Recent advances in index calculus

Maike Massierer

University of New South Wales, Sydney

Discrete Logarithm Problem

$G = \langle g \rangle$ finite group.

DLP: Given $h \in G$, find d such that $g^d = h$.
Notation: $d = \log_g h$

Discrete Logarithm Problem

$G = \langle g \rangle$ finite group.

DLP: Given $h \in G$, find d such that $g^d = h$.
Notation: $d = \log_g h$

In cryptography, need a group G such that

- Computation in G is efficient
- Order of G can be efficiently determined
- DLP in G is hard

Discrete Logarithm Problem

$G = \langle g \rangle$ finite group.

DLP: Given $h \in G$, find d such that $g^d = h$.
Notation: $d = \log_g h$

In cryptography, need a group G such that

- Computation in G is efficient
- Order of G can be efficiently determined
- DLP in G is hard

Possible groups:

- Multiplicative group of finite field
- Elliptic curve over finite field
- Divisor class group of hyperelliptic curve over finite field

Attacking the DLP

- The security of DLP-based cryptosystems depends on the hardness of the DLP (in the relevant group)
- Study the security of cryptosystems by studying algorithms that solve the DLP
  $\rightarrow$ "attack on the DLP"
- For "generic groups" G, the best possible algorithm takes $O(\sqrt{\ell})$ group operations, for ℓ the largest prime factor of $|G|$
- If one knows the group G specifically, better attacks may be possible
  $\rightarrow$ index calculus

Algorithm complexities

Input: x
Input size: $\log x$

$$L_x(\alpha, c) := \exp(c(1 + o(1))(\log x)^{\alpha}(\log \log x)^{1-\alpha})$$

Algorithm complexities

Input: x
Input size: $\log x$

$$L_x(\alpha, c) := \exp(c(1 + o(1))(\log x)^{\alpha}(\log\log x)^{1-\alpha})$$

for $\alpha = 0$: $L_x(\alpha, c) = (\log x)^{c+o(1)}$ **polynomial**

for $\alpha = 1$: $L_x(\alpha, c) = x^{c+o(1)}$ **exponential**

for $0 < \alpha < 1$: **sub-exponential** [write $L(\alpha)$]

Algorithm complexities

Input: x
Input size: $\log x$

$$L_x(\alpha, c) := \exp(c(1 + o(1))(\log x)^{\alpha}(\log\log x)^{1-\alpha})$$

for $\alpha = 0$: $L_x(\alpha, c) = (\log x)^{c+o(1)}$ **polynomial**

for $\alpha = 1$: $L_x(\alpha, c) = x^{c+o(1)}$ **exponential**

for $0 < \alpha < 1$: **sub-exponential** [write $L(\alpha)$]

quasi-polynomial: $(\log x)^{\log\log x + o(1)}$

Index calculus complexities

group	complexity
$\mathcal{E}, \mathcal{H}/\mathbb{F}_p, g = 1, 2$	exponential, same as generic
$\mathcal{E}, \mathcal{H}/\mathbb{F}_{q^n}, g = 1, 2$	exponential, better than generic
$\mathcal{H}, g \geq 3$ small	exponential, better than generic
$\mathcal{C}, g$ large	sub-exponential $L(1/3)$
$\mathbb{F}_q$, large characteristic	sub-exponential $L(1/3)$
$\mathbb{F}_q$, small characteristic	quasi-polynomial

$\mathcal{E}$ = elliptic curve
$\mathcal{H}$ = hyperelliptic curve
$\mathcal{C} = \mathcal{C}_{ab}$ curve
g = genus

Index calculus complexities

group	complexity
$\mathcal{E}, \mathcal{H}/\mathbb{F}_p, g = 1, 2$	exponential, same as generic
$\mathcal{E}, \mathcal{H}/\mathbb{F}_{q^n}, g = 1, 2$	exponential, better than generic
$\mathcal{H}, g \geq 3$ small	exponential, better than generic
$\mathcal{C}, g$ large	sub-exponential $L(1/3)$
$\mathbb{F}_q$, large characteristic	sub-exponential $L(1/3)$
$\mathbb{F}_q$, small characteristic	quasi-polynomial

$\mathcal{E}$ = elliptic curve
$\mathcal{H}$ = hyperelliptic curve
$\mathcal{C} = \mathcal{C}_{ab}$ curve
g = genus

Outline

Introduction

Groups

Index calculus

Finite fields: FFS and its successors

Application to large genus curves?

Index calculus in small genus curves

Finite fields

Let p prime, $q = p^n$ prime power.

$\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$
$\mathbb{F}_q \cong \mathbb{F}_p[x]/k(x)\mathbb{F}_p[x]$, $\deg(k) = n$, k irreducible

$p =$ characteristic of $\mathbb{F}_p, \mathbb{F}_q$

Finite fields

Let p prime, $q = p^n$ prime power.

$\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$
$\mathbb{F}_q \cong \mathbb{F}_p[x]/k(x)\mathbb{F}_p[x]$, $\deg(k) = n$, k irreducible

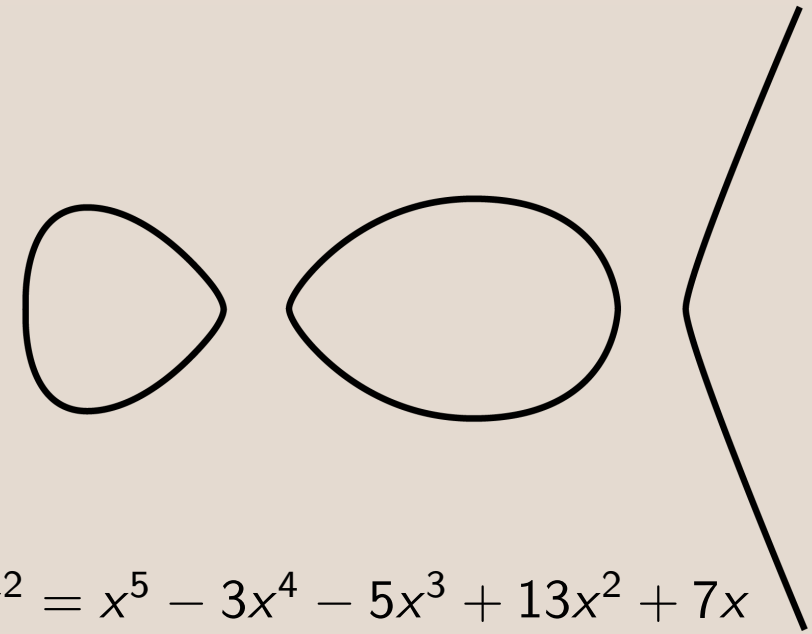
$p =$ characteristic of $\mathbb{F}_p, \mathbb{F}_q$

In crypto:
Group $G = \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ or $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$
$|G| = p - 1$ or $q - 1$

Algebraic curves

Curve:

$\mathcal{C} : C(x, y) = 0$



$y^2 = x^5 - 3x^4 - 5x^3 + 13x^2 + 7x$

Algebraic curves

Curve:

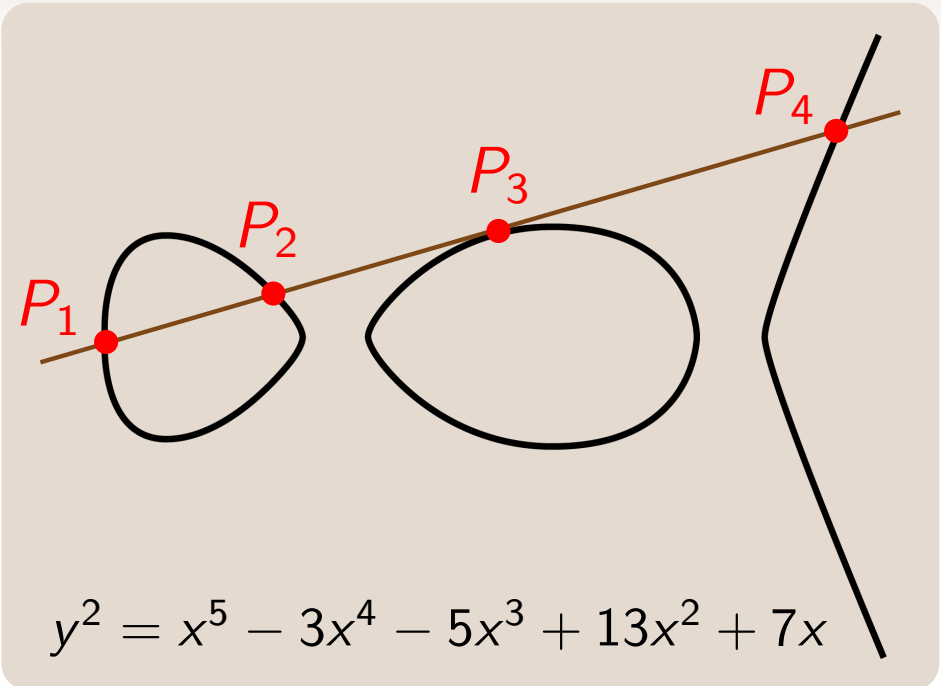
$\mathcal{C} : C(x, y) = 0$

Divisors $\mathrm{Div}_{\mathcal{C}}$:

$D = \sum \nu_i P_i$

Principal divisors $\mathrm{Prin}_{\mathcal{C}}$:

$\mathrm{div}(\phi) = \sum \mathrm{ord}_P(\phi) P$



Algebraic curves

Curve:

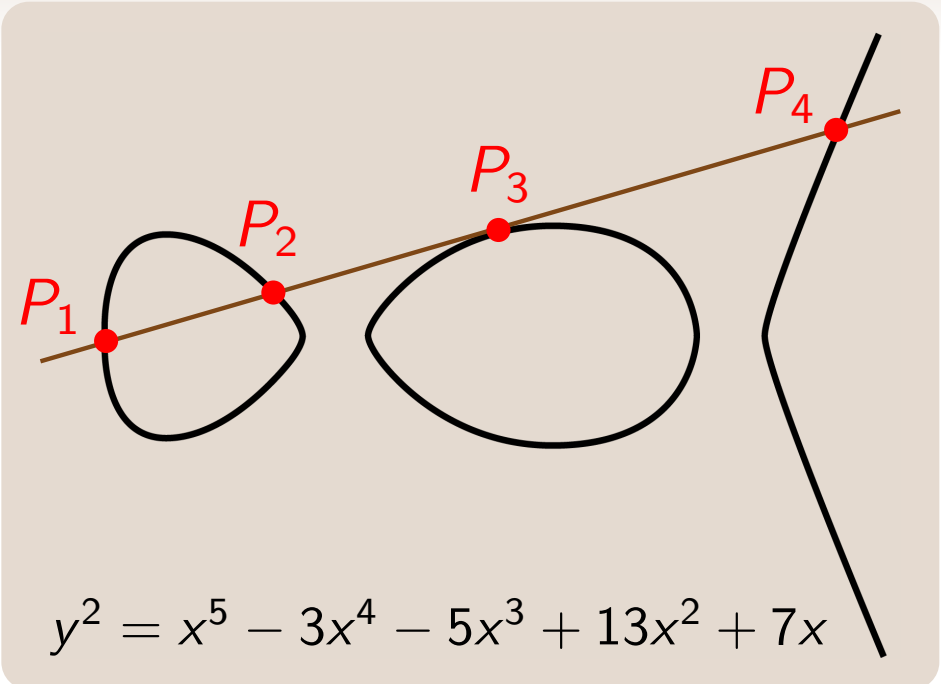
$\mathcal{C} : C(x, y) = 0$

Divisors $\mathrm{Div}_{\mathcal{C}}$:

$D = \sum \nu_i P_i$

Principal divisors $\mathrm{Prin}_{\mathcal{C}}$:

$\mathrm{div}(\phi) = \sum \mathrm{ord}_P(\phi) P$



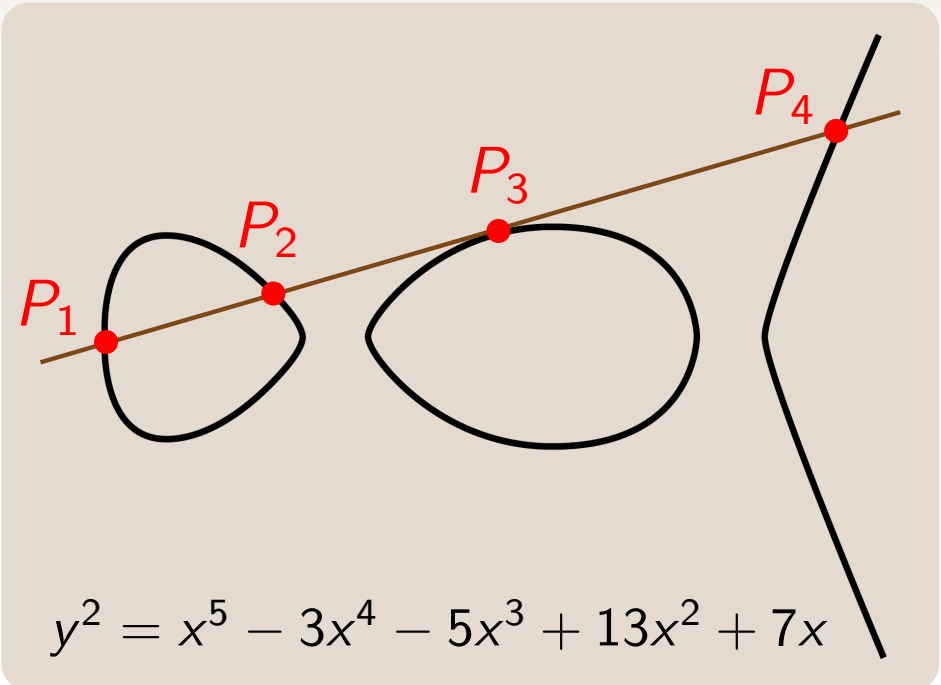
e.g. $\mathrm{div}(\text{brown line}) = P_1 + P_2 + 2P_3 + P_4 - 5\mathcal{O}$

Algebraic curves

Curve:
$\mathcal{C} : C(x, y) = 0$

Divisors $\mathrm{Div}_{\mathcal{C}}$:
$D = \sum \nu_i P_i$

Principal divisors $\mathrm{Prin}_{\mathcal{C}}$:
$\mathrm{div}(\phi) = \sum \mathrm{ord}_P(\phi) P$



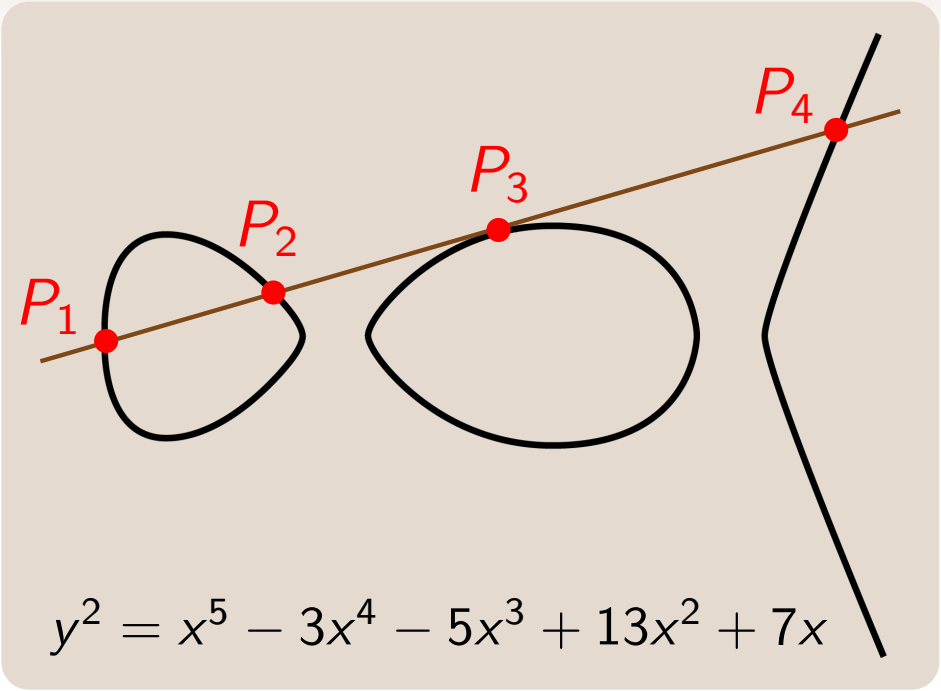
Divisor class group: $\mathrm{Cl}_{\mathcal{C}} \cong \mathrm{Div}^0_{\mathcal{C}} / \mathrm{Prin}_{\mathcal{C}} \ni [D]$
then $[\mathrm{div}(\phi)] = [0]$

Algebraic curves

Curve:
$\mathcal{C} : C(x, y) = 0$

Divisors $\mathrm{Div}_{\mathcal{C}}$:
$D = \sum \nu_i P_i$

Principal divisors $\mathrm{Prin}_{\mathcal{C}}$:
$\mathrm{div}(\phi) = \sum \mathrm{ord}_P(\phi) P$



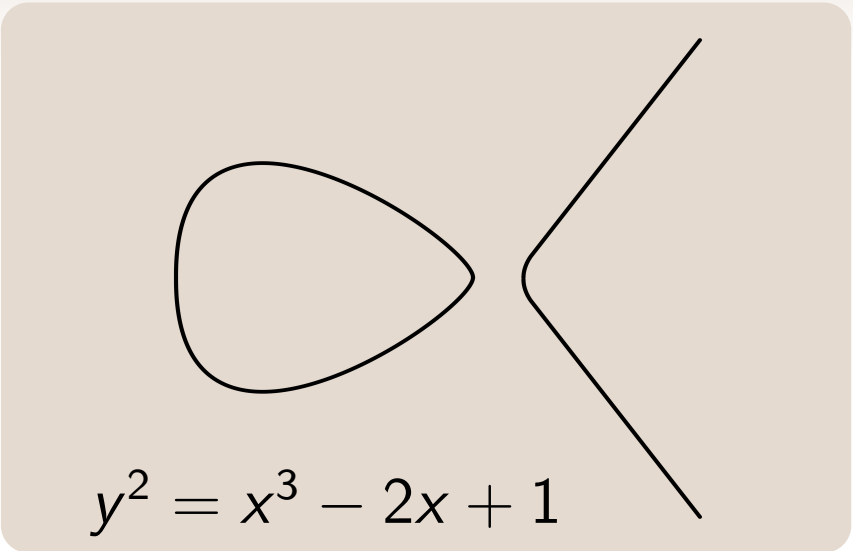
Divisor class group: $\mathrm{Cl}_{\mathcal{C}} \cong \mathrm{Div}^0_{\mathcal{C}} / \mathrm{Prin}_{\mathcal{C}} \ni [D]$
then $[\mathrm{div}(\phi)] = [0]$

In crypto: $C \in \mathbb{F}_q[x, y]$
$\mathrm{Cl}_{\mathcal{C}}(\mathbb{F}_q) = \mathbb{F}_q$-rational divisor classes
$|\mathrm{Cl}_{\mathcal{C}}(\mathbb{F}_q)| \approx q^g$ for $g =$ genus

Elliptic Curves

$\mathcal{E} : y^2 = x^3 + Ax + B$

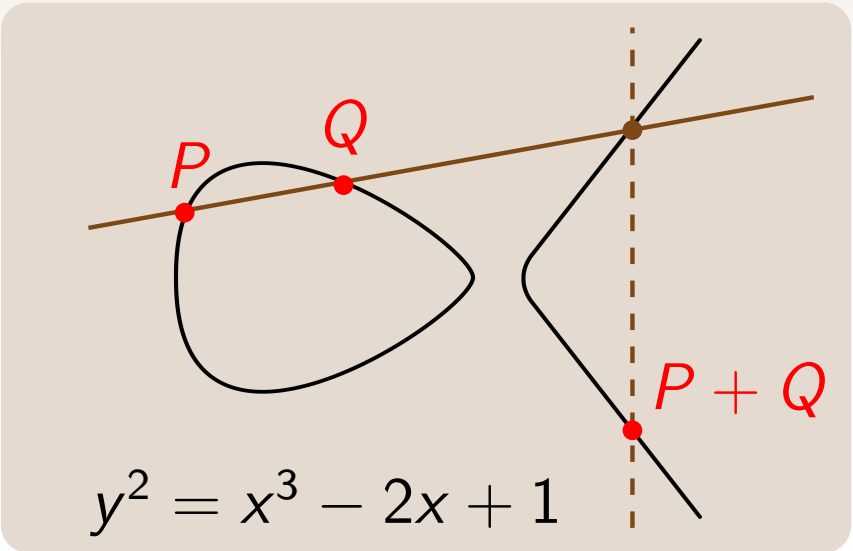
(over field of char $\neq 2, 3$)



Elliptic Curves

$\mathcal{E} : y^2 = x^3 + Ax + B$

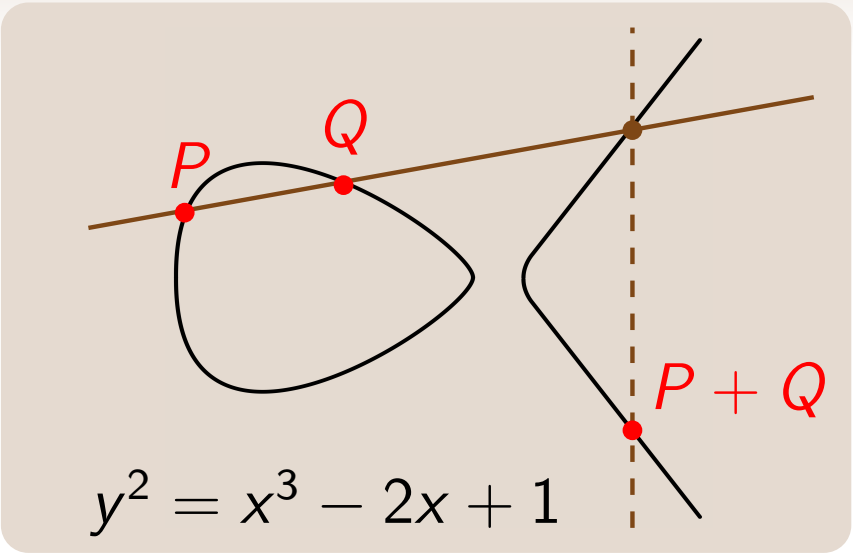
(over field of char $\neq 2, 3$)



Elliptic Curves

$\mathcal{E} : y^2 = x^3 + Ax + B$

(over field of char $\neq 2, 3$)



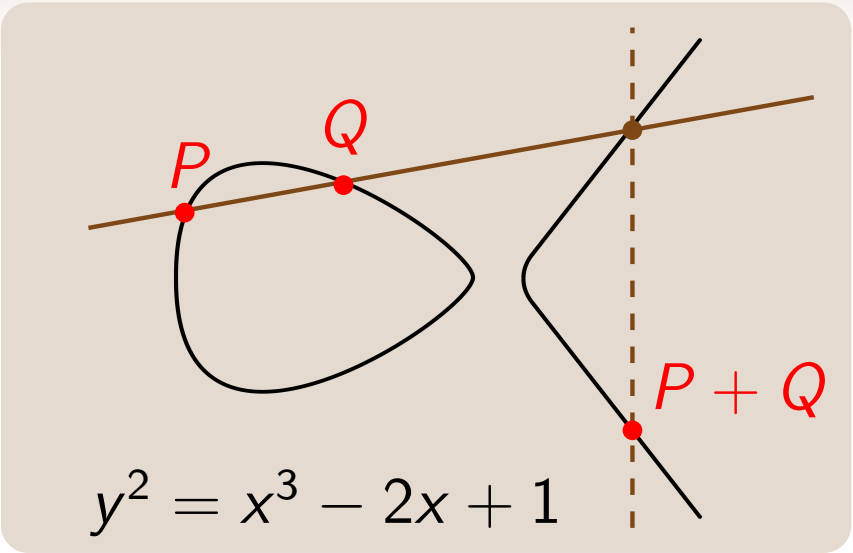
In crypto: $A, B \in \mathbb{F}_q$

Group $G = \mathcal{E}(\mathbb{F}_q) = \{(x, y) \in \mathcal{E} \mid x, y \in \mathbb{F}_q\} \cup \{\mathcal{O}\}$

$|G| \approx q$ ($\mathbb{F}_q$-rational points on $\mathcal{E}$)

Elliptic Curves

$\mathcal{E} : y^2 = x^3 + Ax + B$
(over field of char $\neq 2, 3$)



In crypto: $A, B \in \mathbb{F}_q$
Group $G = \mathcal{E}(\mathbb{F}_q) = \{(x, y) \in \mathcal{E} \mid x, y \in \mathbb{F}_q\} \cup \{\mathcal{O}\}$
$|G| \approx q$ ($\mathbb{F}_q$-rational points on $\mathcal{E}$)

Elliptic curves have genus $g = 1$

For elliptic curves: $\mathcal{E} \cong \mathrm{Cl}_{\mathcal{E}}$

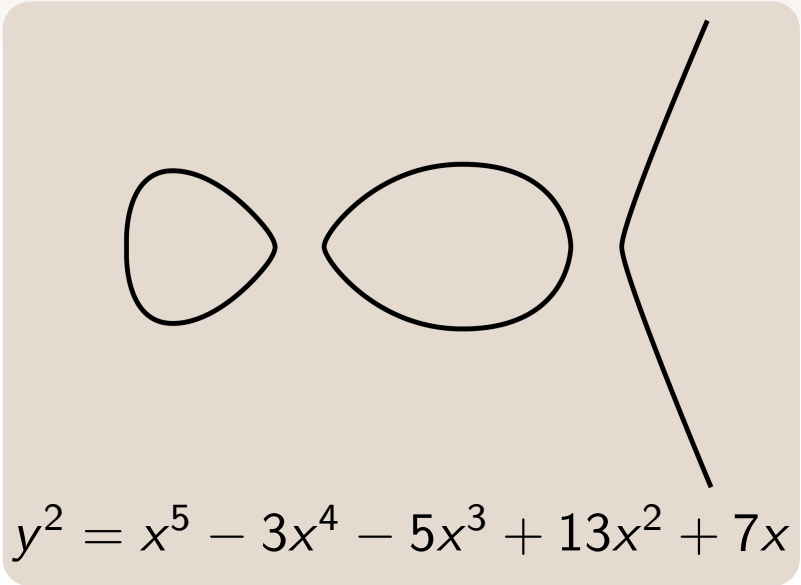
Hyperelliptic curves

$\mathcal{H} : y^2 = f(x)$

$\deg(f) = 2g + 1$

$g =$ genus

(over field of char $\neq 2, 3$)



$y^2 = x^5 - 3x^4 - 5x^3 + 13x^2 + 7x$

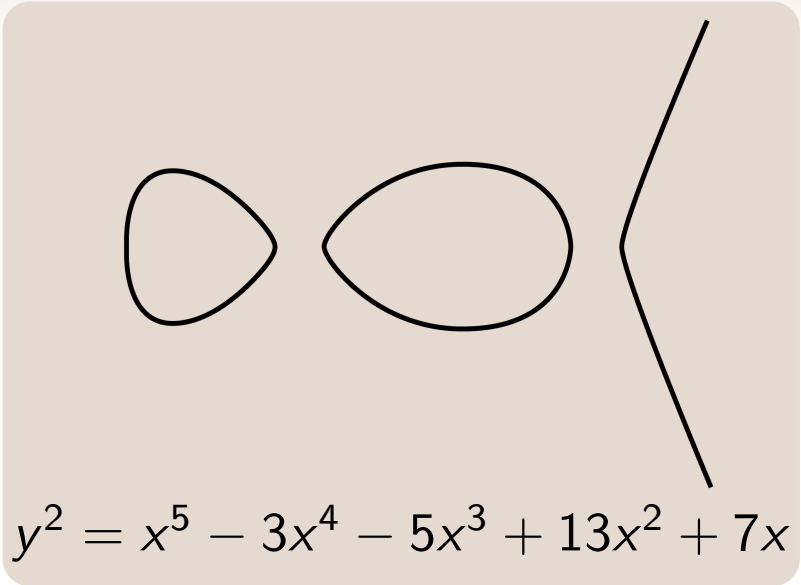
Hyperelliptic curves

$\mathcal{H} : y^2 = f(x)$

$\deg(f) = 2g + 1$

$g =$ genus

(over field of char $\neq 2, 3$)



In crypto: $f \in \mathbb{F}_q[x]$

Group $G = \mathrm{Cl}_{\mathcal{H}}(\mathbb{F}_q)$ ($\mathbb{F}_q$-rational divisor classes)

$|G| \approx q^g$

$\mathcal{C}_{ab}$ curves

Projective curves with smooth affine part defined by

$$\mathcal{C}_{ab} : y^a + x^b + f(x, y) = 0,$$

where

- $\gcd(a, b) = 1$
- $ai + bj \leq ab$ for all monomials $x^i y^j$ of $f \in \mathbb{F}_q[x, y]$
- genus $g = (a - 1)(b - 1)/2$

$\mathcal{C}_{ab}$ curves

Projective curves with smooth affine part defined by

$$\mathcal{C}_{ab} : y^a + x^b + f(x, y) = 0,$$

where

- $\gcd(a, b) = 1$
- $ai + bj \leq ab$ for all monomials $x^i y^j$ of $f \in \mathbb{F}_q[x, y]$
- genus $g = (a - 1)(b - 1)/2$

assume also ("low degree curves")

- $a \approx g^{\alpha}, b \approx g^{1-\alpha}$ with $\alpha \in [1/3, 2/3]$

Index calculus outline

Goal: Compute $\log_g(h)$ in group $G = \langle g \rangle$

Index calculus outline

Goal: Compute $\log_g(h)$ in group $G = \langle g \rangle$

Factor base: $\mathcal{F} = \{g_1, \ldots, g_r\} \subseteq G$

Index calculus outline

Goal: Compute $\log_g(h)$ in group $G = \langle g \rangle$

Factor base: $\mathcal{F} = \{g_1, \ldots, g_r\} \subseteq G$

Relation search: Find relations of the form

$$g^{\alpha_i} = \prod_{j=1}^{r} g_j^{m_{ij}}, \quad i = 1, \ldots, k > r$$

Index calculus outline

Goal: Compute $\log_g(h)$ in group $G = \langle g \rangle$

Factor base: $\mathcal{F} = \{g_1, \ldots, g_r\} \subseteq G$

Relation search: Find relations of the form

$$g^{\alpha_i} = \prod_{j=1}^{r} g_j^{m_{ij}}, \quad i = 1, \ldots, k > r$$

Linear algebra: For $M = (m_{ij}) \in \mathbb{Z}/(|G|)\mathbb{Z}^{k \times r}$, find $\gamma = (\gamma_1, \ldots, \gamma_r)^\intercal$ s.t. $M\gamma = (\alpha_1, \ldots, \alpha_k)^\intercal$ (then $\gamma_j = \log_g g_j$)

Index calculus outline

Goal: Compute $\log_g(h)$ in group $G = \langle g \rangle$

Factor base: $\mathcal{F} = \{g_1, \ldots, g_r\} \subseteq G$

Relation search: Find relations of the form

$$g^{\alpha_i} = \prod_{j=1}^{r} g_j^{m_{ij}}, \quad i = 1, \ldots, k > r$$

Linear algebra: For $M = (m_{ij}) \in \mathbb{Z}/(|G|)\mathbb{Z}^{k \times r}$, find $\gamma = (\gamma_1, \ldots, \gamma_r)^\intercal$ s.t. $M\gamma = (\alpha_1, \ldots, \alpha_k)^\intercal$ (then $\gamma_j = \log_g g_j$)

Individual logarithm: Find β s.t. $g^\beta h = \prod_{j=1}^{r} g_j^{\beta_j}$, then

$$\log_g h = -\beta + \sum_{j=1}^{r} \beta_j \gamma_j$$

Index calculus outline

Goal: Compute $\log_g(h)$ in group $G = \langle g \rangle$

Factor base: $\mathcal{F} = \{g_1, \ldots, g_r\} \subseteq G$

Relation search: Find relations of the form

$$g^{\alpha_i} = \prod_{j=1}^{r} g_j^{m_{ij}}, \quad i = 1, \ldots, k > r$$

Linear algebra: For $M = (m_{ij}) \in \mathbb{Z}/(|G|)\mathbb{Z}^{k \times r}$, find $\gamma = (\gamma_1, \ldots, \gamma_r)^\intercal$ s.t. $M\gamma = (\alpha_1, \ldots, \alpha_k)^\intercal$ (then $\gamma_j = \log_g g_j$)

Individual logarithm: Find β s.t. $g^\beta h = \prod_{j=1}^{r} g_j^{\beta_j}$, then

$$\log_g h = -\beta + \sum_{j=1}^{r} \beta_j \gamma_j$$

Index calculus complexities

group	complexity
$\mathcal{E}, \mathcal{H}/\mathbb{F}_p, g = 1, 2$	exponential, same as generic
$\mathcal{E}, \mathcal{H}/\mathbb{F}_{q^n}, g = 1, 2$	exponential, better than generic
$\mathcal{H}, g \geq 3$ small	exponential, better than generic
$\mathcal{C}, g$ large	sub-exponential $L(1/3)$
$\mathbb{F}_q$, large characteristic	sub-exponential $L(1/3)$
$\mathbb{F}_q$, small characteristic	quasi-polynomial

$\mathcal{E}$ = elliptic curve
$\mathcal{H}$ = hyperelliptic curve
$\mathcal{C} = \mathcal{C}_{ab}$ curve
g = genus

Index calculus complexities

group	complexity
$\mathcal{E}, \mathcal{H}/\mathbb{F}_p, g = 1, 2$	exponential, same as generic
$\mathcal{E}, \mathcal{H}/\mathbb{F}_{q^n}, g = 1, 2$	exponential, better than generic
$\mathcal{H}, g \geq 3$ small	exponential, better than generic
$\mathcal{C}, g$ large	sub-exponential $L(1/3)$
$\mathbb{F}_q$, large characteristic	sub-exponential $L(1/3)$
$\mathbb{F}_q$, small characteristic	quasi-polynomial

$\mathcal{E}$ = elliptic curve
$\mathcal{H}$ = hyperelliptic curve
$\mathcal{C} = \mathcal{C}_{ab}$ curve
g = genus

(r)evolution of the function field sieve

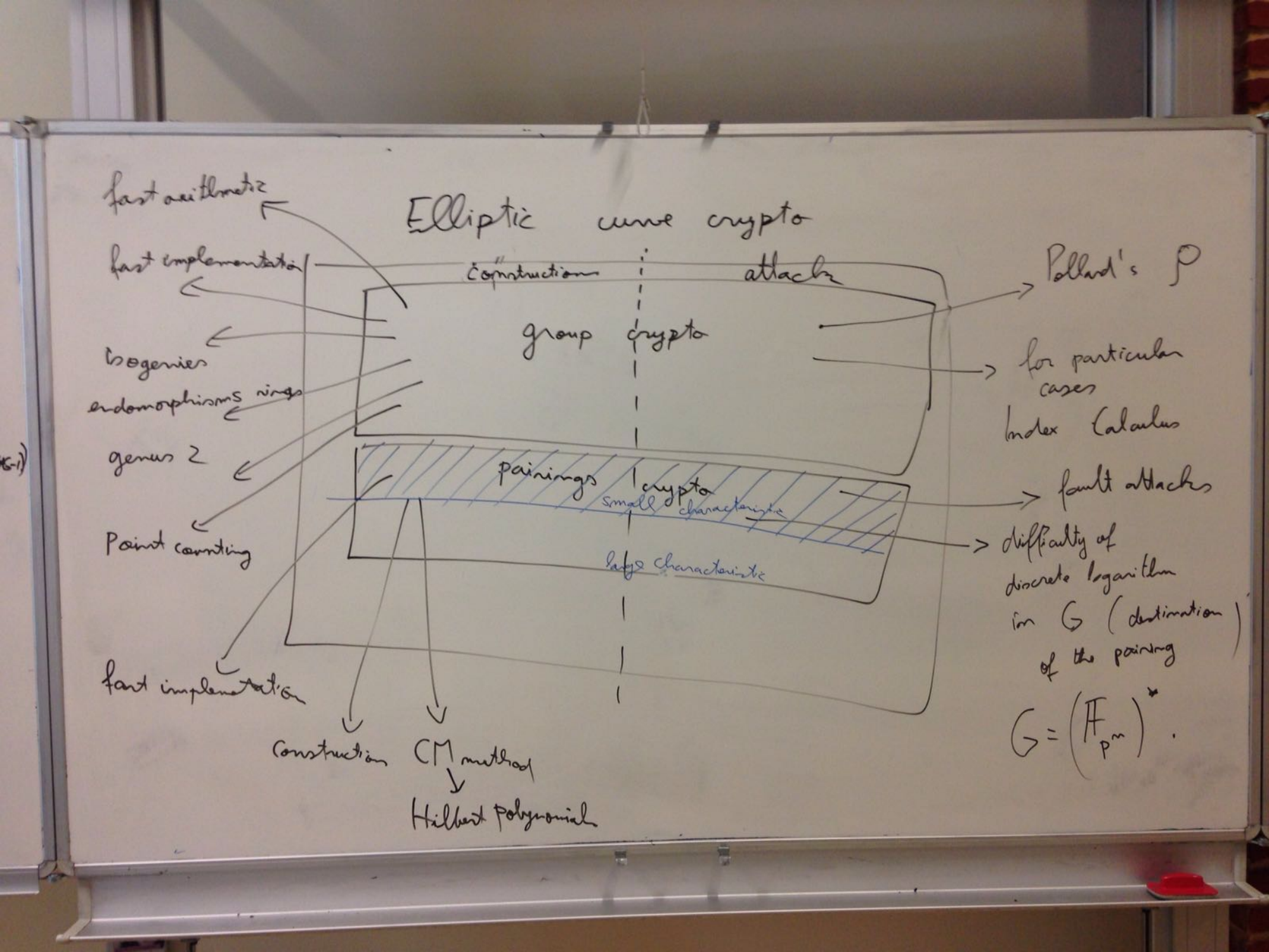
Discrete logarithms in finite fields of small char:

complexity	who		when
$L(1/2)$	Adleman		1979
$L(1/3)$	Coppersmith		1984
	Adleman	(FFS)	1994
$L(1/4 + o(1))$	Joux		2013
$L(1/4)$	Göloğlu–Granger–McGuire–Zumbrägel		2013
quasi-polynomial	Bărbulescu–Gaudry–Joux–Thomé		2013

(r)evolution of the function field sieve

Discrete logarithms in finite fields of small char:

complexity	who		when
$L(1/2)$	Adleman		1979
$L(1/3)$	Coppersmith		1984
	Adleman	(FFS)	1994
$L(1/4 + o(1))$	Joux		2013
$L(1/4)$	Göloğlu–Granger–McGuire–Zumbrägel		2013
quasi-polynomial	Bărbulescu–Gaudry–Joux–Thomé		2013


Elliptic curve crypto
fast arithmetic
fast implementation
isogenies
endomorphisms rings
genus 2
Point counting
fast implementation
construction
attacks
group crypto
pairings
crypto
small characteristic
large characteristic
Construction
CM method
Hilbert polynomial
Pollard's ρ
for particular cases
Index Calculus
fault attacks
difficulty of discrete logarithm in G (destination of the pairing)
$G = \left(\mathbb{F}_{p^m}\right)^*$.

(r)evolution of the function field sieve

Discrete logarithms in finite fields of small char:

complexity	who		when
$L(1/2)$	Adleman		1979
$L(1/3)$	Coppersmith		1984
	Adleman	(FFS)	1994
$L(1/4 + o(1))$	Joux		2013
$L(1/4)$	Göloğlu–Granger–McGuire–Zumbrägel		2013
quasi-polynomial	Bărbulescu–Gaudry–Joux–Thomé		2013

(r)evolution of the function field sieve

Discrete logarithms in finite fields of small char:

complexity	who	when
$L(1/2)$	Adleman	1979
$L(1/3)$	Coppersmith	1984
	Adleman (FFS)	1994
$L(1/4 + o(1))$	Joux	2013
$L(1/4)$	Göloğlu–Granger–McGuire–Zumbrägel	2013
quasi-polynomial	Bărbulescu–Gaudry–Joux–Thomé	2013

Discrete logarithms in curves of large genus:

$L(1/2)$	Adleman–DeMarrais–Huang	1994
$L(1/3 + \varepsilon)$	Enge–Gaudry	2007
$L(1/3)$	Enge–Gaudry–Thomé	2011

(r)evolution of the function field sieve

Discrete logarithms in finite fields of small char:

complexity	who	when
$L(1/2)$	Adleman	1979
$L(1/3)$	Coppersmith	1984
	Adleman (FFS)	1994
$L(1/4 + o(1))$	Joux	2013
$L(1/4)$	Göloğlu–Granger–McGuire–Zumbrägel	2013
quasi-polynomial	Bărbulescu–Gaudry–Joux–Thomé	2013

Discrete logarithms in curves of large genus:

$L(1/2)$	Adleman–DeMarrais–Huang	1994
$L(1/3 + \varepsilon)$	Enge–Gaudry	2007
$L(1/3)$	Enge–Gaudry–Thomé	2011

Question: Do the new ideas apply to curves?

Application to curves?

No for obvious applications.

We don't know for more general applications.

Setting

Goal: Compute discrete logarithms in G using an index calculus approach, where

- $G \subseteq \mathbb{F}_{q^n}^{\times}$, finite field of small characteristic
- $G \subseteq \mathrm{Cl}_{\mathcal{C}}(\mathbb{F}_q)$, divisor class group of a $\mathcal{C}_{ab}$ curve $\mathcal{C}$ of large genus

Factor base

Finite fields $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/k(x)$:

- Represent elements by polynomials $f(x) \in \mathbb{F}_q[x], \deg(f) < n$
- $B =$ smoothness bound
- $\mathcal{F}_B = \{f \in \mathbb{F}_q[x] \mid f \text{ monic, irred., } \deg(f) \leq B\}$

Factor base

Finite fields $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/k(x)$:

- Represent elements by polynomials $f(x) \in \mathbb{F}_q[x], \deg(f) < n$
- $B =$ smoothness bound
- $\mathcal{F}_B = \{f \in \mathbb{F}_q[x] \mid f \text{ monic, irred., } \deg(f) \leq B\}$

Divisor class groups $\mathrm{Cl}_{\mathcal{C}} \cong \mathrm{Div}^0_{\mathcal{C}} \,/\, \mathrm{Prin}_{\mathcal{C}}$:

- Represent elements by divisors
- $B =$ smoothness bound
- $\mathcal{F}_B = \{D \in \mathrm{Div}_{\mathcal{C}} \mid D \text{ prime}, \deg(D) \leq B\}$

Smoothness

An element is B-smooth if it splits in $\mathcal{F}_B$.

Theorem (Odlyzko)

A polynomial in $\mathbb{F}_q[x]$ of degree n is B-smooth with probability $u^{-u(1+o(1))}$ for $u = n/B$.

Smoothness

An element is B-smooth if it splits in $\mathcal{F}_B$.

Theorem (Odlyzko)

A polynomial in $\mathbb{F}_q[x]$ of degree n is B-smooth with probability $u^{-u(1+o(1))}$ for $u = n/B$.

Theorem (Heß)

An effective divisor of degree n on a projective curve defined over $\mathbb{F}_q$ is B-smooth with probability at least $u^{-u(1+o(1))}$ for $u = n/B$.

(up to technical details)

Complexity of basic index calculus

$$L_x(\alpha, c) = \exp(c(1 + o(1))(\log x)^{\alpha}(\log \log x)^{1-\alpha})$$

$x = q^n$ for $G \subseteq \mathbb{F}_{q^n}^*$
$x = q^g$ for $G \subseteq \mathrm{Cl}_{\mathcal{C}}(\mathbb{F}_q)$, $g =$ genus of $\mathcal{C}$

Complexity of basic index calculus

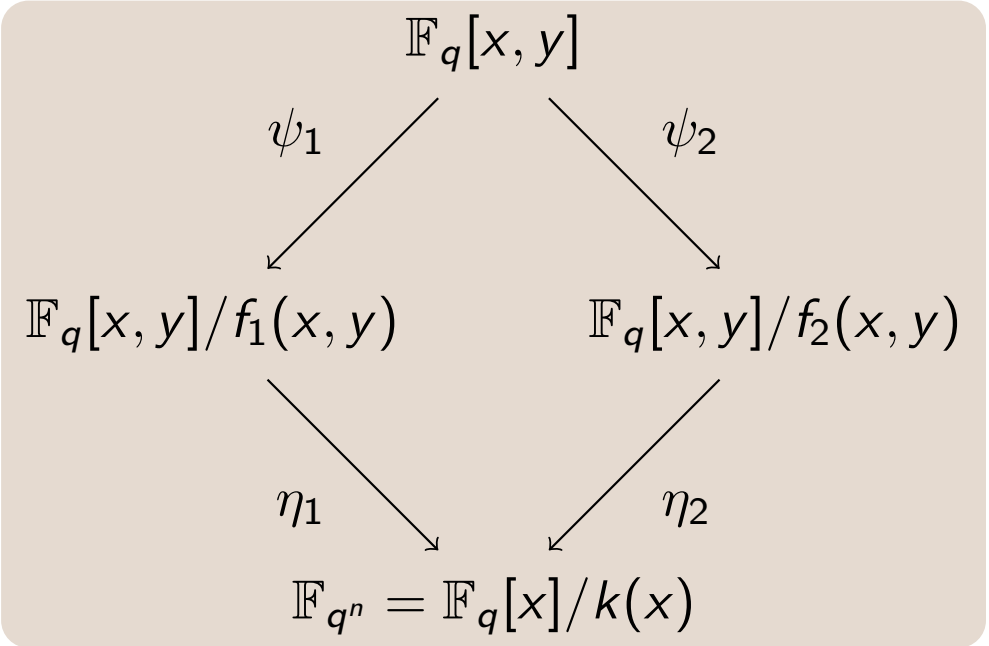
$$L_x(\alpha, c) = \exp(c(1 + o(1))(\log x)^{\alpha}(\log\log x)^{1-\alpha})$$

$x = q^n$ for $G \subseteq \mathbb{F}_{q^n}^*$
$x = q^g$ for $G \subseteq \mathrm{Cl}_{\mathcal{C}}(\mathbb{F}_q)$, $g =$ genus of $\mathcal{C}$

- Choose B s.t. $|\mathcal{F}_B| = L_x(1/2)$
- Then probability of B-smoothness is $L_x(1/2)^{-1}$
- Relation collection (simple strategy): $L_x(1/2)$
- Linear algebra (Lanczos/Wiedemann): $L_x(1/2)$
- Individual log (simple strategy): $L_x(1/2)$

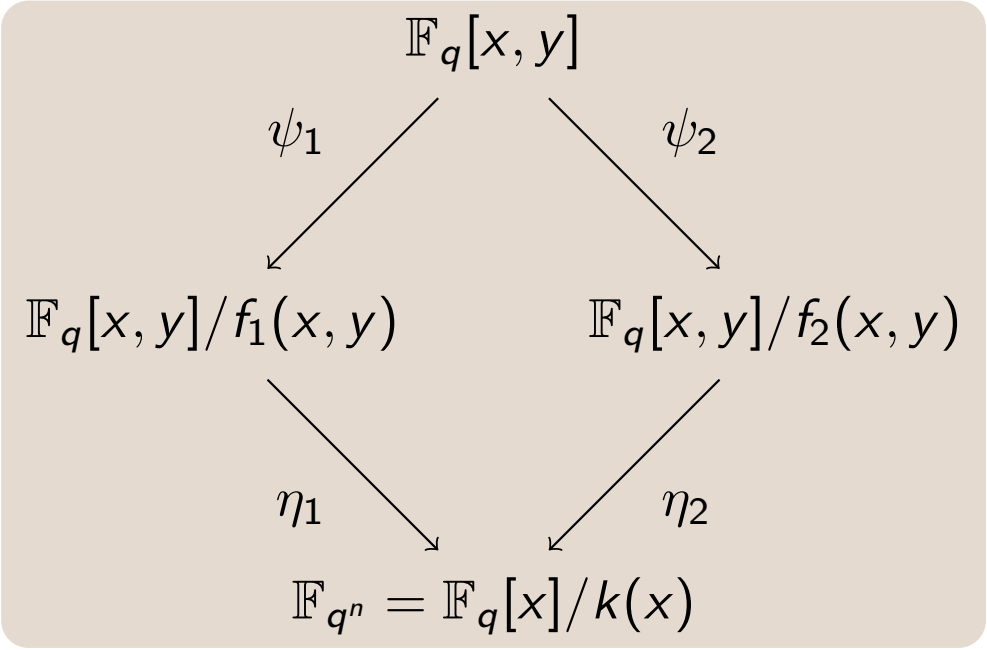
Overall complexity: $L_x(1/2)$

Relation search in FFS and successors



Relation search in FFS and successors

Search for
$\phi(x, y) \in \mathbb{F}_q[x, y]$
such that
$\psi_i(\phi)$ are B-smooth.

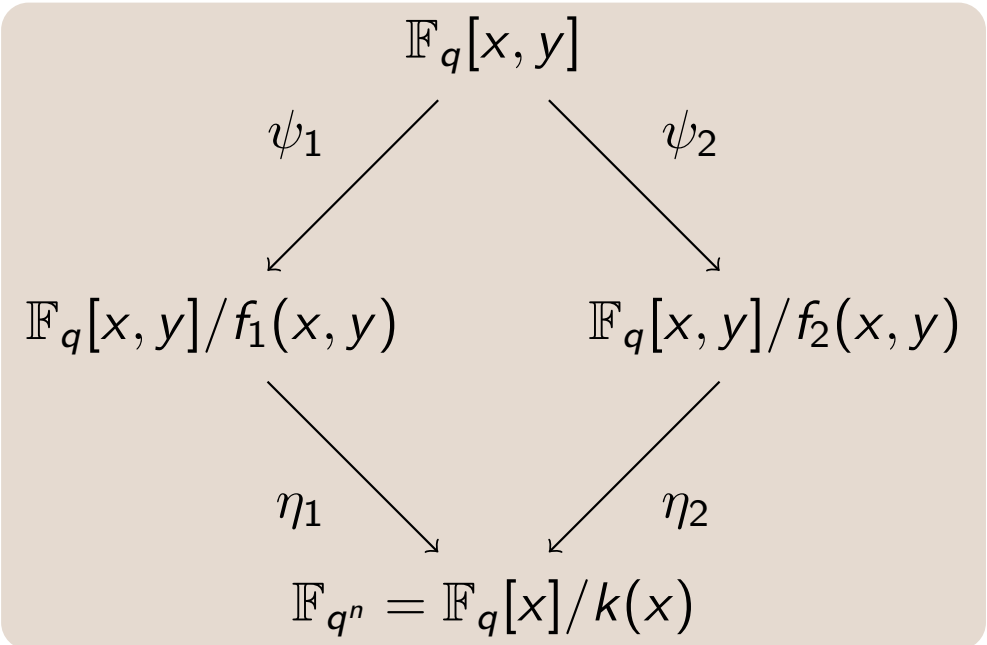


Then $\eta_1(\psi_1(\phi)) = \eta_2(\psi_2(\phi))$ gives a relation in $\mathbb{F}_{q^n}$.

Function fields: $F_i = \mathrm{Frac}(\mathbb{F}_q[x, y]/f_i(x, y))$

Relation search in FFS

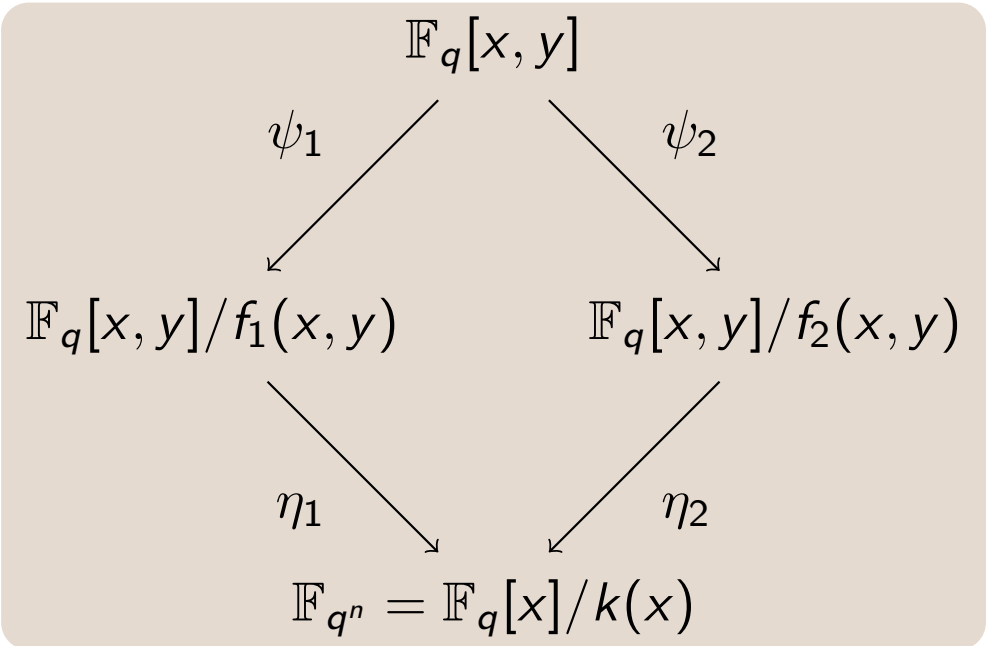
Applicability:
Fields $\mathbb{F}_{q^n}$ of small characteristic $q < L_{q^n}(1/3)$



Relation search in FFS

Applicability:
Fields $\mathbb{F}_{q^n}$ of
small characteristic
$q < L_{q^n}(1/3)$

Choose
$\phi = a(x)y + b(x)$,
deal with ideals.

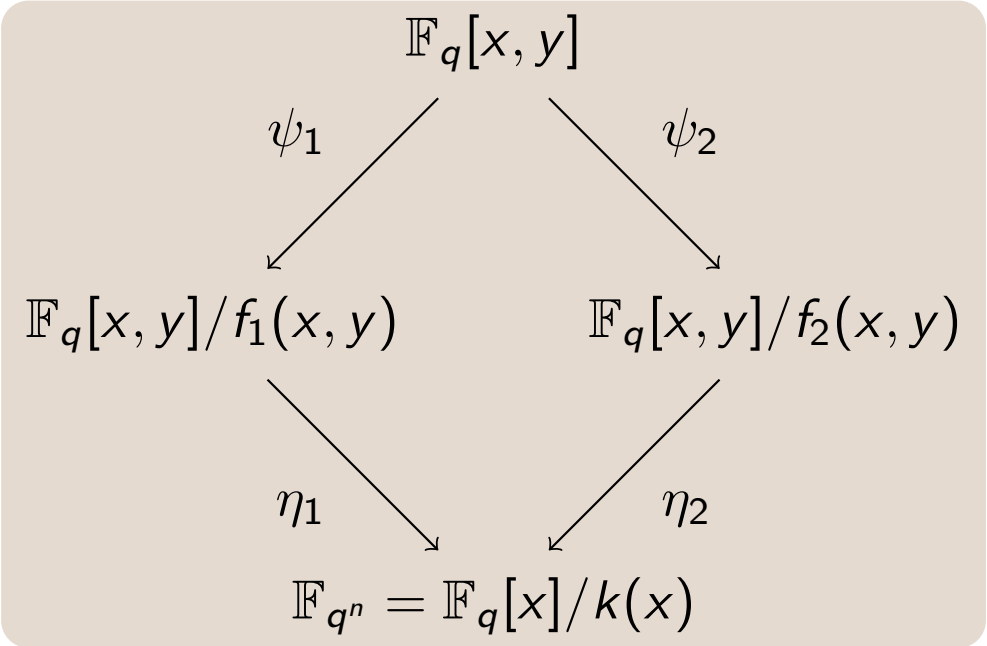


Check smoothness via $\mathrm{N}_{F_i|\mathbb{F}_q(x)}(\psi_i(\phi)) = \mathrm{Res}_y(\phi, f_i)$:
$\mathcal{F}_B = \{\gamma \in \mathbb{F}_q[x,y]/f_i \mid \deg \mathrm{N}_{F_i|\mathbb{F}_q(x)}(\gamma) \leq B\}$

Relation search in FFS

Applicability:
Fields $\mathbb{F}_{q^n}$ of small characteristic $q < L_{q^n}(1/3)$

Choose $\phi = a(x)y + b(x)$, deal with ideals.

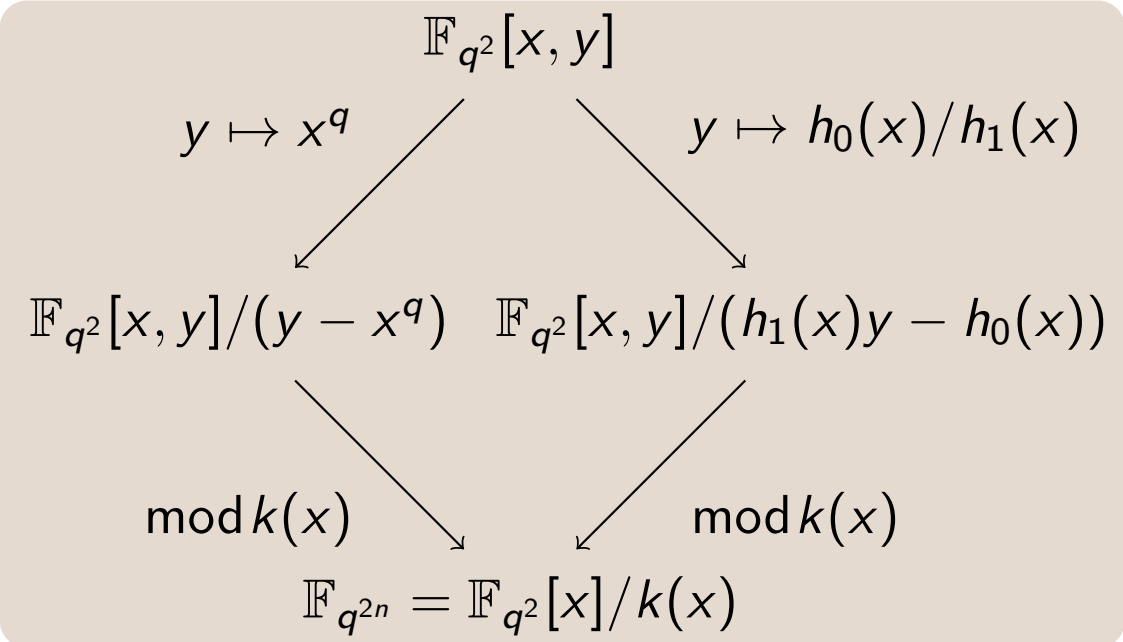


Check smoothness via $\mathrm{N}_{F_i|\mathbb{F}_q(x)}(\psi_i(\phi)) = \mathrm{Res}_y(\phi, f_i)$:
$\mathcal{F}_B = \{\gamma \in \mathbb{F}_q[x,y]/f_i \mid \deg \mathrm{N}_{F_i|\mathbb{F}_q(x)}(\gamma) \leq B\}$

Complexity: Choose B s.t. $|\mathcal{F}_B| = L(1/3)$, then relation search has complexity $L(1/3)$.

French relation search

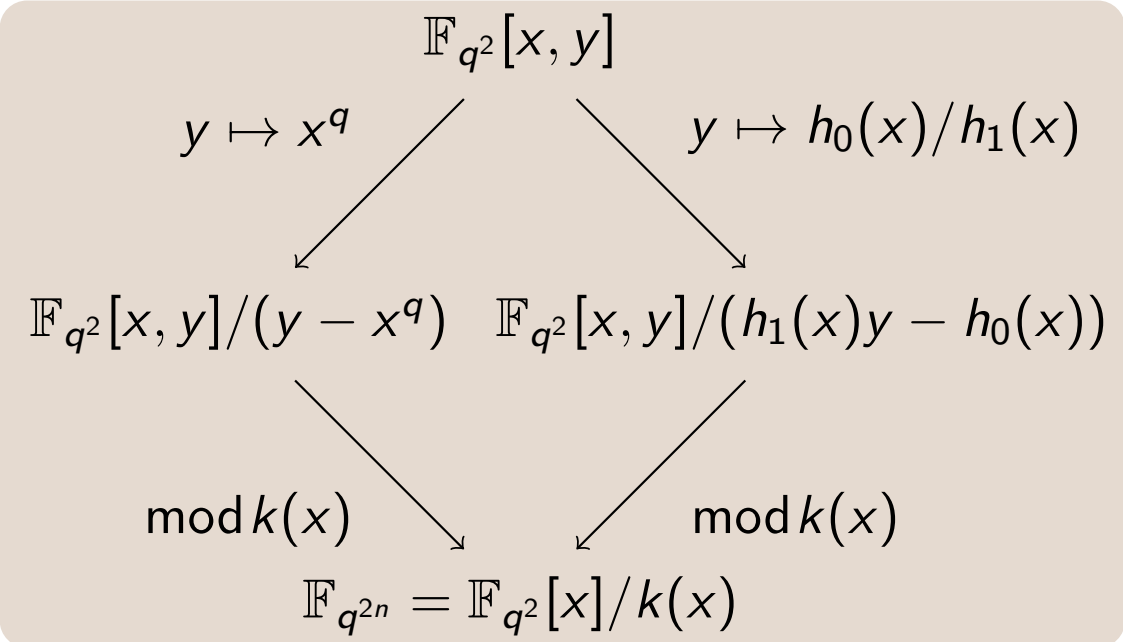
Applicability:
Fields $\mathbb{F}_{q^{2n}}$,
where $q \approx n$



French relation search

Applicability:
Fields $\mathbb{F}_{q^{2n}}$,
where $q \approx n$

Set $B = 1$.

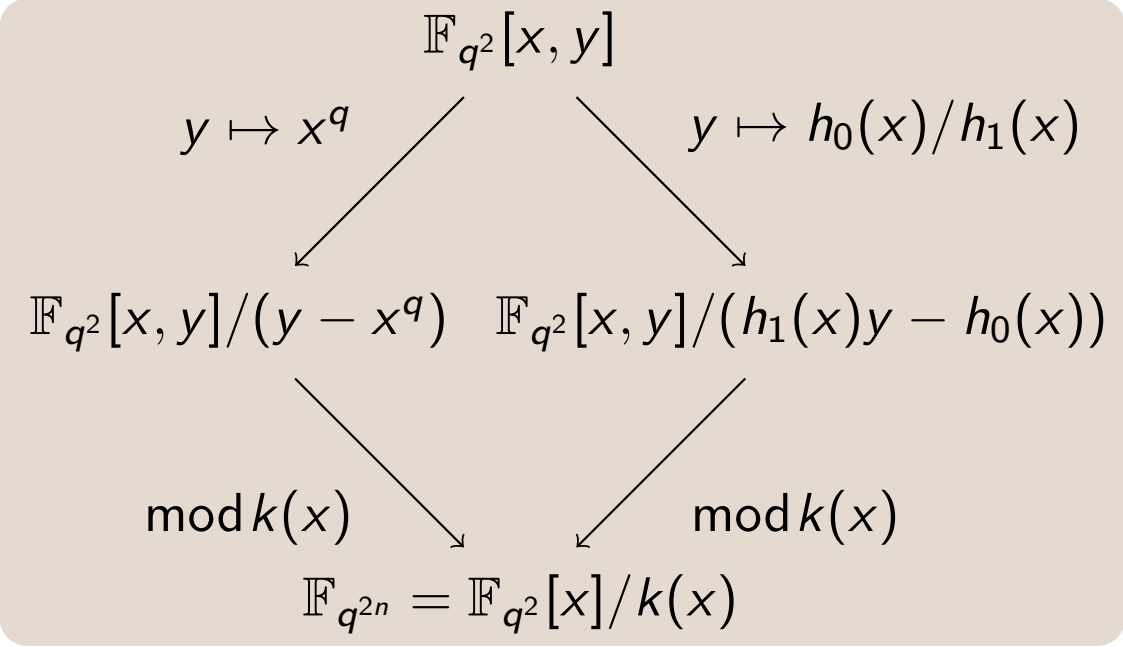


For $(a,b,c,d) \in \mathbb{F}_{q^2}^4 \setminus \mathbb{F}_q^4$,
choose $\phi = (a^q y + b^q)(cx+d) - (ax+b)(c^q y + d^q)$
then $\psi_1(\phi) = (cx+d)\prod_{\alpha \in \mathbb{F}_q}((a-\alpha c)x + (b - \alpha d))$
and $\psi_2(\phi)$ has small constant degree.

French relation search

Applicability:
Fields $\mathbb{F}_{q^{2n}}$,
where $q \approx n$

Set $B = 1$.



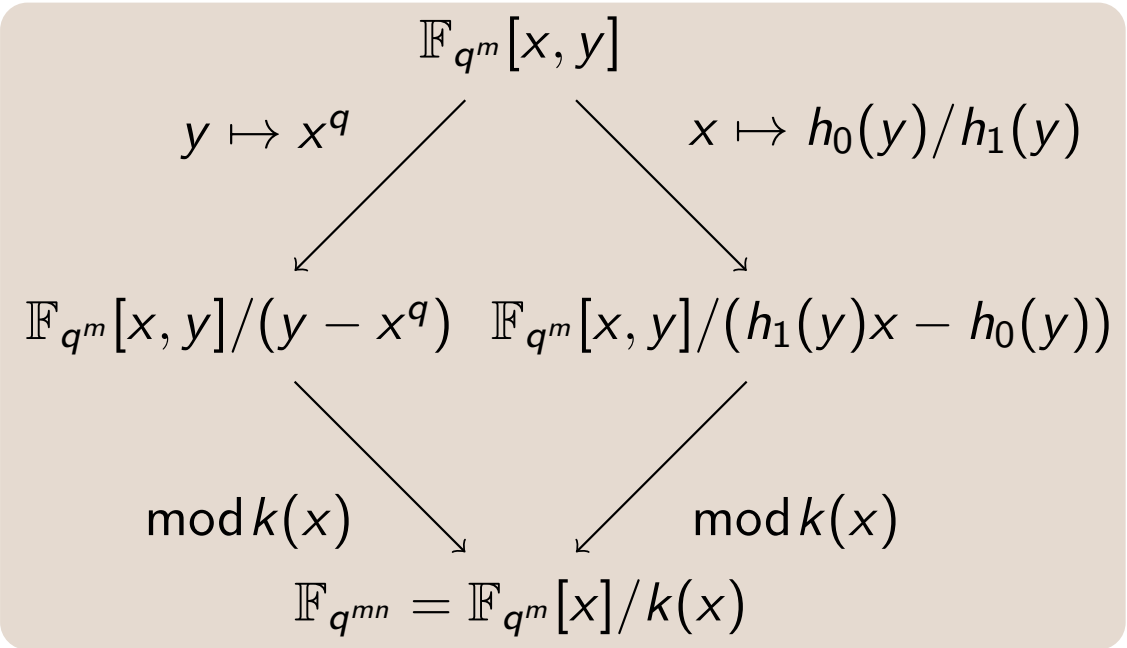
For $(a,b,c,d) \in \mathbb{F}_{q^2}^4 \setminus \mathbb{F}_q^4$,
choose $\phi = (a^q y + b^q)(cx+d) - (ax+b)(c^q y + d^q)$
then $\psi_1(\phi) = (cx+d)\prod_{\alpha \in \mathbb{F}_q}((a-\alpha c)x + (b - \alpha d))$
and $\psi_2(\phi)$ has small constant degree.

Complexity: $O(q^2)$, which is polynomial in q^{2n}.

Irish relation search

Applicability:
Fields $\mathbb{F}_{q^{mn}}$,
where $q \approx n$,
small m

Set $B = 1$.



For $(a, b, c, d) \in \mathbb{F}_{q^m}^4$,
choose $\phi = xy + ay + bx + c$
then $\psi_1(\phi) = x^{q+1} + bx^q + cx + d$ has splitting prob. q^{-3} and $\psi_2(\phi)$ has small constant degree.

Complexity: $O(q^m)$, which is polynomial in q^{mn}.

Relation search in $\mathcal{C}_{ab}$ curves

- $\mathcal{F}_B = \{D \in \mathrm{Div}_{\mathcal{C}_{ab}}(\mathbb{F}_q) | D \text{ prime}, \ \deg(D) \leq B\}$
- Search for polynomial $\phi \in \mathbb{F}_q(\mathcal{C}_{ab})$ such that $\mathrm{div}(\phi)$ is B-smooth, or equivalently, $\mathrm{N}_{\mathbb{F}_q(\mathcal{C}_{ab})|\mathbb{F}_q(x)}(\phi) = \mathrm{Res}_y(\phi, y^a + x^b + f(x,y))$

Relation search in $\mathcal{C}_{ab}$ curves

- $\mathcal{F}_B = \{D \in \mathrm{Div}_{\mathcal{C}_{ab}}(\mathbb{F}_q) | D \text{ prime}, \ \deg(D) \leq B\}$
- Search for polynomial $\phi \in \mathbb{F}_q(\mathcal{C}_{ab})$ such that $\mathrm{div}(\phi)$ is B-smooth, or equivalently, $\mathrm{N}_{\mathbb{F}_q(\mathcal{C}_{ab})|\mathbb{F}_q(x)}(\phi) = \mathrm{Res}_y(\phi, y^a + x^b + f(x,y))$
- Then $\mathrm{div}(\phi) = \sum \nu_i P_i$ with $P_i \in \mathcal{F}_B$ and $\sum \nu_i [P_i] = 0$ gives a relation in $\mathrm{Cl}_{\mathcal{C}_{ab}}$

Relation search in $\mathcal{C}_{ab}$ curves

- $\mathcal{F}_B = \{D \in \mathrm{Div}_{\mathcal{C}_{ab}}(\mathbb{F}_q) | D \text{ prime}, \deg(D) \leq B\}$
- Search for polynomial $\phi \in \mathbb{F}_q(\mathcal{C}_{ab})$ such that $\mathrm{div}(\phi)$ is B-smooth, or equivalently, $\mathrm{N}_{\mathbb{F}_q(\mathcal{C}_{ab})|\mathbb{F}_q(x)}(\phi) = \mathrm{Res}_y(\phi, y^a + x^b + f(x,y))$
- Then $\mathrm{div}(\phi) = \sum \nu_i P_i$ with $P_i \in \mathcal{F}_B$ and $\sum \nu_i [P_i] = 0$ gives a relation in $\mathrm{Cl}_{\mathcal{C}_{ab}}$
- Choose B s.t. $|\mathcal{F}_B| = L(1/3)$
- Overall complexity: $L(1/3)$, where $q, g \to \infty$, due to assumptions on degrees in curve eq'n
- Only one function field involved: $\mathbb{F}_q(\mathcal{C}_{ab})$

Application to curves?

Since we cannot choose the function field, study whether there are curves for which there exist principal divisors with higher-than-expected splitting probability.

Application to curves?

Since we cannot choose the function field, study whether there are curves for which there exist principal divisors with higher-than-expected splitting probability.

The curves used in the $L(1/4)$ and quasi-poly algorithms are not interesting:

$$y - x^q \quad \text{and} \quad h_1(x)y - h_0(x)$$

both have genus 0.

Application to curves?

Since we cannot choose the function field, study whether there are curves for which there exist principal divisors with higher-than-expected splitting probability.

The curves used in the $L(1/4)$ and quasi-poly algorithms are not interesting:

$$y - x^q \quad \text{and} \quad h_1(x)y - h_0(x)$$

both have genus 0.

Want curves of genus about q, s.t. $|\mathrm{Cl}_{\mathcal{C}}(\mathbb{F}_q)| \approx q^q$.

Higher splitting probability in curves?

Write $poly(q) = q^{\Theta(1)}$.

Question: Let $\mathcal{C}$ be a projective curve defined over $\mathbb{F}_q$ of degree $poly(q)$. Under which conditions is the number of lines defining divisors which split completely unexpectedly large, say of the form $poly(q)$?

Diem's theorem

Theorem (Diem)

Let $\mathcal{C}$ be a projective curve of genus at least one, given by a **reflexive** *plane model of degree $d \geq 3$. Then the number of divisors on $\mathcal{C}$ given by lines over $\mathbb{F}_q$ which split completely into distinct points over $\mathbb{F}_q$ is in $\frac{1}{d!}q^2 + O(q^{3/2})$.*

This is what we expect heuristically!

Diem's theorem

Theorem (Diem)

Let $\mathcal{C}$ be a projective curve of genus at least one, given by a **reflexive** *plane model of degree $d \geq 3$. Then the number of divisors on $\mathcal{C}$ given by lines over $\mathbb{F}_q$ which split completely into distinct points over $\mathbb{F}_q$ is in $\frac{1}{d!}q^2 + O(q^{3/2})$.*

This is what we expect heuristically!
Conclusion for **fixed** degree: Only non-reflexive curves may have principal divisors coming from linear functions with higher-than-expected splitting probability.

Diem's theorem

Theorem (Diem)

Let $\mathcal{C}$ be a projective curve of genus at least one, given by a **reflexive** *plane model of degree $d \geq 3$. Then the number of divisors on $\mathcal{C}$ given by lines over $\mathbb{F}_q$ which split completely into distinct points over $\mathbb{F}_q$ is in $\frac{1}{d!}q^2 + O(q^{3/2})$.*

This is what we expect heuristically!
Conclusion for **fixed** degree: Only non-reflexive curves may have principal divisors coming from linear functions with higher-than-expected splitting probability.
Proof: Cebotarev density theorem

Non-reflexive and Hermitian curves

Theorem (Ballico–Hefez)

Any non-reflexive plane curve of degree $d = q + 1 \geq 4$, *for* q *a power of the characteristic of the field of definition, and of genus at least one is projectively equivalent to the curve*

$$x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

This is the Hermitian curve. Hermitian curves are supersingular. The DLP in supersingular curves is already known to be weak.

A more general approach

Question: Let $\mathcal{C}$ be a projective curve defined over $\mathbb{F}_q$ of degree $poly(q)$. Under which conditions is the number of lines defining divisors which split completely unexpectedly large, say of the form $poly(q)$?

Generalized question: Let $\mathcal{C}$ be a projective curve defined over $\mathbb{F}_q$ of degree $poly(q)$. Under which conditions is the number of polynomial functions of degree $O(1)$ defining divisors which split into factors of degree $O(1)$ unexpectedly large, say of the form $poly(q)$?

An observation and a question

Observation

Let $(\mathcal{C}_q)_q$ be a family of projective curves defined over $\mathbb{F}_q$ of genus poly(q), given by an equation of degree poly(q). Assume that there exist poly(q) monic, irreducible polynomial functions $\phi \in \mathbb{F}_{q^2}(\mathcal{C}_q)$ of degree $O(1)$ such that $\mathrm{div}(\phi)$ *is $O(1)$-smooth. Then the curves $\mathcal{C}_q$ are quite "special".*

Question

In which way are they "special"?

One wild guess: "special" $=$ $\mathrm{Jac}_{\mathcal{C}_q}$ is isogenous to a product of elliptic curves, for large enough q

Experiments

We want:

Curve $\mathcal{C} : C(x, y)$

- genus about q, so that $|\mathrm{Cl}_{\mathcal{C}}(\mathbb{F}_q)| \approx q^q$
- DLP not known to be weak for other reasons

and polynomial function $\phi \in \mathbb{F}_{q^m}(\mathcal{C})$, for small m

- irreducible
- involving both x and y

such that $\mathrm{Res}_y(\phi, C)$ is $O(1)$-smooth.

French strategy

Find a curve together with one smooth function, then amplify using homographies.

Example: $y - x^q$

For $\phi = y - x$, have

$$\mathrm{Res}_y(\phi, y - x^q) = x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

French strategy

Find a curve together with one smooth function, then amplify using homographies.

Example: $y - x^q$

For $\phi = y - x$, have

$$\mathrm{Res}_y(\phi, y - x^q) = x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

Apply homography $x \mapsto \frac{ax+b}{cx+d}$, $\quad a, b, c, d \in \mathbb{F}_{q^2}$:

$$(ax+b)^q(cx+d) - (ax+b)(cx+d)^q = (cx+d) \prod_{\alpha \in \mathbb{F}_q} ((ax+b) - \alpha(cx+d))$$

French strategy

Find a curve together with one smooth function, then amplify using homographies.

Example: $y - x^q$

For $\phi = y - x$, have

$$\mathrm{Res}_y(\phi, y - x^q) = x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

Apply homography $x \mapsto \frac{ax+b}{cx+d}$, $\quad a, b, c, d \in \mathbb{F}_{q^2}$:

$$(ax+b)^q(cx+d) - (ax+b)(cx+d)^q = (cx+d) \prod_{\alpha \in \mathbb{F}_q} ((ax+b) - \alpha(cx+d))$$

Set $\phi^{\mathrm{hom}} = (a^q y + b^q)(cx + d) - (ax + b)(c^q y + d^q)$

Then $\mathrm{Res}_y(\phi^{\mathrm{hom}}, y - x^q) = (cx+d) \prod_{\alpha \in \mathbb{F}_q} ((a - \alpha c)x + (b - \alpha d))$

French strategy

Find a curve together with one smooth function, then amplify using homographies.

Example: $y - x^q$

For $\phi = y - x$, have

$$\mathrm{Res}_y(\phi, y - x^q) = x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

Apply homography $x \mapsto \frac{ax+b}{cx+d}$, $\quad a, b, c, d \in \mathbb{F}_{q^2}$:

$$(ax+b)^q(cx+d) - (ax+b)(cx+d)^q = (cx+d) \prod_{\alpha \in \mathbb{F}_q} ((ax+b) - \alpha(cx+d))$$

Set $\phi^{\mathrm{hom}} = (a^q y + b^q)(cx + d) - (ax + b)(c^q y + d^q)$

Then $\mathrm{Res}_y(\phi^{\mathrm{hom}}, y - x^q) = (cx+d) \prod_{\alpha \in \mathbb{F}_q} ((a - \alpha c)x + (b - \alpha d))$

Difficulty: compatibility curve equation, resultant

Irish strategy

Find a curve together with a family of polynomial functions such that the resultant has higher-than-expected splitting probability.

Example: $y - x^q$

For $\phi = xy + ay + bx + c, \quad a, b, c, d \in \mathbb{F}_{q^m}$ (m small), have

$$\mathrm{Res}_y(\phi, y - x^q) = x^{q+1} + ax^q + bx + c$$

which splits into linear factors with probability q^{-3} (Bluher).

Irish strategy

Find a curve together with a family of polynomial functions such that the resultant has higher-than-expected splitting probability.

Example: $y - x^q$

For $\phi = xy + ay + bx + c, \quad a, b, c, d \in \mathbb{F}_{q^m}$ (m small), have

$$\mathrm{Res}_y(\phi, y - x^q) = x^{q+1} + ax^q + bx + c$$

which splits into linear factors with probability q^{-3} (Bluher).

Difficulty: don't know many families of polynomials with high splitting probability

Example: $y^2 - x^{q+1} + 2x + 1$

hyperelliptic, non-supersingular, genus $(q-1)/2$

For $\phi = y - x + 1$:

$$\mathrm{Res}_y(\phi, y^2 - x^{q+1} + 2x + 1) = x(x^q - x)$$

Example: $y^2 - x^{q+1} + 2x + 1$

hyperelliptic, non-supersingular, genus $(q-1)/2$

For $\phi = y - x + 1$:

$$\mathrm{Res}_y(\phi, y^2 - x^{q+1} + 2x + 1) = x(x^q - x)$$

Exhaustive search ($q = 7, 11, 19, 23$): $\phi = y - x + 1$ and $y + x - 1$ are the only functions over $\mathbb{F}_{q^2}$ of degree 1 in x, y such that the resultant splits into linear factors and produces a non-trivial relation.

Example: $y^2 - x^{q+1} + 2x + 1$

hyperelliptic, non-supersingular, genus $(q-1)/2$

For $\phi = y - x + 1$:

$$\mathrm{Res}_y(\phi, y^2 - x^{q+1} + 2x + 1) = x(x^q - x)$$

Exhaustive search ($q = 7, 11, 19, 23$): $\phi = y - x + 1$ and $y + x - 1$ are the only functions over $\mathbb{F}_{q^2}$ of degree 1 in x, y such that the resultant splits into linear factors and produces a non-trivial relation.

Moreover, splitting properties depend on q.

Example: $y^2 - x^{q-1} + 1$

hyperelliptic, non-supersingular, genus $(q-3)/2$

For $\phi = xy$:

$$\mathrm{Res}_y(\phi, y^2 - x^{q-1} + 1) = x^q - x$$

Example: $y^2 - x^{q-1} + 1$

hyperelliptic, non-supersingular, genus $(q-3)/2$

For $\phi = xy$:

$$\mathrm{Res}_y(\phi, y^2 - x^{q-1} + 1) = x^q - x$$

Can show: $\phi = xy$ is the only function of shape $\phi = \phi_1(x)y + \phi_0(x)$ over $\mathbb{F}_{q^2}$ with $\deg \phi_i \leq 1$ such that the resultant is $x^q - x$ or a small multiple thereof. This produces only trivial relations.

Example: $y^2 - x^{q-1} + 1$

hyperelliptic, non-supersingular, genus $(q-3)/2$

For $\phi = xy$:

$$\mathrm{Res}_y(\phi, y^2 - x^{q-1} + 1) = x^q - x$$

Can show: $\phi = xy$ is the only function of shape $\phi = \phi_1(x)y + \phi_0(x)$ over $\mathbb{F}_{q^2}$ with $\deg \phi_i \leq 1$ such that the resultant is $x^q - x$ or a small multiple thereof. This produces only trivial relations.

Allowing $\deg \phi_i \leq 2$ we get $\phi = (x^2 + ax)y$ for any a, which also gives only trivial relations.

Example: $y^2 - x^{q-2} + x + 1$

hyperelliptic, non-supersingular, genus $(q-3)/2$

Can show: there is no $\phi = \phi_1(x)y + \phi_0(x)$ over $\mathbb{F}_{q^2}$ with $\deg \phi_i \leq 2$ such that the resultant is $x^q - x$ or a small multiple thereof.

Example: $y^{q+1} + x^{q+1}y - 1$

non-supersingular, genus $q(q+1)/2$

Exhaustive search ($q = 5, 7, 11, 13, 17, 19, 23$): there is no irreducible polynomial function $\phi = xy + ay + bx + c \in \mathbb{F}_{q^2}[x, y]$ such that the resultant splits completely into linear factors.

French and Irish strategy

Polynomials $(ax+b)^q(cx+d) - (ax+b)(cx+d)^q$ are of the form $Ax^{q+1} + Bx^q + Cx + D$, which have higher-than-expected splitting probability.

French and Irish strategy

Polynomials $(ax+b)^q(cx+d) - (ax+b)(cx+d)^q$ are of the form $Ax^{q+1} + Bx^q + Cx + D$, which have higher-than-expected splitting probability.

Polynomials
$(ax^2+bx+c)^q(dx^2+ex+f) - (ax^2+bx+c)(dx^2+ex+f)^q$
are of the form
$Ax^{2q+2} + Bx^{2q+1} + Cx^{2q} + Dx^{q+2} + Ex^{q+1} + Fx^q + Gx^2 + Hx + I$,
which might have higher-than-expected probability to be 2-smooth?

Heuristic arguments and experiments suggest that yes (q^{-7}).

One positive example (only)

Hermitian curves

$$\mathcal{C} : x^{q+1} + y^{q+1} + 1 = 0$$

which are supersingular, genus $g = q(q-1)/2$.

Set $\phi = xy + ay + bx^2 + cx + d \in \mathbb{F}_{q^2}[x, y]$. Then $\mathrm{Res}_y(\phi, x^{q+1} + y^{q+1} + 1)$ has shape
$Ax^{2q+2} + Bx^{2q+1} + Cx^{2q} + Dx^{q+2} + Ex^{q+1} + Fx^q + Gx^2 + Hx + I$.

Experiments show that the resultant is 2-smooth with probability at least q^{-2}, which is much more than expected.

Summary

- Some obvious ideas of adapting the FFS improvements to curves do not seem to work
- Curves which permit functions whose principal divisors have higher-than-expected splitting probability seem to be very special
- If we could prove such a statement for some precise meaning of "special", this would show that a straightforward application of the ideas of the new algorithms to curves is not possible
- Of course, this still does not prove that there is no better algorithm for curves

More things to try

- Conduct experiments with larger constants, more curves of different degrees
- Identify families of polynomials with higher splitting probability
- Automorphisms for amplification
- Curves with many rational points
- Descent (individual logarithm phase)
- ...

Index calculus in elliptic curves

For elliptic curves over prime fields, we do not know a good way of choosing the factor base. Best attacks are generic algorithms.

Index calculus in elliptic curves

For elliptic curves over prime fields, we do not know a good way of choosing the factor base. Best attacks are generic algorithms.

For elliptic curves $\mathcal{E}$ over extension fields $\mathbb{F}_{q^n}$:

- Set $\mathcal{F} = \{(x, y) \in \mathcal{E}(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\}$
- $|\mathcal{F}| \approx q$
- Describe relations via polynomial systems
- Solve over $\mathbb{F}_q$ to find relations
- Complexity $\tilde{O}(q^{2-2/n})$, i.e. still exponential
- Don't know how to choose factor base of sub-exponential size

A remark of Galbraith and Gaudry

Central equation of quasi-polynomial attack:

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

Idea: Pull back the above equation:

$$\mathrm{div}(x^q - x) = \sum_{P \in \mathcal{E}(\overline{\mathbb{F}}_q), x_P \in \mathbb{F}_q} P \quad - 2q\mathcal{O}$$

Problems: RHS gives a trivial relation, $\mathrm{Aut}(\mathcal{E})$ is very small in comparison to $\mathrm{Aut}(\mathbb{P}^1)$.

A theoretical result of Diem

There exists a sequence of prime powers $Q_i = q_i^{n_i}$ with $n_i \approx \sqrt{\log(q_i)}$ such that the ECDLP in $E(\mathbb{F}_{Q_i})$ can be solved in sub-exponential time $L_{Q_i}(2/3)$ for any elliptic curve E over $\mathbb{F}_{Q_i}$.

Small genus hyperelliptic curves

Let $\mathcal{H}$ be a hyperelliptic curve over $\mathbb{F}_{q^n}$, then $|G| = |\mathrm{Cl}_{\mathcal{H}}(\mathbb{F}_{q^n})| \approx q^{ng}$

Index calculus: $\tilde{O}(q^{2-2/ng})$
Generic attacks: $O(q^{ng/2})$

The larger ng, the more freedom to choose a factor base, but index calculus is still exponential for small n, g.

Index calculus complexities

group	complexity
$\mathcal{E}, \mathcal{H}/\mathbb{F}_p, g = 1, 2$	exponential, same as generic
$\mathcal{E}, \mathcal{H}/\mathbb{F}_{q^n}, g = 1, 2$	exponential, better than generic
$\mathcal{H}, g \geq 3$ small	exponential, better than generic
$\mathcal{C}, g$ large	sub-exponential $L(1/3)$
$\mathbb{F}_q$, large characteristic	sub-exponential $L(1/3)$
$\mathbb{F}_q$, small characteristic	quasi-polynomial

$\mathcal{E}$ = elliptic curve
$\mathcal{H}$ = hyperelliptic curve
$\mathcal{C} = \mathcal{C}_{ab}$ curve
g = genus

Index calculus complexities

group	complexity
$\mathcal{E}, \mathcal{H}/\mathbb{F}_p, g = 1, 2$	exponential, same as generic
$\mathcal{E}, \mathcal{H}/\mathbb{F}_{q^n}, g = 1, 2$	exponential, better than generic
$\mathcal{H}, g \geq 3$ small	exponential, better than generic
$\mathcal{C}, g$ large	sub-exponential $L(1/3)$
$\mathbb{F}_q$, large characteristic	sub-exponential $L(1/3)$
$\mathbb{F}_q$, small characteristic	quasi-polynomial

$\mathcal{E}$ = elliptic curve
$\mathcal{H}$ = hyperelliptic curve
$\mathcal{C} = \mathcal{C}_{ab}$ curve
g = genus