The Discrete Logarithms over Kummer and Artin-Schreier extensions

Qi Cheng

School of Computer Science
University of Oklahoma

August 2020
Carleton

The Discrete Logarithm Problem

- Let G be a group. Given $g \in G$ and $t \in < g >$, find an integer e such that $g^e = t$

The Discrete Logarithm Problem

- Let G be a group. Given $g \in G$ and $t \in < g >$, find an integer e such that $g^e = t$
- In cryptography, we use multiplicative groups of finite fields, or additive groups of elliptic curves, whose discrete logarithms are believed to be hard.

The Discrete Logarithm Problem

- Let G be a group. Given $g \in G$ and $t \in < g >$, find an integer e such that $g^e = t$
- In cryptography, we use multiplicative groups of finite fields, or additive groups of elliptic curves, whose discrete logarithms are believed to be hard.
- The hardness of discrete logarithms underpins the security of the widely adopted Diffie-Hellman key exchange protocol, ElGamal's cryptosystem and the Digital Signature Algorithm (DSA signature).

Discrete Logarithms over Finite Fields

$\mathbf{Z}/11\mathbf{Z}$: mod 11

x	1	2	3	4	5	6	7	8	9	10
$2^x \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Table: Modular exponentiation

Discrete Logarithms over Finite Fields

$\mathbf{Z}/11\mathbf{Z}$: mod 11

x	1	2	3	4	5	6	7	8	9	10
$2^x \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Table: Modular exponentiation

y	1	2	3	4	5	6	7	8	9	10
$\log_2(y) \pmod{11}$	10	1	8	2	4	9	7	3	6	5

Table: Discrete logarithms

One way function

- Exponentiation in $\mathbf{Z}$ is not interesting in crypto.

$$123^{78} = 102943443687041086556712712561297256464439108707995615998161311200551000637347694926511144654271190781700616533751002791494939467498733074511507739021952499604016 9$$

One way function

- Exponentiation in $\mathbf{Z}$ is not interesting in crypto.

$$123^{78} = 102943443687041086556712712561297256464439108707995615998161311200551000637347694926511144654271190781700616533751002791494939467498733074511507739021952499604016 9$$

- $173019370738947249278 47^{375917359365913591765489}$?

One way function

- Exponentiation in $\mathbf{Z}$ is not interesting in crypto.

$$123^{78} = 102943443687041086556712712561297256464439108707995615998161311200551000637347694926511144654271190781700616533751002791494939467498733074511507739021952499604016 9$$

- $173019370738947249278 47^{375917359365913591765489}$?
- $173019370738947249278 47^{375917359365913591765489} \pmod{90237590817358 7347} = 80607419671928 2603$

One way function

- Exponentiation in $\mathbf{Z}$ is not interesting in crypto.

$$123^{78} = 102943443687041086556712712561297256464439108707995615998161311200551000637347694926511144654271190781700616533751002791494939467498733074511507739021952499604016 9$$

- $173019370738947249278 47^{375917359365913591765489}$?
- $173019370738947249278 47^{375917359365913591765489} \pmod{90237590817358 7347} = 80607419671928 2603$
- $173019370738947249278 47^{x} \pmod{90237590817358 7347} = 29571975618561$?

The generic algorithm

- (Trivial) Exhaustively search for e such that $g^e = t$.

The generic algorithm

- (Trivial) Exhaustively search for e such that $g^e = t$.
- Time comlexity $O(N)$. Here $N = | < g > |$.

The generic algorithm

- (Trivial) Exhaustively search for e such that $g^e = t$.
- Time comlexity $O(N)$. Here $N = | < g > |$.
- (The Birthday Attack) Search for i_1, j_1 and i_2, j_2 such that $g^{i_1} t^{j_1} = g^{i_2} t^{j_2}$.

The generic algorithm

- (Trivial) Exhaustively search for e such that $g^e = t$.
- Time comlexity $O(N)$. Here $N = | < g > |$.
- (The Birthday Attack) Search for i_1, j_1 and i_2, j_2 such that $g^{i_1} t^{j_1} = g^{i_2} t^{j_2}$.
- Time complexity $O(\sqrt{N})$.

Smoothness

- An integer is B-smooth if all of its prime factors are at most B.

Smoothness

- An integer is B-smooth if all of its prime factors are at most B.
- $160051827733596222119 43 = 3 * 7^3 * 17^2 * 101 * 127^7$

Smoothness

- An integer is B-smooth if all of its prime factors are at most B.
- $160051827733596222119 43 = 3 * 7^3 * 17^2 * 101 * 127^7$
- A polynomial is b-smooth if all of its irreducible factors have degrees at most b.

Smoothness

- An integer is B-smooth if all of its prime factors are at most B.
- $160051827733596222119 43 = 3 * 7^3 * 17^2 * 101 * 127^7$
- A polynomial is b-smooth if all of its irreducible factors have degrees at most b.
- $x^7 + 5 * x^6 + 11 * x^5 + 5 * x^4 + 11 * x^2 + 6 * x + 14 = (x + 1) * (x + 2)^3 * (x + 5)^3$ over $GF(17)$.

Index Calculus

- Search for *many* (i, j) such that (the lift of) $g^i t^j$ is smooth.

Index Calculus

- Search for *many* (i, j) such that (the lift of) $g^i t^j$ is smooth.
- Example:
  $GF(2^{10}) = GF(2)[x]/(x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1)$

$(x^9 + x^8 + 1)^{977} \quad (= \quad x^{8793} + ...)$

Index Calculus

- Search for *many* (i, j) such that (the lift of) $g^i t^j$ is smooth.
- Example:
  $GF(2^{10}) = GF(2)[x]/(x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1)$

$$
\begin{aligned}
(x^9 + x^8 + 1)^{977} \quad (= \quad & x^{8793} + \ldots\ldots\ldots) \\
\equiv \quad & x^9 + x^7 + x^3 + x \\
& \pmod{x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1}
\end{aligned}
$$

Index Calculus

- Search for *many* (i, j) such that (the lift of) $g^i t^j$ is smooth.
- Example:
  $GF(2^{10}) = GF(2)[x]/(x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1)$

$$
\begin{aligned}
(x^9 + x^8 + 1)^{977} \quad (= \quad & x^{8793} + \ldots\ldots\ldots) \\
\equiv \quad & x^9 + x^7 + x^3 + x \\
& \pmod{x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1} \\
= \quad & x(x+1)^4(x^2 + x + 1)^2
\end{aligned}
$$

- $977 = \log x + 4\log(x+1) + 2\log(x^2 + x + 1)$

Relation

- One pair gives us one *relation*:

$$g^i t^j = \prod_{s \ \ irreducible, deg(s) \leq b} s^{e_s}$$

Relation

- One pair gives us one *relation*:

$$g^i t^j = \prod_{s \ \ irreducible, deg(s) \leq b} s^{e_s}$$

- $i + j \log_g t = \sum e_s \log_g s$

Relation

- One pair gives us one *relation*:

$$g^i t^j = \prod_{s \ \text{irreducible}, \deg(s) \leq b} s^{e_s}$$

- $i + j \log_g t = \sum e_s \log_g s$
- Finding $\log_g t$ is reduced to solving a linear system. We also find the logarithm of all the small prime or low degree irreducible polynomials, which form the *factor base*.

Index Calculus

- Many *relations*:

$$g^i = \prod_{s \text{ irreducible}, deg(s) \leq b} s^{e_s}$$

- Solve the linear system

$$i = \sum e_s \log_g s$$

  to find the discrete logarithms in factor base $\log_g s$.
- One more relation to find $\log_g t$:

$$g^i t = \prod_{s \text{ irreducible}, deg(s) \leq b} s^{e_s}$$

Index Calculus

- Many *relations*:

$$g^i = \prod_{s \text{ irreducible}, deg(s) \leq b} s^{e_s}$$

- Solve the linear system

$$i = \sum e_s \log_g s$$

  to find the discrete logarithms in factor base $\log_g s$.
- One more relation to find $\log_g t$:

$$g^i t = \prod_{s \text{ irreducible}, deg(s) \leq b} s^{e_s}$$

- The first two steps do not involve t.

Logjam Attack– Even you use prime order fields (Adrian et al.)

- Precomputing downgrades the Diffie-Hellman protocol.
- One relation is easier to find than collecting many relations and solving linear equations.

$$\begin{aligned} &\text{Relations in factor base} \\ &\quad \Longrightarrow \text{linear algebra} \\ &\quad \Longrightarrow \text{relation for t and factor base} \end{aligned}$$

Time Complexity

- The probability that a random polynomial of degree k ($\geq b$) over a finite field $\mathbf{F}_q$ is $b-$smooth is about $(k/b)^{-k/b}$.
- There are about q^b/b many irreducible polynomials of degree b.
- In $\mathbf{F}_{2^k}$, take $b \approx \sqrt{k}$.
- Time complexity $exp(\tilde{O}(\sqrt{\log N}))$. (compare to the generic algorithm $exp(O(\log N))$.)
- Number field sieve or function field sieve $exp(\tilde{O}(\sqrt[3]{\log N}))$.

Recent Works

- DL in $\mathbf{F}_{2^{1971}} = \mathbf{F}_{134217728^{73}}$ (GGMZ, Feb, 2013). Note that $73|134217727$.
- $exp(\tilde{O}(\sqrt[4]{\log N}))$ for small characteristic fields (Joux, Feb, 2013).
- DL in $\mathbf{F}_{2^{4080}} = \mathbf{F}_{256^{2*255}}$ (Joux, March, 2013).
- DL in $\mathbf{F}_{2^{6120}} = \mathbf{F}_{16777216^{255}}$ (GGMZ, April, 2013). Note that $255|16777215$.
- DL in $\mathbf{F}_{2^{6168}} = \mathbf{F}_{256^{3*257}}$ (Joux, May, 2013).

- Finding primitive elements (Huang-Narayanan, May 2013).
- The Barbulescu-Gaudry-Joux-Thome algorithm (June, 2013).
- DL in $\mathbf{F}_{3^{6\times 509}}$ is weak (AMOH, July, 2013).
- Traps in BGJT (C.-Wan-Zhuang, Oct, 2013).
- BGJT Version 2, AMOH Version 2 (Nov, 2013).
- DL in $\mathbf{F}_{3^{6\times 1429}}$ and $\mathbf{F}_{2^{4\times 3041}}$ are weak (AMOH, Nov, Dec, 2013).
- Discrete logarithm record in characteristic 3, $GF(3^{5\times 479})$ (a 3796-bit field) (Joux and Pierrot Sept 2014)
- Discrete Logarithms in $GF(2^{1279})$ (Thorsten Kleinjung Oct 2014). Note that 1279 is a prime.
- Discrete logarithms in the finite field $\mathbf{F}_{2^{30750}}$. Robert Granger, Thorsten Kleinjung Arjen Lenstra, Benjamin Wesolowski, Jens Zumbragel. July 2019.

Large characteristic

- $\mathbf{F}_p$ where $p \approx 10^{180}$. (Cyril Bouvier, Pierrick Gaudry, Laurent Imbert, Hamza Jeljeli and Emmanuel Thome. June 11, 2014)
- $\mathbf{F}_{p^2}$ where $p^2 \approx 10^{160}$. (Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, Francois Morain, June 24, 2014.)
- Discrete Logarithms in $GF(p)$ where $p \approx 2^{768} \approx 10^{231}$ (Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, Colin Stahlke, June 2016)
- Discrete logarithm computation in $GF(p^5)$ for a 20-decimal digit prime. Laurent Gremy, Aurore Guillevic, Francois Morain, August 2017.
- $\mathbf{F}_{p^6}$ where $p^6 \approx 10^{423}$. Gary McGuire, Oisin Robinson, Jan 2020.
- Discrete Logarithms in $GF(p)$ where $p \approx 2^{795} \approx 10^{240}$. F. Boudot and P. Gaudry and A. Guillevic and N. Heninger and E. Thome and P. Zimmermann, June 2020.

Quasi-Polynomial Time Algorithm

- A breakthrough result by Barbulescu, Gaudry, Joux and Thomé.

Quasi-Polynomial Time Algorithm

- A breakthrough result by Barbulescu, Gaudry, Joux and Thomé.
- For a finite field $\mathbf{F}_{q^{2k}}$ with $k < q$, their algorithm runs in heuristic time $q^{O(\log k)}$. (compare with $q^{\tilde{O}(\sqrt{k})}$ or $q^{\tilde{O}(\sqrt[3]{k})}$).

Quasi-Polynomial Time Algorithm

- A breakthrough result by Barbulescu, Gaudry, Joux and Thomé.
- For a finite field $\mathbf{F}_{q^{2k}}$ with $k < q$, their algorithm runs in heuristic time $q^{O(\log k)}$. (compare with $q^{\tilde{O}(\sqrt{k})}$ or $q^{\tilde{O}(\sqrt[3]{k})}$).
- This result essentially removes the discrete logarithm over small characteristic fields from the set of hard problems in cryptography.

Set up

- Suppose that the discrete logarithm is sought over the field $\mathbf{F}_{q^{2k}}$ with $k < q$.
- For other small characteristic fields such as $\mathbf{F}_{p^k}$ ($p < k$), one first embeds it into a slightly larger field:

$$\mathbf{F}_{p^k} \hookrightarrow \mathbf{F}_{q^k}, \quad \mathbf{F}_{q^k} \hookrightarrow \mathbf{F}_{q^{2k}}$$

where $q = p^{\lceil \log_p k \rceil}$. For example,

$$\mathbf{F}_{2^{1021}} \hookrightarrow \mathbf{F}_{2^{10\times 1021}}, \quad \mathbf{F}_{2^{10\times 1021}} \hookrightarrow \mathbf{F}_{2^{2\times 10\times 1021}}$$

- A quasi-polynomial time algorithm for $\mathbf{F}_{q^{2k}}$ implies a quasi-polynomial time algorithm for $\mathbf{F}_{p^k}$.

A nice model of the finite field $\mathbf{F}_{q^{2k}}$

- We assume that

$$\mathbf{F}_{q^{2k}} = \mathbf{F}_{q^2}[X]$$

where $X^q = \frac{h_0(X)}{h_1(X)}$. Here h_0 and h_1 are polynomials over $\mathbf{F}_{q^2}$ of degrees at most 2.

A nice model of the finite field $\mathbf{F}_{q^{2k}}$

- We assume that
$$\mathbf{F}_{q^{2k}} = \mathbf{F}_{q^2}[X]$$
where $X^q = \frac{h_0(X)}{h_1(X)}$. Here h_0 and h_1 are polynomials over $\mathbf{F}_{q^2}$ of degrees at most 2.
- To find such a nice ring generator X, one searches over all the polynomials $h_0(x)$ and $h_1(x)$ of degree ≤ 2 in $\mathbf{F}_{q^2}[x]$, until $h_1(x)x^q - h_0(x)$ has an irreducible factor $f(x)$ of degree k.

Discrete logarithms of elements in the factor base

In the new approach, the factor base consists of the linear polynomials $X + \alpha$ for all $\alpha \in \mathbf{F}_{q^2}$, and an algorithm is designed to compute the discrete logarithms of all the elements in the factor base.

Pinpointing

One starts the algorithm with the identity in $\mathbf{F}_{q^2}[x]$:

$$\prod_{\alpha \in \mathbf{F}_q} (x - \alpha) = x^q - x.$$

Pinpointing

One starts the algorithm with the identity in $\mathbf{F}_{q^2}[x]$:

$$\prod_{\alpha \in \mathbf{F}_q} (x - \alpha) = x^q - x.$$

A potential relation:

$$\prod_{\alpha \in \mathbf{F}_q} (x - \alpha) = \frac{h_0(x)}{h_1(x)} - x \pmod{x^q h_1(x) - h_0(x)}$$

Pinpointing – More relations

Apply the Mobius transformation

$$x \mapsto \frac{ax + b}{cx + d}$$

where the matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{F}_{q^2}^{2\times 2}$ is nonsingular.

Pinpointing – More relations

Apply the Mobius transformation

$$x \mapsto \frac{ax+b}{cx+d}$$

where the matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{F}_{q^2}^{2\times 2}$ is nonsingular. We have

$$\prod_{\alpha \in \mathbf{F}_q} \left(\frac{ax+b}{cx+d} - \alpha\right) = \left(\frac{ax+b}{cx+d}\right)^q - \frac{ax+b}{cx+d}$$

An equation in $\mathbf{F}_{q^2}[x]$

Clearing the denominator:

$$\begin{aligned} & (cx+d)\prod_{\alpha\in\mathbf{F}_q}((ax+b)-\alpha(cx+d)) \\ = \quad & (ax+b)^q(cx+d)-(ax+b)(cx+d)^q \end{aligned}$$

An equation in $\mathbf{F}_{q^2}[x]$

Clearing the denominator:

$$\begin{aligned}
& (cx+d)\prod_{\alpha\in\mathbf{F}_q}((ax+b)-\alpha(cx+d)) \\
= \quad & (ax+b)^q(cx+d)-(ax+b)(cx+d)^q \\
= \quad & (a^qx^q+b^q)(cx+d)-(ax+b)(c^qx^q+d^q).
\end{aligned}$$

Moving to the residue class ring $\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x))$

Multiplying both sides by $h_1(x)$ and replacing $x^q h_1(x)$ by $h_0(x)$, we obtain

$$\begin{aligned} & h_1(x)(cx+d) \prod_{\alpha \in \mathbf{F}_q} ((ax+b) - \alpha(cx+d)) \\ = \quad & (a^q h_0(x) + b^q h_1(x))(cx+d) - (ax+b)(c^q h_0(x) + d^q h_1(x)) \\ & \pmod{x^q h_1(x) - h_0(x)}. \end{aligned}$$

Moving to the residue class ring $\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x))$

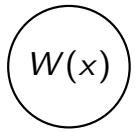
Multiplying both sides by $h_1(x)$ and replacing $x^q h_1(x)$ by $h_0(x)$, we obtain

$$\begin{aligned} & h_1(x)(cx+d) \prod_{\alpha \in \mathbf{F}_q} ((ax+b) - \alpha(cx+d)) \\ = \quad & (a^q h_0(x) + b^q h_1(x))(cx+d) - (ax+b)(c^q h_0(x) + d^q h_1(x)) \\ & \pmod{x^q h_1(x) - h_0(x)}. \end{aligned}$$

- Matrics in each coset in $PGL(2, q^2)/PGL(2, q)$ gives the equation.
- The right hand side has degree at most 3. If it can be factored completely, then we have a relation!

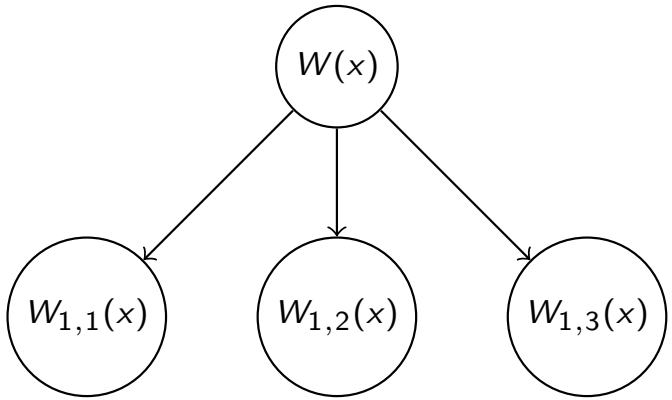
- One hopes to collect enough relations such that the linear system formed by those relations is non-singular over $\mathbf{Z}/(q^{2k}-1)\mathbf{Z}$. It allows us to solve $\log(X+\alpha_i)$ for all the $\alpha \in \mathbf{F}_{q^2}$ in the factor base.

Descending



$degree = w$

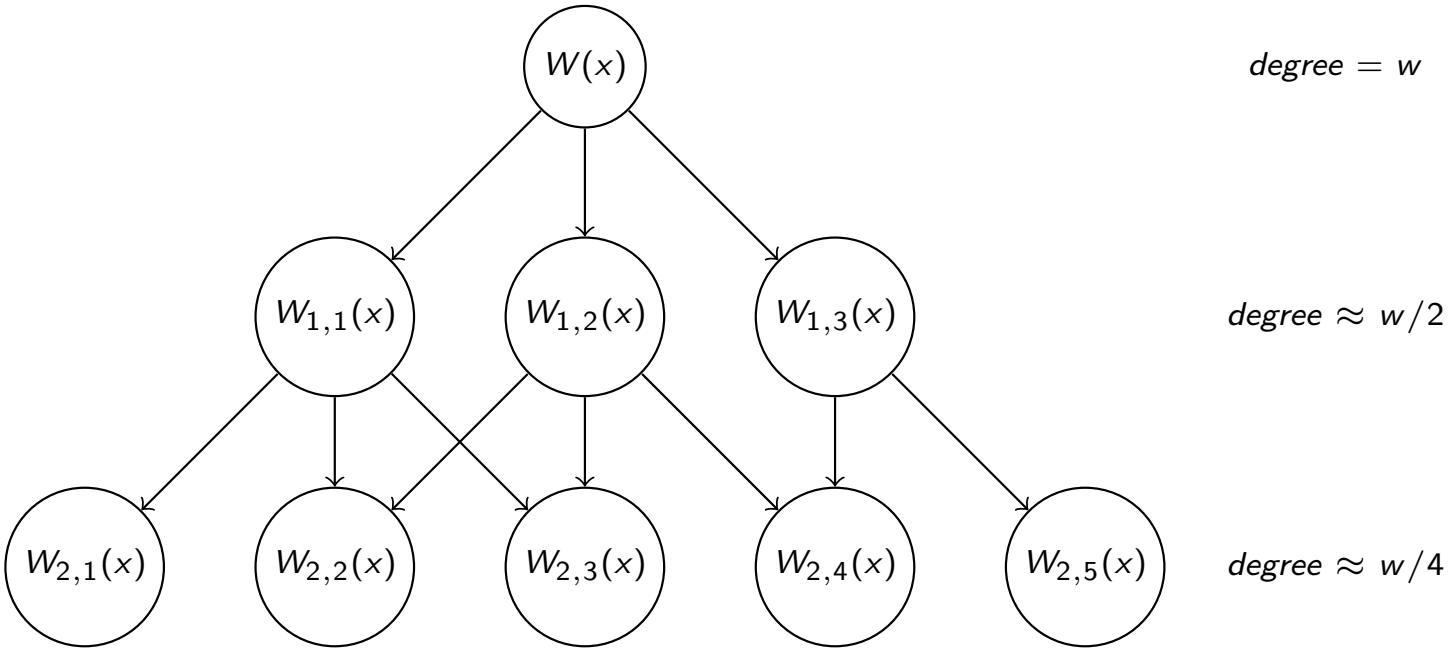
Descending



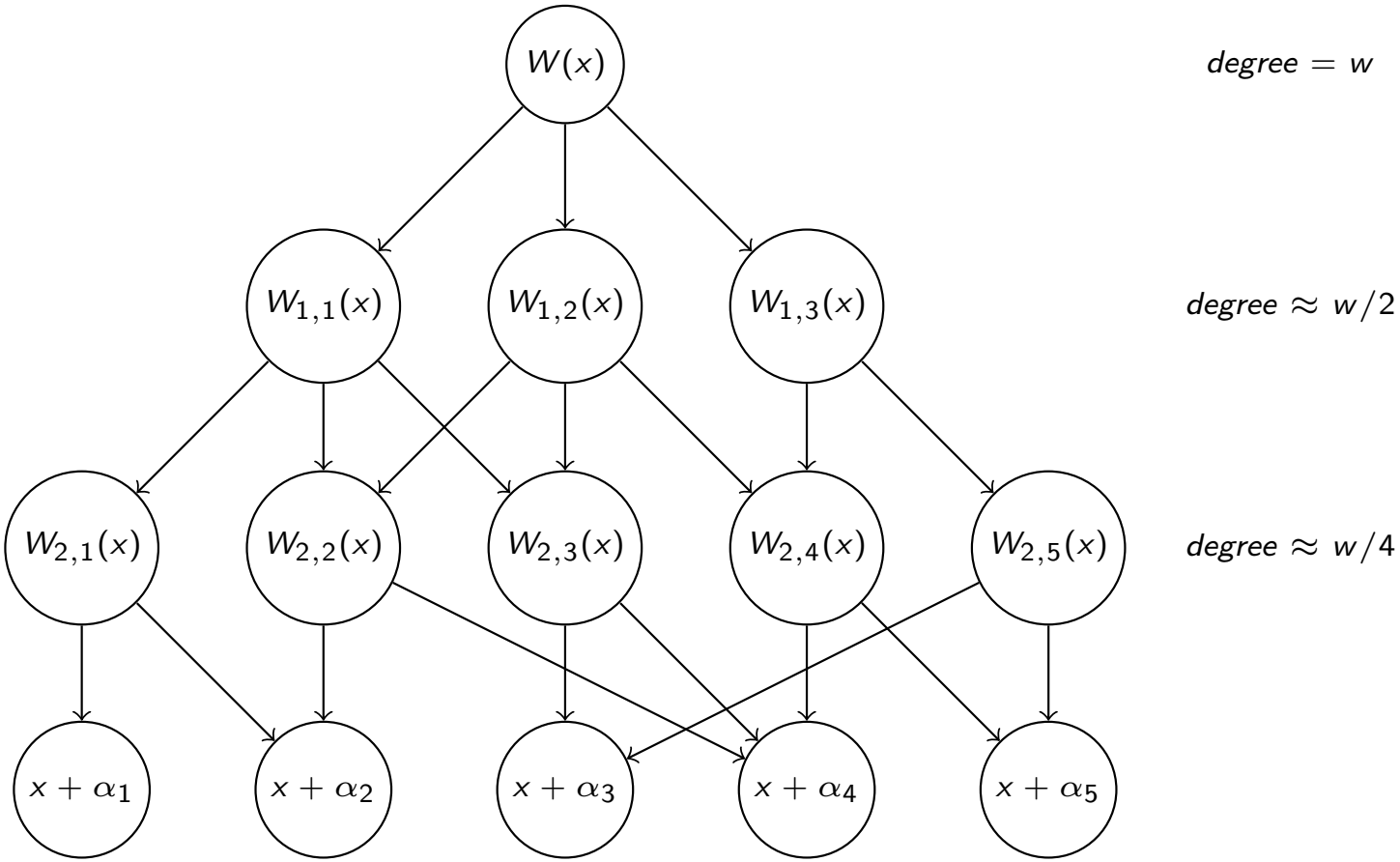
$degree = w$

$degree \approx w/2$

Descending


$W(x)$
$W_{1,1}(x)$
$W_{1,2}(x)$
$W_{1,3}(x)$
$W_{2,1}(x)$
$W_{2,2}(x)$
$W_{2,3}(x)$
$W_{2,4}(x)$
$W_{2,5}(x)$
$degree = w$
$degree \approx w/2$
$degree \approx w/4$

Descending


$W(x)$
$W_{1,1}(x)$
$W_{1,2}(x)$
$W_{1,3}(x)$
$W_{2,1}(x)$
$W_{2,2}(x)$
$W_{2,3}(x)$
$W_{2,4}(x)$
$W_{2,5}(x)$
$x + \alpha_1$
$x + \alpha_2$
$x + \alpha_3$
$x + \alpha_4$
$x + \alpha_5$
$degree = w$
$degree \approx w/2$
$degree \approx w/4$

Toward Provable Deterministic complexity

- For any (n, q) $(n < q)$ of cryptographic interests, the small degree polynomials $h_0(x)$ and $h_1(x)$ can be found easily so that $x^q h_1(x) - h_0(x)$ has an irreducible factor of degree n. However proving that they exist in general is a very hard mathematical problem.
- One can compare it with the much weaker Hansen-Mullen Conjecture concerning the distribution of irreducible polynomials with some prefixed coefficients, and subsequent work.

The Kummer extension $\mathbf{F}_{q^{2(q-1)}}$

- It can be modeled by $\mathbf{F}_{q^2}[x]/(x^{q-1} - A)$, where $A \in \mathbf{F}_{q^2}$ and $x^{q-1} - A$ is irreducible over $\mathbf{F}_{q^2}$.
- In this case, $h_1(x) = 1, h_0(x) = Ax$.
- Let $< g >= \mathbf{F}_{q^2}$

Relations without smoothness assumption

$$
\begin{aligned}
& (cx+d)\prod_{\alpha\in\mathbb{F}_q}((ax+b)-\alpha(cx+d)) \\
= \quad & (a^qAx+b^q)(cx+d)-(ax+b)(c^qAx+d^q) \\
= \quad & A(a^qc-ac^q)x^2+((b^qc-ad^q)-A(bc^q-a^qd))x+(b^qd-bd^q)
\end{aligned}
$$

What if $a^qc-ac^q=0$?

The Borel subgroup

Note that

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbf{F}_{q^2}^*, b \in \mathbf{F}_{q^2} \right\}$$

is the Borel subgroup of $PGL_2(\mathbf{F}_{q^2})$. We should only consider $PGL_2(\mathbf{F}_q)-$coset representatives, which can be partitioned into two subsets

$$\left\{ \begin{pmatrix} a & g \\ 0 & 1 \end{pmatrix} \mid a \in \mathbf{F}_{q^2}^* \right\} \cup \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbf{F}_{q^2}^* / \mathbb{F}_q^* \right\}.$$

The linear system Borel1

We obtain a linear system

$$\forall a \in \mathbf{F}_{q^2}^*, \sum_{\alpha \in \mathbb{F}_q} \log(X + \frac{g - \alpha}{a}) = \log(X + \frac{g^q - g}{a^q A - a}) \qquad (1)$$

of $q^2 - 1$ equations in $q^2 - 1$ variables, which represent $\log(x + h)$ ($h \in \mathbf{F}_{q^2}^*$). Here log is for the group $\mathbf{F}_{q^{2(q-1)}}^* / \mathbf{F}_{q^2}^*$.

The linear system Borel2

The second subset gives us a system of $q+1$ equations:

$$\forall a \in \mathbf{F}_{q^2}^*/\mathbf{F}_q^*, \sum_{\alpha \in \mathbb{F}_q^*} \log(X + \frac{-\alpha}{a}) = 0. \tag{2}$$

Borel1 is not good enough

Theorem

The system (1) has a kernel over $\mathbf{Q}$ *of dimension much bigger than* 1. *(Xiao-Zhuang-C.)*

Borel1+Borel2 is not good enough

Can we avoid the problem by adding the linear equations (2)? In the same paper we found that when $q = 31$, the discrete logarithm over the subgroup of size $l = 2521$ can not be uniquely determined by the linear system (1) plus (2). Furthermore, even in the case that (1) plus (2) is sufficient, it is not efficient, since we need to solve a linear system with $O(q^2)$ many variables, namely $\log(x + \alpha), \alpha \in \mathbf{F}_{q^2}$.

Frobenius comes to rescue

Note that over $\mathbf{F}^*_{q^{2(q-1)}}/\mathbf{F}^*_{q^2}$, $(X+a)^{q^2} = X + \frac{a}{A^{q+1}}$, thus we get

$$\forall a \in \mathbf{F}^*_{q^2},\ q^2 \log(X+a) = \log\left(X + \frac{a}{A^{q+1}}\right). \tag{3}$$

If we add (3), numerical data confirm that discrete logarithm can always be found.

Define four linear transformations C, G, T and F over the $\mathbb{C}$-linear space $\mathbb{C}[x]/(x^{q^2-1}-1)$ as:

$$C(x^k) = \sum_{\alpha \in \mathbb{F}_q} x^{\log_g\left(-\alpha \cdot \frac{Ag^{kq}-g^k}{g^q-g}\right)}$$

$$G(x^k) = x^k \sum_{\alpha \in \mathbb{F}_q} x^{\log_g(g+\alpha)}$$

$$T(x^k) = x^k x^{\log_g \frac{Ag^{k(q-1)}-1}{g^q-g}}$$

$$F(x^k) = q^2 x^{k-\log_g(A^{q+1})}$$

The Conjecture

Let l be a prime factor of $q^{2(q-1)} - 1$ which is greater than $q^2 - 1$. Then over $\mathbf{F}_l$, the vector of the discrete logarithms of the linear polynomials is in the kernel space of C, and it is in the fixed space of GT and F.

Conjecture

The subspace fixed by GT and F is one-dimensional.

It implies that we can find a generator of subgroup of cardinality N, and determine the factor base discrete logarithm with respect to that element in the subgroup. We have verified the conjecture for all the prime power q less than 307.

Theorem

Assume that the conjecture is true. We can find a generator of the subgroup of cardinality N of $\mathbf{F}^*_{q^{2(q-1)}}$, and compute the discrete logarithms of linear factors with respect to the generator in bit complexity $O(q^{1+\omega})$. Here $\omega \leq 2.38$ is the exponent parameter of fast matrix multiplication over rings.

Eigenvalues of M over $\mathbb{C}$

Theorem

The kernel of C is a invariant subspace of M. On that subspace, all of the eigenvalues of M have complex norm $\sqrt{q}$.

Lemma

Acting on any subspace $\mathbb{C}[x]/(x^{q+1} - \zeta_{q-1}^{i})(1 \leq i \leq q-2)$, *all of the eigenvalues of* G_i *have complex norm* $\sqrt{q}$.

Lemma

Let μ *be a multiplicative character for* $\mathbf{F}_{q^2}$ *that is not trivial over* $\mathbb{F}_q^*$, *we have* $|\sum_{\alpha \in \mathbb{F}_q} \mu(g+\alpha)| = \sqrt{q}$.

The Artin-Schreier extension

Consider $K = \mathbf{F}_{p^2}[x]/(x^p - x - 1)$, where p is an odd prime. Let $g \in \mathbf{F}_{p^2} - \mathbf{F}_p$ such that $g^2 \in \mathbf{F}_p$.

- Mobius Transformation

$$\begin{aligned} & AX^2 + BX + C \\ \equiv \quad & (cX + d) \prod_{\alpha \in \mathbf{F}_p} [(a + \alpha c)X + (b + \alpha d)], \end{aligned} \tag{4}$$

  where $A = a^p c - a c^p$, $B = a^p c - a c^p + b^p c - b c^p + a^p d - a d^p$ and $C = a^p d - b c^p + b^p d - b d^p$.

- Borel relations

Frobenius relations

$$(X + \mu_1 g + \mu_2)^{p^i} = \begin{cases} X + \mu_1 g + \mu_2 + i, & \text{if } 2 \mid i \\ X - \mu_1 g + \mu_2 + i, & \text{if } 2 \nmid i \end{cases} \tag{5}$$

Borel+Frobenius are not enough

Theorem

(Xiao-C.)Given $K = \mathbf{F}_{p^2}[x]/(x^p - x - 1)$, *the linear system generated by the degenerated relations of Equation (4) where* $a^q c - a c^q = 0$ *and the Frobenius relation (5) holds a kernel of dimension* $\geq \frac{p-3}{4}$. *That is, these relations generated by transformations in the Borel subgroup and the Frobenius endomorphism are not sufficient to recover the discrete logarithms of linear factor in subgroup* $K^*/\mathbf{F}_{p^2}^*$.

Pinpointing for Artin-Schreier

For every $\mu \in \mathbf{F}_p$,

$$\begin{aligned} &\log(X + \mu g) + \log(X - \mu g + 3) \\ &= \sum_{k^{p+1} = -8\mu^2 g^2 + 2} \log(X + 3\mu g + 1 + k). \end{aligned} \tag{6}$$

Conjecturally there exists an algorithm with bit complexity $\tilde{O}(p^{1+\omega})$ that computes the discrete logarithms of linear factors modulo N, and a primitive element of $K^*/\mathbf{F}_{p^2}^*$.

Future works

- Remove the heuristics.

Future works

- Remove the heuristics.
- Adopt the new ideas for large characteristic fields.

Future works

- Remove the heuristics.
- Adopt the new ideas for large characteristic fields.
- And for the integer factorization problem

Future works

- Remove the heuristics.
- Adopt the new ideas for large characteristic fields.
- And for the integer factorization problem
- Or they are not possible because problems about number fields are inherently harder than problems about function fields?

The end

Thank you! and questions?