

Finite Field Discrete Logarithm Problem

Dr. F. Vercauteren

Katholieke Universiteit Leuven

12 May 2005

Finite Fields

Generic Attacks

Index Calculus

DLOG in Extension Fields

Finite Field DLOG

- ▶ Basis finite field is $\mathbb{F}_p = \{0, \dots, p - 1\}$, with p prime
- ▶ Let $q = p^n$, then \exists extension field $\mathbb{F}_q \simeq \mathbb{F}_p[x]/(f(x))$ with $f(x) \in \mathbb{F}_p[x]$ of degree n and irreducible
- ▶ Multiplicative group \mathbb{F}_q^\times is cyclic, i.e.

$$\exists g \in \mathbb{F}_q \quad \text{with} \quad \mathbb{F}_q^\times = \langle g \rangle$$

- ▶ Let $h \in \mathbb{F}_q^\times$, then $h = g^{\mathbf{d}}$ with $\mathbf{d} = \log_g h$ the DLOG

Square Root Attacks (see ECDL Talk)

- ▶ Pohlig-Hellman: map DLOG to prime order subgroups, i.e. for $l|(q-1)$
- ▶ Baby-Step Giant-Step: $O(\sqrt{l})$ time and $O(\sqrt{l})$ space
- ▶ Pollard-Lambda: $O(\sqrt{l})$ time and $O(\log l)$ space
- ▶ Pollard-Rho: $O(\sqrt{l})$ time and $O(1)$ space
- ▶ Shoup: best possible algorithm in *black box* group of order l , runs in time $O(\sqrt{l})$
- ▶ Does not rely on a specific representation of the elements!

Index Calculus: Overview

- ▶ Original idea: goes back to Kraitchik and Western/Miller, complexity of $L_q[1/2, c]$
- ▶ Gaussian Integer Method: due to Coppersmith, Odlyzko and Schroepel, complexity of $L_p[1/2, 1]$
- ▶ GNFS: adapted by Gordon to compute DLOGs, improved upon by Schirokauer, complexity $L_p[1/3, 1.923]$
- ▶ Coppersmith: for \mathbb{F}_{2^n} , complexity $L_{2^n}[1/3, 1.587]$
- ▶ Function Field Sieve: for \mathbb{F}_{p^m} , p small, time $L_{p^m}[1/3, c]$

$$L_x[a, b] = O\left(e^{(b+O(1))(\log x)^a(\log \log x)^{1-a}}\right)$$

Index Calculus: General Setting

- ▶ G cyclic group of order n , i.e. $G = \langle g \rangle$ and let $h = g^d$
- ▶ Choose a subset $S = \{s_1, \dots, s_t\} \subset G$ called *factor* or *decomposition* base
- ▶ S chosen s.t. almost all elements in G can be expressed *efficiently* as product of elements from S
- ▶ Compute database of $\log_g(s_i)$ for $i = 1, \dots, t$ by collecting *relations*
- ▶ Find the DLOG of individual elements using database

Index Calculus: Algorithm - Phase 1

1. Select random integer $0 \leq k < n$ and compute $\alpha_k = g^k$
2. Try to decompose α_k over the factor base S

$$\alpha_k = g^k = \prod_{i=1}^t s_i^{c_i}, \quad c_i \geq 0$$

3. If α_k factors over S , then take DLOG and obtain

$$k \equiv \sum_{i=1}^t c_i \log_g s_i \pmod{n} \quad (\star)$$

4. Repeat until $t + \varepsilon$ relations found
5. Solve linear system (\star) mod n to obtain $\log_g s_i, 1 \leq i \leq t$

Index Calculus: Algorithm - Phase 2

1. Select random integer $0 \leq k < n$ and compute $\beta_k = h \cdot g^k$
2. Try to decompose β_k over the factor base S

$$\beta_k = hg^k = \prod_{i=1}^t s_i^{d_i}, \quad d_i \geq 0$$

3. Repeat until β_k decomposes over S
4. By taking DLOGs of both sides, obtain

$$\mathbf{d} \equiv \sum_{i=1}^t d_i \log_g s_i - k$$

Index Calculus in \mathbb{F}_p

- ▶ Represent \mathbb{F}_p as $\{0, \dots, p-1\}$ and embed \mathbb{F}_p in \mathbb{Z}
- ▶ Factor base S consists of first t primes $p_i, 0 < i \leq t$
- ▶ $z \in \mathbb{Z}$ is *B-smooth* if all prime factors of z are less than B
- ▶ Element $z \in \mathbb{F}_p$ decomposes over S iff z is p_t -smooth
- ▶ Relation collection: try to factor $\alpha_k = g^k \pmod{p}$ for random exponents k
- ▶ Problem 1: α_k is the same size of p
- ▶ Problem 2: not possible to use a sieve

Index Calculus in \mathbb{F}_p : Linear Sieve

- ▶ Define $H = \lceil \sqrt{p} \rceil$ and $J = H^2 - p$, then $J \in O(\sqrt{p})$
- ▶ Factor base S consists of primes p_i and $H + c$ with c small
- ▶ Relations: search for pairs of small integers (c_1, c_2) with

$$(H + c_1)(H + c_2) \equiv J + (c_1 + c_2)H + c_1 c_2 \pmod{p}$$

- ▶ Note: residue mod p is only $O(\sqrt{p})$, so more likely to factor!
- ▶ Assume that $(H + c_1)(H + c_2) \equiv p_1^{e_1} \cdots p_t^{e_t} \pmod{p}$, then

$$\log_g(H + c_1) + \log_g(H + c_2) = e_1 \cdot \log_g p_1 + \cdots + e_t \cdot \log_g p_t$$

Index Calculus in \mathbb{F}_p : Linear Sieve

- ▶ For fixed c_1 we can sieve for good candidates for c_2
- ▶ Initialise an array indexed by c_2 with zeros
- ▶ For each prime p_i , note that $p_i \mid (H + c_1)(H + x)$ exactly when

$$x \equiv -\frac{(J + c_1 H)}{(H + c_1)} \pmod{p_i}$$

- ▶ Add $\log p_i$ to all values of c_2 with $c_2 \equiv x \pmod{p_i}$
- ▶ Repeat for all the primes p_i (and small powers) in S
- ▶ Compare with the real $\log((H + c_1)(H + c_2) \pmod{p})$

Index Calculus in \mathbb{F}_p : Gaussian Integer Method

- ▶ Idea: map \mathbb{F}_p to \mathbb{Z}^2 using quadratic number field
- ▶ Assume that $p \equiv 1 \pmod{4}$, then -1 is quadratic residue
- ▶ Let $i^2 = -1$, then the polynomial $f_i = X^2 + 1$ defines the quadratic number field $\mathbb{Q}(i)$ with ring of integers $\mathbb{Z}[i]$
- ▶ Using XGCD, compute $V, T \in O(\sqrt{p})$ with $V^2 + T^2 = p$,

$$\left(\frac{V}{T}\right)^2 \equiv -1 \pmod{p}$$

- ▶ Note: $p = (V + Ti)(V - Ti)$, $(V + Ti)$ is maximal ideal and

$$\phi : (\mathbb{Z}[i]/(V + Ti))^\times \rightarrow \mathbb{F}_p^\times : a + bi \mapsto a - bVT^{-1} \pmod{p}$$

Index Calculus in \mathbb{F}_p : Gaussian Integer Method

- ▶ Factor base: small primes p_i , the integer T and prime elements $\alpha + \beta i$ in $\mathbb{Z}[i]$ of small norm
- ▶ The norm of $\alpha + \beta i$ is given by $(\alpha + \beta i)(\alpha - \beta i) = \alpha^2 + \beta^2$
- ▶ Relation collection: find pairs of integers (a, b) such that

$$(a + bi) = \prod_k^{t'} (\alpha_k + \beta_k i)^{d_k} \quad \text{and} \quad aT - bV = \prod_{k=1}^t p_k^{e_k}$$

- ▶ Since $aT - bV = T(a + bi) \pmod{(V + Ti)}$, we find

$$\begin{aligned} \log_g(aT - bV) &= \sum_{k=1}^t e_k \log_g p_k \\ &= \log_g T + d_k \sum_{k=1}^{t'} \log_g (\alpha_k + \beta_k VT^{-1}) \end{aligned}$$

Index Calculus in \mathbb{F}_p : Rational or Linear Sieving

- ▶ Search for pairs (a, b) such that $aT - bV$ factors in $p_i \in S$
- ▶ Fix value of a , then p_i divides $aT - bV$ precisely when

$$b \equiv aTV^{-1} \pmod{p_i}$$

- ▶ Array indexed by b and add $\log p_i$ for $b \equiv aTV^{-1} \pmod{p_i}$
- ▶ Compare with $\log(aT - bV)$ and keep good candidates

Index Calculus in \mathbb{F}_p : Algebraic or Lattice Sieving

- ▶ Fix $(\alpha_j + \beta_j i)$ in S and search for (a, b) such that

$$(\alpha_j + \beta_j i) \mid (a + bi)$$

- ▶ The element $(\alpha_j + \beta_j i)$ is called the special- q
- ▶ Note that above condition defines lattice Λ_q in \mathbb{Z}^2 !
- ▶ Find “good” basis (\vec{u}, \vec{v}) for Λ_q , i.e. short, nearly orthogonal vectors \vec{u} and \vec{v}
- ▶ Any other $q_k = \alpha_k + \beta_k i \in S$ also defines lattice Λ_{q_k}
- ▶ Sieve by intersecting Λ_q with Λ_{q_k} for all k in the (\vec{u}, \vec{v}) space

Index Calculus in \mathbb{F}_p : GNFS

- ▶ GNFS extends Gaussian integer method, by using two number fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$
- ▶ α and β are zeros of $f_\alpha(X)$ and $f_\beta(X)$ that satisfy

$$\exists m : f_\alpha(m) \equiv f_\beta(m) \equiv 0 \pmod{p}$$

- ▶ Example: for Gaussian integer method, we had

$$f_\alpha(X) = X^2 + 1 \quad \text{and} \quad f_\beta(X) = TX + V$$

- ▶ Works with ideals i.o. complex numbers since no UFD!
- ▶ Mapping from ideals to \mathbb{F}_p^\times rather complicated due to non-trivial unit groups and class number > 1

Index Calculus in \mathbb{F}_{2^n} : Function Field Sieve

- ▶ Since $\mathbb{F}_{2^n} \simeq \mathbb{F}_2[x]/(f(x))$, can naturally embed \mathbb{F}_{2^n} in $\mathbb{F}_2[x]$
- ▶ $\mathbb{F}_2[x]$ also provides notion of smoothness and prime elements, i.e. irreducible polynomials
- ▶ Analog of NFS: Function Field Sieve by embedding $\mathbb{F}_2[x]$ into $\mathbb{F}_2(x, y)/(C(x, y))$ with $C(x, y) = 0$ a curve
- ▶ Rational side FB: irreducible polynomials of small degree
- ▶ Algebraic side FB: prime divisors of small degree
- ▶ Sieving methods can be adapted to this setting
- ▶ Note: somewhat easier to implement than GNFS

DLOG in extension fields

- ▶ Consider extension field $K = \mathbb{F}_{q^n}$ of degree n of $k = \mathbb{F}_q$
- ▶ Let g be a generator of K^\times , i.e. $\langle g \rangle = K^\times$ and $h = g^s$
- ▶ For every $d|n$ we have a homomorphism

$$\varphi_d : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^d} : x \mapsto x^{(q^n-1)/(q^d-1)}$$

- ▶ By applying the homomorphisms φ_d for each $d|n$, we get

$$\varphi_d(g) = \varphi_d(h) = \varphi_d(g)^{s_d}$$

- ▶ Repeating for all $d|n$ and applying CRT gives $s \pmod{M}$

$$M = \text{lcm}\{q^d - 1\}_{d|n, d \neq n}$$

DLOG in extension fields

- ▶ Recall $x^n - 1 = \prod_{d|n} \Phi_d(x)$, $\Phi_d(x)$ the d -th cyclotomic polynomial
- ▶ Compute DLOG modulo $M = \text{lcm}\{\Phi_d(q)\}_{d|n, d \neq n}$, by working in subfields
- ▶ Let $f(n, q)$ measure the co-primality of the $\Phi_d(q)$, i.e.

$$M = \text{lcm}\{\Phi_d(q)\}_{d|n, d \neq n} = \frac{\prod_{d|n, d \neq n} \Phi_d(q)}{f(n, q)} = \frac{q^n - 1}{\Phi_n(q) \cdot f(n, q)}$$

- ▶ Factor $f(n, q) \in O(n^{2C})$ with $C \simeq 0.374$ Artin's constant
- ▶ Conclusion: work in subgroup of order $\Phi_n(q)$!
- ▶ Note: this subgroup isomorphic to torus $T_n(\mathbb{F}_q)$, consists of elements whose norm is 1 to every \mathbb{F}_{q^d} with $d|n, d \neq n$

Algebraic Index Calculus

- ▶ Purely algebraic index calculus method possible for \mathbb{F}_{q^m}
- ▶ Consider $\mathbb{F}_{q^m} = \mathbb{F}_q[t]/(f(t))$ with $f(t) \in \mathbb{F}_q[t]$ irreducible
- ▶ Decomposition base S consists of any one dimensional subspace of \mathbb{F}_{q^m} , not contained in \mathbb{F}_q , e.g.

$$S = \{1 + at \mid a \in \mathbb{F}_q\}$$

- ▶ Note that $|S| = q$ and $|\mathbb{F}_{q^m}| = q^m$
- ▶ Relation collection: for random k, l try to decompose

$$\alpha_{k,l} = g^k \cdot h^l$$

Algebraic Index Calculus

$$\begin{aligned}\alpha_{k,l} &= s_1 \cdot s_2 \cdots s_{m-1} \cdot s_m \\ &= (1 + a_1 t) \cdot (1 + a_2 t) \cdots (1 + a_{m-1} t) \cdot (1 + a_m t) \\ &= 1 + \sigma_1 t + \sigma_2 t^2 + \cdots + \sigma_m t^m\end{aligned}$$

- ▶ σ_i is the i -th elementary symmetric polynomial
- ▶ Writing out on basis of $\{1, t, \dots, t^{m-1}\}$ of \mathbb{F}_{q^m} gives m linear equations over \mathbb{F}_q in the m unknowns σ_j
- ▶ Factor $p(x) := x^m - \sigma_1 x^{m-1} + \cdots + (-1)^m \sigma_m$ over \mathbb{F}_q

If $p(x)$ splits completely, found a relation!

- ▶ Note: m -products in S generate about $q^m/m!$ elements in \mathbb{F}_{q^m} , thus probability of finding relation is about $1/m!$

Conclusions

- ▶ Index calculus methods exploit representation of elements
 - ▶ Classically: involves notion of smoothness
 - ▶ Recently: purely algebraic index calculus due to Gaudry
- ▶ Possible to compute DLOGs in \mathbb{F}_q in expected time

$$L_q[1/2, c]$$

- ▶ Better complexity $L_q[1/3, c]$ possible for \mathbb{F}_p and \mathbb{F}_{2^n}
- ▶ Do not work in full multiplicative group of \mathbb{F}_{p^n} , but only in prime order subgroup of the algebraic torus $T_n(\mathbb{F}_p)$, i.e. the subgroup of order $\Phi_n(p)$

References

- ▶ H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag 1993
- ▶ D. Coppersmith, *Fast Evaluation of Discrete Logarithms in Fields of Characteristic Two*, IEEE transactions IT-30(4):587–595, 1984
- ▶ D. Gordon, *Discrete Logarithms in \mathbb{F}_p using the Number Field Sieve*, SIAM J. Discrete Math, 6:124–138, 1993
- ▶ B. A. LaMacchia and A. M. Odlyzko, *Computation of Discrete Logarithms in Prime Fields*, Designs, Codes and Cryptography, 1:47–62, 1991
- ▶ A. Lenstra and H. Lenstra, *The Development of the Number Field Sieve*, LNM 1554, Springer-Verlag, 1993