A Bird's Eye View on Discrete Logarithm Problems over Finite Fields

Xiao'ou He

December 14, 2017

Key Laboratory of Mathematics Mechanization, AMSS

Outline

Outline

Outline

Motivation

Public-Key Cryptography

- Proposed by Diffie and Hellman, 1976
- Based on number-theoretical hard problems
  - Integer Factorizations
  - Discrete Logarithms

    Concerning with two class of groups:

    1. Elliptic curves
    2. Multiplicative groups of finite fields

Case in General

- Cyclic group: $(G, \cdot) = < g >$.
- Exponential v. Logarithm
  - $x \mapsto h = g^x$
  - $h \mapsto x = \log_g h$
- Generic Algorithms:
  - Pohlig-Hellman: Two reductions - CRT and p^e to p
  - Collision Making: Baby-step giant-step, Pollard's rho Method, etc.

Case over Finite Fields

- Given: Q, g and h, where $< g >= \mathbb{F}_Q^\times$ containing h.
- Find: $\log_g h$.

Previous Work

The $\mathcal{L}$ Notation: Complexity

$$\mathcal{L}_Q(\beta, c) = \exp((c + o(1))(\log Q)^{\beta}(\log\log Q)^{1-\beta})$$

- $c > 0$ and $0 \leq \beta \leq 1$
- $\mathcal{L}_Q(0, c) = (\log Q)^{c+o(1)} = \text{poly}(\log Q)$,
  $\mathcal{L}_Q(1, c) = (\exp(\log Q))^{c+o(1)} = \exp(\log Q)$.
- When $0 < \beta < 1$, $\mathcal{L}_Q(\beta, c)$ is **sub-exponential**.

Overview

- **Index Calculus Method**
  - 1st sub-exp algo., complexity $\mathcal{L}_Q(\frac{1}{2}, \cdot)$
  - Adleman, 1979 and Pohlig, 1977 independently
- **Coppersmith's Method, 1984**
  - 1st algo. of complexity $\mathcal{L}_Q(\frac{1}{3}, \cdot)$.
  - Originally $\mathbb{F}_{2^n}$, then generalized to prime powers (easily).
- **Function Field Sieve, 1999**
  - More general: used for several record breaking comutations.
  - Adleman and Huang
- **Number Field Sieve**,

Overview: Until 2013

All cases solved in $\mathcal{L}_Q(\frac{1}{3}, \cdot)$

- Small char.: function field sieve (FFS)
- Medium and large char.: number field sieve (NFS)
- Measure: solve $p = \mathcal{L}_Q(\beta, c)$ where $Q = p^n$,
  for relation between β and $\frac{1}{3}$, $\frac{2}{3}$

Overview: Small Char.

- 1st algo. of complexity $\mathcal{L}_Q(\frac{1}{4}, \cdot)$:
  Frobenius representation, Joux, 2013
- 1st algo. of complexity quasi-poly:
  Barbulescu, 2014

Smooth - Set A Bound

Definition
Given $B > 0$. $\forall n \in \mathbb{Z}$ is called B-smooth if all its prime factors are no larger than B. Thus denote factor basis as

$$\mathcal{F}(B) = \{p \in \mathbb{N} : \text{prime and } p \leq B\}$$

Definition
Given $\beta \in \mathbb{Z}_{>0}$. $\forall f[X] \in \mathbb{F}_q[X]$ is called β-smooth if all its irreducible factors are of degree no higher than β. Thus denote respective factor basis as

$$\mathcal{F}_q(\beta) = \{I_k \in \mathbb{F}_q[X] : \text{irre. monic and deg. } k \leq \beta\}$$

Index Calculus Method - Framework of Following Algo.

- Given: $h \in \mathbb{F}_Q^{\times} =< g >$; Find: $\log_g h$

Index Calculus Method - Framework of Following Algo.

- Given: $h \in \mathbb{F}_Q^{\times} =< g >$; Find: $\log_g h$
- Process:
  1. **Main Phase**
  2. **Individual Logarithm**

Index Calculus Method - Framework of Following Algo.

- Given: $h \in \mathbb{F}_Q^\times =< g >$; Find: $\log_g h$
- Process:
  1. **Main Phase**
     - Fix parameter B, thus $\mathcal{F}(B)$ is also given.
  2. **Individual Logarithm**

Index Calculus Method - Framework of Following Algo.

- Given: $h \in \mathbb{F}_Q^{\times} =< g >$; Find: $\log_g h$
- Process:
  1. **Main Phase**
     - Fix parameter B, thus $\mathcal{F}(B)$ is also given.
     - Smoothness Selection: random $x \in [1, Q-2]$ s.t. g^x is B-smooth:

$$g^x = \prod_{p \in \mathcal{F}(B)} p^{v(p,x)}$$

  2. **Individual Logarithm**

Index Calculus Method - Framework of Following Algo.

- Given: $h \in \mathbb{F}_Q^\times =< g >$; Find: $\log_g h$
- Process:
  1. **Main Phase**
     - Fix parameter B, thus $\mathcal{F}(B)$ is also given.
     - Smoothness Selection: random $x \in [1, Q-2]$ s.t. g^x is B-smooth:
       $$g^x = \prod_{p \in \mathcal{F}(B)} p^{v(p,x)}$$
     - Relation Collection: take $\log_g \cdot$ on both sides and substitute $\log_g p$ by unknown variable x_p (denoted as $\log_g p \leftrightarrow x_p$):
       $$x \equiv \sum_{p \in \mathcal{F}(B)} v(p,x) x_p \mod Q-1$$
  2. **Individual Logarithm**

Index Calculus Method - Framework of Following Algo.

- Given: $h \in \mathbb{F}_Q^\times =< g >$; Find: $\log_g h$
- Process:
  1. **Main Phase**
     - Fix parameter B, thus $\mathcal{F}(B)$ is also given.
     - Smoothness Selection: random $x \in [1, Q-2]$ s.t. g^x is B-smooth:
       $$g^x = \prod_{p \in \mathcal{F}(B)} p^{v(p,x)}$$
     - Relation Collection: take $\log_g \cdot$ on both sides and substitute $\log_g p$ by unknown variable x_p (denoted as $\log_g p \leftrightarrow x_p$):
       $$x \equiv \sum_{p \in \mathcal{F}(B)} v(p,x) x_p \mod Q-1$$
     - Linea Algebra: Solve system of linear equations.
  2. **Individual Logarithm**

Index Calculus Method - Framework of Following Algo.

- Given: $h \in \mathbb{F}_Q^\times =< g >$; Find: $\log_g h$
- Process:
  1. **Main Phase**
     - Fix parameter B, thus $\mathcal{F}(B)$ is also given.
     - Smoothness Selection: random $x \in [1, Q-2]$ s.t. g^x is B-smooth:
$$g^x = \prod_{p \in \mathcal{F}(B)} p^{v(p,x)}$$
     - Relation Collection: take $\log_g \cdot$ on both sides and substitute $\log_g p$ by unknown variable x_p (denoted as $\log_g p \leftrightarrow x_p$):
$$x \equiv \sum_{p \in \mathcal{F}(B)} v(p,x) x_p \mod Q-1$$
     - Linea Algebra: Solve system of linear equations.
  2. **Individual Logarithm**
     Find $y \in [1, Q-2]$ s.t. $g^y h$ is B-smooth.

Index Calculus Method - Framework of Following Algo.

- Given: $h \in \mathbb{F}_Q^\times =< g >$; Find: $\log_g h$
- Process:
  1. **Main Phase**
     - Fix parameter B, thus $\mathcal{F}(B)$ is also given.
     - Smoothness Selection: random $x \in [1, Q-2]$ s.t. g^x is B-smooth:
     $$g^x = \prod_{p \in \mathcal{F}(B)} p^{v(p,x)}$$
     - Relation Collection: take $\log_g \cdot$ on both sides and substitute $\log_g p$ by unknown variable x_p (denoted as $\log_g p \leftrightarrow x_p$):
     $$x \equiv \sum_{p \in \mathcal{F}(B)} v(p,x) x_p \mod Q-1$$
     - Linea Algebra: Solve system of linear equations.
  2. **Individual Logarithm**

     Find $y \in [1, Q-2]$ s.t. $g^y h$ is B-smooth. Then factorization $g^y h = \prod p^{v_0(p)}$ implies
     $$\log_g h \equiv \sum v_0(p) \log_g p - y \mod Q-1$$

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times =< g >$ where $Q = q^k$; Find: $\log_g h$.

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times =< g >$ where $Q = q^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times = < g >$ where $Q = q^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Fix parameter β then obtain $\mathcal{F}_q(\beta) = \{F(X) : \cdots\}$. Find n satisfying $q^{n-1} < k \leq q^n$, fix $n_1 + n_2 = n$.
  2. **Individual Logarithm**

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times =< g >$ where $Q = q^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Fix parameter β then obtain $\mathcal{F}_q(\beta) = \{F(X) : \cdots\}$. Find n satisfying $q^{n-1} < k \leq q^n$, fix $n_1 + n_2 = n$.
     - Find $S(X)$ of deg.$\leq \beta$ s.t. $\exists I_k(X) | X^{q^n} - S(X)$ with a root α.

  2. **Individual Logarithm**

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times =< g >$ where $Q = q^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Fix parameter β then obtain $\mathcal{F}_q(\beta) = \{F(X) : \cdots\}$. Find n satisfying $q^{n-1} < k \leq q^n$, fix $n_1 + n_2 = n$.
     - Find $S(X)$ of deg.$\leq \beta$ s.t. $\exists I_k(X) | X^{q^n} - S(X)$ with a root α.
     - Smoothness Selection: random $A(X)$, $B(X)$ of deg.$\leq \beta$ s.t. both $C(X) = A(X) + X^{q^{n_1}} B(X)$ and $D(X) = C(X)^{q^{n_2}}$ are β-smooth, notice deg.$\leq q^{n_1} + \beta$ and $(q^{n_2} + 1)\beta$ respectively.
  2. **Individual Logarithm**

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times = < g >$ where $Q = q^k$; Find: $\log_g h$.
- Process:

1. **Main Phase**
   - Fix parameter β then obtain $\mathcal{F}_q(\beta) = \{F(X) : \cdots\}$. Find n satisfying $q^{n-1} < k \leq q^n$, fix $n_1 + n_2 = n$.
   - Find $S(X)$ of deg.$\leq \beta$ s.t. $\exists I_k(X) | X^{q^n} - S(X)$ with a root α.
   - Smoothness Selection: random $A(X)$, $B(X)$ of deg.$\leq \beta$ s.t. both $C(X) = A(X) + X^{q^{n_1}} B(X)$ and $D(X) = C(X)^{q^{n_2}}$ are β-smooth, notice deg.$\leq q^{n_1} + \beta$ and $(q^{n_2} + 1)\beta$ respectively.
   - Relation Collection: known

   $$(\prod F(X)^{v(C,F)})^{q^{n_2}} \equiv \prod F(X)^{v(D,F)} \mod I_k(X)$$

   $X \leftrightarrow \alpha$, take $\log_g \cdot$ on both sides, and $\log_g F(\alpha) \leftrightarrow x_F$

   $$\sum (q^{n_2} v(C, F) - v(D, F)) x_F \equiv 0 \mod Q - 1$$

2. **Individual Logarithm**

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times =< g >$ where $Q = q^k$; Find: $\log_g h$.
- Process:

1. **Main Phase**
    - Fix parameter β then obtain $\mathcal{F}_q(\beta) = \{F(X) : \cdots\}$. Find n satisfying $q^{n-1} < k \leq q^n$, fix $n_1 + n_2 = n$.
    - Find $S(X)$ of deg.$\leq \beta$ s.t. $\exists I_k(X) | X^{q^n} - S(X)$ with a root α.
    - Smoothness Selection: random $A(X)$, $B(X)$ of deg.$\leq \beta$ s.t. both $C(X) = A(X) + X^{q^{n_1}} B(X)$ and $D(X) = C(X)^{q^{n_2}}$ are β-smooth, notice deg.$\leq q^{n_1} + \beta$ and $(q^{n_2} + 1)\beta$ respectively.
    - Relation Collection: known
      $$(\prod F(X)^{v(C,F)})^{q^{n_2}} \equiv \prod F(X)^{v(D,F)} \mod I_k(X)$$
      $X \leftrightarrow \alpha$, take $\log_g \cdot$ on both sides, and $\log_g F(\alpha) \leftrightarrow x_F$
      $$\sum (q^{n_2} v(C,F) - v(D,F)) x_F \equiv 0 \mod Q - 1$$
    - Linear Algebra
2. **Individual Logarithm**

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times =< g >$ where $Q = q^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Fix parameter β then obtain $\mathcal{F}_q(\beta) = \{F(X) : \cdots\}$. Find n satisfying $q^{n-1} < k \leq q^n$, fix $n_1 + n_2 = n$.
     - Find $S(X)$ of deg.$\leq \beta$ s.t. $\exists I_k(X) | X^{q^n} - S(X)$ with a root α.
     - Smoothness Selection: random $A(X)$, $B(X)$ of deg.$\leq \beta$ s.t. both $C(X) = A(X) + X^{q^{n_1}} B(X)$ and $D(X) = C(X)^{q^{n_2}}$ are β-smooth, notice deg.$\leq q^{n_1} + \beta$ and $(q^{n_2} + 1)\beta$ respectively.
     - Relation Collection: known

$$(\prod F(X)^{v(C,F)})^{q^{n_2}} \equiv \prod F(X)^{v(D,F)} \mod I_k(X)$$

       $X \leftrightarrow \alpha$, take $\log_g \cdot$ on both sides, and $\log_g F(\alpha) \leftrightarrow x_F$

$$\sum (q^{n_2} v(C, F) - v(D, F)) x_F \equiv 0 \mod Q - 1$$

     - Linear Algebra
  2. **Individual Logarithm** Descent Method.

NFS

Joux 13 and Barbulescu 14

Research Plan