Fast arithmetics in Artin-Schreier towers over finite fields

L. De Feo and E. Schost

C4, École Polytechnique

June 10, 2008

Plan

1. Artin-Schreier towers
2. Couveignes' algorithm
3. Arithmetics
4. Benchmarks

Artin-Schreier

Definition (Artin-Schreier polynomial)

$\mathbb{K}$ a field of characteristic p, $\alpha \in \mathbb{K}$

$$X^p - X - \alpha$$

is an Artin-Schreier polynomial.

Theorem

$X^p - X - \alpha$ irreducible $\Leftrightarrow \ \mathrm{Tr}_{\mathbb{K}/\mathbb{F}_p}(\alpha) \neq 0$.
If $\eta \in \mathbb{K}$ is a root, then $\eta + 1, \ldots, \eta + (p-1)$ are roots.

Definition (Artin-Schreier extension)

$\mathcal{P}$ an irreducible Artin-Schreier polynomial.

$$\mathbb{L} = \mathbb{K}[X]/\mathcal{P}(X).$$

$\mathbb{L}/\mathbb{K}$ is called an Artin-Schreier extension.

Artin-Schreier towers over finite fields

Base field

$\mathbb{U}_0 = \mathbb{F}_{p^d}$ reasonably sized, d odd, "easy" arithmetics.

- Crypto size : $\mathbb{F}_{2^{199}}$ YES
- *Record* size : $\mathbb{F}_{2^{1999}}$ YES
- Huge size : $\mathbb{F}_{2^{2^{30}-1}}$ NO

Tower : $\mathbb{U}_0, \mathbb{U}_1, \ldots, \mathbb{U}_k$

- height k;
- $\alpha_i \in \mathbb{U}_i, \qquad \mathcal{P}_i = X^p - X - \alpha_i$;
- $\mathbb{U}_{i+1} = \mathbb{U}_i[X_{i+1}]/\mathcal{P}_i(X_{i+1})$.

Motivation

- p^k-torsion points of elliptic curves;
- isogeny computation via Couveignes II;
- many more ?

Arithmetics

- $\mathsf{M}(n)$ = complexity of multiplication of polynomials of degree n in $\mathbb{F}_p[X]$.
- Elements of $\mathbb{U}_i$ represented as polynomials of degree $< p^i d$ over $\mathbb{F}_p$.

Operations over $\mathbb{U}_i$

Addition, subtraction, equality in $\mathbb{U}_i$		$O(p^i d)$
Multiplication in $\mathbb{U}_i$	$\mathsf{M}(\mathbb{U}_i)$	$O(\mathsf{M}(p^i d))$
Inversion in $\mathbb{U}_i$		$O(\mathsf{M}(\mathbb{U}_i))$
Vector space isomorphism $\mathbb{U}_i \cong \mathbb{U}_{i-1}^p$	$\mathsf{P}(i)$, $\mathsf{L}(i)$	$O(\mathsf{M}(2p^i d) i \log_p d)$
n-th power		$O(\mathsf{M}(\mathbb{U}_i) \log n)$
$\mathrm{Tr}_{\mathbb{F}_{p^d}/\mathbb{F}_p}$	$\mathsf{T}(d)$	
$\mathrm{Tr}_{\mathbb{U}_i/\mathbb{U}_j}$		$O\left(\sum_{l=j}^{i} \mathsf{P}(i)\right)$
$\mathrm{Tr}_{\mathbb{U}_i/\mathbb{F}_p}$		$O\left(\sum_{l=0}^{i} \mathsf{P}(i) + \mathsf{T}(d)\right)$
$p^j d$-th pseudotrace $\mathrm{PTr}_{p^j d}$	$\mathsf{PT}_{\mathbb{U}_i}(j)$	$O\left(\mathsf{F}_{\mathbb{U}_i}(j-1) + d^2 \mathsf{M}(p^i d)\right)$
$p^j d$-iterated frobenius	$\mathsf{F}_{\mathbb{U}_i}(j)$	$\tilde{O}(\mathsf{M}(2p^i d) i^2 p)$
Arithmetics in $\mathbb{U}_i[X]$, degree n	$\mathsf{M}_{\mathbb{U}_i}(n)$	$O(\mathsf{M}(p^i dn))$

Unusual arithmetics

Vector space isomorphism

- $v \in \mathbb{U}_i \mapsto v_0, \ldots, v_{p-1} \in \mathbb{U}_{i-1}$ such that $v = \sum_{l=0}^{p-1} v_l X_i^l$; P($i$)
- $v_0, \ldots, v_{p-1} \in \mathbb{U}_{i-1} \mapsto v \in \mathbb{U}_i$ such that $v = \sum_{l=0}^{p-1} v_l X_i^l$. L($i$)

Pseudotrace

- $\mathrm{PTr}_{p^j d}(v) = \sum_{l=0}^{p^j d-1} v^{p^l}$;
- if $v \in \mathbb{U}_i$ then $\mathrm{PTr}_{p^i d}(v) = \mathrm{Tr}_{\mathbb{U}_i/\mathbb{F}_p}(v)$.

Iterated frobenius

- $v \mapsto v^{p^j d}$

Plan

1. Artin-Schreier towers
2. Couveignes' algorithm
3. Arithmetics
4. Benchmarks

Isomorphism between towers

Goal

- We want quasi-linear complexity for all arithmetic operations.
- Unfortunately, for generic elements $\alpha_0, \alpha_1, \ldots, \alpha_k$ there's no way of controlling both $\mathsf{M}(\mathbb{U}_i)$ and $\mathsf{P}(i)$, $\mathsf{L}(i)$.

Isomorphism

- $\mathbb{U}_0 = \mathbb{U}'_0$;
- $\mathbb{U}_0, \mathbb{U}_1, \ldots, \mathbb{U}_k$ defined by $\alpha_0, \ldots, \alpha_{k-1}$;
- $\mathbb{U}'_0, \mathbb{U}'_1, \ldots, \mathbb{U}'_k$ defined by $\alpha'_0, \ldots, \alpha'_{k-1}$;
- the two towers are isomorphic.

Idea

- One tower has faster arithmetics.
- If one can efficiently compute the isomorphism, all arithmetics can be done in the faster tower.

Couveignes' algorithm

- The isomorphism can be computed by factorising each $X^p - X - \alpha'_i$ into $\mathbb{U}_{i+1}$.
- Standard algorithms for factorisation are too slow.
- Couveignes' algorithm gives a good solution.

Couveignes

Entrée : $\alpha_i \in \mathbb{U}_{i+1}$ with $\mathrm{Tr}_{\mathbb{U}_{i+1}/\mathbb{F}_p}(\alpha_i) = 0$
Sortie : a root of $X^p - X - \alpha_i$ in $\mathbb{U}_{i+1}$

1. $\beta = \mathrm{PTr}_{p^i d}(\alpha_i)$; $\qquad \mathsf{PT}_{\mathbb{U}_{i+1}}(i)$
2. $\gamma =$ root of $X^{p^{p^i d}} - X - \beta$; $\qquad O(p\mathsf{F}_{\mathbb{U}_{i+1}}(i-1) + p^3\mathsf{M}(\mathbb{U}_i))$
3. $\delta_{i+1} = \beta - \gamma^p + \gamma \in \mathbb{U}_i$ and $\mathrm{Tr}_{\mathbb{U}_i/\mathbb{F}_p}(\delta) = 0$ $\qquad O(\mathsf{P}(i))$
4. $z =$ Couveignes(δ);
5. return $z + \gamma \in \mathbb{U}_{i+1}$ $\qquad O(\mathsf{L}(i))$.

Plan

A fast tower

Theorem

- $\mathbb{U}_0 = \mathbb{F}_{p^d} = \mathbb{F}_p[X_0]/P(X_0)$. *If* d *is odd, one of* $X^p - X - X_0$ *and* $X^p - X - (X_0 + 1)$ *is irreducible over* $\mathbb{U}_0$*.*
- *If* $p = 2$, $X^p - X - X_1$ *is irreducible over* $\mathbb{U}_1$*.*
- *If* $p > 2$ *or* $p = 2$ *and* $i \geqslant 2$, $X^p - X - X_i^{2p-1}$ *is irreducible over* $\mathbb{U}_i$*.*

$\mathbb{U}_i = \mathbb{F}_p[X_i]/Q_i(X_i)$

We want to compute such Q_i, we know Q_{i-1}.

Construction of the tower

Entrée : $Q_{i-1} \in \mathbb{F}_p[X]$, a $(2p-1)$-th root of unity ω
Sortie : $Q_i \in \mathbb{F}_p[X]$

1. $g_i(X^{2p-1}) = \prod_{l=0}^{2p-2} Q_{i-1}(\omega^i X)$; $\quad O(\mathsf{M}(p^{i+1}d))$
2. $Q_i(X) = g_i(X^p - X)$; $\quad O(p^{i+1}di \log_p d)$

Vector space isomorphism, Push-down

Push-down

Entrée : $v \in \mathbb{U}_i$
Sortie : $v_0, \ldots, v_{p-1} \in \mathbb{U}_{i-1}$ such that $v = v_0 + v_1 X_i + \ldots + v_{p-1} X_i^{p-1}$

1. Reduce v modulo $X_i^p - X_i - X_{i-1}^{2p-1}$; $O(p^{i+1} di \log_p d)$
2. Reduce each of the p coefficients of X_i by Q_{i-1} $O(p\mathsf{M}(2p^{i-1}d))$

Complexity

$$\mathsf{P}(i) = O(\mathsf{M}(2p^i d) i \log_p d)$$

Vector space isomorphism, Lift-up

Transposition principle

Every algorithm that computes a function f can be transformed in an algorithm that computes the *transpose* of f in the same running time up to a constant factor.

Push-down

- Given $v \in \mathbb{F}_p(X_i)$, $\qquad v = \sum_{l=0}^{p^i d-1} a_l X^l$,
- let $y_i^{(l,m)} \in \mathbb{F}_p(X_{i-1})$ such that $X_i^l = y_i^{(l,p-1)} X_i^{p-1} + \cdots + y_i^{(l,0)}$,
- Push-down computes $v_m = \sum_{l=0}^{p^i d-1} a_l y_i^{(l,m)}$ for $m = 0, \ldots, p-1$.

Transposition of push-down

- given $v_m \in \mathbb{F}_p(X_{i-1})$ for $m = 0, \ldots, p-1$,
- let $y_i^{(l,m)} \in \mathbb{F}_p(X_{i-1})$ such that $X_i^l = y_i^{(l,p-1)} X_i^{p-1} + \cdots + y_i^{(l,0)}$,
- given a linear form L over $\mathbb{F}_p[X_i]$,
- push-down^T computes $L(y_i^{(l,p-1)} X_i^{p-1} + \cdots + y_i^{(l,0)})$ for $l = 0, \ldots, p^i d - 1$.

Vector space isomorphism, Lift-up

Lift-up

Entrée : $v_0, \ldots, v_{p-1} \in \mathbb{U}_{i-1}$

Sortie : $v \in \mathbb{U}_i$ such that $v = v_0 + v_1 X_i + \ldots + v_{p-1} X_i^{p-1}$

1. Let R be the linear form of the residue, compute $r_l = R(y_i^{(l,p-1)} X_i^{p-1} + \cdots + y_i^{(l,0)})$ for $l < p^i d$; $O(\mathsf{P}(i))$
2. compute $v.R$, the linear form $x \mapsto R(v \cdot x)$; $O(\mathsf{M}(p^i d))$
3. compute $r'_l = v.R(y_i^{(l,p-1)} X_i^{p-1} + \cdots + y_i^{(l,0)})$ for $l < p^i d$; $O(\mathsf{P}(i))$
4. use XGCD in $\mathbb{F}_p[X]$ to compute $s = \frac{1}{\sum r_l Z^l}$; $O(\mathsf{M}(p^i d))$
5. return $s \cdot \sum r'_l Z^l$; $O(\mathsf{M}(p^i d))$

Complexity

$$\mathsf{L}(i) = O(\mathsf{P}(i))$$

Iterated frobenius

Theorem

$$X_i^{p^h} = X_i + \mathrm{PTr}_h(\alpha_{i-1})$$

Iterated frobenius

Entrée : $v \in \mathbb{U}_i$, $j \leqslant i$

Sortie : $v^{p^{p^j d}}$

1. if $j = i$ return v.
2. $v = v_0 + \cdots + v_{p-1} X_i^{p-1}$; $O(\mathsf{P}(i))$
3. $u_m =$ Iterated frobenius$(v_m \in \mathbb{U}_{i-1}, j)$ for $m < p$; $p\mathsf{F}_{\mathbb{U}_{i-1}}(j)$
4. $t =$ Pseudotrace(X_i, j); precomputed
5. return $\sum_{l=0}^{p-1} u_l (X_i + t)^l$. $O(\mathsf{M}(p^i d) p \log p + \mathsf{L}(i))$

Complexity

$$O(\mathsf{M}(2p^i d) i^2 p \log_p d \log p)$$

Trace, pseudotrace

Theorem

- $\mathrm{PTr}_{p^i d}(v) = \mathrm{Tr}_{\mathbb{U}_i/\mathbb{F}_p}(v) = \mathrm{Tr}_{\mathbb{U}_{i-1}/\mathbb{F}_p} \circ \mathrm{Tr}_{\mathbb{U}_i/\mathbb{U}_{i-1}}(v)$;
- $\mathrm{Tr}_{\mathbb{U}_i/\mathbb{U}_{i-1}} \left(\sum_{m=0}^{p-1} v_m X_i^m \right) = -v_m$.

Trace

Entrée : $v \in \mathbb{U}_i$
Sortie : $\mathrm{Tr}_{\mathbb{U}_i/\mathbb{F}_p}(v)$

1. if $v \in \mathbb{U}_0$ return $\mathrm{Tr}_{\mathbb{F}_{p^d}/\mathbb{F}_p}(v)$. $O(\mathsf{T}(d))$
2. $v = v_0 + \cdots + v_{p-1} X_i^{p-1}$; $O(\mathsf{P}(i))$
3. return Trace$(-v_{p-1})$.

Complexity

$$O\left(\sum_{l=0}^{i} \mathsf{P}(l) + \mathsf{T}(d)\right)$$

Trace, pseudotrace

Theorem

- $\mathrm{PTr}_{p^j d}(v) = \mathrm{PTr}_{p^{j-1} d}(v) + \left(\mathsf{PT}_{p^{j-1} d}(v)\right)^{p^{j-1} d}$;
- $\mathrm{PTr}_{p^i d}(v) = \mathrm{Tr}_{\mathbb{U}_i/\mathbb{F}_p}(v) = \mathrm{Tr}_{\mathbb{U}_{i-1}/\mathbb{F}_p} \circ \mathrm{Tr}_{\mathbb{U}_i/\mathbb{U}_{i-1}}(v)$;

Pseudotrace

Entrée : $v \in \mathbb{U}_i$, $j < i$
Sortie : $\mathrm{PTr}_{p^j d}(v)$

1. if $j = 0$ return $\sum_{l=0}^{d-1} v^{p^l}$. $\quad O(d^2\mathsf{M}(p^i d))$
2. $t =$ Pseudotrace$(v, j-1)$; $\quad \mathsf{PT}_{U_i}(j-1)$
3. return $t+$ Iterated frobenius$(t, j-1)$. $\quad \mathsf{F}_{\mathbb{U}_i}(j-1)$

Complexity

$$O\left(\sum_{l=0}^{j-1} \mathsf{F}_{\mathbb{U}_i}(l-1) + d^2\mathsf{M}(p^i d)\right)$$

Plan

Benchmarks

- Implementation in NTL for $p = 2$ (no FFT).
- Two fields: $\mathbb{F}_{2^{101}}$ and $\mathbb{F}_{2^{1999}}$.
- Up to 15 levels.

	$\mathbb{F}_{2^{101}}$	$\mathbb{F}_{2^{1999}}$	levels
Construction of Q_i	$0:42$	$42:00$	15
Precomputations for lift-up	$3:00$	$> 60:00:00$	15
Push-down, lift-up	$0:30$		15
Push-down, lift-up	$0:02$	$2:00$	12
Couveignes	$3:40:00$		15
Couveignes	$14:00$	$24:40:00$	12