The Function Field Sieve

Abhijit Das

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

CEP Course on Public-Key Cryptography
SAG, DRDO, New Delhi, 27-Sep-2013

Last revised on 18-May-2014

Section 1

THE FINITE-FIELD DISCRETE LOGARITHM PROBLEM (DLP)

What is DLP?

- Let $K = \mathbb{F}_q = \mathrm{GF}(q)$ be a finite field of size q.
- q can be a prime (p) or a power of a prime (p^n).
- The multiplicative group of K is $K^* = K \setminus \{0\}$.
- K^* is cyclic. Let g be a generator (or an element of large order) in K^*.
- DLP in K: Given $a \in K^*$, find an integer i such that $a = g^i$.
- i is called the *discrete logarithm* or *index* of a to the base g. It is unique modulo $q-1$ (or the order of g). We denote $i = \mathrm{ind}_g\, a$.
- DLP is apparently a difficult computational problem.
- Many cryptosystems derive their security from this apparent intractability of DLP.

Representation of Finite Fields

- Prime field $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$.
- Arithmetic in $\mathbb{F}_p$ is the integer arithmetic modulo the prime p.

- Extension fields $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/\langle f(x)\rangle$, where $f(x)$ is a (monic) *irreducible polynomial* of degree n in $\mathbb{F}_p[x]$.
- $\mathbb{F}_{p^n} = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_p\}$.
- The arithmetic of $\mathbb{F}_{p^n}$ is the polynomial arithmetic of $\mathbb{F}_p[x]$ modulo the *defining polynomial* $f(x)$.

- Extensions of extension fields $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/\langle f(x)\rangle$, where $f(x) \in \mathbb{F}_q[x]$ is monic, irreducible and of degree n. Here, $q = p^m$ for some prime p and $m \in \mathbb{N}$.
- $\mathbb{F}_{q^n} = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_q\}$.
- The arithmetic of $\mathbb{F}_{q^n}$ is the polynomial arithmetic of $\mathbb{F}_q[x]$ modulo the *defining polynomial* $f(x)$.

Algorithms for Solving DLP

Fully Exponential Algorithms

- Shanks' Baby-Step-Giant-Step (BSGS) method
- Pollard rho and lambda methods
- Pohlig-Hellman method

Subexponential Algorithms

- Based on the index calculus method
- Running times for $\mathbb{F}_q$ are of the form

$$L_q(\omega, c) = \exp\left[\Big(c + \mathrm{o}(1)\Big)(\log q)^{\omega}(\log\log q)^{1-\omega}\right],$$

where $c > 0$ and $0 < \omega < 1$.

- Smaller values of ω and c are desired.

Quasi-Polynomial Algorithms

- Running time $(\log q)^{\mathrm{O}(\log\log q)} = 2^{\mathrm{O}\left((\log\log q)^2\right)}$ for certain fields.

Variants of the Index Calculus Method

Slower variants ($\omega = 1/2$)

- Basic method
- Linear sieve method (LSM)
- Cubic sieve method (CSM)

Faster variants ($\omega = 1/3$)

- Coppersmith's method
- Number field sieve method (NFSM)
- Function field sieve method (FFSM)

Recent variants

- Joux–Lercier medium-prime case
- Joux's pinpointing method
- Barbulescu et al.'s quasi-polynomial method

Three Stages of the Index Calculus Method

- **Relation collection:** A set of *small* elements are chosen as the *factor base*. Linear congruences modulo $q - 1$ are generated involving the indices of the factor-base elements. This stage uses trial division, sieving or pinpointing.
- **Linear algebra:** The linear congruences obtained from the first stage are solved modulo $q - 1$. Sparse system solvers are used (like Lanczos method or Wiedemann method). The number of congruences should be sufficiently more than (like twice) the number of unknown indices of factor-base elements. This ensures that the system is of full or close-to-full rank.
- **Individual logarithms:** The desired index is expressed as a linear combination of the indices of the factor-base elements. Substituting the known indices (of the factor-base elements), we get the desired index.
- The first stage is usually the most time-consuming stage.

The Basic Method for Extension Fields

Assumption: $\mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_p[x]/\langle f(x)\rangle$ with p small (like $2, 3, 5$)

- We choose a smoothness bound $B \approx \sqrt{n}$.
- The factor base consists of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degrees $\leqslant B$.
- Compute $g^j \pmod{f(x)}$ for randomly chosen j. If this polynomial factors completely over the factor base, we get a relation

$$g^j \equiv p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \pmod{f(x)},$$

that is,

$$e_1 \operatorname{ind}_g p_1 + e_2 \operatorname{ind}_g p_2 + \cdots + e_t \operatorname{ind}_g p_t \equiv j \pmod{q-1}.$$

- The linear system of relations is solved to get the indices $\operatorname{ind}_g p_i$.
- For individual logarithm calculation, a single relation is generated:

$$a g^i \equiv p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t} \pmod{f(x)},$$

which gives

$$\operatorname{ind}_g a \equiv -i + f_1 \operatorname{ind}_g p_1 + f_2 \operatorname{ind}_g p_2 + \cdots + f_t \operatorname{ind}_g p_t \pmod{q-1}.$$

Passage from $\omega = 1/2$ to $\omega = 1/3$

- The running time of the basic method is $L_q(1/2, c)$.
- If we take a large B (smoothness bound), then getting each relation is easy, but we have to generate many relations to get a full-rank system.
- If we take a small B, then generating each relation needs many trials with random values of j.
- $B \approx \sqrt{n}$ gives the optimal performance for the basic method.
- The smoothness candidates are of degree $\approx n$.
- Some variants achieve better values of c by generating smoothness candidates of degrees about $n/2$ (LSM) or $n/3$ (CSM). But B is still about $\sqrt{n}$.
- Faster methods (Coppersmith, NFSM, FFSM) manage with $B \approx \sqrt[3]{n}$.
- Now, relations cannot be generated from factorizations of random g^j. This is where function fields play a critical role. A relation involves two smooth polynomials of degrees about $n^{2/3}$.
- Individual logarithm calculations need to be modified too, because random values of ag^i have little chance of being smooth over the factor base.

Analogy to the Number Field Sieve

- Both $\mathbb{Z}$ and $K[x]$ are Euclidean domains (and so principal ideal domains and so unique factorization domains and so normal domains). They share many algebraic properties.
- The field of fractions (the (total) quotient field) of $\mathbb{Z}$ and $K[x]$ are $\mathbb{Q}$ and $K(x)$, respectively.
- A finite algebraic extension L of $\mathbb{Q}$ is a **number field**, whereas a finite algebraic extension F of $K(x)$ is a **function field**.
- The NFS works in the integral closure $\mathfrak{O}_L$ of $\mathbb{Z}$ in L.
- If we work in the integral closure of $K[x]$ in F, we get an analog of NFS for DLP.
- FFS works in F itself (well, loosely speaking).
- The apparent similarity between NFS and FFS may be misleading.
- FFS produces faster algorithms than NFS in many situations.

Section 2

PROPERTIES OF ALGEBRAIC FUNCTION FIELDS

What is a Function Field?

Let K be an arbitrary field. We call it the **base field**. Only when necessary, we restrict the study to the case of finite fields $K = \mathbb{F}_p$ or $K = \mathbb{F}_q$.

- A **rational function field** over K is a field $K(x)$, where x is transcendental over K. It is the field of rational functions in one variable x.

$$K(x) = \left\{ \frac{g(x)}{h(x)} \;\middle|\; g(x), h(x) \in K[x],\ h(x) \neq 0 \right\}.$$

- An **(algebraic) function field** F over K is a finite (and therefore algebraic) extension of $K(x)$.
- For simplicity, we assume that the algebraic extension is simple. But then, there exists a polynomial

$$C(x,y) = \alpha_d(x)y^d + \alpha_{d-1}(x)y^{d-1} + \cdots + \alpha_1(x)y + \alpha_0(x) \in K(x)[y]$$

with $\alpha_d(x) \neq 0$ such that $F = K(x)[y]/\langle C(x,y)\rangle$.

- Without loss of generality, we can assume that each $\alpha_i \in K[x]$, so $C(x,y) \in K[x,y]$. If necessary, we will further assume that $\alpha_d = 1$ (this is loss of generality though).
- We require $C(x,y)$ to be *absolutely irreducible*, that is, irreducible in $\overline{K}[x,y]$, where $\overline{K}$ is the algebraic closure of K.

What is a Function Field?

- $C(x,y) = 0$ represents a plane curve. F is called the **function field** of C, denoted $F = K(C)$.
- $F = K(C) = \left\{ \beta_0(x) + \beta_1(x)y + \beta_2(x)y^2 + \cdots + \beta_{d-1}y^{d-1} \mid \beta_i(x) \in K(x) \right\}$.
- The arithmetic in F is the polynomial arithmetic of $K(x)[y]$ modulo the defining polynomial $C(x,y)$.
- **Unique factorization of non-zero elements in $K(x)$:** $\gamma(x) = a\prod_{i=1}^{t} p_i(x)^{e_i}$, where $a \in K^* = K \setminus \{0\}$, $t \geqslant 0$, $p_i(x)$ are pairwise distinct monic irreducible polynomials in $K[x]$, and $e_i \in \mathbb{Z}$.
- This notion of unique factorization is not carried to the case of general function fields $F = K(C)$. We cannot even clearly identify irreducible elements in F.
- Number rings are Dedekind domains where unique factorization holds at the level of ideals. Function fields are fields, so the notion of factorization at the level of ideals makes little sense.
- Despite that, we need to generate multiplicative relations in F. We have to take a new approach.

Field of Constants

Let $F = K(C)$ be a function field over K.

- $\hat{K} = \{\alpha \in F \mid \alpha \text{ is algebraic over } K\}$ is a field containing K.
- $\hat{K}$ is called the field of constants of F over K.
- $\hat{K}$ is a finite extension of K.
- The field of constants of the rational function field $K(x)$ is K itself.
- If $C(x,y)$ is absolutely irreducible, then $\hat{K} = K$.
- **Example:** Take $K = \mathbb{R}$ (or any prime field $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$). Since -1 does not have a square root in K, the polynomial $C(x,y) = x^2 + y^2$ is irreducible in $K[x]$. Take $F = K(C)$ for this C. Since $x, y \in K(C)$, and $K(C)$ is a field, the element $x/y \in K(C)$, that is, $\pm \mathrm{i} \in K(C)$. Here, $\hat{K} = K(\mathrm{i})$ and $[\hat{K} : K] = 2$. This happened because $C(x,y)$ is not absolutely irreducible. In $K[x,y]$, we have the factorization $C(x,y) = (x + \mathrm{i}y)(x - \mathrm{i}y)$.
- We assumed that $C(x,y)$ is absolutely irreducible. So we will henceforth assume that $\hat{K} = K$.

Valuations in Rational Function Fields

- Let $p(x)$ be a monic irreducible polynomial of $K[x]$.
- Every non-zero $\alpha(x) \in K(x)$ can be written as

$$\alpha(x) = p(x)^e \, \frac{g(x)}{h(x)},$$

with $g(x), h(x) \in K[x]$, $p(x) \not| \, g(x)h(x)$, and $e \in \mathbb{Z}$. We write $e = v_{p(x)}(\alpha(x))$.

- The function $v_{p(x)} : K(x)^* \to \mathbb{Z}$ is called the ***p*-adic valuation** of $K(x)$. It is a surjective group homomorphism.
- It is often convenient to take $v_p(0) = \infty$ with the convention that $m < \infty$, and $\infty + \infty = m + \infty = \infty + m = \infty$ for any $m \in \mathbb{Z}$.
- For any $\alpha(x), \beta(x) \in K(x)$, we then have

$$v_{p(x)}(\alpha(x)\beta(x)) = v_{p(x)}(\alpha(x)) + v_{p(x)}(\beta(x))$$

and

$$v_{p(x)}(\alpha(x) + \beta(x)) \geqslant \min\left(v_{p(x)}(\alpha(x)), v_{p(x)}(\beta(x))\right).$$

Moreover, if $v_{p(x)}(\alpha(x)) \neq v_{p(x)}(\beta(x))$, then

$$v_{p(x)}(\alpha(x) + \beta(x)) = \min\left(v_{p(x)}(\alpha(x)), v_{p(x)}(\beta(x))\right).$$

Valuation Rings of Rational Function Fields

- The valuation ring of $K(x)$ (with respect to $p(x)$) is defined as

$$\begin{aligned}\mathcal{O}_{p(x)} &= \left\{ \frac{g(x)}{h(x)} \;\middle|\; g(x), h(x) \in K[x],\ p(x) \nmid h(x) \right\} \\ &= \left\{ \alpha(x) \in K(x) \mid v_{p(x)}(\alpha(x)) \geqslant 0 \right\}.\end{aligned}$$

- For every $\alpha(x) \in K(x)^*$, either $\alpha(x) \in \mathcal{O}_{p(x)}$ or $\alpha(x)^{-1} \in \mathcal{O}_{p(x)}$ (or both).
- $\mathcal{O}_{p(x)}$ is a local ring with the unique maximal ideal

$$\begin{aligned}\mathfrak{p}_{p(x)} &= \left\{ \frac{g(x)}{h(x)} \;\middle|\; g(x), h(x) \in K[x],\ p(x) \mid g(x),\ p(x) \nmid h(x) \right\} \\ &= \left\{ \alpha(x) \in K(x) \mid v_{p(x)}(\alpha(x)) > 0 \right\}.\end{aligned}$$

- The group of units in $\mathcal{O}_{p(x)}$ is

$$\mathcal{O}_{p(x)}^* = \mathcal{O}_{p(x)} \setminus \mathfrak{p}_{p(x)} = \left\{ \alpha(x) \in K(x) \mid v_{p(x)}(\alpha(x)) = 0 \right\}.$$

- $\mathcal{O}_{p(x)}$ is a principal ideal domain. Its non-zero ideals are generated by $p(x)^m$ for $m \in \mathbb{N}$. The polynomial $p(x)$ itself generates $\mathfrak{p}_{p(x)}$.
- The map $\mathcal{O}_{p(x)}/\mathfrak{p}_{p(x)} \to K[x]/\langle p(x) \rangle$ taking $\alpha(x) + \mathfrak{p}_{p(x)} \mapsto \alpha(x) \operatorname{rem} p(x)$ is a field isomorphism. These fields have extension degree $\deg p(x)$ over K.

The Infinite Valuation of Rational Function Fields

- Let $\alpha(x) = g(x)/h(x) \neq 0$. We define the infinite valuation of $\alpha(x)$ as

$$v_\infty(\alpha(x)) = \deg h(x) - \deg g(x).$$

We also take $v_\infty(0) = \infty$.

- The corresponding valuation ring is

$$\begin{aligned} \mathcal{O}_\infty &= \left\{ \frac{g(x)}{h(x)} \;\middle|\; g(x), h(x) \in K[x],\ \deg g(x) \leqslant \deg h(x) \right\} \\ &= \{\alpha(x) \in K(x) \mid v_\infty(\alpha(x)) \geqslant 0\}. \end{aligned}$$

- $\mathcal{O}_\infty$ is a local ring with the unique maximal ideal

$$\begin{aligned} \mathfrak{p}_\infty &= \left\{ \frac{g(x)}{h(x)} \;\middle|\; g(x), h(x) \in K[x],\ \deg g(x) < \deg h(x) \right\} \\ &= \{\alpha(x) \in K(x) \mid v_\infty(\alpha(x)) > 0\}. \end{aligned}$$

- The group of units in $\mathcal{O}_\infty$ are

$$\mathcal{O}_\infty^* = \mathcal{O}_\infty \setminus \mathfrak{p}_\infty = \{\alpha(x) \in K(x) \mid v_\infty(\alpha(x)) = 0\}.$$

- $\mathcal{O}_\infty$ is a principal ideal domain with $\mathfrak{p}_\infty$ generated by $1/x$.

Zeros and Poles of Rational Functions

- Let $p(x)$ be a monic irreducible polynomial in $K[x]$, and $\alpha(x) \in K(x)$.
- If $v_{p(x)}(\alpha(x)) = m > 0$, then $p(x)$ is a zero of $\alpha(x)$ of order m.
- If $v_{p(x)}(\alpha(x)) = -m < 0$, then $p(x)$ is a pole of $\alpha(x)$ of order m.
- Zeros and poles at infinity are likewise defined in terms of the infinite valuation v_∞.
- A non-zero rational function $\alpha(x)$ has only finitely many zeros and poles.
- Let $\mathbb{P}$ denote the set of all monic irreducible polynomials in $K[x]$.
- For any non-zero rational function $\alpha(x)$, we have

$$\sum_{p \in \mathbb{P} \cup \{\infty\}} \Big[v_p(\alpha(x)) \deg p \Big] = 0.$$

The above sum is actually a sum of only finitely many non-zero terms. Here, $\deg \infty = 1$ (for the infinite valuation).

Places in a Function Field

- Much of the study made for rational function fields holds for arbitrary function fields $F = K(C) = K(x)[y]/\langle C(x,y)\rangle$.
- A **valuation ring** of F over K is a ring $\mathcal{O}$ satisfying the properties:
  1. $K \subsetneq \mathcal{O} \subsetneq F$.
  2. For every $\alpha(x,y) \in F$, either $\alpha(x,y) \in \mathcal{O}$ or $\alpha(x,y)^{-1} \in \mathcal{O}$ (or both).
- A function field contains infinitely many such valuation rings.
- $\mathcal{O}$ is a local ring with its unique maximal ideal $\mathfrak{p} = \mathcal{O} \setminus \mathcal{O}^*$, where $\mathcal{O}^*$ is the group of units in $\mathcal{O}$.
- $\mathfrak{p}$ is called a **place** in F. Let $\mathbb{P}$ denote the set of all places in F.
- The finite places in the rational function field $K(x)$ correspond to monic irreducible polynomials in $K[x]$, and the infinite place to $1/x$.
- For a general function field, we have to play with places.

Places in a Function Field

- Let $\mathcal{O}$ be a valuation ring of $F = K(C)$ with maximal ideal $\mathfrak{p}$.
- $\mathcal{O}$ is a principal ideal domain.
- A generator $p(x,y)$ of $\mathfrak{p}$ is called a **prime** or a **uniformizer** for $\mathfrak{p}$.
- The non-zero proper ideals of $\mathcal{O}$ are generated by $p(x,y)^m$ for $m \in \mathbb{N}$.
- Every non-zero $\alpha(x,y) \in F$ has a (unique) representation of the form $\alpha(x,y) = p(x,y)^e u(x,y)$ with $e \in \mathbb{Z}$ and $u(x,y) \in \mathcal{O}^*$. The value of e does not depend on the generator $p(x,y)$ of $\mathfrak{p}$.
- The **$\mathfrak{p}$-adic valuation** of F is the function $v_{\mathfrak{p}}(\alpha(x,y)) = e$ (where e is as above). We also take $v_{\mathfrak{p}}(0) = \infty$. For all $\alpha(x,y), \beta(x,y) \in F$, we have:

1. $v_{\mathfrak{p}}(\alpha(x,y)\beta(x,y)) = v_{\mathfrak{p}}(\alpha(x,y)) + v_{\mathfrak{p}}(\beta(x,y))$.
2. $v_{\mathfrak{p}}(\alpha(x,y)+\beta(x,y)) \geqslant \min(v_{\mathfrak{p}}(\alpha(x,y)), v_{\mathfrak{p}}(\beta(x,y)))$ with equality holding if $v_{\mathfrak{p}}(\alpha(x,y)) \neq v_{\mathfrak{p}}(\beta(x,y))$.
3. $v_{\mathfrak{p}}(\alpha(x,y)) \geqslant 0$ if and only if $\alpha(x,y) \in \mathcal{O}$.
4. $v_{\mathfrak{p}}(\alpha(x,y)) = 0$ if and only if $\alpha(x,y) \in \mathcal{O}^*$.
5. $v_{\mathfrak{p}}(\alpha(x,y)) > 0$ if and only if $\alpha(x,y) \in \mathfrak{p}$.
6. $v_{\mathfrak{p}}(\alpha(x,y)) = 1$ if and only if $\alpha(x,y)$ is a generator of $\mathfrak{p}$, that is, $\alpha(x,y) = u(x,y)p(x,y)$ for some $u(x,y) \in \mathcal{O}^*$.

Places in a Function Field

- Since $\mathfrak{p}$ is a maximal ideal in $\mathscr{O}$, the quotient ring $\mathscr{O}/\mathfrak{p}$ is a field.
- $\mathscr{O}/\mathfrak{p}$ is a finite extension of K.
- The extension degree $[(\mathscr{O}/\mathfrak{p}) : K]$ is called the **degree** of $\mathfrak{p}$, denoted $\deg \mathfrak{p}$.
- Let $\alpha(x,y) \in F$ be non-zero.
  - If $v_{\mathfrak{p}}(\alpha(x,y)) = m > 0$, then $\mathfrak{p}$ is called a **zero** of $\alpha(x,y)$ of order m.
  - If $v_{\mathfrak{p}}(\alpha(x,y)) = -m < 0$, then $\mathfrak{p}$ is called a **pole** of $\alpha(x,y)$ of order m.
- Every non-zero $\alpha(x,y) \in F$ has only finitely many poles and zeros.
- For every non-zero $\alpha(x,y) \in F$, we have

$$\sum_{\mathfrak{p} \in \mathbb{P}} \left[v_{\mathfrak{p}}(\alpha(x,y)) \deg \mathfrak{p} \right] = 0.$$

Here, $\mathbb{P}$ consists of all the finite and all the infinite places in F.

Relation between Places in $K(x)$ and Places in $K(C)$

- The finite places in $K(x)$ are in one-to-one correspondence with monic irreducible polynomials $p(x)$ of $K[x]$. They are the ideals $\langle p(x)\rangle = p(x)K[x]$. Let $\mathcal{O}_{p(x)}$ denote the valuation ring with respect to $p(x)$, $\mathfrak{p}_{p(x)}$ its maximal ideal and $v_{p(x)}$ the $p(x)$-adic valuation of $K(x)$.
- A place $\mathfrak{p}$ in F is said to **lie over** the irreducible polynomial $p(x)$ (or its ideal $\langle p(x)\rangle$ in $K[x]$) if $\langle p(x)\rangle \subseteq \mathfrak{p}$. Let $\mathcal{O}_{\mathfrak{p}}$ be the valuation ring with respect to $\mathfrak{p}$, and $v_{\mathfrak{p}}$ the corresponding $\mathfrak{p}$-adic valuation of $F = K(C)$.
- If $\mathfrak{p}$ lies over $p(x)$, we have the following:

1. $\mathcal{O}_{p(x)} \subseteq \mathcal{O}_{\mathfrak{p}}$.
2. $\mathfrak{p}_{p(x)} = \mathfrak{p} \cap K(x)$.
3. $\mathcal{O}_{p(x)} = \mathcal{O}_{\mathfrak{p}} \cap K(x)$.
4. There is a positive integer $e = e(\mathfrak{p}|p(x))$ such that $v_{\mathfrak{p}}(\alpha(x)) = e\, v_{p(x)}(\alpha(x))$ for all $\alpha(x) \in K(x)$. We call e the **ramification index** of $\mathfrak{p}$ over $p(x)$. If $e > 1$, we say that $\mathfrak{p}$ ramifies over $p(x)$. If $e = 1$, we say that $\mathfrak{p}$ does not ramify over $p(x)$.
5. The field $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ is a finite extension of $\mathcal{O}_{p(x)}/\mathfrak{p}_{p(x)}$. The extension degree is denoted by $d(\mathfrak{p}|p(x))$. It is sometimes called the **inertial degree** of $\mathfrak{p}$ over $p(x)$.

Places in $K(C)$ that Lie Over $p(x)$

Let $p(x)$ be a monic irreducible polynomial in $K[x]$. How can we find all the places $\mathfrak{p}$ of F that lie over $p(x)$?

Mathematical notes

- Every place $\mathfrak{p}$ of F lies on exactly one place $\mathfrak{p}_{p(x)}$ of $K(x)$. Indeed, $\mathfrak{p}_{p(x)} = \mathfrak{p} \cap K(x)$.
- Given a place $\mathfrak{p}_{p(x)}$ of $K(x)$ (that is, given a monic irreducible polynomial $p(x)$ in $K[x]$), there exist only finitely many (but at least one) places in F, that lie over $p(x)$.

Computational notes

- For simplicity, assume that $C(x,y) \in K[x,y]$ is monic in y.
- Consider the algebraic extension $L = K[x]/\langle p(x) \rangle$ of K. For example, if $K = \mathbb{F}_q$ and $\deg p(x) = \delta$, then $L = \mathbb{F}_{q^\delta}$.
- Treat $C(x,y) \in L[y]$, since x is now algebraic over K.
- Factor $C(x,y) = \pi_1^{e_1}(y)\pi_2^{e_2}(y)\cdots p_r^{e_r}(y)$ in $L[y]$, where $\pi_i(y)$ are monic (mutually distinct) irreducible polynomials in $L[y]$. Let $d_i = \deg \pi_i(y)$.
- Each $\pi_i(y)$ gives a place $\mathfrak{p}_i$ in F, that lies over $p(x)$. We have $e(\mathfrak{p}_i|p(x)) = e_i$ and $d(\mathfrak{p}_i|p(x)) = d_i$. These are the only places that lie over $p(x)$.
- If d is the y-degree of $C(x,y)$, we have $d = \sum_{i=1}^{r} e_i d_i = \sum_{i=1}^{r} e(\mathfrak{p}_i|p(x))d(\mathfrak{p}_i|p(x))$.

Places are Actually *Places*

- Let K be an *algebraically closed* field.
- Let $C(x,y) \in K[x,y]$ be an irreducible polynomial with y-degree d.
- The only irreducible polynomials of $K[x]$ are $p_a(x) = x - a$ with $a \in K$.
- Put $x = a$ in the equation for C to get $C(a,y) = 0$.
- $C(a,y)$ splits into linear factors.
- There are at most d solutions for y in $C(a,y) = 0$.
- For any solution b, we have a point (a,b) on C that lies over $p_a(x)$.
- Let v be the corresponding valuation of F.
- We have $v(x-a) > 0$ and $v(y-b) > 0$.
- We say the valuation v is **centered** at the point (a,b) on C.

Infinite Places

- Let K and C continue to be as in the last slide.
- $K(x)$ has a unique infinite place with uniformizer $1/x$.
- What are the places in $F = K(C)$ that lie over this infinite place?
- Let m be the x-degree of $C(x,y)$.
- Consider the curve $C_\infty(x,y) = x^m C(1/x,y)$.
- Points on C_∞ of the form $(0,b)$ stand for points at infinity on C.
- We determine all such points by solving $C(0,y) = 0$.
- For an infinite valuation v of $F = K(C)$ corresponding to the point $(0,b)$, we have $v(x) < 0$ (x has a zero at $(0,b)$ on C_∞ and so a pole on C at (∞,b)) and $v(y-b) > 0$.
- We say that the infinite valuation v is **centered** at $(0,b)$.

Divisors

- Let $\mathbb{P}$ be the set of all places in a function field F over K. We treat the elements of $\mathbb{P}$ as symbols. To highlight this fact, we write $[\mathfrak{p}]$ for $\mathfrak{p} \in \mathbb{P}$.
- A **divisor** is an integer-linear combination of the symbols of $\mathbb{P}$:
$$\sum_{\mathfrak{p} \in \mathbb{P}} n_{\mathfrak{p}} [\mathfrak{p}],$$
where all $n_{\mathfrak{p}} \in \mathbb{Z}$, and $n_{\mathfrak{p}} = 0$ except for only finitely many $\mathfrak{p} \in \mathbb{P}$.
- Two divisors are added as
$$\sum_{\mathfrak{p} \in \mathbb{P}} m_{\mathfrak{p}} [\mathfrak{p}] + \sum_{\mathfrak{p} \in \mathbb{P}} n_{\mathfrak{p}} [\mathfrak{p}] = \sum_{\mathfrak{p} \in \mathbb{P}} (m_{\mathfrak{p}} + n_{\mathfrak{p}}) [\mathfrak{p}].$$
- Under this operation, the set $\mathrm{Div}(F)$ of all divisors is an additive Abelian group.
- The identity of this group is the **zero divisor**
$$0 = \sum_{\mathfrak{p} \in \mathbb{P}} 0 [\mathfrak{p}].$$
- The additive inverse of a divisor is
$$- \sum_{\mathfrak{p} \in \mathbb{P}} n_{\mathfrak{p}} [\mathfrak{p}] = \sum_{\mathfrak{p} \in \mathbb{P}} (-n_{\mathfrak{p}}) [\mathfrak{p}].$$
- $\mathrm{Div}(F)$ is the free Abelian group generated by $\mathbb{P}$.

Degrees of Divisors

- The degree of the divisor $D = \sum_{\mathfrak{p} \in \mathbb{P}} n_{\mathfrak{p}} [\mathfrak{p}]$ is the integer

$$\deg D = \sum_{\mathfrak{p} \in \mathbb{P}} n_{\mathfrak{p}} \deg \mathfrak{p}.$$

  By definition, this is a sum of only finitely many non-zero terms.

- The function $\deg : \mathrm{Div}(F) \to \mathbb{Z}$ is a homomorphism of additive groups.

- The set of divisors of degree zero

$$\mathrm{Div}^0(F) = \{D \in \mathrm{Div}(F) \mid \deg D = 0\}$$

  is the kernel of the degree map, and is a subgroup of $\mathrm{Div}(F)$.

- Let $0 \neq \alpha(x,y) \in F$. The divisor of $\alpha(x,y)$ is

$$\mathrm{Div}(\alpha(x,y)) = \sum_{\mathfrak{p} \in \mathbb{P}} v_{\mathfrak{p}}(\alpha(x,y))[\mathfrak{p}].$$

  Such a divisor is called a **principal divisor**.

- The set of all principal divisors is denoted as $\mathrm{Prin}(F)$.

- $\mathrm{Prin}(F)$ is a subgroup of $\mathrm{Div}^0(F)$.

- As groups, we have $\mathrm{Prin}(F) \subseteq \mathrm{Div}^0(F) \subseteq \mathrm{Div}(F)$.

Class Groups and Class Numbers

- Two divisors $D_1, D_2 \in \mathrm{Div}(F)$ are said to be **equivalent**, denoted $D_1 \sim D_2$, if $D_1 = D_2 + \mathrm{Div}(\alpha(x,y))$ for some non-zero $\alpha(x,y) \in F$.
- $\sim$ is an equivalence relation on $\mathrm{Div}(F)$.
- The set of all equivalence classes of $\mathrm{Div}(F)$ under $\sim$ is called the **divisor class group** $\mathrm{Cl}(F)$ of F over K.
- $\mathrm{Cl}(F)$ is actually the quotient group $\mathrm{Div}(F)/\mathrm{Prin}(F)$.
- The degree-zero part of $\mathrm{Cl}(F)$ is likewise defined as $\mathrm{Cl}^0(F) = \mathrm{Div}^0(F)/\mathrm{Prin}(F)$.
- The size $h = h_F$ of $\mathrm{Cl}^0(F)$ is called the **class number** of F over K.
- If K is a finite field, then the class number of $F = K(C)$ is finite.

Principal Divisors

Let $0 \neq \alpha(x,y), \beta(x,y) \in F = K(C)$.

- $\mathrm{Div}(\alpha(x,y)\beta(x,y)) = \mathrm{Div}(\alpha(x,y)) + \mathrm{Div}(\beta(x,y))$.
- $\mathrm{Div}(\alpha(x,y)) = 0$ if and only if $\alpha(x,y) \in K^*$.
- Any $\alpha(x,y)$ transcendental over K has at least one zero and at least one pole.
- $\mathrm{Div}(\alpha(x,y)^{-1}) = -\mathrm{Div}(\alpha(x,y))$.
- $\mathrm{Div}(\alpha(x,y)) = \mathrm{Div}(\beta(x,y))$ if and only if $\alpha(x,y) = c\beta(x,y)$ for some $c \in K^*$.
- The function $\mathrm{Div} : F^* \to \mathrm{Prin}(F)$ is a group homomorphism.
- $\alpha(x,y)$ has no finite poles if and only if $\alpha(x,y) \in K[x,y]$.
- Let the class number h of F over K be finite, and let D be a divisor of degree zero. Then, hD is a principal divisor, that is, $hD = \mathrm{Div}(\gamma(x,y))$ for some non-zero $\gamma(x,y) \in K(C)$. The function $\gamma(x,y)$ is uniquely determined up to multiplication by non-zero elements of K.

Norms

- Let $C(x,y) = y^d + \alpha_{d-1}(x)y^{d-1} + \alpha_{d-2}(x)y^{d-2} + \cdots + \alpha_1(x)y + \alpha_0(x) \in K[x,y]$.
- Let $y_1, y_2, \ldots, y_d$ be the conjugates of y in $\bar{K}(C)$. Any one of these can be taken as $y \in K(C)$. They are algebraically indistinguishable from one another.
- $C(x,y) = (y-y_1)(y-y_2)\cdots(y-y_d)$.
- Let $\alpha(x,y) \in K(C)$.
- Let the minimal polynomial of α over $K(x)$ have degree t. We have $t|d$.
- Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be the conjugates of α.
- The **norm** of α as an element of F over K is defined as
$$\mathrm{N}(\alpha) = \mathrm{N}_{F|K}(\alpha) = (\alpha_1\alpha_2\cdots\alpha_t)^{d/t}.$$
- We have $\mathrm{N}(\alpha) \in K(x)$. Moreover, if α is integral over $K[x]$ (that is, the minimal polynomial of α is a monic polynomial in $K[x]$), then $\mathrm{N}(\alpha) \in K[x]$.

Norms of Linear Elements

- Let $\alpha(x,y) = r(x)y + s(x)$ with $r(x), s(x) \in K[x]$, $r(x) \neq 0$.
- All the conjugates of α in $\bar{K}(C)$ are $\alpha_i = r(x)y_i + s(x)$ for $i = 1, 2, \ldots, d$.
- The minimal polynomial of α is therefore $(y-\alpha_1)(y-\alpha_2)\cdots(y-\alpha_d) \in K[x,y]$.
- The norm of $\alpha(x,y)$ is

$$\begin{aligned} \mathrm{N}(\alpha(x,y)) &= \prod_{i=1}^{d} \alpha_i = \prod_{i=1}^{d} (r(x)y_i + s(x)) = (-r(x))^d \prod_{i=1}^{d} \Big(\big(-s(x)/r(x) \big) - y_i \Big) \\ &= (-r(x))^d C(x, -s(x)/r(x)) \in K[x]. \end{aligned}$$

- Since $\alpha(x,y) \in K[x,y]$, it has no finite poles.
- All the zeros of $\alpha(x,y)$ lie over zeros of $\mathrm{N}(\alpha(x,y))$.
- We factor $\mathrm{N}(\alpha(x,y))$ (or equivalently $r^d C(x, -s/r)$) in $K[x]$.
- For each irreducible factor $p(x)$ of $\mathrm{N}(\alpha(x,y))$, we look at all the places $\mathfrak{p}$ of F that lie over $p(x)$.
- All such $\mathfrak{p}$ need not be zeros of $\alpha(x,y)$. Indeed, $\alpha(x,y)$ has a zero at $\mathfrak{p}$ if and only if $v_{\mathfrak{p}}(\alpha) > 0$. This would give us $\mathrm{Div}(\alpha(x,y))$.

Section 3

THE ADLEMAN–HUANG VARIANT OF THE FUNCTION FIELD SIEVE METHOD (THE SMALL PRIME CASE)

Setup: Polynomial Selection

To compute discrete logarithms in $\mathbb{F}_{p^n}$ with p small. The base field is $K = \mathbb{F}_p$.

- Choose a monic irreducible polynomial $f(x) = x^n + f_1(x) \in K[x]$ with $\deg f_1(x) < n^{2/3}$. Represent $\mathbb{F}_{p^n}[x] = \mathbb{F}_p[x]/\langle f(x)\rangle$.
- Let $d \approx n^{1/3}$ and $d' = \lceil n/d \rceil \approx n^{2/3}$. Choose a monic $m(x) \in K[x]$ of degree d'.
- Choose a plane curve $C(x,y) = 0$ defined over $K = \mathbb{F}_p$ such that the substitution $y = m(x)$ gives $C(x, m(x)) \equiv 0 \pmod{f(x)}$.
- Let $dd' = n + \delta$ with $\delta < d$. We have

$$x^\delta f(x) = m(x)^d + \alpha_{d-1}(x)m(x)^{d-1} + \alpha_{d-2}(x)m(x)^{d-2} + \cdots + \alpha_1(x)m(x) + \alpha_0(x)$$

with $\alpha_i(x) \in K[x]$ and $\deg \alpha_i(x) < d'$ for all $i = 0, 1, 2, \ldots, d-1$. Take the curve

$$C(x,y) = y^d + \alpha_{d-1}(x)y^{d-1} + \alpha_{d-2}(x)y^{d-2} + \cdots + \alpha_1(x)y + \alpha_0(x) \in K[x,y].$$

We have $C(x, m(x)) \equiv x^\delta f(x) \equiv 0 \pmod{f(x)}$ as required.

- **Example construction**
  - Take $m(x) = x^{d'}$. This implies $C(x,y) = y^d + x^\delta f_1(x)$.
  - Try random $f_1(x)$ until one with at least one simple root is found and $f(x) = x^n + f_1(x)$ is irreducible in $K[x]$. These choices guarantee that $C(x,y)$ is absolutely irreducible.
  - We need the class number h of $F = K(C)$ over K to be coprime to $(p^n - 1)/(p-1)$. No known easy check ensures this. So we assume that this condition holds. If the algorithm fails, we retry with a different $f_1(x)$.

Setup: Factor Base

- We choose a smoothness bound $B \approx n^{1/3}$.
- The factor base consists of two parts.
- The first part $S = \{p_1(x), p_2(x), \ldots, p_t(x)\}$ contains all monic irreducible polynomials of $K[x]$ of degrees $\leqslant B$.
- Let $\mathfrak{p}$ be a place in $K(C)$ that lies over some $p_i(x) \in S$. Choose any fixed place $\mathfrak{q}$ of degree one in $K(C)$. Then, the divisor $D = [\mathfrak{p}] - (\deg \mathfrak{p})[\mathfrak{q}]$ is of degree zero, that is, hD is a principal divisor, that is, $hD = \mathrm{Div}(\mu(x,y))$ for some $\mu(x,y) \in K(C)$. This function $\mu(x,y)$ is uniquely determined up to multiplication by elements of K^*.
- The second part $S' = \{\mu_1(x,y), \mu_2(x,y), \ldots, \mu_T(x,y)\}$ contains all functions $\mu_j(x,y)$ constructed as above from all the places lying over all the irreducible polynomials of S. Additionally, S' contains functions constructed from all the infinite places of $F = K(C)$.
- We do not need these functions explicitly. We will instead work only with their indices (not exactly, see later).
- Let μ_j be constructed from the place $\mathfrak{p}_j$. Denote by $v_{\mathfrak{p}_j}$ the corresponding $\mathfrak{p}_j$-adic valuation. We require the capability to compute these valuations for functions of a particular form.

Relation Generation

- Choose random polynomials $r(x), s(x) \in K[x]$ of degree about $n^{1/3}$.
- Both $r(x)m(x)+s(x)$ and $r(x)y+s(x)$ should be smooth.
- $r(x)m(x)+s(x)$ is smooth if and only if it factors completely over the irreducible polynomials in S:

$$r(x)m(x)+s(x) = \prod_{i=1}^{t} p_i(x)^{e_i}.$$

- $r(x)y+s(x)$ is smooth if and only if its norm factors completely over S. If so, we compute $a_j = v_{\mathfrak{p}_j}(r(x)y+s(x))$ for $j = 1, 2, \ldots, T$. We have $\sum_{j=1}^{T} a_j \deg \mathfrak{p}_j = 0$, and

$$\mathrm{Div}(r(x)y+s(x)) = \sum_{j=1}^{T} a_j [\mathfrak{p}_j] = \sum_{j=1}^{T} a_j [\mathfrak{p}_j] - \left(\sum_{j=1}^{T} a_j \deg \mathfrak{p}_j \right) [\mathfrak{q}] = \sum_{j=1}^{T} a_j \Big([\mathfrak{p}_j] - \deg \mathfrak{p}_j [\mathfrak{q}] \Big).$$

Therefore,

$$\mathrm{Div}\left((r(x)y+s(x))^h \right) = \mathrm{Div}\left(\prod_{j=1}^{T} \mu_j(x,y)^{a_j} \right),$$

that is,

$$\big(r(x)y+s(x)\big)^h = c \prod_{j=1}^{T} \mu_j(x,y)^{a_j}$$

for some $c \in K^*$.

The Homomorphism ϕ

- Define $\phi : K[x,y]/C(x,y) \to K[x]/\langle f(x)\rangle$ by $y \mapsto m(x)$.
- The integral domain $K[x,y]/C(x,y)$ is not the same as $K(C) = K(x)[y]/\langle C(x,y)\rangle$. Adleman and Huang prove that $\phi(\mu_j)$ is defined for all $\mu_j \in S'$.
- Apply ϕ to the multiplicative relation involving $r(x)y + s(x)$ to get

$$\phi\left(\left(r(x)y + s(x)\right)^h\right) = \left(r(x)m(x) + s(x)\right)^h = c\prod_{j=1}^{T}\phi(\mu_j(x,y))^{a_j} \in \mathbb{F}_{p^n}.$$

- Since $c \in \mathbb{F}_p^*$, we have $c^{p-1} = 1$ (by Fermat's little theorem). This gives

$$\left(r(x)m(x) + s(x)\right)^{(p-1)h} = \prod_{i=1}^{t} p_i(x)^{(p-1)he_i} = \prod_{j=1}^{T}\phi(\mu_j(x,y))^{(p-1)a_j} \in \mathbb{F}_{p^n}.$$

- Taking discrete logarithm to a base $g(x)$ gives

$$(p-1)h\sum_{i=1}^{t} e_i \operatorname{ind}_{g(x)} p_i(x) \equiv (p-1)\sum_{j=1}^{T} a_j \operatorname{ind}_{g(x)}\left(\phi(\mu_j(x,y))\right) \pmod{p^n - 1},$$

that is,

$$h\sum_{i=1}^{t} e_i \operatorname{ind}_{g(x)} p_i(x) \equiv \sum_{j=1}^{T} a_j \operatorname{ind}_{g(x)}\left(\phi(\mu_j(x,y))\right) \pmod{(p^n - 1)/(p-1)}.$$

A Relation Finally

- Assume that $\gcd(h,(p^n-1)/(p-1))=1$. Then, we have

$$\sum_{i=1}^{t} e_i \operatorname{ind}_{g(x)} p_i(x) \equiv \sum_{j=1}^{T} a_j \left[h^{-1} \operatorname{ind}_{g(x)} \left(\phi(\mu_j(x,y)) \right) \right] \pmod{(p^n-1)/(p-1)}.$$

- Let us denote $w_i \equiv \operatorname{ind}_{g(x)} p_i(x) \pmod{(p^n-1)/(p-1)}$ for $i=1,2,\ldots,t$, and $z_j \equiv h^{-1} \operatorname{ind}_{g(x)} \left(\phi(\mu_j(x,y)) \right) \pmod{(p^n-1)/(p-1)}$ for $j=1,2,\ldots,T$.
- Then, we have the linear congruence in $t+T$ variables:

$$\sum_{i=1}^{t} e_i w_i \equiv \sum_{j=1}^{T} a_j z_j \pmod{(p^n-1)/(p-1)}.$$

- Assume that $g(x)=p_i(x)$ for some $i=1,2,\ldots,t$. We then get the dehomogenizing relation $w_i \equiv 1 \pmod{(p^n-1)/(p-1)}$.
- All collected relations are solved modulo $(p^n-1)/(p-1)$.
- Since p is small, the correct values of w_i and z_j modulo p^n-1 can be obtained by looking at the $p-1$ possibilities of each.

More about the Adleman–Huang Algorithm

Two questions remain unanswered from the exposition given so far.

1. *How can we compute* $a_j = v_{\mathfrak{p}_j}(r(x)y + s(x))$*?*

Adleman and Huang propose the **Newton polygon method** to solve this problem. It involves some power series calculations and can be done in time polynomial in n.

2. *What about individual logarithm calculations?*

The factors base S now contains too few primes to make a randomly chosen $g^j a$ smooth over S with a decent probability. Moreover, it is not clear how the indices corresponding to the elements of S' can be used in this stage.

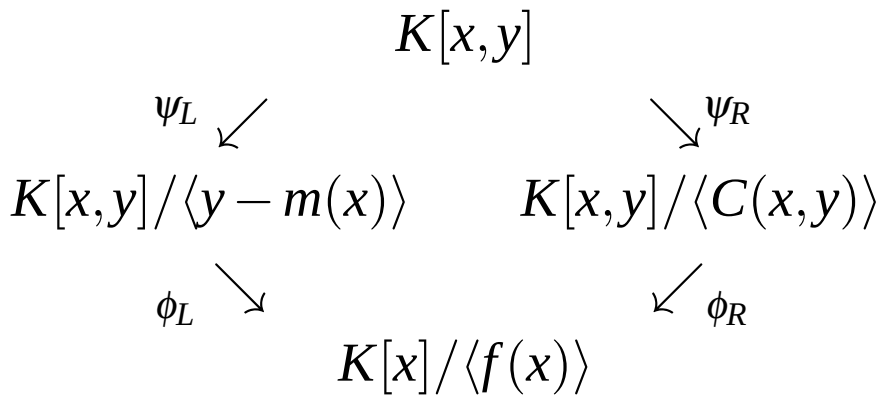
A common way to get around this difficulty is to use some kind of **descent**. Factor $g^j a$ into irreducible polynomials of moderate degrees. Express each polynomial of moderate degree as a product of two or more polynomials of smaller degrees (modulo $f(x)$, of course). Repeat until the polynomials reduce to those in S.

Section 4

THE JOUX–LERCIER VARIANT OF THE FUNCTION FIELD SIEVE METHOD (THE MEDIUM PRIME CASE)

A Renewed Look at the Adleman–Huang Algorithm

- Consider the following commutative diagram.



- On the left, we first set $y = m(x)$ via ψ_L. Then, we put $C(x,y) = 0$ (this is ϕ_L). But $y = m(x)$, so putting $C(x,m(x)) = 0$ essentially means reduction modulo $f(x)$.
- On the right,we first put $C(x,y) = 0$ (this is ψ_R) and then we put $y = m(x)$ modulo $f(x)$ (this is ϕ_R or ϕ).
- For $u(x,y) \in K[x,y]$, we get the same object $\phi_L(\psi_L(u(x,y))) = \phi_R(\psi_R(u(x,y)))$.
- For the special case $u(x,y) = r(x)y + s(x)$, the left side **(linear side)** gives $r(x)m(x) + s(x) \pmod{f(x)}$.
- The right side **(algebraic side)** involves working in the function field $K(C)$.
- Joux and Lercier propose $C(x,y)$ of a very specific form so that both sides behave as the linear side, and function field computations are eliminated altogether.

Setup: Polynomial Selection and Factor Base

- Let $K = \mathbb{F}_q$ be the base field. We want to compute indices in $\mathbb{F}_Q$, where $Q = q^n$. Note that q may already be a prime power. The Joux–Lercier method is effective when q is medium-sized.
- Two polynomial relations in x, y give two different representations of $\mathbb{F}_Q$:

$$x = m_1(y) \text{ and } y = m_2(x).$$

Let $d_1 = \deg m_1(x)$ and $d_2 = \deg m_2(y)$ with $d_1 d_2 \geqslant n$.

- We now have the commutative diagram:

$$\begin{array}{ccc} & \mathbb{F}_q[x,y] & \\ {\scriptstyle x = m_1(y)} \swarrow & & \searrow {\scriptstyle y = m_2(x)} \\ \mathbb{F}_q[x,y]/\langle x - m_1(y)\rangle & & \mathbb{F}_q[x,y]/\langle y - m_2(x)\rangle \\ {\scriptstyle y = m_2(x)} \searrow & & \swarrow {\scriptstyle x = m_1(y)} \\ & \mathbb{F}_Q = \mathbb{F}_{q^n} & \end{array}$$

- We have $x = m_1(y) = m_1(m_2(x))$. Let $f(x)$ be a monic irreducible polynomial of degree n with $f(x) | [m_1(m_2(x)) - x]$. This gives $\mathbb{F}_Q = \mathbb{F}_q[x]/\langle f(x)\rangle$.
- Similarly, $y = m_2(x) = m_2(m_1(y))$. The minimal polynomial of $y = m_2(x) \in \mathbb{F}_Q$ over $\mathbb{F}_q$ must be of degree n and must divide $m_2(m_1(y)) - y$.
- The factor base consists of the $2q$ elements $x + a$ and $y + a$ for all $a \in \mathbb{F}_q$.

Relation

- Let $u(x,y) \in \mathbb{F}_q[x,y]$.
- The left side gives $u(x, m_2(x))$, whereas the right side gives $u(m_1(y), y)$. Since the diagram is commutative, these two elements are equal.
- Take $u(x,y) = r(x)y + s(x)$ with linear polynomials $r(x), s(x) \in \mathbb{F}_q[x]$.
- We have the equality in $\mathbb{F}_Q$:

$$r(x)m_2(x) + s(x) = r(m_1(y))y + s(m_1(y)).$$

The left side is a polynomial of degree $d_2 + 1$ and the right side is a polynomial of degree $d_1 + 1$.

- If both sides split into linear factors, we have

$$(x+a_1)(x+a_2)\cdots(x+a_{d_2+1}) = \lambda(y+b_1)(y+b_2)\cdots(y+b_{d_1+1})$$

for some $\lambda \in \mathbb{F}_q^*$.

- Taking logarithm gives

$$\begin{aligned} & \operatorname{ind}_g(x+a_1) + \operatorname{ind}_g(x+a_2) + \cdots + \operatorname{ind}_g(x+a_{d_2+1}) \\ \equiv\ & \operatorname{ind}_g \lambda + \operatorname{ind}_g(y+b_1) + \operatorname{ind}_g(y+b_2) + \cdots + \operatorname{ind}_g(y+b_{d_1+1}) \pmod{Q-1}, \end{aligned}$$

or

$$\begin{aligned} & \operatorname{ind}_g(x+a_1) + \operatorname{ind}_g(x+a_2) + \cdots + \operatorname{ind}_g(x+a_{d_2+1}) \\ \equiv\ & \operatorname{ind}_g(y+b_1) + \operatorname{ind}_g(y+b_2) + \cdots + \operatorname{ind}_g(y+b_{d_1+1}) \pmod{(Q-1)/(q-1)}. \end{aligned}$$

Why Medium Prime?

- **Parasitic solutions:** Each relation is satisfied if we set $\mathrm{ind}_g(x+a) = d_1+1$ and $\mathrm{ind}_g(y+a) = d_2+1$ for all $a \in \mathbb{F}_q$.
- Suppose that there exists an $a \in \mathbb{F}_q$ for which $y+a = m_2(x)+a$ splits into linear factors (in x). This removes the obvious parasitic solutions.
- The size of the factor base is $2q$. We need at least as many relations.
- The probability that a polynomial of degree d splits into linear factors is about $1/d!$. Therefore, $r(x)m_2(x)+s(x)$ and $r(m_1(y))y+s(m_1(y))$ are simultaneously smooth with probability about $1/((d_1+1)!(d_2+1)!)$.
- We take $r(x) = wx+1$ and $s(x) = ux+v$ with $w,u,v \in \mathbb{F}_q$. So we must have

$$q^3/((d_1+1)!(d_2+1)!) \geqslant 2q,$$

that is,

$$q^2 \geqslant 2(d_1+1)!(d_2+1)!.$$

- If we take $r(x) = 1$ and $s(x) = ux+v$, we require

$$q \geqslant 2(d_1+1)!(d_2+1)!.$$

- Removal of parasitic solutions requires $q > (d_1+1)!(d_2+1)!$.
- Good choice: $d_1 \approx d_2 \approx \sqrt{n}$.

Working with Smaller Medium Primes

- So far, the factor base consists of only linear polynomials. Also, $r(x), s(x)$ are taken as linear polynomials.
- Now, we introduce a smoothness bound B, and take $d_1 \approx \sqrt{n/B}$ and $d_2 \approx \sqrt{Bn}$.
- Choose $r(x), s(x)$ as polynomials of degrees $\leqslant B$.
- $r(x)m_2(x) + s(x)$ is of degree $\leqslant d_2 + B \approx \sqrt{Bn} + B$.
- $r(m_1(y))y + s(m_1(y))$ is of degree $\leqslant Bd_1 + 1 \approx \sqrt{Bn} + 1$.
- If $B \ll n$, both these degrees are approximately $\sqrt{Bn}$.
- The factor base consists of all monic irreducible polynomials in x and y of degrees $\leqslant B$. There are at most $2q^B$ such polynomials.
- Total size of the sieving space is q^{2B+1}.
- The smoothness probability (of two sides together) is $\exp(-\sqrt{n/B}\ln(n/B))$.
- In order to get sufficiently many relations, we require $(B+1)\ln q \geqslant \sqrt{n/B}\ln(n/B)$.

Section 5

JOUX'S PINPOINTING ALGORITHM FOR THE MEDIUM PRIME CASE

One-Sided Pinpointing

- For simplicity, let us restrict to $B = 1$.
- Take $x = y^{d_1}$ and $y = m(x)$, where $m(x) \in \mathbb{F}_q[x]$ is of degree d_2.
- For $r(x) = x + b$ and $s(x) = ax + c$, we now have the equality in $\mathbb{F}_Q$:

$$r(x)y + s(x) = y^{d_1+1} + ay^{d_1} + by + c = xm(x) + ax + bm(x) + c.$$

- Look at the y side. Find a single polynomial of the form $u^{d_1+1} + u^{d_1} + By + C$ that decomposes completely into linear factors in $\mathbb{F}_q[u]$. We need to try about $(d_1+1)!$ random values of $B, C \in \mathbb{F}_q$. This can be done by trial division or sieving.
- For each $a \in \mathbb{F}_q^*$, substitute $u = y/a$ to get the polynomial $y^{d_1+1} + ay^{d_1} + by + c$, where $b = Ba^{d_1}$ and $c = Ca^{d_1+1}$. Each of these polynomials decomposes into linear factors in $\mathbb{F}_q[y]$. For about $(q-1)/(d_2+1)!$ choices of a, the x side is smooth too.
- Get one relation with some effort. Get many other relations for free.
- Efficiency increases by a factor of $\geqslant \frac{1}{2}\min(q-1, (d_1+1)!)$.

Kummer Extensions

- Let $n = d_1 d_2 - 1$.
- Assume that $\mathbb{F}_q$ contains all the n-th roots of unity.
- Choose $\kappa \in \mathbb{F}_q$ such that $f(x) = x^n - \kappa$ is irreducible in $\mathbb{F}_q[x]$. Define the extension $\mathbb{F}_Q = \mathbb{F}_{q^n} = \mathbb{F}_q[x]/\langle f(x) \rangle$.
- $x^n = \kappa$ in $\mathbb{F}_Q$, so $(x^q)^n = \kappa^q = \kappa$, that is, x^q is again a root of $f(X) = X^n - \kappa$. Therefore, there exists a primitive root μ of unity in $\mathbb{F}_q$ such that $x^q = \mu x$.

  (**Note:** $X^n - \kappa = (X - \mu_1 x)(X - \mu_2 x) \cdots (X - \mu_n x)$, where $\mu_1, \mu_2, \ldots, \mu_n \in \mathbb{F}_q$ are the n-th roots of unity. Furthermore, the root μ with $x^q = \mu x$ must be primitive. If not, let $\mu^m = 1$ for some $m < n$. But then, $(x^q)^m = x^m$, that is, $(x^m)^{q-1} = 1$, that is, $x^m \in \mathbb{F}_q$, a contradiction to that $f(X) = X^n - \kappa$ is the minimal polynomial of x.)
- Take $x = y^{d_1}/\kappa$ and $y = x^{d_2}$. Then, $x^{d_1 d_2} - \kappa x = 0$, that is, $xf(x) = 0$, as required.

Reduction in the Size of the Factor Base

- Take $a \in \mathbb{F}_q^*$.
- We have $(x+a)^{q^i} = x^{q^i} + a = \mu^i x + a = \mu^i (x + a/\mu^i)$ for all $i = 0, 1, 2, \ldots, n-1$.
- Therefore, $\operatorname{ind}_g(x + a/\mu^i) \equiv q^i \operatorname{ind}_g(x+a) \pmod{(Q-1)/(q-1)}$.
- Since $n = d_1 d_2 - 1$, we have $\gcd(n, d_2) = 1$, that is, $\mu' = \mu^{d_2}$ is again a primitive root of unity in $\mathbb{F}_q$.
- We have $y = x^{d_2}$, so $y^q = x^{d_2 q} = (x^q)^{d_2} = (\mu x)^{d_2} = \mu^{d_2} y$, that is, $y^q = \mu' y$.
- Therefore, $\operatorname{ind}_g(y + a/(\mu')^i) \equiv q^i \operatorname{ind}_g(y+a) \pmod{(Q-1)/(q-1)}$ for all $i = 0, 1, 2, \ldots, n-1$.
- These free relations reduce the number of unknown indices (of the elements of the factor base) by roughly a factor of n.
- Now, take $a = 0$. Since $x^n = \kappa \in \mathbb{F}_q$, we have $(x^n)^{q-1} = 1$, that is, $n \operatorname{ind}_g x \equiv 0 \pmod{(Q-1)/(q-1)}$. If, in addition, n is coprime to $(Q-1)/(q-1)$, then $\operatorname{ind}_g x \equiv 0 \pmod{(Q-1)/(q-1)}$. Likewise, $\operatorname{ind}_g y \equiv 0 \pmod{(Q-1)/(q-1)}$.

Two-Sided Pinpointing

- An equation of the form $r(x)y+s(x)$ now has the form
$$xy+ay+bx+c=x^{d_2+1}+ax^{d_2}+bx+c=y^{d_1+1}/\kappa+by^{d_1}/\kappa+ay+c.$$
- Choose a triple (A,B,λ) with $A\neq 0$, $B\neq 0$, and BA^{d_1} an n-th power in $\mathbb{F}_q$. Suppose that both the polynomials $u^{d_2+1}+u^{d_2}+A(u+\lambda)$ and $(v^{d_1+1}+v^{d_1})/\kappa+B(v+\lambda)$ split into linear factors.
- Now, substitute $u=x/a$ and $v=y/b$ to get the polynomials $x^{d_2+1}+ax^{d_2}+Aa^{d_2}x+Aa^{d_2+1}\lambda$ and $y^{d_1+1}/\kappa+by^{d_1}/\kappa+Bb^{d_1}y+Bb^{d_1+1}\lambda$ which split completely into linear factors.
- In order that these two polynomials are of the desired form, we must have $Aa^{d_2}=b$, $Bb^{d_1}=a$, $Aa^{d_2+1}\lambda=Bb^{d_1+1}\lambda=ab\lambda=c$.
- Eliminating b from the first two equations give $a^{d_1d_2-1}=a^n=1/(BA^{d_1})$. Thus, we take as a any n-th root of $1/(BA^{d_1})$, and get $b=Aa^{d_2}$ and $c=ab\lambda$.
- Different choices for a (as the n-th root) give the same equation because of the action of the q-th power Frobenius map.

Other Extensions of Pinpointing

- The Kummer extension with $n = d_1 d_2 + 1$ can be analogously handled using $x = \kappa / y^{d_1}$ and $y = x^{d_2}$.
- Both one-sided and two-sided pinpointing can be generalized to the case $B > 1$.
- For example, the polynomial $x^d + \sum_{i=0}^{d-1} a_i x^i$ decomposes into factors of degrees $\leqslant B$ if and only if the polynomial $u^d + u^{d-1} + \sum_{i=0}^{d-2} a_i a_{d-1}^{d-i} u^i$ decomposes into factors of degrees $\leqslant B$.
- The substitution $u = x / a_{d-1}$ will now do the trick.

Section 6

BEYOND PINPOINTING:
A QUASI-POLYNOMIAL ALGORITHM

The BGJT Algorithm

- Proposed by Barbulescu, Gaudry, Joux and Thomé (eprint 2013/400).
- Joux's algorithm takes $L(1/4+\varepsilon)$ time for small characteristic.
- To compute discrete logarithms in $\mathbb{F}_Q$, embed $\mathbb{F}_Q$ in a field $\mathbb{F}_{q^{2k}}$ with $q \approx k$.
- $\mathbb{F}_q^2$ acts as the medium subfield. We use two polynomials $m_1(x)$ and $m_2(x)$ for representing $\mathbb{F}_{q^{2k}}$ over $\mathbb{F}_{q^2}$. We take x^q congruent to $m_1(x)/m_2(x)$ modulo the defining polynomial.
- In many cases, the running time is $n^{\mathrm{O}(\log n)} = 2^{\mathrm{O}(\log^2 n)}$, where n is the bit size of Q.
- The basic innovation is an efficient descent algorithm for calculating individual discrete logarithms.
- The same descent algorithm applies to the relation-generation phase too.
- To compute the index of $P(x) \in \mathbb{F}_{q^2}(x)$ with $D = \deg P$ satisfying $1 \leqslant D \leqslant k-1$.
- Express $\operatorname{ind} P$ as a linear combination of $\operatorname{ind} m_2$ and a few $\operatorname{ind} P_i$, $\deg P_i \leqslant \lceil D/2 \rceil$.
- During relation generation, $D = 1$, that is, each P_i is a linear polynomial.

Homographic Action

- Take a matrix with entries from $\mathbb{F}_{q^2}$:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

- M acts on P as

$$M \cdot P = \frac{aP + b}{cP + d}.$$

- The action is trivial if $a, b, c, d \in \mathbb{F}_q$, so we actually take M from

$$\mathscr{P}_q = \mathrm{PGL}(\mathbb{F}_q^2)/\mathrm{PGL}(\mathbb{F}_q),$$

where PGL stands for the projective general linear group of invertible 2×2 matrices.

Systematic Equation

- We have $x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$.
- Take the projective line $\mathbb{P}^1(\mathbb{F}_q)$ (all the points $(a:1)$ with $a \in \mathbb{F}_q$ and the point $(1:0)$ at infinity).
- Choose a set of representatives $\mathscr{S}$ of the $q+1$ points such that

$$x^q y - x y^q = \prod_{(\alpha,\beta) \in \mathscr{S}} (\beta x - \alpha y).$$

- Apply the homography $M \in \mathscr{P}_q$ to get:

$$\begin{aligned}
(aP+b)^q(cP+d) - (aP+b)(cP+d)^q &= \prod_{(\alpha,\beta)\in\mathscr{S}} [\beta(aP+b) - \alpha(cP+d)] \\
&= \prod_{(\alpha,\beta)\in\mathscr{S}} [(a\beta - c\alpha)P - (d\alpha - b\beta)] \\
&= \lambda \prod_{(\alpha,\beta)\in\mathscr{S}} \left[P - x\left(M^{-1}\cdot(\alpha:\beta)\right)\right],
\end{aligned}$$

where $\lambda \in \mathbb{F}_{q^2}^*$, and $x\left(M^{-1}\cdot(\alpha:\beta)\right)$ is $\frac{d\alpha - b\beta}{a\beta - c\alpha}$ if the point is finite or 1 for the point at infinity.

Relations

- The right-hand side is a product of $q+1$ translates of P by elements of $\mathbb{F}_{q^2}$.
- Let $\overline{P}(x)$ be $P(x)$ with all coefficients raised to the q-th power.
- Since $x^q = m_1(x)/m_2(x)$ in $\mathbb{F}_{q^{2k}}$, the left-hand side becomes

$$(a^q\overline{P}(m_1/m_2)+b^q)(cP+d)-(aP+b)(c^q\overline{P}(m_1/m_2)+d^q).$$

- The denominator is a power of $m_2(x)$.
- The numerator is of degree $\leqslant (1+\delta)D$, where $\delta = \max(\deg m_1, \deg m_2)$.
- We get a relation if the numerator is $\lceil D/2 \rceil$-smooth.
- By varying $M \in \mathscr{P}_q$, we hope to generate a full-rank system involving the q^2+1 translates of P as variables.
- This gives $\operatorname{ind} P$ as a linear combination of $\operatorname{ind} m_2$ and $\mathrm{O}(q^2 D)$ indices of polynomials P_i of degrees $\leqslant \lceil D/2 \rceil$.
- The indices of P_i are computed recursively.
- The recursion tree has a depth of $\mathrm{O}(\log D)$.
- Since $D \leqslant k-1$, we express $\operatorname{ind} P$ as a linear combination of indices of linear polynomials in time $\max(q,k)^{\mathrm{O}(\log k)}$.

Cases of Applicability

- $\mathbb{F}_Q = \mathbb{F}_{q^{2k}}$ with $q \approx k$.
- $p = \mathrm{char}\,\mathbb{F}_Q = \mathrm{O}(\log Q)^{\mathrm{O}(1)}$. Let $Q = p^n$. If p is small (like 2) and n has no small prime factors, we embed $\mathbb{F}_Q$ in a larger field. Let k be n if n is odd, or $n/2$ if n is even. We take $q = p^{\lceil \log_p k \rceil}$, and work in $\mathbb{F}_{p^{2k}}$.
- In both the above cases, the running time is $2^{\mathrm{O}\left((\log\log Q)^2\right)}$.
- This is quasi-polynomial time.

Implications to Public-Key Cryptography

Classical Cryptography (ElGamal Encryption and Signature)

- For prime fields, NFS is the champion.
- For fields of small characteristics, the Coppersmith method is superseded by the Adleman–Huang FFS method.
- Adaptations of the NFS are also good contenders.

Elliptic-Curve Cryptography (ECDSA)

- No apparent direct implications of FFS.

Pairing-Based Cryptography (IBE, IBS)

- Bilinear pairing maps on supersingular curves are frequently used.
- For extension fields of small characteristics, the medium prime case may occur or be forced.
- The recent developments make the schemes vulnerable.

Practical Estimates for Supersingular Curves

Curve over	DL in field	Security	Reference
$\mathbb{F}_{3^{509}}$	$\mathbb{F}_{3^{6\cdot 509}}$	81.7	Adj et al. (eprint 2013/446)
$\mathbb{F}_{3^{1429}}$	$\mathbb{F}_{3^{6\cdot 1429}}$	96	Adj et al. (eprint 2013/737)
$\mathbb{F}_{2^{3041}}$	$\mathbb{F}_{2^{4\cdot 3041}}$	129	Adj et al. (eprint 2013/737)
$\mathbb{F}_{2^{1223}}$	$\mathbb{F}_{2^{4\cdot 1223}}$	59	Granger et al. (eprint 2014/119)

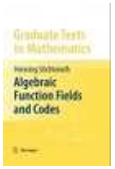
Selected References: Papers

1. G. Adj, A. Menezes, T. Oliviera and F. Rodríguez-Henríquez, *Weakness of $\mathbb{F}_{3^{6\cdot 509}}$ for discrete logarithm cryptography*, ePrint 2013/446.
2. G. Adj, A. Menezes, T. Oliviera and F. Rodríguez-Henríquez, *Weakness of $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{2^{4\cdot 3041}}$ for discrete logarithm cryptography*, ePrint 2013/737.
3. L. M. Adleman and M. A. Huang, *Function field sieve method for discrete logarithms over finite fields*, Information and Computation 151, 5–16, 1999.
4. R. Barbulescu, P. Gaudry, A. Joux and E. Thomé, *A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, ePrint 2013/400.
5. R. Granger, A. J. Holt, D. Page, N. P. Smart and F. Vercauteren, *Function field sieve in characteristic three*, ANTS VI, LNCS 3076, 223–234, 2004.
6. R. Granger, T. Kleinjung and J. Zumbrägel, *Breaking '128-bit secure' supersingular binary curve*, ePrint 2014/119.
7. A. Joux, *Faster index calculus for the medium prime case: Application to 1175-bit and 1425-bit finite fields*, EUROCRYPT 2013, LNCS 7881, 177–193, 2013.
8. A. Joux and R. Lercier, *The function field sieve in the medium prime case*, EUROCRYPT 2006, LNCS 4004, 254–270, 2006.
9. N. Shinohara, T. Shimoyama, T. Hayashi and T. Takagi, *Key length estimation of pairing-based cryptosystems using η_T pairing*, ePrint 2012/042.
10. O. Schirokauer, *Discrete logarithms and local units*, Philosophical Transactions of the Royal Society of London, Series A, 345, 409–423, 1993.
11. O. Schirokauer, *Using number fields to compute logarithms in finite fields*, Mathematics of Computation, 69(231), 1267–1283, 2000.

Selected References: Books

Abhijit Das, *Computational Number Theory*, Chapman and Hall/CRC, 2013.

Antoine Joux, *Algorithmic Cryptanalysis*, Chapman and Hall/CRC, 2009.



Henning Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 2008.

Robert J. Walker, *Algebraic Curves*, Springer, 1978.

Gabriel Daniel Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Birkhäuser, 2006.

Thanks for your kind attention!