ECC, Chennai — October 8, 2014

A heuristic quasi-polynomial algorithm for discrete logarithm in small characteristic

Razvan Barbulescu[1] Pierrick Gaudry[2] Antoine Joux[3]
Emmanuel Thomé[2]

IMJ-PRG, Paris

Loria, Nancy

LIP6, Paris

Context

The discrete logarithm problem (DLP)

In a cyclic group G, given a generator g and an element g^a, FIND a.
We can search the smallest positive integer solution a or, more common, the residue of a modulo a prime factor ℓ of $\#G$.

Choices for G

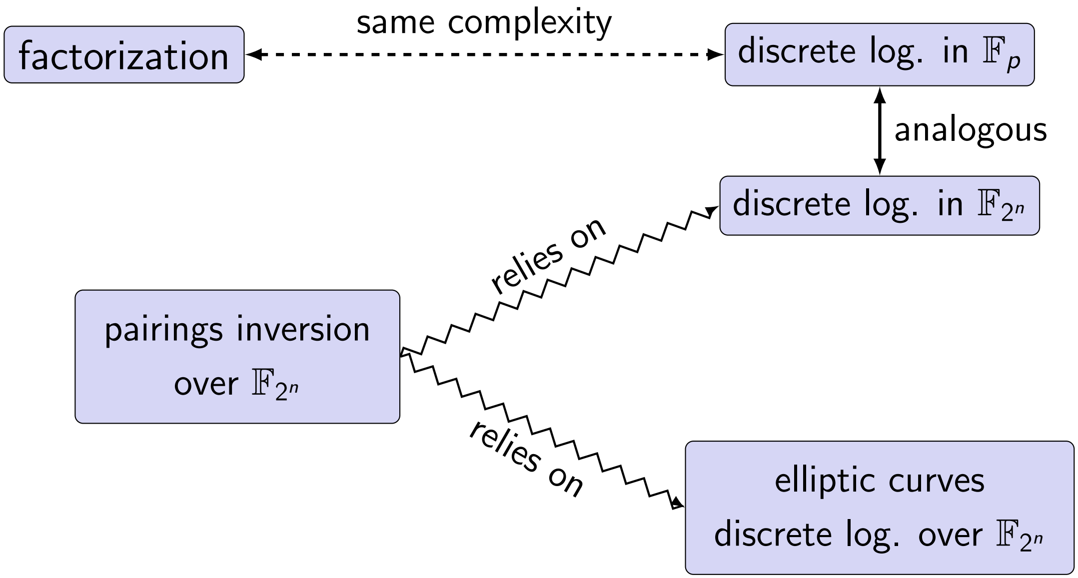
1. elliptic curves (estimated of exponential difficulty);
2. multiplicative group of finite fields (subexponential)
   2.1 small characteristic, e.g. $\mathbb{F}_{2^n}$ and $\mathbb{F}_{3^n}$,
   2.2 non-small characteristic, e.g. $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$

Example

When $G = (\mathbb{F}_p)^*$, given two integers g and h, if it exists, FIND x in

$$g^x \equiv h \mod p.$$

Motivation



F_Q is the field of Q elements, Q prime power.

Shanks' baby-step giant-step algorithm

Let $K \approx \sqrt{N}$ and write the discrete log of x as

$$x = x_0 + K\, x_1, \quad \text{with} \quad 0 \leq x_0 < K \text{ and } 0 \leq x_1 < N/K.$$

Algorithm

1. Compute **Baby Steps**:
   For all i in $[0, K-1]$, compte g^i.
   Store in a hash table the resulting pairs (g^i, i).
2. Compute **Giant Steps**:
   For all j in $[0, \lfloor N/K \rfloor]$, compute hg^{-Kj}.
   If the resulting element is in the BS table, then get the corresponding i, and return $x = i + Kj$.

Theorem

Discrete logarithms in a cyclic group of order N can be computed in less than $2\lceil\sqrt{N}\rceil$ operations.

Shanks' baby-step giant-step algorithm

Let $K \approx \sqrt{N}$ and write the discrete log of x as

$$x = x_0 + K\,x_1, \quad \text{with} \quad 0 \leq x_0 < K \text{ and } 0 \leq x_1 < N/K.$$

Algorithm

1. Compute **Baby Steps**:
   For all i in $[0, K-1]$, compte g^i.
   Store in a hash table the resulting pairs (g^i, i).
2. Compute **Giant Steps**:
   For all j in $[0, \lfloor N/K \rfloor]$, compute hg^{-Kj}.
   If the resulting element is in the BS table, then get the corresponding i, and return $x = i + Kj$.

Theorem

Discrete logarithms in a cyclic group of order N can be computed in less than $2\lceil\sqrt{N}\rceil$ operations.

$\boxed{\text{Multiplicative group of finite fields is } \textbf{not} \text{ a generic groups!}}$

History

For two constatnts $\alpha \in [0,1]$ and $c > 0$, we put

$$L_Q(\alpha, c) = \exp\left((c + o(1))(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\right)$$

Put $n = \log Q$.

- $L_Q(0) = n^{O(1)}$ i.e. polynomial;
- $L_Q(1) = 2^{O(n)}$ i.e. exponential;
- $L_Q(1/2) \approx 2^{\sqrt{n}}$; DLP algorithms invented in $1979 - 1994$.
- $L_Q(1/3) \approx 2^{\sqrt[3]{n}}$; DLP algorithms invented in $1984 - 2006$.

Smoothness

Definition

A polynomial in $\mathbb{F}_q[t]$ is m-smooth if it factors into polynomials of degree less than or equal to m.

Computation

One can test if a polynomial is smooth by factoring it (probabilistic polynomial).

Theorem (Panario–Gourdon–Flajolet)

The probability that a degree-n polynomial is m-smooth is $1/u^{u(1+o(1))}$ where $u = \frac{n}{m}$.

Cases:

- $n = D$, $m = D/6$ gives a constant probability;
- $n = D$, $m = 1$ gives a probability $1/D! \approx 1/D^D$.
- $n = \log_q L_x(\alpha, \cdot)$, $m = \log_q L_x(\beta, \cdot)$ gives a probability of $1/L_x(\alpha - \beta, \cdot)$;

Obtaining relations

The finite field $\mathbb{F}_{q^k}$ is represented as $\mathbb{F}_q[t]/\varphi$
for an irreducible polynomial $\varphi \in \mathbb{F}_q[t]$ of degree k.

Example

Take $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$. We have

$$t^5 \equiv 2(t+1)(t^3+t^2+2t+1) \mod \varphi$$

Obtaining relations

The finite field $\mathbb{F}_{q^k}$ is represented as $\mathbb{F}_q[t]/\varphi$
for an irreducible polynomial $\varphi \in \mathbb{F}_q[t]$ of degree k.

Example

Take $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$. We have

$$\begin{aligned} t^5 &\equiv 2(t+1)(t^3+t^2+2t+1) && \mod \varphi \\ t^6 &\equiv 2(t^2+1)(t^2+t+2) && \mod \varphi \end{aligned}$$

Obtaining relations

The finite field $\mathbb{F}_{q^k}$ is represented as $\mathbb{F}_q[t]/\varphi$
for an irreducible polynomial $\varphi \in \mathbb{F}_q[t]$ of degree k.

Example

Take $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$. We have

$$\begin{aligned} t^5 &\equiv 2(t+1)(t^3+t^2+2t+1) && \mod \varphi \\ t^6 &\equiv 2(t^2+1)(t^2+t+2) && \mod \varphi \\ t^7 &\equiv 2(t+2)(t+1)(t+1) && \mod \varphi \end{aligned}$$

Obtaining relations

The finite field $\mathbb{F}_{q^k}$ is represented as $\mathbb{F}_q[t]/\varphi$
for an irreducible polynomial $\varphi \in \mathbb{F}_q[t]$ of degree k.

Example

Take $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$. We have

$$\begin{aligned} t^5 &\equiv 2(t+1)(t^3+t^2+2t+1) && \mod \varphi \\ t^6 &\equiv 2(t^2+1)(t^2+t+2) && \mod \varphi \\ t^7 &\equiv 2(t+2)(t+1)(t+1) && \mod \varphi \end{aligned}$$

The last relation gives:

$$7 \log_g t \equiv \log_g 2 + 1 \log_g(t+2) + 2 \log_g(t+1) \mod 11$$

Obtaining relations

The finite field $\mathbb{F}_{q^k}$ is represented as $\mathbb{F}_q[t]/\varphi$ for an irreducible polynomial $\varphi \in \mathbb{F}_q[t]$ of degree k.

Example

Take $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$. We have

$$\begin{aligned} t^5 &\equiv 2(t+1)(t^3+t^2+2t+1) && \mod \varphi \\ t^6 &\equiv 2(t^2+1)(t^2+t+2) && \mod \varphi \\ t^7 &\equiv 2(t+2)(t+1)(t+1) && \mod \varphi \end{aligned}$$

The last relation gives:

$$7 \log_g t \equiv 1 \log_g(t+2) + 2 \log_g(t+1) \mod 11$$

Proposition

If $a \in \mathbb{F}_q^*$ and ℓ is a factor of $q^k - 1$ coprime to $(q-1)$, then $\log a \equiv 0 \mod \ell$.

Obtaining relations

The finite field $\mathbb{F}_{q^k}$ is represented as $\mathbb{F}_q[t]/\varphi$ for an irreducible polynomial $\varphi \in \mathbb{F}_q[t]$ of degree k.

Example

Take $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$. We have

$$\begin{array}{lcll} t^5 & \equiv & 2(t+1)(t^3+t^2+2t+1) & \mod \varphi \\ t^6 & \equiv & 2(t^2+1)(t^2+t+2) & \mod \varphi \\ & & & \\ t^8 & \equiv & \dots & \end{array}$$

The last relation gives:

$$\begin{array}{lcll} 7\log_g t & \equiv & 1\log_g(t+2) + 2\log_g(t+1) & \mod 11 \\ 8\log_g(t+1) & = & 1\log_g(t+2) & \mod 11 \\ 9\log_g(t+2) & = & 2\log_g t & \mod 11 \end{array}$$

We find $\log_g(t+1) \equiv 158 \mod 11$ and $\log_g(t+2) \equiv 54 \mod 11$.

Proposition

If $a \in \mathbb{F}_q^*$ and ℓ is a factor of $q^k - 1$ coprime to $(q-1)$, then $\log a \equiv 0 \mod \ell$.

Descent

Example (cont'd)

Let us compute $\log_g P$ for an arbitrary polynomial, say $P = t^4 + t + 2$.
We have

$$\begin{aligned} P^{2} &\equiv t^4 + t^3 + 2t^2 + 2t + 2 && \bmod \varphi \\ P^{3} &\equiv 2(t+1)(t+2)(t^2+1) && \bmod \varphi \\ P^{4} &\equiv (t+1)(t+2)t^2 && \bmod \varphi. \end{aligned}$$

Descent

Example (cont'd)

Let us compute $\log_g P$ for an arbitrary polynomial, say $P = t^4 + t + 2$.
We have

$$\begin{aligned} P^2 &\equiv t^4 + t^3 + 2t^2 + 2t + 2 &&\mod \varphi \\ P^3 &\equiv 2(t+1)(t+2)(t^2+1) &&\mod \varphi \\ P^4 &\equiv (t+1)(t+2)t^2 &&\mod \varphi. \end{aligned}$$

By taking discrete logarithms we obtain

$$4 \log_g P = 1 \log_g(t+1) + 1 \log_g(t+2) + 2 \log_g t.$$

So $\log_g P = 114$.

Discrete logarithms of constants

Here ℓ is a prime factor of the group order $q^k - 1$, larger than $q - 1$.

Elements of $\mathbb{F}_q$

Elements of $\mathbb{F}_q \subset \mathbb{F}_{q^k}$ are represented in $\mathbb{F}_q[t]/\langle\varphi\rangle$ by constants a. They satisfy $a^{q-1} = 1$, so we have

$$\log_g(a^{q-1}) \equiv \log_g(1) \equiv 0 \mod \ell.$$

Hence,

$$(q-1)\log_g a \equiv 0 \mod \ell.$$

Since ℓ is prime and larger than $q - 1$,

$$\log_g a \equiv 0 \mod \ell.$$

Comments

Index calculus family

All $L(1/2)$ and $L(1/3)$ DLP algorithms follow the same scheme (of Kraitchik 1922):

- Relation collection;
- Linear algebra to get logs of factor base elements;
- Individual log, to handle any element.

New algorithms

Joux's $L(1/4)$ algorithm still uses this terminology (but very different in nature).

Quasi-polynomial time algorithm: it's time to stop speaking about factor base!

Records for fields $\mathbb{F}_{2^n}$ with prime n

Let us compare to the factoring record: $\boxed{768}$ bits in 2009.

FFS is the choice in practice, and its variants

- Coppersmith (inseparable polynomials);
- Two rational sides FFS (Joux-Lercier).

GIPS=giga instructions per second

n	date	GIPS year	algo.	author
401	1992	0.2	Copp.	Gordon,McCurley
512[1]	2002	0.4	FFS	Joux,Lercier
607	2002	20	Copp.	Thomé
607	2005	1.6	FFS	Joux,Lercier
613	2005	1.6	FFS	Joux,Lercier
619	2012	≈ 0	FFS	Caramel
809	2013	16	FFS	Caramel

[1]Using the same algorithm as for prime degrees.

Records for fields $\mathbb{F}_{2^n}$ with prime n

Let us compare to the factoring record: $\boxed{768}$ bits in 2009.

FFS is the choice in practice, and its variants

- Coppersmith (inseparable polynomials);
- Two rational sides FFS (Joux-Lercier).

GIPS=giga instructions per second

n	date	GIPS year	algo.	author
401	1992	0.2	Copp.	Gordon,McCurley
512[1]	2002	0.4	FFS	Joux,Lercier
607	2002	20	Copp.	Thomé
607	2005	1.6	FFS	Joux,Lercier
613	2005	1.6	FFS	Joux,Lercier
619	2012	≈ 0	FFS	Caramel
809	2013	16	FFS	Caramel

The Caramel group completed the relation collection stage for $n = 1039$ with a computation of 384 GIPS years. Linear algebra must be adapted to larger sizes.

[1]Using the same algorithm as for prime degrees.

Composite degrees n

Motivation

To attack pairing-based cryptosystems, one can solve DLP in fields $\mathbb{F}_{p^{\kappa n}}$ for a small constant $c \neq 1$.
The security of pairings is evaluated under the hypothesis

DLP in $\mathbb{F}_{p^n}$ is equally hard when n is prime or composite.

Theorem (Joux & Lercier 2006)

Under the same assumptions as in the classical variante of FFS, if n has a small factor κ, then one can speed up

1. the relations collection phase by a factor κ;
2. the linear algebra stage by a factor κ^2.

Joux-Lercier improvement in practice

Two teams computed discrete logs in $\mathbb{F}_{3^{6n}}$ (pairings):

- a 2010 record for $n = 71$ (676 bits) using $\kappa = 6$; cost 14 GIPS year.
- a 2012 record for $n = 97$ (923 bits) using $\kappa = 3$; cost 290 GIPS years.

Complexity improvements in 2013 for small characteristic

Linear polynomials

One computes discrete logs. of linear polynomials in polynomial time.

- Göloğlu, Granger, McGuire and Zumbrägel;
- Joux.

Expressing $\log P$ as a sum of logs. of linear polynomials dominates the computations.

Any polynomial

- Joux: $L_Q(1/4 + o(1))$ operations;
- (this work): quasi-polynomial $L_Q(o(1))$ operations.

Main result

Theorem (based on heuristics)

Let K be any finite field $\mathbb{F}_{q^k}$. A discrete logarithm in K can be computed in heuristic time

$$\max(q, k)^{O(\log k)}.$$

Cases:

- $K = \mathbb{F}_{2^n}$, with prime n. Complexity is $n^{O(\log n)}$. Much better than $L_{2^n}(1/4 + o(1)) \approx 2^{\sqrt[4]{n}}$.
- $K = \mathbb{F}_{q^k}$, with $q = k^{O(1)}$. Complexity is $\log Q^{O(\log\log Q)}$, where $Q = \#K$. Again, this is $L_Q(o(1))$.
- $K = \mathbb{F}_{q^k}$, with $q \approx L_{q^k}(\alpha)$. Complexity is $L_{q^k}(\alpha + o(1))$, i.e. better than Joux-Lercier or FFS for $\alpha < 1/3$.

A well-chosen model for $\mathbb{F}_{q^{2k}}$

Simple case first

We suppose first $k \approx q$ and $k \leq q+2$.

Choosing φ (same as for Joux' algorithm)

Try random $h_0, h_1 \in \mathbb{F}_{q^2}[t]$ with $\deg h_0, \deg h_1 \leq 2$ until $T(t) := h_1(t)t^q - h_0(t)$ has an irreducible factor φ of degree k.

Heuristic

The existence of h_0 and h_1 is heuristic, but found in practice in $O(k)$ trials.

Properties of φ

- $h_1(t)t^q \equiv h_0(t) \mod \varphi$;
- $P(t^q) \equiv P\left(\frac{h_0}{h_1}\right) \mod \varphi$;
- $P^q \equiv \tilde{P}(t^q) \equiv \tilde{P}\left(\frac{h_0}{h_1}\right) \mod \varphi$,
  where the tilde denotes the conjugation in $\mathbb{F}_{q^2}$.

A famous identity

Recall the identity

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

We further have $x^q y - x y^q = \prod_{(\alpha:\beta) \in \mathbb{P}^1(\mathbb{F}_q)} (\beta x - \alpha y)$.

A famous identity

Recall the identity

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

We further have $x^q y - x y^q = \prod_{(\alpha:\beta) \in \mathbb{P}^1(\mathbb{F}_q)} (\beta x - \alpha y)$.

A machine to make relations

- $x = t$ and $y = 1$: $h_0/h_1 - t \equiv t^q - t \equiv \prod_{\alpha \in \mathbb{F}_q} (t - \alpha)$.
  If the numerator of the left hand side is smooth, we obtain relations among linear polynomials.
- $x = t + a$, $a \in \mathbb{F}_q$, and $y = 1$: same relation.
- $x = t + a$, $a \in \mathbb{F}_{q^2}$, and $y = 1$: new relations. Joux' algorithm uses this idea.
- Let P be the polynomial whose logarithm is requested.

A famous identity

Recall the identity

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

We further have $x^q y - x y^q = \prod_{(\alpha:\beta) \in \mathbb{P}^1(\mathbb{F}_q)} (\beta x - \alpha y)$.

A machine to make relations

- $x = t$ and $y = 1$: $h_0/h_1 - t \equiv t^q - t \equiv \prod_{\alpha \in \mathbb{F}_q} (t - \alpha)$.
  If the numerator of the left hand side is smooth, we obtain relations among linear polynomials.
- $x = t + a$, $a \in \mathbb{F}_q$, and $y = 1$: same relation.
- $x = t + a$, $a \in \mathbb{F}_{q^2}$, and $y = 1$: new relations. Joux' algorithm uses this idea.
- Let P be the polynomial whose logarithm is requested.
  $x = aP + b$ and $y = cP + d$, $a, b, c, d \in \mathbb{F}_{q^2}$: let us show that the left side is congruent to a small degree polynomial, whereas the right hand side is smooth in some new sense.

The right hand side is "smooth"

$$
\begin{aligned}
(aP+b)^q(cP+d)-(aP+b)(cP+d)^q &= \prod_{(\alpha,\beta)\in\mathbb{P}^1(\mathbb{F}_q)} \beta(aP+b)-\alpha(cP+d) \\
&= \prod_{(\alpha,\beta)\in\mathbb{P}^1(\mathbb{F}_q)} (-c\alpha+a\beta)P-(d\alpha-b\beta) \\
&= \lambda \prod_{(\alpha,\beta)\in\mathbb{P}^1(\mathbb{F}_q)} \left(P-\frac{d\alpha-b\beta}{a\beta-c\alpha}\right),
\end{aligned}
$$

Here $q+1$ out of the q^2+1 elements of $\{1\}\bigcup\{P+\gamma : \gamma\in\mathbb{F}_{q^2}\}$ occur.

The left hand side is small

For $m \in \mathrm{GL}_2(\mathbb{F}_{q^2})$, let $\mathcal{L}_m$ be the residue

$$\mathcal{L}_m := h_1^{\deg P}\left((aP+b)^q(cP+d) - (aP+b)(cP+d)^q\right) \mod \varphi(t).$$

The left hand side is small

For $m \in \mathrm{GL}_2(\mathbb{F}_{q^2})$, let $\mathcal{L}_m$ be the residue

$$\mathcal{L}_m := h_1^{\deg P}\left((aP+b)^q(cP+d) - (aP+b)(cP+d)^q\right) \mod \varphi(t).$$

We have $\deg \mathcal{L}_m \leq 3 \deg P$. Indeed, we have

$$\begin{aligned} \mathcal{L}_m &= h_1^{\deg P}(\tilde{a}\tilde{P}(t^q) + \tilde{b})(cP+d) - (aP(t)+b)(\tilde{c}\tilde{P}(t^q)+\tilde{d}) \\ &= h_1^{\deg P}\left(\tilde{a}\tilde{P}\left(\frac{h_0}{h_1}\right) + \tilde{b}\right)(cP+d) - (aP+b)\left(\tilde{c}\tilde{P}\left(\frac{h_0}{h_1}\right)+\tilde{d}\right). \end{aligned}$$

For a constant proportion of matrices m, $\mathcal{L}_m$ is $(\deg P)/2$-smooth.

Procedure to "break" a polynomial P

Each matrix m in the quotient set $\mathcal{P}_q := \mathrm{PGL}_2(\mathbb{F}_{q^2})/\mathrm{PGL}_2(\mathbb{F}_q)$ such that $\mathcal{L}_m$ is $(\deg P)/2$-smooth leads to a different equation

$$\prod_i P_{i,m}^{e_{i,m}} = \lambda \prod_{\gamma \in \mathbb{P}^1(\mathbb{F}_{q^2})} (P+\gamma)^{v_m(\gamma)},$$

where

- $\deg P_i \leq (\deg P)/2$;
- $v_m(\gamma)$ are integer exponents;
- λ is a costant in $\mathbb{F}_{q^2}$.

By taking discrete logarithm we find

$$\sum_i e_{i,m} \log P_{i,m} \equiv \sum_\gamma v_m(\gamma) \log(P+\gamma) \mod \ell.$$

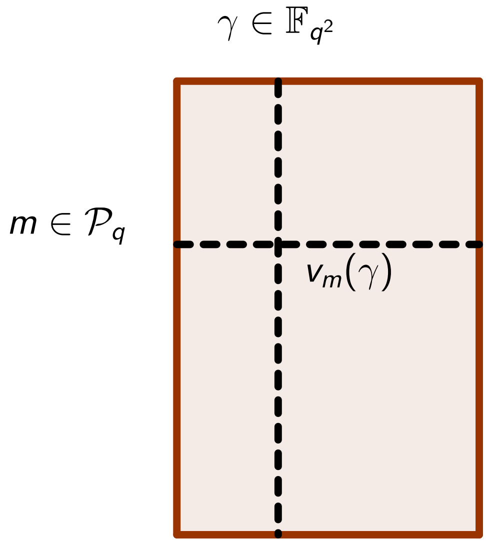
Heuristic

We have enough equations and we can combine them to obtain

$$\sum_{i,m} e'_{i,m} \log P_{i,m} \equiv \log P \mod \ell.$$

Linear algebra step for P

Since $\#\mathrm{PGL}_2(\mathbb{F}_{q^i}) = q^{3i} - q^i$, $\#\mathcal{P}_q = q^3 + q$. A constant fraction give linear equations among logarithms, so the matrix below has more rows than columns.



The heuristic states that we can combine the rows to obtain row

$$(1, 0, \ldots, 0).$$

Arguments in favor of the heuristic

Experiments

- The discriminant of matrices obtained for various polynomials P have no systematic common factor other than the divisors of $q^3 - q$.
- The heuristic is used in the algorithm of Joux for degree two polynomials.
- For random instances of P, every randomly chosen matrix formed of $q^2 + 1$ rows has maximal rank.

Theory

The full matrix of $q^3 + q$ rows has maximal rank. We use the fact that

- there are a fixed number c_1 of blocks passing by each point of $\mathbb{F}_{q^2}$;
- there are a fixed number c_2 of blocks passing by two points.

Does the matrix formed of a constant fraction of rows have maximal rank?

Building block of the quasi-polynomial algorithm

We have just proved:

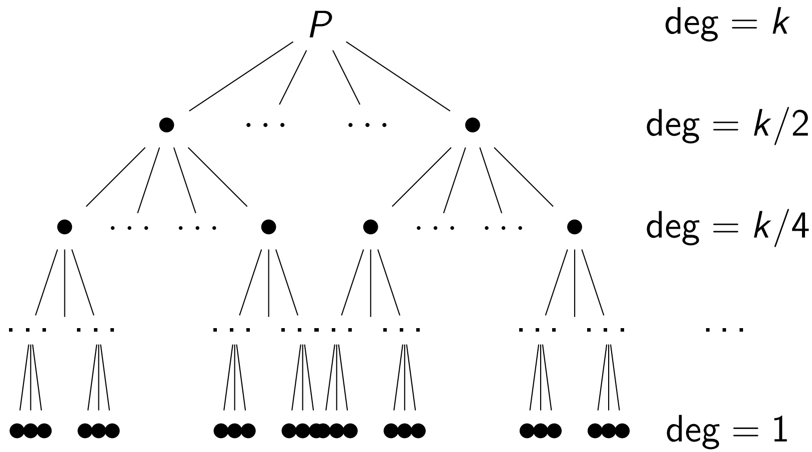
Proposition (Under heuristic assumptions)

There exists an algorithm whose complexity is polynomial in q and k and which can be used for the following two tasks.

1. Given an element of $\mathbb{F}_{q^{2k}}$ represented by a polynomial $P \in \mathbb{F}_{q^2}[t]$ with $2 \leq \deg P \leq k-1$, the algorithm returns an expression of $\log P$ as a linear combination of at most $O(kq^2)$ logarithms $\log P_i$ with $\deg P_i \leq \lceil \frac{1}{2} \deg P \rceil$ and of $\log h_1$.

2. The algorithm returns the logarithm of h_1 and the logarithms of all the elements of $\mathbb{F}_{q^{2k}}$ of the form $t + a$, for a in $\mathbb{F}_{q^2}$.

Complexity



Tree characteristics

- depth=$\log k$ because we half the degree at each level;
- arity=$O(q^2k)$ because the sons are polynomials in the LHS of the q^2 equations used;
- number of nodes=$q^{O(\log k)}$ because $k \leq q+2$.

Extending to the general case

When $q < k - 2$ we embed $\mathbb{F}_{q^k}$ in $\mathbb{F}_{q'^{2k}}$ with $q' = q^{\lceil \log_q k \rceil}$.
The complexity $q^{O(\log k)}$ transforms into $\max(q, k)^{O(\log k)}$.

Note that $q' \leq qk$. The input size n is replaced by $n \log n$. For any constant c

$$\exp\left(c(\log n)^2\right) \Rightarrow \exp\left(c(\log n + \log\log n)^2\right) = \exp\left((c + o(1))(\log n)^2\right).$$

Extending to the general case

When $q < k - 2$ we embed $\mathbb{F}_{q^k}$ in $\mathbb{F}_{q'^{2k}}$ with $q' = q^{\lceil \log_q k \rceil}$.
The complexity $q^{O(\log k)}$ transforms into $\max(q, k)^{O(\log k)}$.

Note that $q' \leq qk$. The input size n is replaced by $n \log n$. For any constant c

$$\exp\left(c(\log n)^2\right) \Rightarrow \exp\left(c(\log n + \log\log n)^2\right) = \exp\left((c + o(1))(\log n)^2\right).$$

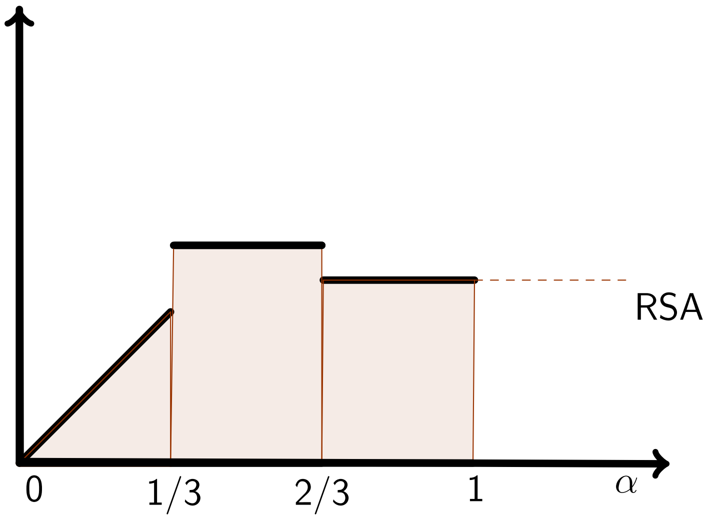
Example

1. For $\mathbb{F}_{2^{1003}}$ we compute logs in $\mathbb{F}_{1024^{2\cdot 1003}} = \mathbb{F}_{2^{20060}}$.
2. The field $\mathbb{F}_{3^{6\cdot 509}}$ can be embedded in $\mathbb{F}_{q^{2k}}$ with $q = 3^6$ and $k = 509$.

$\boxed{\text{Fields of composite degree (specific to pairings) embed in small fields.}}$

Hardness of DLP with respect to the size of characteristic

The complexity of QPA when $q = L_{q^k}(\alpha)$ is $L_{q^k}\left(\alpha + o(1)\right)$



The traps of Cheng–Wan–Zhuang

Trap

In reaction to our preprint, Cheng, Wan and Zhuang noticed that our descent fails on divisors of $h_1 t^q - h_0$.
Indeed, if P is such a divisor we cannot find relations

$$\prod_i P_{i,m}^{e_{i,m}} = \lambda \prod_{\gamma \in \mathbb{P}^1(\mathbb{F}_{q^2})} (P+\gamma)^{v_m(\gamma)} \mod (h_1 t^q - h_0),$$

containing P in the RHS. Indeed, it forces P to occur in the LHS too, so it cannot be $(\deg P)/2$-smooth.

Our solution

We have

$$h_1^D P^q \equiv h_1^D \tilde{P}(h_0/h_1) \mod x^q h_1 - h_0.$$

The RHS is always divisible by P (it is problematic).
Taking logs, we get

$$D \log h_1 + (q-1) \log P = \log Q,$$

where Q is the RHS divided by P.
In general, $P \nmid Q$, and, if $\deg h_0, h_1 \leq 2$, then $\deg Q \leq D$. So we have related $\log P$ to other logarithms, and the descent can continue.

Very weak fields

Assume that $k = q - 1$ (same is true for $q + 1$ and q). For many values of q we can take $h_1 = 1$ and $h_0 = Ax$ for some generator A of $\mathbb{F}_{q^2}^*$. Then $\varphi = x^{q-1} - A$.

Then, for any $a \neq \mathbb{F}_{q^2}$, we have

$$\begin{aligned}(x+a)^q &= x^q + \tilde{a} \\ &= x^{q-1}x + \tilde{a} \\ &= A(x + \tilde{a}/A),\end{aligned}$$

where $\tilde{a}$ is the Frobenius conjugate of a. We obtain $q \log(x + a) = \log(x + \tilde{a}/A)$.

Hence we can reduce the factor base by a factor k. For example for 2^{6168}, the linear algebra time was accelerated by $k^2 = 66049$.

Remark

The smoothness probabilities are improved. For example, The proportion of matrices $m \in \mathcal{P}_q$ which produce relations for the linear polynomials is $1/6! = 1/620$ when $\max(\deg h_0, \deg h_1) = 2$ and it is $1/3!$ for the weak case (Kummer).

Records

Algorithms in practice

1. relations collection (degree one and two): variants of GGMZ or Joux algorithm;
2. descent (degree three and more): variants of Joux' algorithm.

No QPA descent yet.

Kummer and twisted Kummer extensions

field	bitsize	date	CPU time	author
$\mathrm{GF}(2^{24\cdot 255})$	6120	Apr 13	0.7k h	GGMZ
$\mathrm{GF}((2^{24\cdot 257})$	6168	May 13	0.5k h	J
$\mathrm{GF}(2^{18\cdot 513})$	9234	Jan 14	400k h	GKZ

General extensions of composite degree

field	bitsize	date	CPU time	author
$\mathrm{GF}(3^{6\cdot 137})$	1303	Jan 14	1k h	AMOR
$\mathrm{GF}(2^{12\cdot 367})$ *	4404	Jan 14	52k h	GKZ
$\mathrm{GF}(3^{5\cdot 479})$	3796	Aug 14	9k h	JP

* using a non-general speed-up: target elements in a subfield.

Consequences and perspectives

Consequences

- DLP in small characteristic finite fields is asymptotically weak.
- Small characteristic pairings are broken for the sizes proposed for cryptography.

Perspectives

- even more practical improvements and records;
- eliminating the heuristics (a new quasi-polynomial algorithm was proposed by Granger, Kleinjung and Zumbrägel)(next talk);
- improvements in non-small characteristic: multiple field variants, new methods of polynomial selection.