RAIM — November 18-20, 2013

A quasi-polynomial algorithm for discrete logarithm in small characteristic

Razvan Barbulescu Pierrick Gaudry Antoine Joux
Emmanuel Thomé

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Inria informatics mathematics

CNRS

UNIVERSITÉ DE LORRAINE

UPMC SORBONNE UNIVERSITÉS

Discrete logarithm

Definition

Let t and s be two elements in a cyclic group. We call discrete logarithm of s in base t, if it exists, the smallest positive integer x such that

$$t^x = s.$$

Example

DSA signature relies on the difficulty of solving the equation

$$t^x \equiv s \mod p,$$

for a prime p and integers t and s.

Example

Pairing based crypto-systems relies on the difficulty of solving the equation

$$t(X)^x \equiv s(X) \mod \varphi(X),$$

for an irreducible polynomial $\varphi(X)$ in $\mathrm{F}_2[X]$ or $\mathrm{F}_3[X]$.

Motivation

The security of the public key protocols relies on the difficulty of primitives:

1. **factorization (RSA);**
2. **discrete logarithm (DSA);**
3. **elliptic curve discrete logarithm (ECDSA).**
4. ...

$$\begin{tikzcd} & \textbf{factorization} \arrow[r, leftrightarrow, "\textbf{same complexity}"'] & \textbf{discrete log.} \arrow[d, leftrightarrow, "\textbf{is analoguous to}"] \\ \textbf{elliptic discrete log.} \arrow[r, "\textbf{pairing-friendly curves reduce to}"'] & \textbf{discrete log.} & \textbf{in } \mathbb{F}_{2^n} \textbf{ and } \mathbb{F}_{3^n} \end{tikzcd}$$

Quick remarks

Quick remarks

- $\mathbb{F}_{q^k}$ **is represented as** $\mathbb{F}_q[x]/\langle\varphi\rangle$ **; we can choose** φ**;**

Quick remarks

- $\mathbb{F}_{q^k}$ **is represented as** $\mathbb{F}_q[x]/\langle\varphi\rangle$ **; we can choose** φ**;**
- $\log_t s$ **is defined modulo the group cardinal; by CRT it is enough to compute it modulo a prime divisor** ℓ **of** $(q^k-1)/(q-1)$**;**

Quick remarks

- $\mathbb{F}_{q^k}$ **is represented as** $\mathbb{F}_q[x]/\langle\varphi\rangle$ **; we can choose** φ**;**
- $\log_t s$ **is defined modulo the group cardinal; by CRT it is enough to compute it modulo a prime divisor** ℓ **of** $(q^k-1)/(q-1)$**;**
- $\log_{t_1} t_2 \cdot \log_{t_2} s = \log_{t_1} s$**; we simply write** $\log s$**;**

Quick remarks

- $\mathbb{F}_{q^k}$ **is represented as** $\mathbb{F}_q[x]/\langle\varphi\rangle$ **; we can choose** φ**;**
- $\log_t s$ **is defined modulo the group cardinal; by CRT it is enough to compute it modulo a prime divisor** ℓ **of** $(q^k-1)/(q-1)$**;**
- $\log_{t_1} t_2 \cdot \log_{t_2} s = \log_{t_1} s$**; we simply write** $\log s$**;**
- **if** $a \in \mathbb{F}_q^*$**, then** $a^{q-1}=1$**. So** $(q-1)\log a \equiv 0 \mod \ell$**, hence** $\log a \equiv 0 \mod \ell$**.**

Smoothness in $\mathbb{F}_q[x]$

Definition

A polynomial is m-smooth if all its irreducible factors have degree less or equal to m.

Proposition

Put $N_q(n, m)$ the number of degree-n monic m-smooth polynomials.

- $N_q(D, 1)/q^D \approx 1/D!$;
- $N_q(D, \frac{1}{6}D)/q^D = c + o(1)$ for a constant $c > 0$.

idea.

$N_q(D, 1) = \binom{q}{D} + \cdots \approx q^D/D!$. $\square$

Obtaining relations

Example

Take $q = 3$, $k = 5$, $\varphi = x^5 + x^4 + 2x^3 + 1$ and $\ell = 11$ (divisor of $3^5 - 1$). We have

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

Obtaining relations

Example

Take $q = 3$, $k = 5$, $\varphi = x^5 + x^4 + 2x^3 + 1$ and $\ell = 11$ (divisor of $3^5 - 1$). We have

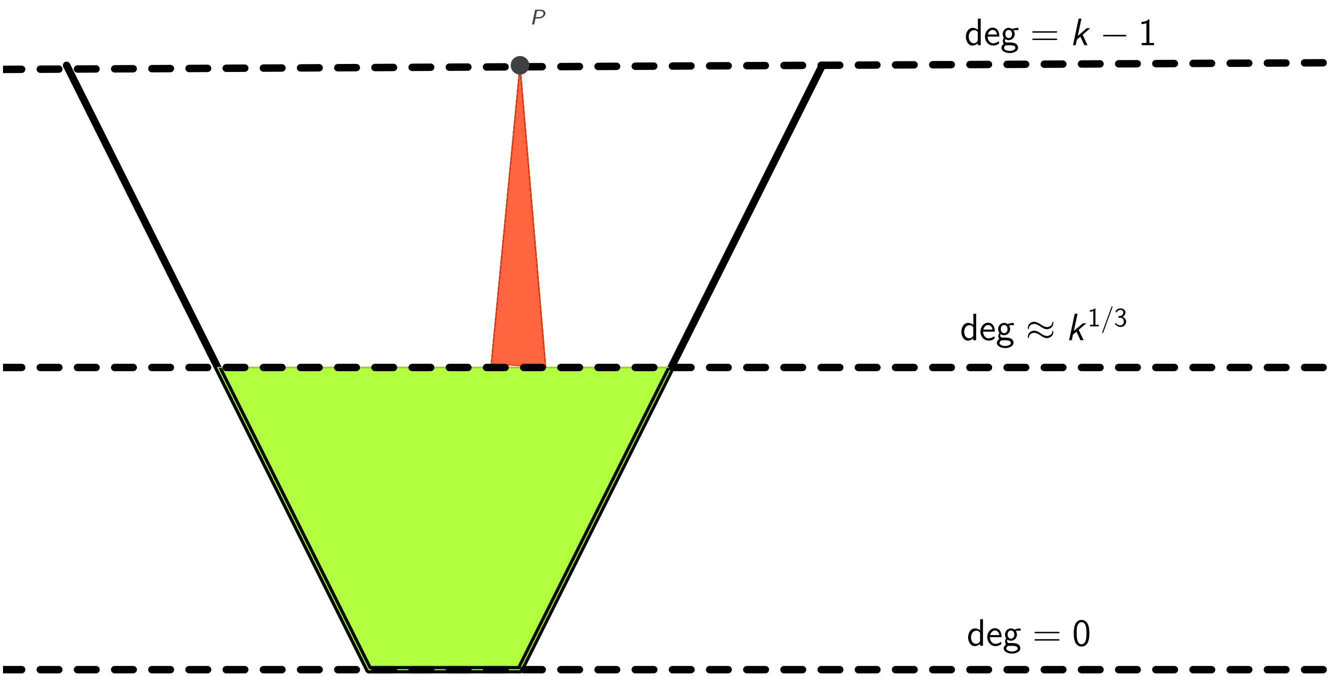
$$\begin{aligned} x^5 &\equiv 2(x+1)(x^3+x^2+2x+1) \mod \varphi \\ x^6 &\equiv 2(x^2+1)(x^2+x+2) \mod \varphi \\ x^7 &\equiv 2(x+2)(x+1)^2 \mod \varphi. \end{aligned}$$

The last relation gives:

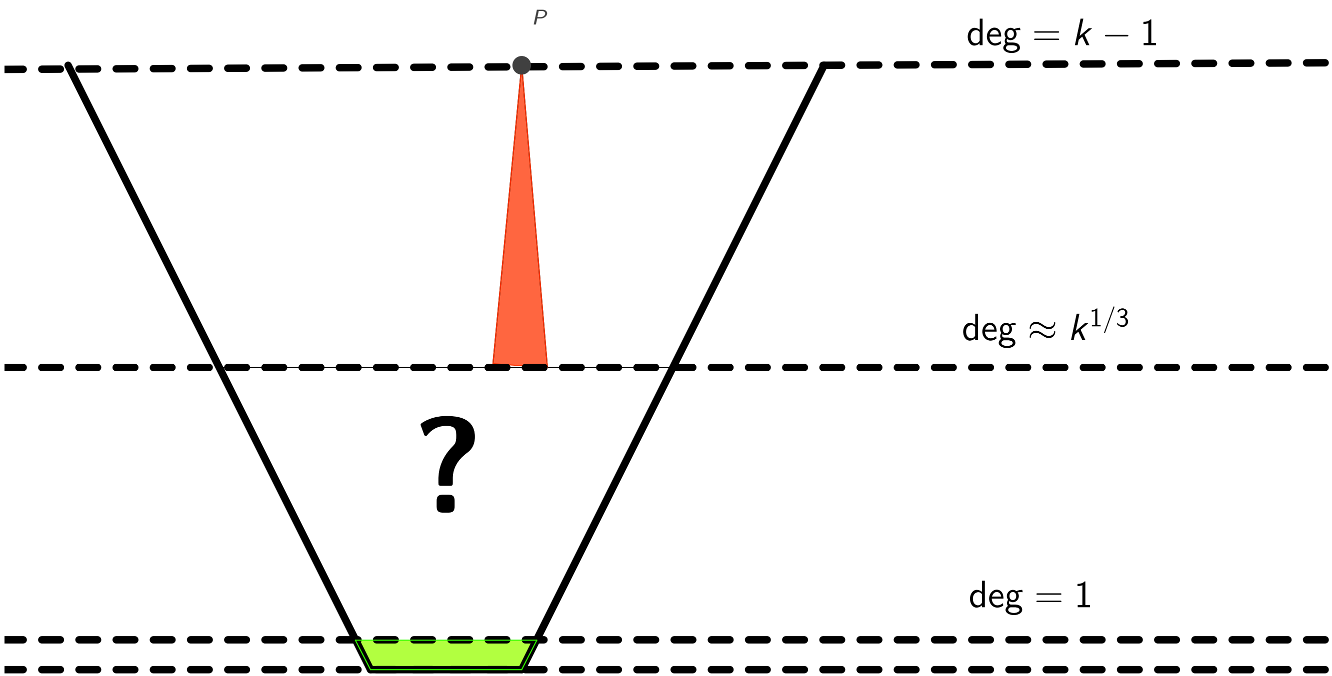
$$7 \log x \equiv 1 \log(x+2) + 2 \log(x+1) \mod 11.$$

With 3 equations we compute $\log x$, $\log(x+1)$ and $\log(x+2)$.

Illustration of the classical algorithms



Speeding up Joux' algorithm



Representing $\mathbb{F}_{q^{2k}}$

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

Representing $\mathbb{F}_{q^{2k}}$

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

Remark

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

Representing $\mathbb{F}_{q^{2k}}$

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

Remark

- The existence of h_0 and h_1 is heuristic but found in practice in time $O(k)$.
-
$$h_1(x)x^q \equiv h_0(x) \mod T(x).$$

Representing $\mathbb{F}_{q^{2k}}$

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

Remark

- The existence of h_0 and h_1 is heuristic but found in practice in time $O(k)$.
- $$h_1(x)x^q \equiv h_0(x) \mod T(x).$$
- If $P \in \mathbb{F}_{q^2}[x]$ then

$$\begin{aligned} h_1(x)^{\deg P} P(x)^q &= h_1(x)^{\deg P} \tilde{P}(x^q) \\ &\equiv h_1(x)^{\deg P} \tilde{P}\left(\frac{h_0}{h_1}\right) \mod T(x). \end{aligned}$$

Building block

Proposition

Under plausible heuristics explained below, for any polynomial P one finds in polynomial time a relation

$$\log P \equiv e_1 \log P_1 + \cdots + e_k \log P_k \mod \ell,$$

with $\deg P_i \leq \frac{1}{2} \deg P$.

Proof: The left hand side

Let $\log P$ be the required computation. For random $a, b, c, d \in \mathbb{F}_{q^2}$ we have

$$h_1(x)^{\deg P}\left((aP+b)^q(cP+d)-(aP+b)(cP+d)^q\right) \equiv \text{ small degree } \mod T(X).$$

Proof: The left hand side

Let $\log P$ be the required computation. For random $a, b, c, d \in \mathbb{F}_{q^2}$ we have

$$h_1(x)^{\deg P}\left((aP+b)^q(cP+d)-(aP+b)(cP+d)^q\right) \equiv \text{small degree} \mod T(X).$$

If the small degree polynomial is smooth we obtain

$$\log\left((aP+b)^q(cP+d)-(aP+b)(cP+d)^q\right) \equiv e_1 \log P_1 + \cdots + e_n \log P_n \mod \ell,$$

with $\deg P_i \leq \frac{1}{2}\deg P$.

The right hand side

Recall the identity

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

It gives $x^q y - y^q x = \prod_{(\alpha \in \mathrm{F}_q \bigcup \{\infty\}} (x - \alpha y)$ and

The right hand side

Recall the identity

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

It gives $x^q y - y^q x = \prod_{(\alpha \in \mathbb{F}_q \bigcup \{\infty\}} (x - \alpha y)$ and

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

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

Linear algebra step for P

- Each relation gives a linear equation for the logs of $\{P + a : a \in \mathbb{F}_{q^2}\}$.

- There are $\#\mathrm{PGL}(2, q^2)/\#\mathrm{PGL}(2, q) = (q^6 - q^2)/(q^3 - q) = q^3 + q$ distinct quadruples (a, b, c, d); a constant fraction of relations.

- We have a matrix of cq^3 rows (c constant) and $q^2 + 1$ columns. Heuristically, the rank is always full, so we can make a linear combination of the rows equal to $\log P$.

- Each relation brings $O(k)$ polynomials of smaller degree. The linear combination uses q^2 equations. So $\log P$ requires $O(q^2 k)$ logs.

The algorithm

We construct a descent tree in which each node is a polynomial. At each step we divide the degree by 2.

- arity of the descent tree is $O(q^2 k)$;
- height is $\log_2 k$;
- cardinality $\max(q, k)^{O(\log k)}$.

Complexity

Put $Q = q^{2k}$. When $q \approx k$ we have

$$\log Q = 2k \log q,$$

so $k = O(\log Q)$ and $q = O(\log Q)$. Then the complexity is

$$\max(q, k)^{\log k + O(1)} = (\log Q)^{O(\log \log Q)}.$$

Characteristic 2 and 3

Example

Joux computed the discrete logarithm in the field of $2^{4080} = q^{2k}$ for $q = 2^8 = k + 1$.

Characteristic 2 and 3

Example

Joux computed the discrete logarithm in the field of $2^{4080} = q^{2k}$ for $q = 2^8 = k + 1$.

When $q < k$ we embed $\mathbb{F}_{q^{2k}}$ in $\mathbb{F}_{q'^{2k}}$ with $q' = q^{\lceil \log qk \rceil}$.

Example

For $\mathbb{F}_{2^{1003}}$ we compute logs in $\mathbb{F}_{1024^{2\cdot 1003}} = \mathbb{F}_{2^{20060}}$. Complexity $\log Q^{O(\log\log Q)}$ with a larger constant.

Conclusion and open questions

- The complexity of the discrete log in $\mathbb{F}_{q^k}$ for small q was improved, replacing FFS except for a small range.
- Pairings-based cryptography in small characteristic has a much smaller complexity than expected.

Open questions:

1. The rank of the matrix in the computations is full.
2. The polynomials h_0 and h_1 can be chosen for any k and q.
3. How should one combine the various algorithms?

Thank you for your attention

Questions?