] P. Stevenhagen, The number field sieve. Algorithmic number theory: lattices, number fields, curves and cryptography, 83100, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.

論文の内容の要旨

論文題目　On The Discrete Logarithm Problem in Finite Fields
(有限体上の離散対数問題について)

氏　名　張　祺智

位数nの巡回群G、その生成元gとGの元bを与えて、$g^x = b$であるような整数xを求める問題を離散対数問題と言う。

Gが有限体の乗法群や有限体上の楕円曲線の有理点の群の場合において離散対数問題の多項式時間アルゴリズムは知られていない。これらの群上の離散対数問題の困難性は暗号系の構築によく利用されている。だからこれらの群上の離散対数問題の計算量の下限を評価するのは重要かつ難しい問題である。この論文はこの問題を調べる。

第2節で一般的な巡回群における離散対数問題に対する指数時間アルゴリズムを三つ紹介する。2.1節で中国の剰余定理を利用する自然なアルゴリズムを紹介する。群の指数のすべての素因子が小さい場合にこのアルゴリズムは有効である。2.2節でShanksのアルゴリズム（[Shanks 1971]）を紹介する。このアルゴリズムの時間計算量と空間計算量はともに$O(\sqrt{n})$である。2.3節でPollardのアルゴリズム（[Pollard 1978]）を紹介する。このアルゴリズムの時間計算量は$O(\sqrt{n})$であり、空間計算量は$O(1)$である。

第3節で有限体の乗法群における離散対数問題に対する準指数時間アルゴリズムを三つ紹介する。セクション3.1でIndex Calculusアルゴリズムを紹介する。Index Calculusアルゴリズムは1922年にKraitchik氏[Kraitchik 1992]によって提案されて、有限素体の乗法群上の離散対数問題を解くアルゴリズムである。素体$\mathbb{F}_p$の乗法群上の離散対数問題を解く場合にこのアルゴリズムの計算量は$exp(c(\log p)^{\frac{1}{2}}(\log\log p)^{\frac{1}{2}})$である（$c$は正の実数定数である）。3.2節で代数体篩い法を紹介する。代数体篩い法は最初1993年に因数分解アルゴリズムとして提案された。後その類似としての離散対数アルゴリズムが発見された（[Gordon 1993]）。素体$\mathbb{F}_p$の乗法群上の離散対数問題を解く場合にこのアルゴリズムの計算量は$exp((\frac{64}{9}+o(1))(\log p)^{\frac{1}{2}}(\log\log p)^{\frac{1}{2}})$と予想される。3.3節で関数体篩い法を紹介する。関数体篩い法は1994年にAdleman氏によって提案されて、1999年にAdleman氏とHuang氏によって改良された（[Adleman and Huang 1999]）。有限体$\mathbb{F}_q$の乗法群上の

離散対数問題を解く場合にこのアルゴリズムの計算量は$exp(c(\log q)^{\frac{1}{2}}(\log\log q)^{\frac{1}{2}})$と予想される。

離散対数問題の計算量下限を評価するため、直接この問題を解くアルゴリズムを探す他にこの問題と同値な問題を探す手法もある。2009年にHuang氏とRaskind氏は有限素体上の離散対数問題を実2次体と結びつけた（[Huang-Raskind 2009]）。彼らは実2次体に対してramification signatureというものを定義し、ある二つの仮定の下で、有限素体上の離散対数問題と実2次体上のramification signatureの計算問題の同値性を証明した。仮定の一つは実2次体の類数に関するもので、もう一つは実2次体のある単数に関する仮定である。この仕事を第4節で紹介する。

この論文の主要部である第5節では実二次体のramification signatureを一般化する。もとのramification signatureは「pとlは両方分解する」という場合に定義されたが、このセクションでは「pが不分岐でlが分解する」という場合へ一般化する。それから有限素体と位数が素数の平方であるような有限体上の乗法群上の離散対数問題と実2次体上のramification signatureの計算問題の同値性をある仮定の下で証明する。この仮定は実2次体の類数に関する仮定である。特に、Huang氏とRaskind氏の証明から単数に関する仮定を削除してもよいということを示す。具体的には、実2次体と単数を構成するアルゴリズムを改良し（本文の5.3節のStep 4）、[Huang-Raskind 2009]の中の4.1節の命題2の条件(2), (3)が自動的に満たされるようにする。

References

[Adleman and Huang 1999] L.M. Adleman, M.-D. Huang, Function field method for discrete logarithms over finite fields, Inform. and Comput. 151:1-2 (1999), 5-16.

[Buhler 1993] J.P. Buhler, H.W. Lenstra, Jr., C. Pomerance, Factoring Integers with the Number Field Sieve, in A.K. Lenstra and H.W. Lenstra, Jr. (eds), The Development of the Number Field Sieve, Lecture Notes in Mathematics 1554, Springer-Verlag, New York, 1993, pp. 50-94

[Gordon 1993] D.M.Gordon, "Discrete logarithms in GF(p) using the number field sieve", SIAM J. Discrete Math. 6:1 (1993), 124-138

[Huang-Raskind 2009] Ming-Deh Huang and Wayne Raskind , Global Duality, Signature Calculus and the Discrete Logarithm Problem, LMS Journal of Computation and Mathematics , Volume 12 , Jan 2009 , pp 228-263.

[Kraitchik 1992] M. Kraitchik, Thorie des nombres, Gauthier–Villards, 1922

[Pollard 1978] Pollard, J. M. (1978). "Monte Carlo methods for index computation (mod p)". Mathematics of Computation 32 (143): 918924. JSTOR 2006496.

[Shanks 1971] D. Shanks. Class number, a theory of factorization and genera. In Proc. Symp. Pure Math. 20, pages 415440. AMS, Providence, R.I., 1971.