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

Xiao'ou He

December 14, 2017

Key Laboratory of Mathematics Mechanization, AMSS

Outline

Outline

Outline

Motivation

Outline

DLP in Cryptography

- Key-exchange scheme [Diffie and Hellman, 1976]

DLP in Cryptography

- Key-exchange scheme [Diffie and Hellman, 1976]
- Encryption algorithm [ElGamal, 1985]

DLP in Cryptography

- Key-exchange scheme [Diffie and Hellman, 1976]
- Encryption algorithm [ElGamal, 1985]
- Digital Signature Algorithm (DSA) [NIST, 1991]

Outline

Case in General

- Cyclic group: $(G, \cdot) = \langle g \rangle$

Case in General

- Cyclic group: $(G, \cdot) = \langle g \rangle$
- Based on number-theoretical hard problem

Case in General

- Cyclic group: $(G, \cdot) = \langle g \rangle$
- Based on number-theoretical hard problem
  - $\mathbb{Z} \to G, x \mapsto h = g^x$
  - $G \to \mathbb{Z}, h \mapsto x = \log_g h$

Case in General

- Cyclic group: $(G, \cdot) = \langle g \rangle$
- Based on number-theoretical hard problem
  - $\mathbb{Z} \to G, x \mapsto h = g^x$
  - $G \to \mathbb{Z}, h \mapsto x = \log_g h$
- Generic Algorithms - $O(\exp(\log |G|))$
  - Pohlig-Hellman
  - Collision Making
    Shanks' baby-step giant-step, Pollard's ρ, etc.

Case in General

- Cyclic group: $(G, \cdot) = \langle g \rangle$
- Based on number-theoretical hard problem
  - $\mathbb{Z} \to G, x \mapsto h = g^x$
  - $G \to \mathbb{Z}, h \mapsto x = \log_g h$
- Generic Algorithms - $O(\exp(\log |G|))$
  - Pohlig-Hellman
  - Collision Making
    Shanks' baby-step giant-step, Pollard's ρ, etc.
- Concerning with two class of groups
  1. Elliptic curves
  2. Multiplicative groups of finite fields

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

$$\mathcal{L}_Q(\alpha) = \exp(O((\log Q)^\alpha (\log \log Q)^{1-\alpha}))$$

- $0 \leq \alpha \leq 1$

Complexity

The $\mathcal{L}$ Notation

$$\mathcal{L}_Q(\alpha) = \exp(O((\log Q)^{\alpha}(\log\log Q)^{1-\alpha}))$$

- $0 \leq \alpha \leq 1$
- $\mathcal{L}_Q(0) = (\log Q)^{O(1)} = \mathrm{poly}(\log Q)$,
  $\mathcal{L}_Q(1) = (\exp(\log Q))^{O(1)} = \exp(\log Q)$

Complexity

The $\mathcal{L}$ Notation

$$\mathcal{L}_Q(\alpha) = \exp(O((\log Q)^{\alpha}(\log\log Q)^{1-\alpha}))$$

- $0 \leq \alpha \leq 1$
- $\mathcal{L}_Q(0) = (\log Q)^{O(1)} = \mathrm{poly}(\log Q)$,
  $\mathcal{L}_Q(1) = (\exp(\log Q))^{O(1)} = \exp(\log Q)$
- When $0 < \alpha < 1$, $\mathcal{L}_Q(\alpha)$ is **sub-exponential**

Complexity

The $\mathcal{L}$ Notation

$$\mathcal{L}_Q(\alpha) = \exp(O((\log Q)^\alpha (\log\log Q)^{1-\alpha}))$$

- $0 \leq \alpha \leq 1$
- $\mathcal{L}_Q(0) = (\log Q)^{O(1)} = \text{poly}(\log Q)$,
  $\mathcal{L}_Q(1) = (\exp(\log Q))^{O(1)} = \exp(\log Q)$
- When $0 < \alpha < 1$, $\mathcal{L}_Q(\alpha)$ is **sub-exponential**

Quasi-poly

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

Outline

Overview

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

[Pohlig, 1977] and [Adleman, 1979] independently

Overview

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

[Pohlig, 1977] and [Adleman, 1979] independently

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

- Originally $\mathbb{F}_{2^n}$
- **Number Field Sieve** by [Gordon, 1993]
- **Function Field Sieve** by [Adleman and Huang, 1999]

Overview

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

[Pohlig, 1977] and [Adleman, 1979] independently

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

- Originally $\mathbb{F}_{2^n}$
- **Number Field Sieve** by [Gordon, 1993]
- **Function Field Sieve** by [Adleman and Huang, 1999]

$\mathcal{L}_Q(\frac{1}{4})$ by [Joux, 2013] to quasi-poly by [BGJT@EC'14]

- Originated from [Joux and Lercier@EC'06]
- For small char., roughly $p \leq \mathcal{L}_Q(\frac{1}{3})$.
- 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

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

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

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

Index Calculus Method - Framework of Following Algorithms

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

Index Calculus Method - Framework of Following Algorithms

- 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 Algorithms

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

Index Calculus Method - Framework of Following Algorithms

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

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

  2. **Individual Logarithm**

Index Calculus Method - Framework of Following Algorithms

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

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

     - Relation Collection Take $\log_g$ on both sides and substitute $\log_g p$ by unknown variable x_p (denoted as $\log_g p \leftarrow x_p$):

$$c \equiv \sum_{p \in \mathcal{F}(B)} v(p,c) x_p \mod Q-1$$

  2. **Individual Logarithm**

Index Calculus Method - Framework of Following Algorithms

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

Index Calculus Method - Framework of Following Algorithms

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

Index Calculus Method - Framework of Following Algorithms

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$; Find: $\log_g h$
- Process:
  1. **Main Phase**
     - Initialization Fix parameter B, thus $\mathcal{F}(B)$ is also given.
     - Smoothness Selection Random $c \in [1, Q-2]$ s.t. g^c is B-smooth:
       $$g^c = \prod_{p \in \mathcal{F}(B)} p^{v(p,c)}$$
     - Relation Collection Take $\log_g$ on both sides and substitute $\log_g p$ by unknown variable x_p (denoted as $\log_g p \leftarrow x_p$):
       $$c \equiv \sum_{p \in \mathcal{F}(B)} v(p,c) x_p \mod Q-1$$
     - Linea Algebra Solve system of linear equations.
  2. **Individual Logarithm**
     Find $b \in [1, Q-2]$ s.t. $g^b h$ is B-smooth. Then factorization $g^b h = \prod p^{v_0(p)}$ implies
     $$\log_g h \equiv \sum v_0(p) \log_g p - b \mod Q-1$$

Coppersmith's Method - $\mathbb{F}_Q = \mathbb{F}_q[X]/\langle I_k(X)\rangle = \mathbb{F}(\alpha)$

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

Coppersmith's Method - $\mathbb{F}_Q = \mathbb{F}_q[X]/\langle I_k(X)\rangle = \mathbb{F}(\alpha)$

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

  2. **Individual Logarithm Phase**

Coppersmith's Method - $\mathbb{F}_Q = \mathbb{F}_q[X]/\langle I_k(X)\rangle = \mathbb{F}(\alpha)$

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ where $Q = p^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Initialization Fix B then obtain $\mathcal{F}_q(B)$.
       Find n satisfying $p^{n-1} < k \leq p^n$, fix $n_1 + n_2 = n$.
  2. **Individual Logarithm Phase**

Coppersmith's Method - $\mathbb{F}_Q = \mathbb{F}_q[X]/\langle I_k(X)\rangle = \mathbb{F}(\alpha)$

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

Coppersmith's Method - $\mathbb{F}_Q = \mathbb{F}_q[X]/\langle I_k(X)\rangle = \mathbb{F}(\alpha)$

- Given: $h \in \mathbb{F}_Q^\times = \langle g\rangle$ where $Q = p^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Initialization Fix B then obtain $\mathcal{F}_q(B)$.
       Find n satisfying $p^{n-1} < k \leq p^n$, fix $n_1 + n_2 = n$.
       Find $S(X)$ of $\deg \leq B$ s.t. $\exists I_k(X) | X^{p^n} - S(X)$ with a root α.
     - Smoothness Selection Random $G_1(X)$, $G_2(X)$ of $\deg \leq B$ s.t. both $C(X) = G_1(X) + X^{p^{n_1}} G_2(X)$ and $D(X) = C(X)^{p^{n_2}}$ are B-smooth, notice $\deg \leq p^{n_1} + B$ and $(p^{n_2} + 1)B$ respectively.
  2. **Individual Logarithm Phase**

Coppersmith's Method - $\mathbb{F}_Q = \mathbb{F}_q[X]/\langle I_k(X)\rangle = \mathbb{F}(\alpha)$

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ where $Q = p^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Initialization Fix B then obtain $\mathcal{F}_q(B)$.
       Find n satisfying $p^{n-1} < k \le p^n$, fix $n_1 + n_2 = n$.
       Find $S(X)$ of $\deg \le B$ s.t. $\exists I_k(X) | X^{p^n} - S(X)$ with a root α.
     - Smoothness Selection Random $G_1(X)$, $G_2(X)$ of $\deg \le B$ s.t. both $C(X) = G_1(X) + X^{p^{n_1}} G_2(X)$ and $D(X) = C(X)^{p^{n_2}}$ are B-smooth, notice $\deg \le p^{n_1} + B$ and $(p^{n_2} + 1)B$ respectively.
     - Relation Collection Known

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

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

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

  2. **Individual Logarithm Phase**

Coppersmith's Method - $\mathbb{F}_Q = \mathbb{F}_q[X]/\langle I_k(X)\rangle = \mathbb{F}(\alpha)$

- Given: $h \in \mathbb{F}_Q^\times = \langle g\rangle$ where $Q = p^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Initialization Fix B then obtain $\mathcal{F}_q(B)$.
       Find n satisfying $p^{n-1} < k \leq p^n$, fix $n_1 + n_2 = n$.
       Find $S(X)$ of $\deg \leq B$ s.t. $\exists I_k(X) | X^{p^n} - S(X)$ with a root α.
     - Smoothness Selection Random $G_1(X)$, $G_2(X)$ of $\deg \leq B$ s.t. both $C(X) = G_1(X) + X^{p^{n_1}} G_2(X)$ and $D(X) = C(X)^{p^{n_2}}$ are B-smooth, notice $\deg \leq p^{n_1} + B$ and $(p^{n_2}+1)B$ respectively.
     - Relation Collection Known
       $$(\prod F(X)^{v(C,F)})^{p^{n_2}} \equiv \prod F(X)^{v(D,F)} \mod I_k(X)$$
       $X \leftarrow \alpha$, take $\log_g$ on both sides, and $\log_g F(\alpha) \leftarrow x_F$
       $$\sum (p^{n_2} v(C,F) - v(D,F)) x_F \equiv 0 \mod Q-1$$
     - Linear Algebra Solve system of linear equations.
  2. **Individual Logarithm Phase**

Coppersmith's Method - $\mathbb{F}_Q = \mathbb{F}_q[X]/\langle I_k(X)\rangle = \mathbb{F}(\alpha)$

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ where $Q = p^k$; Find: $\log_g h$.
- Process:
  1. **Main Phase**
     - Initialization Fix B then obtain $\mathcal{F}_q(B)$.
       Find n satisfying $p^{n-1} < k \le p^n$, fix $n_1 + n_2 = n$.
       Find $S(X)$ of $\deg \le B$ s.t. $\exists I_k(X) | X^{p^n} - S(X)$ with a root α.
     - Smoothness Selection Random $G_1(X)$, $G_2(X)$ of $\deg \le B$ s.t. both $C(X) = G_1(X) + X^{p^{n_1}} G_2(X)$ and $D(X) = C(X)^{p^{n_2}}$ are B-smooth, notice $\deg \le p^{n_1} + B$ and $(p^{n_2}+1)B$ respectively.
     - Relation Collection Known
       $$\left(\prod F(X)^{v(C,F)}\right)^{p^{n_2}} \equiv \prod F(X)^{v(D,F)} \mod I_k(X)$$
       $X \leftarrow \alpha$, take $\log_g$ on both sides, and $\log_g F(\alpha) \leftarrow x_F$
       $$\sum (p^{n_2} v(C,F) - v(D,F)) x_F \equiv 0 \mod Q-1$$
     - Linear Algebra Solve system of linear equations.
  2. **Individual Logarithm Phase** Descent strategy

Joux&Lercier@EC'06

Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ **where** $Q = q^k$

Find $S_1(X), S_2(X) \in \mathbb{F}_q[X]$ s.t. $\exists I_k(X) | X - S_1(S_2(X))$, a root α. Let $\beta = S_2(\alpha)$, then $\exists J_k(Y) | Y - S_2(S_1(Y))$ with root β.

Joux&Lercier@EC'06

Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ **where** $Q = q^k$

Find $S_1(X), S_2(X) \in \mathbb{F}_q[X]$ s.t. $\exists I_k(X) | X - S_1(S_2(X))$, a root α. Let $\beta = S_2(\alpha)$, then $\exists J_k(Y) | Y - S_2(S_1(Y))$ with root β.

$$
\begin{tikzcd}
 & \mathbb{F}_q[X, Y] \arrow[dl, "\text{mod } Y - S_2(X)"'] \arrow[dr, "\text{mod } X - S_1(Y)"] & \\
\mathbb{F}_q[X] \arrow[dr, "\text{mod } X - \alpha"'] & & \mathbb{F}_q[Y] \arrow[dl, "\text{mod } Y - \beta"] \\
 & \mathbb{F}_Q &
\end{tikzcd}
$$

Joux&Lercier@EC'06

Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ **where** $Q = q^k$

Find $S_1(X), S_2(X) \in \mathbb{F}_q[X]$ s.t. $\exists I_k(X) | X - S_1(S_2(X))$, a root α. Let $\beta = S_2(\alpha)$, then $\exists J_k(Y) | Y - S_2(S_1(Y))$ with root β.

$$\begin{tikzcd}
 & \mathbb{F}_q[X, Y] \arrow[dl, "\bmod\ Y - S_2(X)"'] \arrow[dr, "\bmod\ X - S_1(Y)"] & \\
\mathbb{F}_q[X] \arrow[dr, "\bmod\ X - \alpha"'] & & \mathbb{F}_q[Y] \arrow[dl, "\bmod\ Y - \beta"] \\
 & \mathbb{F}_Q &
\end{tikzcd}$$

Start with $G_1(Y)X + G_2(Y)$, we will reach the relation

$$G_1(S_2(\alpha))\alpha + G_2(S_1(\alpha)) = G_1(\beta)S_1(\beta) + G_2(\beta)$$

Joux&Lercier@EC'06

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ where $Q = q^k$; Find: $\log_g h$
- Process:
  1. **Main Phase**
     - Initialization Fix parameter B then obtain $\mathcal{F}_q(B)$. Find $S_1(X)$, $S_2(X) \in \mathbb{F}_q[X]$ of $\deg d_1, d_2$ satisfying $d_1 d_2 \geq k$ s.t. $\exists I_k(X) | X - S_1(S_2(X))$ with a root α
     - Smoothness Selection Random $G_1(X), G_2(X)$ of $\deg \leq B$ s.t. both $G_1(S_2(X))X + G_2(S_1(X))$ and $G_1(X)S_1(X) + G_2(X)$ are B-smooth, notice $\deg \leq Bd_2 + 1, Bd_1$ respectively.
     - Relation Collection Known $G_1(S_2(\alpha))\alpha + G_2(S_1(\alpha)) = G_1(\beta)S_1(\beta) + G_2(\beta)$ and smoothness implies $\prod F(\alpha)^{v(F)} = \prod F(\beta)^{w(F)}$. Then take $\log_g$ and $F(\alpha) \leftarrow x_F$, $F(\beta) \leftarrow y_F$

       $$\sum v(F)x_F \equiv \sum w(F)y_F \mod Q - 1$$
     - Linear Algebra Solve system of linear equations.
  2. **Individual Logarithm Phase** Descent strategy.

[Joux, 2013] and [BGJT@EC'14] - Half Relation

Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ **where** $Q = q^k$ **and** $q > k$

Take advantage of the itentity $X^q - X = \prod_{\gamma \in \mathbb{F}_q} (X - \gamma)$.

[Joux, 2013] and [BGJT@EC'14] - Half Relation

Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ **where** $Q = q^k$ **and** $q > k$

Take advantage of the itentity $X^q - X = \prod_{\gamma \in \mathbb{F}_q}(X - \gamma)$.

Find $S(X) \in \mathbb{F}_q$ s.t. $\exists I_k(X) | X^q - S(X)$ with a root α.

$$\begin{tikzcd}
 & \mathbb{F}_q[X, Y] \arrow[dl, "\mathrm{mod}\ Y - X^q"'] \arrow[dr, "\mathrm{mod}\ Y - S(X)"] & \\
\mathbb{F}_q[X] \arrow[dr, "\mathrm{mod}\ X - \alpha"'] & & \mathbb{F}_q[Y] \arrow[dl, "\mathrm{mod}\ X - \alpha"] \\
 & \mathbb{F}_Q &
\end{tikzcd}$$

[Joux, 2013] and [BGJT@EC'14] - Half Relation

Given: $h \in \mathbb{F}_Q^{\times} = \langle g \rangle$ **where** $Q = q^k$ **and** $q > k$

Take advantage of the itentity $X^q - X = \prod_{\gamma \in \mathbb{F}_q}(X - \gamma)$.

Find $S(X) \in \mathbb{F}_q$ s.t. $\exists I_k(X) | X^q - S(X)$ with a root α.

$$\begin{tikzcd}
 & \mathbb{F}_q[X, Y] \arrow[dl, "\text{mod } Y - X^q"'] \arrow[dr, "\text{mod } Y - S(X)"] & \\
\mathbb{F}_q[X] \arrow[dr, "\text{mod } X - \alpha"'] & & \mathbb{F}_q[Y] \arrow[dl, "\text{mod } X - \alpha"] \\
 & \mathbb{F}_Q &
\end{tikzcd}$$

From $G_1(Y)G_2(X) - G_1(X)G_2(Y)$ we can reach the relation

$$\prod_{\gamma \in \mathbb{F}_q} (G_1(\alpha) - \gamma G_2(\alpha)) = G_1(S(\alpha))G_2(\alpha) - G_1(\alpha)G_2(S(\alpha))$$

[Joux, 2013] and [BGJT@EC'14]

- Given: $h \in \mathbb{F}_Q^\times = \langle g \rangle$ where $Q = q^k$ and $q > k$; Find: $\log_g h$
- Process
  1. **Main Phase**
     - Initialization Fix parameter B then we obtain $\mathcal{F}_q(B)$ Find $S(X) \in \mathbb{F}_q$ of deg $\leq B$ s.t. $\exists I_k(X) | X^q - S(X)$ with a root α.
     - Smoothness Selection Random $G_1(X), G_2(X)$ of deg $\leq B$ s.t. $G_1(S_2(X))G_2(X) - G_1(X)G_2(S(X))$ is B-smooth, notice deg $\leq B(B+1)$.
     - Relation Collection Known $\prod_{\gamma \in \mathbb{F}_q} (G_1(\alpha) - \gamma G_2(\alpha)) = G_1(S(\alpha))G_2(\alpha) - G_1(\alpha)G_2(S(\alpha))$ and smoothness implies $\prod (G_1(\alpha) - \gamma G_2(\alpha)) = \prod F(\alpha)^{v(F)}$. Then take $\log_g$ and $G_1(\alpha) - \gamma G_2(\alpha) \leftarrow x_\gamma$, $F(\alpha) \leftarrow x_F$
       $$\sum x_\gamma \equiv \sum v(F) x_F \mod Q - 1$$
     - Linear Algebra Solve system of linear equations.
  2. **Individual Logarithm Phase** Descent strategy.

Outline

Paradigm with Transitions

1. **Main Phase**
    - Initiation
    - Smoothness Selection
    - Relation Collection

    - Linear Algebra
2. **Individual Logarithm Phase**

Paradigm with Transitions

1. **Main Phase**
    - Initiation Field extension brings freedom in presentation
    - Smoothness Selection
    - Relation Collection
    - Linear Algebra
2. **Individual Logarithm Phase**

Paradigm with Transitions

1. **Main Phase**
    - Initiation Field extension brings freedom in presentation
    - Smoothness Selection Randomly choose $\Rightarrow$ Sieve
    - Relation Collection
    - Linear Algebra
2. **Individual Logarithm Phase**

Paradigm with Transitions

1. **Main Phase**
   - Initiation Field extension brings freedom in presentation
   - Smoothness Selection Randomly choose $\Rightarrow$ Sieve
   - Relation Collection
     Understanding (virtual) logarithms
   - Linear Algebra
2. **Individual Logarithm Phase**

Paradigm with Transitions

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

Paradigm with Transitions

1. **Main Phase**
   - Initiation Field extension brings freedom in presentation
   - Smoothness Selection Randomly choose $\Rightarrow$ Sieve
   - Relation Collection

     Understanding (virtual) logarithms
   - Linear Algebra Take advantage of the sparseness
2. **Individual Logarithm Phase** Descent Strategy

Research Plan

Preparations

- **Algorithm**
- **Number theory**
- **Polynomials over finite fields**
- **Lattice**
- **Algebraic geometry**

Preparations

- **Algorithm**
  Algorithmic Cryptanalysis by Joux
  Course taken: Computational Number Theory
- **Number theory**
  A Classical Introduction to Modern Number Theory
  by Kenneth, Ireland and Rosen
- **Polynomials over finite fields** 2017 summer schools
- **Lattice** Lectures
- **Algebraic geometry** Course taken

Research Plan

- **Heuristics**: From assumption to rigorous.
  CWZ, 2014: Three Heuristics

Research Plan

- **Heuristics**: From assumption to rigorous.
  CWZ, 2014: Three Heuristics
- **Relation obtaining**
  Use other identities in finite fields and number theory.

Research Plan

- **Heuristics**: From assumption to rigorous.
  CWZ, 2014: Three Heuristics
- **Relation obtaining**
  Use other identities in finite fields and number theory.
- **As for other characteristics**
  Generalization of FFS and NFS.

Thank you! Any questions?

References

1. Diffie W., Hellman M.E., *New directions in cryptography*, IEEE Trans. Inf. Theory, **22**(6), 644-654(1976).
2. Adleman L., *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, In: Proceedings of the 20th Annual Syposium on Foundations of Computer Science: FOCS'79, 55-60.
3. Coppersmith D., *Fast evaluation of logarithms in fields of characteristic two*, IEEE Trans. Inf. Theory, **30**(4): 587-593(1984).
4. ElGmal T., *A publick key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inf. Theory, **31**(4): 469-472(1985).
5. Adleman L., Huang M.D., *Function field sieve method for discrete logarithms over finite fields*, Inf. Comput., **151**(1-2): 5-16(1999).
6. Joux A., Lercier R., *The function field sieve in the medium prime case*, In:Advances in Cryptography: EUROCRYPT'2006, 254-270.
7. Joux A., *A new index calculus algorithm with complexity* $\mathcal{L}(1/4 + o(1))$ *in small characteristic*, In: Selected Areas in Cryptography: SAC'2013, 355-379.
8.
9. Barculescu R., Gaudry P., Joux A., Thomé E., *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, In: Advances in Cryptography: EUROCRYPT'2014, 1-16.
10. Joux A., Pierrot C., *Technical history of discrete logarithms in small characteristic finite fields*, Des. Codes Cryptogr. **78**: 73-85(2016).