A Bird’s Eye View over Discrete Logarithm Problems in Finite Fields

Xiao’ou He

December 14, 2017

Key Laboratory of Mathematics Mechanization, AMSS

Outline

Motivation

Outline

Diffie-Hellman, 1976

- The basis of public key cryptography.
- One-way function.
- An example: discrete logarithm problem

Outline

Case in General

- Cyclic group: $(G, \cdot) =< g >$.
- Exponential v. Logarithm
- Generic Algorithms:
  Pohlig-Hellman, Baby-step giant-step, Pollard's rho Method etc.

Case in Finite Fields

- Given: finite filed $\mathbb{F}_Q$ where Q is power of prime p, a generator g of $\mathbb{F}_Q^\times$ and arbitrary element $h \in \mathbb{F}_Q^\times$.
- Find: $\log_g h$.

Previous Work

Outline

The $\mathcal{L}$ Notation

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

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

Outline

Overview

- Index Calculus Method
  - 1st sub-exp algorithm, complexity $\mathcal{L}_Q(\frac{1}{2}, \cdot)$
  - Adleman, 1979 and Pohlig 1977 independently
- Coppersmith's Method
  - 1st algorithm of complexity $\mathcal{L}_Q(\frac{1}{3}, \cdot)$
  - Originally for Q power of 2
  - Generalized to prime powers easily

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)

Overview: Small Char

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

Outline

Index Calculus Method

Coppersmith’s Method

NFS

Joux 13 and Barbulescu 14

Research Plan