MPRI – Cours 2.12.2

F. Morain

DLP: the case of $\mathbb{F}_{p^n}$

2019/10/22

The slides are available on `http://www.lix.polytechnique.fr/Labo/Francois.Morain/MPRI/2019`

I. Smoothness theory

Thm. $I(n,q) = \#\{f \in \mathbb{F}_q[X], f \text{ irreducible}\} \approx \frac{q^n}{n}$

Smoothness for polynomials:

$$N_q(n,m) = \#\{f \in \mathbb{F}_q[X], \deg(f) \leq n, g \mid f \Rightarrow \deg(g) \leq m\}$$

Thm. (Soundararajan) Let $u = n/m$ and assume $1 \leq m \leq n$. Uniformly for all prime powers $q \geq (n \log^2 n)^{1/m}$, we have

$$N_q(n,m) = \frac{q^n}{u^{(1+o(1))u}}$$

as $m, u \to \infty$.

Detecting smooth polynomials: (see Coppersmith) compute

$$g(X) = f'(X) \prod_{k \leq m} (X^{q^k} - X) \bmod f(X);$$

f is m-smooth iff $g \equiv 0$.

II. Early history for $\mathbb{F}_{2^n}$

- 1983: Hellman & Reyneri adapt Adleman's algorithm to $\mathbb{F}_{2^n}$.
- 1983-84: Blake, Juji-Hara, Mullin and Vanstone targeted the finite field $\mathbb{F}_{2^{127}} = \mathbb{F}_2[x]/(x^{127}+x+1)$ to implement Adleman's algorithm.
  - Systematic equation: $x^{2^i} \equiv x^{2^{i-6}} + x^{2^{i-7}} = x^{2^{i-7}}(1 + x^{2^{i-7}}) \bmod f(x)$ for any $i \geq 7$. Moreover, $(1+x^{2^i}) = (1+x)^{2^i} \equiv (x^{127})^{2^i}$ so that $\log_x(1+x^{2^i}) = 127 \cdot 2^i$.
  - write $t(X)(X^k a(X)) \equiv r(X) \bmod f(X)$ with $\deg(t(X)), \deg(r(X)) \leq (n-1)/2$; smoothness probability is better.
- Coppersmith.

B) Coppersmith's algorithm for $\mathbb{F}_{2^n}$

$$\mathbb{F}_{2^{127}} = \mathbb{F}_2[X]/(f(X)) = \mathbb{F}_2[X]/(X^{127}+X+1)$$

$\mathcal{B} = \{P_i(X), \text{irreducible}, \deg(P_i) \leq 17\}$. Consider

$$C(X) = X^{32}A(X) + B(X)$$

with A, B of degrees ≤ 10 (there are 2^{21} of them).

$$D(X) \equiv C(X)^4 \bmod f(X) \equiv (X^2+X)A(X)^4 + B(X)^4 \bmod f(X),$$

where r.h.s. has degree ≤ 42.
If $C(X)$ and $D(X)$ are smooth

$$D(X) = \prod_{i=1}^{\ell} P_i(X)^{e_i}, C(X) = \prod_{i=1}^{\ell} P_i(X)^{f_i}$$

then

$$\sum_{i=1}^{\ell} e_i \log P_i \equiv 4 \sum_{i=1}^{\ell} f_i \log P_i \mod (2^{127}-1).$$

Coppersmith (cont'd)

Thm. For $\mathbb{F}_{2^n}$, Coppersmith's algorithm is in $O(\exp(cn^{1/3}(\log n)^{2/3}))$.

Rem. Gordon & McCurley: smoothness testing of $(C(X), D(X))$ can be done using a sieve.

Record: Joux & Lercier with $n = 613$ (in 2005).

III. Quasi polynomial algorithms

2012: Joux's pinpointing
2^{1175}, 2^{1425}

↙ 2013: Joux's $L[1/4]$
$\ldots 2^{6168}$

↓ 2013: Barbulescu/Gaudry Joux/Thomé QPA

↓ 2013: Adj *et al.*
$2^{4\cdot 3041}$

↘ 2013: Göloglu/Granger McGuire/Zumbrägel
2^{1971}, 2^{3164}

↓ 2014: Granger/Kleinjung/Zumbrägel
2^{9234}

↓ 2019: Granger/Kleinjung/Lenstra Wesolowski/Zumbrägel
2^{30750}

Common point: phase 1 is polynomial time and very fast; phase 2 has to be vastly improved to meet QPA complexity.

The diagram

$$\begin{tikzcd} & \mathbb{F}_q[X,Y] \arrow[dl, "Y \leftarrow g_2(X)"'] \arrow[dr, "X \leftarrow g_1(X)"] & \\ \mathbb{F}_q[X] \arrow[dr, "X \leftarrow x"'] & & \mathbb{F}_q[Y] \arrow[dl, "Y \leftarrow y"] \\ & \mathbb{F}_{q^n} & \end{tikzcd}$$

$$f_1(X,Y) = X - g_1(Y), \quad f_2(X,Y) = -g_2(X) + Y, \ \deg(g_i) = d_i.$$

Requires: $-g_2(g_1(Y)) + Y$ has an irreducible factor $F(Y)$ of degree n over $\mathbb{F}_q$ and defines $\mathbb{F}_{q^n}$.

Relation: for all A, B polynomials in $\mathbb{F}_q[X]$

$$A(Y)g_1(Y) + B(Y) = A(g_2(X))X + B(g_2(X)).$$

A) Pinpointing (Joux, 2012)

$d_1, d_2 \approx \sqrt{n}$. If A and B of degree 1, degree $d_1 + 1$ in Y related to degree $d_2 + 1$ in X.

Use $X = Y^{d_1}$, $Y = g_2(X)$ to get:

$$Y^{d_1+1} + aY^{d_1} + bY + c = Xg_2(X) + aX + bg_2(X) + c,$$

a, b and c in $\mathbb{F}_q$; lhs splits into linear factors iff

$$U^{d_1+1} + U^{d_1} + ba^{-d_1}U + ca^{-d_1-1}$$

does.

Pinpointing: find B and C in $\mathbb{F}_q$ such that $U^{d_1+1} + U^{d_1} + BU + C$ splits. Scaling with $U = Y/a$ yields many good candidates. This yields a reduced cost from $(d_1+1)!(d_2+1)!/(q-1)$.

B) $L[1/4]$: Joux (2013)

1. Consider for a, b, c, d in $\mathbb{F}_q$:

$$X \rightarrow \frac{aX+b}{cX+d}.$$

If $f(Y) = \prod_{i=1}^{k} F_i(Y)^{e_i}$, then

$$(cX+d)^{\deg(f)} f\left(\frac{aX+b}{cX+d}\right) = \prod_{i=1}^{k}\left((cX+d)^{\deg(F_i)} F_i\left(\frac{aX+b}{cX+d}\right)\right)^{e_i}$$

(not necessarily monic, perhaps not irreducible).

2. Enough to start from $f(X) = X^q - X$.

3. Force $x^q = h_0(x)/h_1(x)$ in $\mathbb{F}_{q^n}$, which requires $h_1(X)X^q - h_0(X)$ to have an irreducible factor of degree n.

$L[1/4]$: set up

Setup:

- $\mathbb{F}_{p^n} \rightarrow \mathbb{F}_{q^{2k}}$ = degree k extension of $\mathbb{F}_{q^2} = \mathbb{F}_q(u)$.
- Find two low degree $h_i(X)$ in $\mathbb{F}_{q^2}[X]$ s.t. $h_1(X)X^q - h_0(X)$ has an irreducible deg k factor $\mathcal{I}(X)$.

Expanding the idea: start from $\prod_{\alpha\in\mathbb{F}_q}(Y-\alpha) = Y^q - Y$ and make $Y = (aX+b)/(cX+d)$ with a, b, c, d in $\mathbb{F}_{q^2}$. This yields

$$(cX+d)\prod_{\alpha\in\mathbb{F}_q}((a-\alpha c)X+(b-\alpha d)) = (cX+d)(aX+d)^q-(aX+b)(cX+d)^q$$

and rhs is

$$\frac{(ca^q-ac^q)Xh_0(X)+(da^q-bc^q)h_0(X)+(cb^q-ad^q)Xh_1(X)+(db^q-bd^q)h_1(X)}{h_1(X)}$$

with numerator of small degree.
Thm. The number of candidate equations is q^3+q (action of $\mathrm{PGL}_2(\mathbb{F}_q)$).
$\Rightarrow$ ok for degree 1 polynomials.

$L[1/4]$: finding logs of degree 2 polynomials

1. Keep degree 2 polynomials in rhs relations? But number of quadratic polynomials is $O(q^4)$ compared to $O(q^3)$ relations.

2. Put

$$Y = \frac{aX^2+bX+c}{dX^2+eX+f},$$

so lhs has degree 2 factors; if degree 2 in rhs, we get a relation. But resulting system is too large.

3. Trick: for fixed $\alpha \in \mathbb{F}_{q^2}$:

$$Y = \frac{a(X^2+\alpha X)+b}{c(X^2+\alpha X)+d},$$

all factors in lhs are $X^2+\alpha X+K$; and keep rhs with linear polynomials only; we need solve a $q^2\times q^2$ system with q non-zero entries per row.

$L[1/4]$: individual logarithms (aka. *descent*)

Input: $\mathcal{Q} \in \mathbb{F}_{q^2}[X]$ of degree $< k/2$.
Output: an identity relating $\log\mathcal{Q}$ to some known logs.

Idea: find $k_1(X)$ and $k_2(X)$ in $\mathbb{F}_{q^2}[X]$ s.t. $\mathcal{Q}(X) \mid R(X)$, where

$$R(X) \equiv (k_1(X)^q k_2(X) - k_1(X)k_2(X)^q) \bmod \mathcal{I}(X).$$

If $R(X) = Q(X)\cdot$(1-smooth) then

$$(k_1(X)^q k_2(X) - k_1(X)k_2(X)^q) \equiv Q(X)\cdot(\text{1-smooth}) \bmod \mathcal{I}(X).$$

We use

$$k_1(X)^q k_2(X) - k_1(X)k_2(X)^q = k_2(X)^{q+1}\left\{\left(\frac{k_1(X)}{k_2(X)}\right)^q - \frac{k_1(X)}{k_2(X)}\right\}$$

leading to

$$k_2(X)\prod_{\alpha\in\mathbb{F}_q}(k_1(X)-\alpha k_2(X)) \equiv Q(X)\cdot(\text{1-smooth}) \bmod \mathcal{I}(X).$$

Degree at most $D = \max(\deg(k_1),\deg(k_2))$ in lhs.

$L[1/4]$: finding k_1 and k_2

$$h_1^{d_1+d_2}R(X) \equiv \left(\sum_{i=0}^{d_1} k_{1,i}^q h_1^{d_1-i}(h_1X^q)^i\right)\left(\sum_{i=0}^{d_2} k_{2,i}X^i\right)$$
$$-\left(\sum_{i=0}^{d_1} k_{1,i}X^i\right)\left(\sum_{i=0}^{d_2} k_{2,i}^q h_1^{d_2-i}(h_1X^q)^i\right) \bmod \mathcal{I}(X)$$

and replace h_1X^q by h_0.

Write $k_{i,j} = k_{i,j,0} + uk_{i,j,1}$ with $k_{i,j,r} \in \mathbb{F}_q \Rightarrow k_{i,j}^q = k_{i,j,0} + u^q k_{i,j,1}$.

Compute $R(X) \bmod Q(X)$ and rewrite as system of multivariate polynomials in the $k_{i,j,r}$'s. Use Gröbner bases (in Magma) to solve the systems.

$L[1/4]$: numerical example

$q = 11$, $k = 5$, $\mathbb{F}_{q^2} = \mathbb{F}_{11}[X]/(X^2+1) = \mathbb{F}_{11}(u)$.
Take: $h_1(X) = X, \quad h_0(X) = X+1$
$\mathcal{I} = X^5 + u^{39}\cdot X^4 + u^{64}\cdot X^3 + u^{101}\cdot X^2 + u^8\cdot X + u^{110} \mid h_1(X)X^q - h_0(X)$.
$\mathcal{Q} = X^3 + uX + u + 5$

$k_1(X) = (6u+6)X + 1$, $k_2(X)$ with 4 variables over $\mathbb{F}_q$:

$$R(X) \equiv ((3u+9)k_{2,0,0} + (9u+8)k_{2,0,1} + (9u+4)k_{2,1,0} + 7uk_{2,1,1})X^4 + \cdots$$

$R(X) \bmod \mathcal{Q}(X)$

$$= ((8u+5)k_{2,0,0} + (5u+3)k_{2,0,1} + 5k_{2,1,0} + (6u+7)k_{2,1,1})X^2 + \cdots$$

$$\mathcal{G} = \langle k_{2,0,0} + (9u+5)k_{2,1,0} + (2u+4)k_{2,1,1},$$
$$k_{2,0,1} + (2u+6)k_{2,1,0} + (9u+5)k_{2,1,1}\rangle$$
$$\Rightarrow R(X) = (k_{2,1,0} - k_{2,1,1})(X+3)\mathcal{Q}(X).$$

$L[1/4]$: analysis

Finding logs of degree ≤ 2: dominated by solving q^2 linear systems of dimension $O(q^2)$ with $O(q)$ entries per row: $O(q^7)$ arithmetic operations.

Individual log: $k = \alpha q$ with $\alpha \leq 1 + \deg(h_1)/q$. Also, take $q = p^\ell$ for $\ell \geq 2$.

$\log \mathcal{Q}$ involves $O(q)$ logs of polynomials of degree $D/2$.

...

running time is $O(L[1/4])$.

C) QPA

Barbulescu, Gaudry, Joux, Thomé, 2013.

Let $K = \mathbb{F}_{q^{2k}}$.
Hypothesis: there exists two polynomials h_i of small degree over $\mathbb{F}_{q^2}$ s.t. $h_1X^q - h_0$ has a degree k irreducible factor.

Thm.
1. if $K \ni a = P(X)$ with $P \in \mathbb{F}_{q^2}[X]$ and $2 \leq \deg(P) \leq k-1$, the algorithm returns $\log P(X)$ as a linear combination of at most $O(kq^2)$ $\log P_i(X)$ with $\deg(P_i) \leq \lceil \deg(\mathrm{P})/2 \rceil$.
2. the algorithm returns the log of $h_1(X)$ and all linear elements of K of the form $X+a$, $a \in \mathbb{F}_{q^2}$.

Thm. Any discrete log in K can be computed in a time bounded by $\max(q,k)^{O(\log k)}$.

Proof (1/2)

$P(X)$ of degree $1 \leq D < k$.

$\mathcal{S} = \{(\alpha, \beta)\}$ set of representatives of the $q+1$ points $(\alpha : \beta) \in \mathbb{P}^1(\mathbb{F}_q)$ s.t.

$$X^q Y - XY^q = \prod_{(\alpha,\beta)\in\mathcal{S}} (\beta X - \alpha Y).$$

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to m \cdot P = \frac{aP+b}{cP+d}.$$

$$(E_m)(aP+b)^q(cP+d) - (aP+b)(cP+d)^q = \lambda \prod_{(\alpha,\beta)\in\mathcal{S}} (P-u)$$

where $m^{-1} \cdot (\alpha : \beta) = (u : 1)$.

lhs treated as in $L[1/4]$ using the relations with h_i's.

Proof (2/2)

For each possible m, we associate a row vector $v(m)$ of dimension q^2+1: coordinates indexed by $\mu \in \mathbb{P}^1(\mathbb{F}_{q^2})$ with coordinate for μ is 1 if $\mu = m^{-1} \cdot (\alpha : \beta)$. There are $q+1$ coordinates that are 1.

Heuristic: the set of rows has full rank q^2+1.

Heuristic: the number of rows is $\Theta(q^3)$.

Hence we win and find $\log P$, that is expressible as a linear combination of at most $O(q^2 D)$ polynomials of degree less than $\lceil D/2 \rceil$.

Practical improvements: combine $L[1/4]$ and QPA (Adj *et al.*, 2013), $\mathbb{F}_{2^{4\cdot 3041}}$.

Recent results

Thm. (Kleinjung, Wesolowski, 2018; building on Granger/Kleinjung/Zumbrägel)
Given a prime power q, a positive integer d, coprime polynomials h_0 and h_1 in $\mathbb{F}_{p^d}[x]$ of degree ≤ 2, and an irreducible degree ℓ factor I of $h_1 x^q - h_0$, DLP in $\mathbb{F}_{q^{d\ell}} \simeq \mathbb{F}_{q^d}[x]/(I)$ can be solved in expected time $q^{\log_2 \ell + O(d)}$.

Thm. (Kleinjung, Wesolowski, 2019)
Given any prime number p and any positive integer n, DLP in $\mathbb{F}_{p^n}^*$ can be solved in expected time $(pn)^{2\log_2(n)+O(1)}$.

(uses elliptic curves...)