Journal of Number Theory 134 (2014) 29–37

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the signature calculus for finite fields of order square of prime numbers

Qizhi Zhang

Q20, Huawei, Huanbaoyuan, No. 156 Beiqing rd., Haidian District, Beijing 100095, China

ARTICLE INFO

Article history:
Received 13 April 2012
Received in revised form 6 June 2013
Accepted 6 June 2013
Available online 13 September 2013
Communicated by David Goss

MSC:
11R37
11Y40
68W20

Keywords:
Discrete logarithm problem
Signature calculus
Real quadratic field
Class field theory
Étale fundamental group

ABSTRACT

In this paper it is proved that the discrete logarithm problem in a quadratic extension of a prime field is random polynomial time equivalent to computing the ramification signature of a real quadratic field. This extends a result in [4] from a prime field to its quadratic extensions.

© 2013 Elsevier Inc. All rights reserved.

1. Introduction

Let p be a big prime number and E be an elliptic curve over $\mathbb{F}_p$. The hardness assumption on the discrete logarithm problem in $\mathbb{F}_p^\times$ or in $E(\mathbb{F}_p)$ is the basis of many public-key encryption schemes. Estimating the greatest lower bound in the complexity of solving the discrete logarithm problem is an important and difficult problem.

E-mail address: zqz.math@gmail.com.

0022-314X/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jnt.2013.06.011

In the case of $\mathbb{F}_p^\times$, the best algorithm known so far is the number field sieve. For example, see [3] and [7]. It solves the discrete logarithm problem in $\mathbb{F}_p^\times$ in a conjectural running time $L_p(\frac{1}{3}, c) = \exp((c+o(1))(\log p)^{1/3}(\log\log p)^{2/3})$, with $c = (64/9)^{1/3}$. In the case of $E(\mathbb{F}_p)$, the problem can be reduced to the discrete logarithm problem in $\mathbb{F}_q^\times$ using the MOV attack [5], where $q = p^k$ and k is a positive integer so that $p^k - 1$ is divisible by the cardinality of $E(\mathbb{F}_p)$. The discrete logarithm problem in $\mathbb{F}_q^\times$ can be solved using the function field sieve [1,2] or a modified number field sieve [8]. Let e be the real number such that $k = (\log q/\log\log q)^e$. Then, the running time of the function field sieve is conjecturally equal to $L_q(\max\{\frac{1}{3}, 1-e\}, O(1))$, and that of the modified number field sieve is conjecturally equal to $L_q(\max\{\frac{1}{3}, \frac{1+e}{4}\}, O(1))$.

Alternatively, we can estimate the greatest lower bound by studying an equivalent problem of a discrete logarithm problem. In [4], 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 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.

In this paper, we lift the discrete logarithm problem in $\mathbb{F}_{p^2}^\times$ to a real quadratic field. We then define the "ramification signature" for the real quadratic field and prove that the discrete logarithm problem in $\mathbb{F}_{p^2}^\times$ 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 [4] one can remove the assumption on the global unit. More precisely, we give an improvement (Step 4 in Section 3.2.**b** in the text) on the construction of real quadratic field and global unit that makes the condition in Proposition 2 in Section 4.1 in [4] be satisfied automatically.

In Section 2, we define the ramification signature for a real quadratic field. In Section 3, we prove the equivalence of the discrete logarithm problem in $\mathbb{F}_{q^2}^\times$ and the computation of a ramification signature of a real quadratic field. Consequently, we also prove the equivalence in [4] without the assumption on the global unit.

2. Signature

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

Proposition 2.1. *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 inerts over p. We denote the ring of integers in K by A_K, the points over l in Spec A_K by u and $\tilde{u}$, and the point over p in Spec A_K by v. Let I_u, $I_{\tilde{u}}$, and I_v be the prime ideals of A_K corresponding to u, $\tilde{u}$, and v, respectively. Let $Z := \{u, v\}$, and $U :=$ Spec $A_K \setminus Z$. Let A_u and A_v be the completions of A_K at u and v respectively. Denote $A_U := \Gamma(U, \mathcal{O}_U)$.*

Suppose that $p^2 - 1$ 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

$$\alpha^{l-1} \neq 1 \mod I_u^2, \qquad \alpha^{\frac{p^2-1}{l}} \neq 1 \mod I_v.$$

Then, we have the following:

a. *There is an exact sequence*

$$1 \to A_K^\times / A_K^{\times l} \xrightarrow{i} A_u^\times / A_u^{\times l} \oplus A_v^\times / A_v^{\times l} \xrightarrow{j} \pi_1(U)^{ab} / \pi_1(U)^{ab^l} \to 1. \tag{2.2.1}$$

b. $\dim_{\mathbb{Z}/l\mathbb{Z}} \pi_1(U)^{ab} / \pi_1(U)^{ab^l} = 1$, *where the* $\pi_1(U)$ *is the étale fundamental group of* U (*see, for example,* [6]).

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

Proof. a. Denote the idele group of K by $\mathbb{I}_K$. Through the class field theory, we have the isomorphism $\pi_0(\mathbb{I}_K / K^\times) \cong \mathrm{Gal}(K^{ab}/K)$, where π_0 means the "group consisting of the connected components". Therefore we have a surjection $\pi_0(\mathbb{I}_K/K^\times) \to \pi_1(U)^{ab}$, whose kernel is $\prod_{x \neq u,v} A_x^\times$. Therefore we have an isomorphism

$$\frac{\{\pm 1\}^{\oplus 2} \oplus K_u^\times \oplus K_v^\times \oplus \bigoplus_{x \neq u,v} \mathbb{Z}}{K^\times} \cong \pi_1(U)^{ab}.$$

Let us consider the following commutative diagram:

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

Through the snake lemma, we have the following exact sequence:

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

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 map

$$K_u^\times \oplus K_v^\times \to \{\pm 1\}^{\oplus 2} \oplus K_u^\times \oplus K_v^\times \oplus \bigoplus_{x \neq u,v} \mathbb{Z} \to \pi_1(U)^{ab}.$$

As the class number of K is assumed to be non-divisible by l, a diagram chasing shows an exact sequence

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

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 a $\mathbb{Z}/l\mathbb{Z}$-linear space of dimension 1. Therefore, we obtain the exact sequence (2.2.1).

b. The complete discrete valuation rings A_u and A_v are isomorphic to $\mathbb{Z}_l$ and $W(\mathbb{F}_{p^2})$ (the Witt ring over $\mathbb{F}_{p^2}$) respectively. Therefore, the middle term in the sequence (2.2.1) is isomorphic to $(\mathbb{Z}/l^2\mathbb{Z})^\times/(\mathbb{Z}/l^2\mathbb{Z})^{\times l} \oplus \mathbb{F}_{p^2}^\times/\mathbb{F}_{p^2}^{\times l}$, and is of $\mathbb{Z}/l\mathbb{Z}$-dimension 2. Since we know that $A_K^\times/A_K^{\times l}$ is a $\mathbb{Z}/l\mathbb{Z}$-linear space of dimension 1, the right term in (2.2.1) has $\mathbb{Z}/l\mathbb{Z}$-dimension 1.

c. We consider the dual sequence

$$\begin{aligned} 0 \to Hom\big(\pi_1(U)^{ab}, \mathbb{Z}/l\mathbb{Z}\big) &\xrightarrow{j^\star} Hom\big(A_u^\times/A_u^{\times l} \oplus A_v^\times/A_v^{\times l}, \mathbb{Z}/l\mathbb{Z}\big) \\ &\to Hom\big(A_K^\times/A_K^{\times l}, \mathbb{Z}/l\mathbb{Z}\big) \to 0 \end{aligned} \tag{2.2.2}$$

of (2.2.1). Denote the image of α under the morphism i by (α_u, α_v). For any $\chi \neq 0 \in Hom(\pi_1(U)^{ab}, \mathbb{Z}/l\mathbb{Z})$, denote the image of χ under the morphism $j^\star$ by (χ_u, χ_v), then we have

$$\langle \alpha_u, \chi_u \rangle + \langle \alpha_v, \chi_v \rangle = 0 \tag{2.2.3}$$

by (2.2.2). Therefore, the following four conditions are equivalent:

(i) χ is ramified at u,
(ii) $\langle \alpha_u, \chi_u \rangle \neq 0$,
(iii) $\langle \alpha_v, \chi_v \rangle \neq 0$,
(iv) χ is ramified at v.

The map $j^\star$ is injective, indicating that there is not non-trivial character $\chi : \pi_1(U) \to \mathbb{Z}/l\mathbb{Z}$ 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 2.1.**c**.

Corollary 2.2. *Under the conditions in Proposition 2.1, for any non-trivial character $\chi : \pi_1(U) \to \mathbb{Z}/l\mathbb{Z}$, we have the following*:

(i) $\langle \alpha_u, \chi_u \rangle \neq 0$,
(ii) $\langle \alpha_v, \chi_v \rangle \neq 0$,
(iii) $\langle \alpha_u, \chi_u \rangle + \langle \alpha_v, \chi_v \rangle = 0$.

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 $\mathbb{F}_{p^2}^\times/\mathbb{F}_{p^2}^{\times l}$, we regard it as a generator of $A_v^\times/A_v^{\times l}$ through the natural isomorphism $A_v^\times/A_v^{\times l} \cong \mathbb{F}_{p^2}^\times/\mathbb{F}_{p^2}^{\times l}$. 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*.

3. Signature computation problem and discrete logarithm problem in $\mathbb{F}_{p^2}^{\times}$

In this section, we show that the discrete logarithm problem in $\mathbb{F}_{p^2}^{\times}$ is random polynomial time equivalent to computing the ramification signature of some real quadratic field.

3.1. Reduction from signature computation problem to discrete logarithm problem

Suppose given p, l, $K = \mathbb{Q}(\sqrt{D})$, U, $u, \tilde{u}$, v, α, g, as in Proposition 2.1. Then the computation of the ramification signature of U with respect to g can be reduced to a discrete logarithm problem in $\mathbb{F}_{p^2}$ as follows by using Corollary 2.2.

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 (2.2.3) $\langle \alpha_u, \chi_u \rangle = y\langle 1+l, \chi_v \rangle$.

For the second term in (2.2.3), if the image of α under the morphism $A_K^{\times} \to A_v^{\times}/A_v^{\times l} \cong \mathbb{F}_{p^2}^{\times}/\mathbb{F}_{p^2}^{\times l}$ is $a = g^m$, then $\langle \alpha_v, \chi_v \rangle = m\langle g, \chi_v \rangle$.

By Corollary 2.2, if we can compute m from $a = g^m$, then we can compute

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

3.2. Reduction from discrete logarithm problem to signature computation problem

For a field k and an element a in k, let $\sqrt{a}$ denote a square root of a in the algebraic closure of k.

Let g be a generator of $\mathbb{F}_{p^2}^{\times}$, $a \in \mathbb{F}_{p^2}^{\times}$ and l be a prime dividing p^2-1. The computation of discrete logarithm $\log_g a \bmod l$ can then be reduced to computing the ramification signature of a real quadratic field as follows, by using Corollary 2.2.

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

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

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

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

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

We choose $k \in \{0, 1, \ldots, l-1\}$ randomly, until $(\frac{(a_0+kp)^2-1}{l}) = 1$. Lemma 3.1 below 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 $(a_1 + \sqrt{a_1^2-1})^{l-1} \not\equiv 1 \bmod l^2$, we know also $(a_1 - \sqrt{a_1^2-1})^{l-1} \not\equiv 1 \bmod l^2$, let $x = a_1$. Else, let $x = a_1 + pl$. Lemma 3.2 below for $c = 1$ shows that $(x + \sqrt{x^2-1})^{l-1} \not\equiv 1 \bmod l^2$ and $(x - \sqrt{x^2-1})^{l-1} \not\equiv 1 \bmod l^2$.

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 $v \in \mathit{Spec}\, A_K$ be the point over p and $u \in \mathit{Spec}\, A_K$ be a point over l. Fix isomorphisms $A_v/I_v \cong \mathbb{F}_{p^2}$ and $A_u/I_u \cong \mathbb{F}_l$. We have $\sqrt{x^2-1} \equiv \pm b_0\sqrt{t} \bmod v$, because $x^2 - 1 \equiv a_1^2 - 1 \equiv b_0^2 t \bmod v$. Let $\alpha := x + \sqrt{x^2-1} \in A_K$, if $\sqrt{x^2-1} \equiv b_0\sqrt{t} \bmod v$; or $\alpha := x - \sqrt{x^2-1} \in A_K$, otherwise. Then we have $\alpha^{l-1} \not\equiv 1 \bmod I_u^2$ and

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

implying that $\alpha^{\frac{p^2-1}{l}} \not\equiv 1 \bmod I_v$ 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 $U := \mathit{Spec}\, A_K \setminus \{u, v\}$. We assume that $l \nmid h_K$, which is likely to be satisfied. Proposition 2.1 then shows $\langle \alpha_u, \chi\rangle + \langle \alpha_v, \chi\rangle = 0$, for any $\chi \neq 0 \in \mathit{Hom}(\pi_1(U), \mathbb{Z}/l\mathbb{Z})$. Let $(1+l)^y$ be the image of α under the morphism

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

For the first term in (2.2.3), we have $\langle \alpha_u, \chi\rangle = y\langle 1+l, \chi\rangle$. For the second term in (2.2.3), we have $\langle \alpha_v, \chi\rangle = m\langle \tilde{g}, \chi\rangle$. By Corollary 2.2(iii), 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 $l \mid p-1$, we have $Nm(a) = Nm(g)^m$ as elements in $\mathbb{F}_p$. The construction in [4] gives us a real quadratic field and a global unit in the field that enable us to 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 [4]. However, the construction requires some conditions on the class number of the field and the unit to be satisfied [4, Section 4.2]. We give an improvement in Step 4 below on the construction recalled below. With the improvement, one of the condition (condition 2 in Proposition 2 of Section 4.1 in [4]) is satisfied automatically.

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

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

2. Put $c := \frac{\tilde{a}+\tilde{b}}{2}$, $d := \frac{\tilde{a}-\tilde{b}}{2}$. Note that $c^2 - d^2 = 1$ and $\tilde{a} = c + d$. We can assume $d \neq 0$; otherwise, $\tilde{a}^2 = 1$ 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 $k \in \{0, 1, \ldots, l-1\}$ randomly until $(\frac{(d+kp)^2+1}{l}) = 1$. Lemma 3.1 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 $(d_1 + \sqrt{d_1^2+1})^{l-1} \equiv 1 \bmod l^2$, let $x = d_1$; otherwise let $x = d_1 + pl$. Lemma 3.2 below for $c = -1$ shows that $(x+\sqrt{x^2+1})^{l-1} \not\equiv 1 \bmod l^2$, $(x-\sqrt{x^2+1})^{l-1} \not\equiv 1 \bmod l^2$.

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

6. Let v be the point in $Spec\,\mathcal{O}_K$ responding to the prime ideal $(p, \sqrt{x^2-1} - c)$, v' be the point in $Spec\,\mathcal{O}_K$ responding to the prime ideal $(p, \sqrt{x^2-1} + c)$, u and u' be the points in $Spec\,\mathcal{O}_K$ over l. Thus, $\alpha \equiv d + c \equiv \tilde{a} \bmod v$, $\alpha \equiv d - c \equiv -\tilde{b} \bmod v'$, $\alpha^{l-1} \neq 1 \bmod I_u^2$ and $\alpha^{l-1} \neq 1 \bmod I_{u'}^2$. □

In [4], they proved the reduction from a signature computation to a discrete logarithm problem in $\mathbb{F}_p$ without any heuristic assumption. Therefore, we conclude that the discrete logarithm problems in $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$ 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 3.1 and Lemma 3.2.

Lemma 3.1. *Let l be an odd prime, $c \in \mathbb{F}_l^\times$. Define a map $f : \mathbb{Z}/l\mathbb{Z} \to \{0, 1, -1\}$ by $a \mapsto (\frac{a^2-c}{l})$. Then, we have*

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

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

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:

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

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,

$$f^{-1}(0) = \{\sqrt{c}, -\sqrt{c}\} \quad \text{if } \left(\frac{c}{l} = 1\right),$$
$$f^{-1}(0) = \phi \qquad\qquad \text{if } \left(\frac{c}{l} = -1\right),$$

and the lemma follows easily from $|f^{-1}1| + |f^{-1}(-1)| + |f^{-1}(0)| = l$ and $|f^{-1}(1)| - |f^{-1}(-1)| = \sum_{a\in\mathbb{F}_l} f(a) = -1$. □

Lemma 3.2. *Let p and l be two distinct odd prime numbers. Let c be an integer such that $c^{l-1} \equiv 1 \bmod l^2$ 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 its image under the morphism $x \mapsto 0 : \mathbb{Z}_l[[x]] \to \mathbb{Z}_l$ is $\sqrt{a^2-c}$. Let $h(x) := (a+x) + \sqrt{(a+x)^2 - c}$, then we 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

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

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

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

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

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

Acknowledgments

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

References

[1] L.M. Adleman, The function field sieve, in: L.M. Adleman, M.-D. Huang (Eds.), Algorithmic Number Theory, ANTS-I, in: Lecture Notes in Comput. Sci., vol. 877, Springer-Verlag, Berlin, 1994, pp. 108–121.
[2] L.M. Adleman, M.-D. Huang, Function field method for discrete logarithms over finite fields, Inform. and Comput. 151 (1–2) (1999) 5–16.
[3] D.M. Gordon, Discrete logarithms in GF(p) using the number field sieve, SIAM J. Discrete Math. 6 (1) (1993) 124–138.
[4] Ming-Deh Huang, Wayne Raskind, Global duality, signature calculus and the discrete logarithm problem, LMS J. Comput. Math. 12 (2009) 228–263.
[5] Alfred J. Menezes, Tatsuaki Okamoto, Scott A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Trans. Inform. Theory 39 (5) (1993) 1639–1646.
[6] J.S. Milne, Étale Cohomology, Princeton Math. Ser., vol. 33, Princeton University Press, 1980.
[7] O. Schirokauer, Discrete logarithms and local units, in: R.C. Vaughan (Ed.), Theory and Applications of Numbers without Large Prime Factors, Philos. Trans. R. Soc. Lond. Ser. A 345 (1993) 409–423.
[8] O. Schirokauer, Using number fields to compute logarithms in finite fields, Math. Comp. 69 (231) (2000) 1267–1283.