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

- Motivation
  - Origin of The Problem in Cryptography
  - Exposition of The Problem
- Previous Work
  - Preliminaries
  - From Sub-exp to Quasi-poly
  - Summary

Outline

Motivation

Outline

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

Outline

Case in General

- Cyclic group: $(G, \cdot) = \langle g \rangle$.
- 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 $\langle g \rangle = \mathbb{F}_Q^\times$ containing h.
- Find: $\log_g h$.

Previous Work

Outline

Complexity

The $\mathcal{L}$ Notation

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

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

Quasi-poly

$(\log Q)^{O(\log \log Q)}$ is **quasi-polynomial**, which is smaller than any $\mathcal{L}_Q(\beta, \cdot)$ for $\beta > 0$.

Outline

Overview

$\mathcal{L}_Q(\frac{1}{2}, \cdot)$ Index Calculus Method

Adleman, 1979 and Pohlig, 1977 independently

$\mathcal{L}_Q(\frac{1}{3}, \cdot)$ by Coppersmith, 1984

- Originally $\mathbb{F}_{2^n}$
- More general: FFS by Adleman and Huang, 1999
- Medium and large char.: NFS by Gordon, 1993

$\mathcal{L}_Q(\frac{1}{4}, \cdot)$ Joux, 2013 to quasi-poly by BGJT, 2014

- For small char.: Take $\mathbb{F}_{2^n}$ for instace. Roughly $p \leq \mathcal{L}_Q(\frac{1}{3}, \cdot)$.
- Heuristics

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

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

Index Calculus Method - Framework of Following Algo.s

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

Index Calculus Method - Framework of Following Algo.s

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$; Find: $\log_g h$
- Process:
  1. **Main Phase**

  2. **Individual Logarithm**

Index Calculus Method - Framework of Following Algo.s

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$; 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.s

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$; 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.s

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$; 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.s

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$; 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.s

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$; 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.s

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

Coppersmith's Method

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

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ 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: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ 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: $h \in \mathbb{F}_Q^{\times} = \langle g \rangle$ 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: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ 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: $h \in \mathbb{F}_Q^{\times} = \langle g \rangle$ 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: Solve system of linear equations.
  2. **Individual Logarithm**

Coppersmith's Method

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ 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: Solve system of linear equations.
  2. **Individual Logarithm** Descent Method.

Joux, 2013

BGJT, 2014

Outline

Paradigm with Transitions

1. **Main Phase**
   - Initiation: field extension brings freedom in presentation
   - Smoothness Selection:
     Randomly choose $\Rightarrow$ Sieve $\Rightarrow$ Generate
   - Relation Collection:
     Understanding the factor basis and (virtual) logarithms
   - Linear Algebra: Take advantage of the sparseness
2. **Individual Logarithm Phase**: Descent Strategy

Research Plan

Future Work

- In Theory
  - **Heuristics**: From assumption to rigorous.
    - CWZ, 2014: Three Heuristics
    - Existence of (S_0, S_1) s.t. $\exists I_k(X) | S_1(X)X^q - S_0(X)$.
  - **Construction of the finite fields**:
    $\mathbb{F}_q[X]/\langle I_k[X]\rangle \Rightarrow \mathcal{O}_{\mathbb{K}}/P \Rightarrow$?
  - **Relation Obtaining**:
    Balance two medium-deg. poly.s $\Rightarrow$ half-relation $\Rightarrow$?
  - **Tiny Goal**:
    Generalize small char. cases to medium and large ones?
    Truly poly. algo.?
- In Practice: TBD.