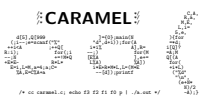
JNCF — May 13–17 , 2013

Selecting polynomials for the Function Field Sieve

Razvan Barbulescu
CARAMEL project-team, LORIA
University of Lorraine, INRIA, CNRS



Introduction

- Discrete logarithm is a cryptographic primitive which consists in, for two elements t and s in cyclic group, finding x such that

$$t^x = s.$$

- The Function Field Sieve computes discrete logarithm in $\mathbb{F}_{q^n}$ when q is a small prime power. In our examples $q = 2$. An asymptotically faster algorithm was proposed by Antoine Joux, the crossing point beeing unknown.
- The Caramel team recently announced records in $\mathbb{F}_{2^n}$ for $n = 619$ and 809.
- We study the first step of FFS which selects two polynomials in $\mathbb{F}_q[t][x]$. This choice has consequences on the global time of the computations.

Notations

- We put $F(X, Y) = f(X/Y)Y^{\deg f}$ and we define $G(X, Y)$ similarly.
- For an integer β, a polynomial is β-smooth if it factors into polynomials of degree up to β.
- Example: $f(x) = x^3 + t^2x + 1$, $F(X, Y) = X^3 + t^2XY^2 + Y^3$. For $a = t + 1$ and $b = t^2 + 1$, $F(a, b) = t(t + 1)^3(t^3 + t^2 + 1)$ is 3-smooth.

The Function Field Sieve

Algorithm (Adleman 1994)

Require: a finite field $\mathbb{F}_{q^n}$, two nonzero elements T (a generator) and S
Ensure: $\log_T S$

1: (Polyselect) Select two polynomials f and g in $\mathbb{F}_q[t][x]$ as will be explained;

2: (Sieve) Collect pairs (a, b) in $\mathbb{F}_q[t]$ such that $F(a, b)$ and $G(a, b)$ are smooth;

3: (Linear algebra) Obtain the logarithms of "small" elements by solving a homogeneous system;

4: (Individual logarithm) Express the logarithm of S in terms of the logarithms of the "small" elements.

The polynomial selection method

Algorithm (Joux & Lercier 2002)

Require: a prime power q and a positive integer n

Ensure: two polynomials f and g in $\mathbb{F}_q[t][x]$ and an irreducible polynomial φ in $\mathbb{F}_q[t]$, of degree n, such that f and g have a common root modulo φ

The polynomial selection method

Algorithm (Joux & Lercier 2002)

Require: a prime power q and a positive integer n

Ensure: two polynomials f and g in $\mathbb{F}_q[t][x]$ and an irreducible polynomial φ in $\mathbb{F}_q[t]$, of degree n, such that f and g have a common root modulo φ

1: Select a polynomial f with given degree in x and small degree in t;
2: **repeat**
3: $\quad g \leftarrow g_1 x + g_0$ with random g_0, g_1 of given degree
4: **until** $\mathrm{Res}(f, g)$ has a degree n irreducible factor.

The polynomial selection method

Algorithm (Joux & Lercier 2002)

Require: a prime power q and a positive integer n

Ensure: two polynomials f and g in $\mathbb{F}_q[t][x]$ and an irreducible polynomial φ in $\mathbb{F}_q[t]$, of degree n, such that f and g have a common root modulo φ

1: Select a polynomial f with given degree in x and small degree in t;
2: **repeat**
3: $\quad g \leftarrow g_1 x + g_0$ with random g_0, g_1 of given degree
4: **until** $\mathrm{Res}(f, g)$ has a degree n irreducible factor.

Implication The selection of f is a precomputation. For $\mathbb{F}_{2^n}$ with $n \in [600, 1100]$ one can use:

$$f_{619,1039} = x^6 + (t^2 + t + 1)x^5 + (t^2 + t)x + (t^{12} + t^{10} + t^8 + t^5 + t^3 + t).$$

$$\begin{aligned} g_{619} &= x + t^{104} + 0\text{x6dbb} \\ g_{1039} &= x + t^{174} + 0\text{x1ef9a3} \end{aligned}$$

Candidate polynomials f

- The smoothness probability of $F(a, b)$ and $G(a, b)$ depends on the degree. This imposes the degrees of f and g, e.g. for $\mathbb{F}_2^{809}$ we have $\deg_x f = 6$.
- Sieved coprime pairs (a, b) subject to

$$\begin{aligned} \deg a &\leq e + s/2 \\ \deg b &\leq e - s/2, \end{aligned}$$

where e (sieve param.) and s (skewness) are parameters. We search polynomials f of type

$$f = x^6 + (t^2 + \cdots)x^5 + (t^4 + \cdots)x^4 + \cdots + (t^{12} + \cdots).$$

Problem exposition

We keep the notations previously made.

Problem

Find $f \in \mathbb{F}_q[t][x]$ in order to maximize the number of coprime pairs (a, b) in the sieving domain such that

$$F(a, b) \text{ is } \beta\text{-smooth.}$$

Outline of the talk

- Introduction
- Root property
- Cancellation property
- Conclusion

Outline of the talk

- Introduction
- Root property
- Cancellation property
- Conclusion

Root property: example

Let us now consider the example of $f = x(x-1) - (t^{64} - t)$. For all irreducible ℓ of degree 2, 3 or 6, the reduction of f mod ℓ has two roots. Compare this to a random polynomial having one root modulo each ℓ.

Root property: example

Let us now consider the example of $f = x(x-1) - (t^{64} - t)$. For all irreducible ℓ of degree 2, 3 or 6, the reduction of f mod ℓ has two roots. Compare this to a random polynomial having one root modulo each ℓ.

For any irreducible polynomial ℓ in $\mathbb{F}_q[t]$ we denote by k_ℓ the field $\mathbb{F}_q[t]/\langle \ell \rangle$. Next we put

$$\mathrm{N}(\ell) := \#k_\ell = q^{\deg \ell}.$$

Let ℓ be an irreducible polynomial. The average of $\mathrm{val}_\ell P$ when P is a random polynomial is $\sum_{k \geq 1} \frac{1}{\mathrm{N}(\ell)^k} = \frac{1}{\mathrm{N}(\ell)-1}$.

Alpha

Basic idea Prob($F(a,b)$ smooth)=Prob(P smooth) when $\deg P = \alpha(f) + \deg F(a,b)$.

Definition

For a polynomial f in $\mathbb{F}_q[t][x]$ and an irreducible polynomial ℓ in $\mathbb{F}_q[t]$, we set:

$$\begin{aligned} a_{\text{hom}}^{(\ell)}(f) &= \text{ average of } \operatorname{val}_\ell F(a,b) \text{ when } \gcd(a,b,\ell) = 1; \\ \alpha_\ell(f) &= \deg(\ell)\left(\frac{1}{\mathrm{N}(\ell)-1} - a_{\text{hom}}^{(\ell)}(f)\right); \\ \alpha(f) &= \sum_{\ell \in L} \alpha_\ell(f), \end{aligned}$$

where the last sum will be shown to converge and the average is in the sense of natural density.

Alpha

Basic idea Prob($F(a,b)$ smooth)=Prob(P smooth) when $\deg P = \alpha(f) + \deg F(a,b)$.

Definition

For a polynomial f in $\mathbb{F}_q[t][x]$ and an irreducible polynomial ℓ in $\mathbb{F}_q[t]$, we set:

$$\begin{aligned} a_{\text{hom}}^{(\ell)}(f) &= \text{ average of } \text{val}_\ell F(a,b) \text{ when } \gcd(a,b,\ell) = 1; \\ \alpha_\ell(f) &= \deg(\ell)\left(\frac{1}{\mathrm{N}(\ell)-1} - a_{\text{hom}}^{(\ell)}(f)\right); \\ \alpha(f) &= \sum_{\ell \in L} \alpha_\ell(f), \end{aligned}$$

where the last sum will be shown to converge and the average is in the sense of natural density.

Note that good polynomials have negative values of alpha.

Equation of alpha

Proposition

Let $f \in \mathbb{F}_q[x][t]$ and ℓ a monic irreducible polynomial in $\mathbb{F}_q[t]$ such that ℓ does not divide $\mathrm{Disc}(f)\,\mathrm{Disc}\,F(1,x)$. Then

$$\alpha_\ell(f) = \frac{\deg \ell}{\mathrm{N}(\ell)-1}\left(1 - \frac{\mathrm{N}(\ell)}{\mathrm{N}(\ell)+1} n_\ell\right),$$

where n_ℓ is the number of points $(a : b)$ of $\mathbb{P}^1(k_\ell)$ such that $F(a,b) \equiv 0 \bmod \ell$.

Equation of alpha

Proposition

Let $f \in \mathbb{F}_q[x][t]$ and ℓ a monic irreducible polynomial in $\mathbb{F}_q[t]$ such that ℓ does not divide $\mathrm{Disc}(f)\,\mathrm{Disc}\,F(1,x)$. Then

$$\alpha_\ell(f) = \frac{\deg \ell}{\mathrm{N}(\ell)-1}\left(1 - \frac{\mathrm{N}(\ell)}{\mathrm{N}(\ell)+1} n_\ell\right),$$

where n_ℓ is the number of points $(a:b)$ of $\mathbb{P}^1(k_\ell)$ such that $F(a,b) \equiv 0 \bmod \ell$.

Proof.

Equation of alpha

Proposition

Let $f \in \mathbb{F}_q[x][t]$ and ℓ a monic irreducible polynomial in $\mathbb{F}_q[t]$ such that ℓ does not divide $\mathrm{Disc}(f)\,\mathrm{Disc}\,F(1,x)$. Then

$$\alpha_\ell(f) = \frac{\deg \ell}{\mathrm{N}(\ell)-1}\left(1 - \frac{\mathrm{N}(\ell)}{\mathrm{N}(\ell)+1} n_\ell\right),$$

where n_ℓ is the number of points $(a:b)$ of $\mathbb{P}^1(k_\ell)$ such that $F(a,b) \equiv 0 \bmod \ell$.

Proof.

- $$\mathrm{Prob}\left(F(a,b) \equiv 0 \bmod \ell \mid \gcd(a,b,\ell) = 1\right) = \frac{n_\ell}{\mathrm{N}(\ell)+1}.$$

Equation of alpha

Proposition

Let $f \in \mathbb{F}_q[x][t]$ and ℓ a monic irreducible polynomial in $\mathbb{F}_q[t]$ such that ℓ does not divide $\mathrm{Disc}(f)\,\mathrm{Disc}\,F(1,x)$. Then

$$\alpha_\ell(f) = \frac{\deg \ell}{\mathrm{N}(\ell)-1}\left(1 - \frac{\mathrm{N}(\ell)}{\mathrm{N}(\ell)+1} n_\ell\right),$$

where n_ℓ is the number of points $(a:b)$ of $\mathbb{P}^1(k_\ell)$ such that $F(a,b) \equiv 0 \bmod \ell$.

Proof.

- $$\mathrm{Prob}\left(F(a,b) \equiv 0 \bmod \ell \mid \gcd(a,b,\ell) = 1\right) = \frac{n_\ell}{\mathrm{N}(\ell)+1}.$$
- For all $k \geq 1$, one has

$$\mathrm{Prob}\left(F(\overline{a} + a_k\ell^k, \overline{b} + b_k\ell^k) \equiv 0 \bmod \ell^{k+1} \mid F(\overline{a},\overline{b}) \equiv 0 \bmod \ell^k\right) = \frac{1}{\mathrm{N}(\ell)}.$$

□

Studying alpha

Theorem

Let $f \in \mathbb{F}_q[t][x]$ be absolutely irreducible. Then $\alpha(f)$ is well defined and has a bound depending on $\deg_x f$, $\deg_t f$ and q.

Example

Denote by $\alpha(f, \beta_1)$ the partial sum of f up to degree β_1. Take $q = 2$, and let $f \in \mathbb{F}_q[t][x]$ such that $\deg_x f = 6$ and $g = 19$ and suppose that all the ramified ℓ have degree less than 15. Then one has

$$\begin{aligned} |\alpha(f) - \alpha(f, 15)| &< 0.57 \\ |\alpha(f) - \alpha(f, 20)| &< 0.01. \end{aligned}$$

A sieve procedure for alpha

Instead of considering polynomials f one at a time, we consider pairs ℓ, r and we update the value of $\alpha_\ell(f)$ for all f such that $f_0 \equiv -\sum_{i=1}^{d} f_i r^i \bmod \ell$.

A sieve procedure for alpha

Instead of considering polynomials f one at a time, we consider pairs ℓ, r and we update the value of $\alpha_\ell(f)$ for all f such that $f_0 \equiv -\sum_{i=1}^{d} f_i r^i \bmod \ell$.

Example

Paul Zimmermann computed $\sum_{\deg \ell \leq 5} \alpha_\ell(f)$ for 2^{48} polynomials.
The best alpha is -5.5 (while $\alpha(f_{619}) = -4.9$):

$$f_{809} = x^6 + (0x7)x^5 + (0x6b)x^3 + (0x1ab)x^2 + (0x326)x + 0x19b3.$$

Outline of the talk

- Introduction
- Root property
- Cancellation property
- Conclusion

Cancellation property: α_∞

Example

$f = x^3 - t^2x + 1 \in \mathbb{F}_2[t][x]$.
For all (a, b), one has $F(a, b) = a^3 - t^2ab^2 + b^3$.

Cancellation property: α_∞

Example

$f = x^3 - t^2x + 1 \in \mathbb{F}_2[t][x]$.
For all (a, b), one has $F(a, b) = a^3 - t^2ab^2 + b^3$.

- if $\deg(a) = \deg(b) - 2$ then $\deg F(a, b)$ decreases of 1.

Cancellation property: α_∞

Example

$f = x^3 - t^2 x + 1 \in \mathbb{F}_2[t][x]$.
For all (a, b), one has $F(a, b) = a^3 - t^2 a b^2 + b^3$.

- if $\deg(a) = \deg(b) - 2$ then $\deg F(a, b)$ decreases of 1.
- if $\deg(a) = \deg(b) + 1$ then $\deg F(a, b)$ decreases of 2.

Cancellation property: α_∞

Example

$f = x^3 - t^2x + 1 \in \mathbb{F}_2[t][x]$.
For all (a, b), one has $F(a, b) = a^3 - t^2ab^2 + b^3$.

- if $\deg(a) = \deg(b) - 2$ then $\deg F(a, b)$ decreases of 1.
- if $\deg(a) = \deg(b) + 1$ then $\deg F(a, b)$ decreases of 2.

We call Laurent series (in $1/t$) any expression of the form:

$$r = t^3 + 1/t^2 + 1/t^8 + \cdots .$$

We call $\deg r$, the degree of any of the non-zero truncations.
The non-zero truncations of a Laurent series, together with the degree of their last term are called Laurent polynomials.

Laurent roots

Definition

Let $f \in \mathbb{F}_q[t][x]$ be a polynomial and call d its degree in x. Let (r, m) be a Laurent polynomial. We say that (r, m) is a Laurent root of f if

$$\max_{i \in [0,d]} \deg(f_i r^i) - \deg f(r) > 0. \tag{1}$$

We call gap of (r, m) the least value in the left hand side of the inequality above when we replace r by any Laurent series extending r.

Example

For $f = x^3 + t^2 x + 1$,

$$\begin{aligned} a/b = t + 1/t + O(1/t^2) &\Rightarrow \deg F(a, b) \text{ decreases of } 3 \\ a/b = 1/t^2 + 1/t^8 + O(1/t^9) &\Rightarrow \deg F(a, b) \text{ decreases of } 7. \end{aligned}$$

Laurent roots

Definition

Let $f \in \mathbb{F}_q[t][x]$ be a polynomial and call d its degree in x. Let (r, m) be a Laurent polynomial. We say that (r, m) is a Laurent root of f if

$$\max_{i \in [0,d]} \deg(f_i r^i) - \deg f(r) > 0. \tag{1}$$

We call gap of (r, m) the least value in the left hand side of the inequality above when we replace r by any Laurent series extending r.

Example

For $f = x^3 + t^2 x + 1$,

$$\begin{aligned} a/b = t + 1/t + O(1/t^2) &\Rightarrow \deg F(a, b) \text{ decreases of } 3 \\ a/b = 1/t^2 + 1/t^8 + O(1/t^9) &\Rightarrow \deg F(a, b) \text{ decreases of } 7. \end{aligned}$$

Laurent roots correspond to real roots when $f \in \mathbb{Q}[x]$.

Computing Laurent roots

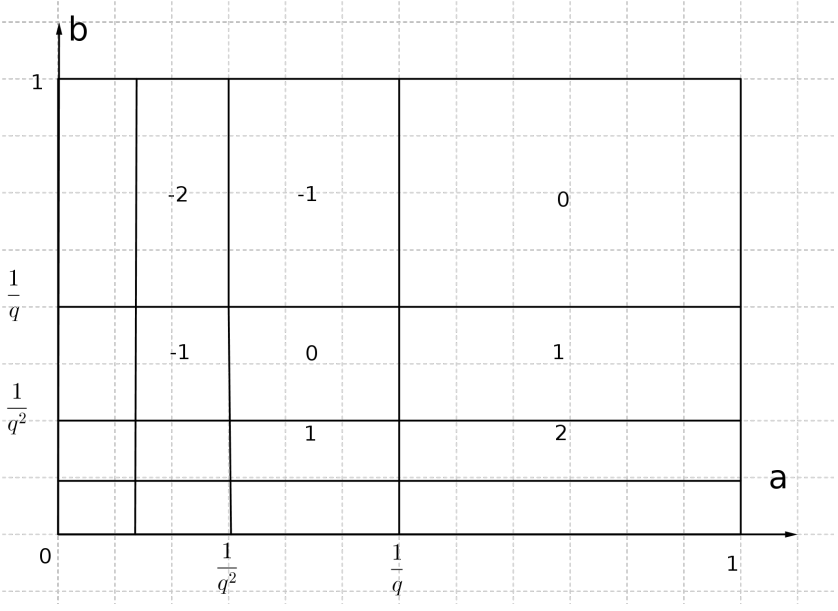
- The first term is found using the integer slopes of the Newton polygon (as for Puiseux series).
- The other terms are computed as in Hensel's lift.
- The gap is computed by trying several expansions of r.

Equation of α_∞

Lemma

For a Laurent root $r + O(\frac{1}{t^{m+1}})$ of $f \in \mathbb{F}_q[t][x]$, and skewness S, one has

$$\text{Prob}\left(\frac{a}{b} = r + O\left(\frac{1}{t^{m+1}}\right)\right) = \frac{q^{-\deg r - m - |s - \deg r|}}{q+1}(1 + O_{e\to\infty}(1/q^{2e})).$$



One obtains a formula for α_∞ similar to α_ℓ, measuring the average loss in degree.

Epsilon

- Recall that we sieve on a domain of skewness s if we impose the condition $\deg a \leq e + s/2$ and $\deg b \leq e - s/2$. We call $\sigma(f, s, e)$ the average degree of $F(a, b)$ if no cancellations occurred.

Epsilon

- Recall that we sieve on a domain of skewness s if we impose the condition $\deg a \leq e + s/2$ and $\deg b \leq e - s/2$. We call $\sigma(f, s, e)$ the average degree of $F(a, b)$ if no cancellations occurred.
- Heuristically, epsilon is the degree of a random polynomial with the same smoothness probability as $F(a, b)$.

Notation

$$\epsilon(f, s, e) = \alpha(f) + \alpha_\infty(f, s) + \sigma(f, s, e),$$

with σ the size of f.

Epsilon

- Recall that we sieve on a domain of skewness s if we impose the condition $\deg a \leq e + s/2$ and $\deg b \leq e - s/2$. We call $\sigma(f, s, e)$ the average degree of $F(a, b)$ if no cancellations occurred.
- Heuristically, epsilon is the degree of a random polynomial with the same smoothness probability as $F(a, b)$.

Notation

$$\epsilon(f, s, e) = \alpha(f) + \alpha_\infty(f, s) + \sigma(f, s, e),$$

with σ the size of f.

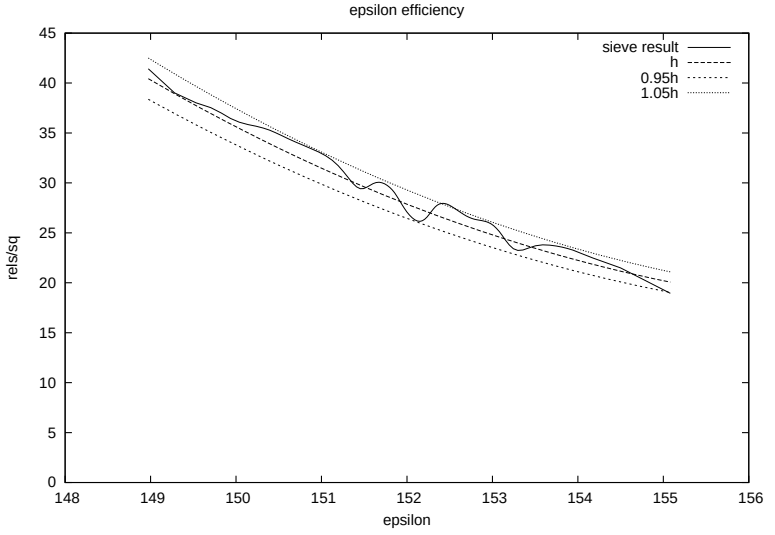
- Epsilon can be used to estimate the speedup of a polynomial using Dickman's ρ function.

Outline of the talk

- Introduction
- Root property
- Cancellation property
- Conclusion

Experimental validation

Figure: Epsilon and sieve efficiency for the polynomials f in our experiment. The function h is a function of type $a + bx + c \log x$, with no special significance.



Conclusion and future work

Conclusion.

- Epsilon compares arbitrary polynomials with a 5% relative error.
- Best polynomials are at least twice as effective as poor ones.
- The results were consistent to the results of the cado-nfs implementation.

The computation of discrete logarithm in $\mathbb{F}_{2^{809}}$.

- Sieve took 17.8k CPU hours and found 117 million pairs (a, b).
- Filtering reduced the number of unknown to 3.68 million.
- Linear algebra, done on GPU, took 13.2 equivalent CPU hours.
- Individual logarithm is negligible and can be run for as many elements as needed.