2nd MAGC Workshop

November 17–19, 2000

Building robust (hyper)elliptic curve cryptosystems

F. Morain

`http://www.lix.polytechnique.fr/Labo/Francois.Morain/`

Slide 1

I. Introduction and motivations

Goal: build an effective group of cryptographic strength, resisting all known attacks.

Dream: find **Nechaev** groups G, in which the best attack will be $O(\sqrt{\#G})$ (existence?)

Best groups so far: hyperelliptic curves of genus g, with size $\approx q^g$ over some finite field $\mathbb{F}_q$. Typical size $q^g \approx 2^{160--200} \approx 10^{50--60}$.

- Miller, Koblitz (1986): elliptic curves are suggested for use, following the breakthrough of Lenstra in integer factorization (1985).
- Koblitz (1988): hyperelliptic cryptosystems.

In this series of talks:

- Put the emphasis on elliptic curves, but take a more general view from time to time; $g > 1$ is the **next case**; sometimes, hec's yield info on ec's.
- Consider **any base field**, with some preference for large prime fields, or $\mathbb{F}_{2^n}$; few places where it really matters.

Slide 2

General overview of the three lectures

I. Point counting algorithms: basic approaches.

II. Point counting algorithms: elaborate methods.

III. Discrete log algorithms.

Bibliography and links

- *A course in algorithmic algebraic number theory* (Cohen);
- *The arithmetic of elliptic curves* (Silverman);
- *Elliptic curve public key cryptosystems* (Menezes);
- *Elliptic curves in cryptography* (Blake, Seroussi, Smart);
- Lercier's thesis.
- *Algebraic aspects of cryptography* (Koblitz, appendix on hec by Menezes, Wu, Zuccherato).


```
www.lix.polytechnique.fr/Labo/
 {Francois.Morain,Pierrick.Gaudry,
  Mireille.Fouquet}
cristal.inria.fr/~harley/
```

Slide 3

2nd MAGC Workshop

November 17, 2000

I. Point counting algorithms: basic approaches

F. Morain

Slide 4

Plan

I. Elements of theory.

II. Generic methods.

III. Particular curves.

IV. Schoof's algorithm.

Slide 5

I. Elements of theory

Let C be a plane smooth projective curve of genus g with equation $F(X,Y)=0$ with coefficients in $\mathbb{K}$, $\mathrm{char}(\mathbb{K})=p$.

Conic: (genus 0) $x^2+y^2=1$.

Elliptic curve: (genus 1) $y^2=x^3+x+1$.

Hyperelliptic curve: (genus g) $y^2=x^{2g+1}+\cdots$ (or in some cases $y^2=x^{2g+2}+\cdots$).

Rem. To simplify things, we assume that C is "at most" hyperelliptic (no C_{ab} or $X_0(N)$).

Def. $C(\mathbb{K})=\{P=(x,y)\in\mathbb{K}^2, F(x,y)=0\}$.

Thm. When $g\leq 1$, there is a group law on $C(\mathbb{K})$. When $g>1$, there is a group law on the *jacobian* of the curve.

Slide 6

Elliptic curves

$$E: Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6$$

$$b_2=a_1^2+4a_2, b_4=2a_4+a_1a_3, b_6=a_3^2+4a_6,$$
$$b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2,$$
$$c_4=b_2^2-24b_4, c_6=b_2^3+36b_2b_4-216b_6,$$

$$\Delta=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6\neq 0$$
$$j(E)=\frac{c_4^3}{\Delta}$$

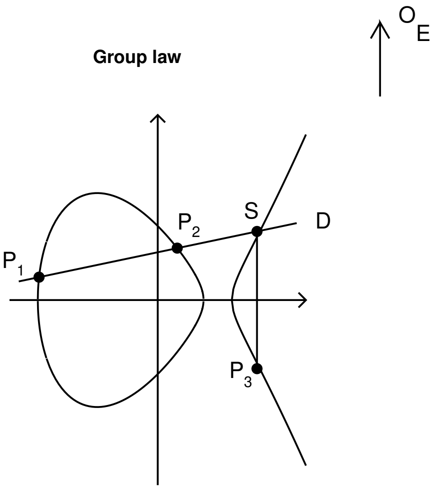
When $p=2$**:** $Y^2+XY=X^3+a_2X^2+a_6$, $j=1/a_6$.

When $p>3$**:** $Y^2=X^3+AX+B$, $\Delta=-16(4A^3+27B^2)$.

$E(\mathbb{K})$, tangent-and-chord ($\oplus$, O_E), multiplication by n noted $[n]P$.

Slide 7

Group law



$$P_3=P_1\oplus P_2$$
$$[k]P=\underbrace{P\oplus\cdots\oplus P}_{k\text{ times}}$$

Slide 8

Hyperelliptic curves

$$y^2 + h(x)y = f(x) = x^{2g+1} + \cdots$$

Representing $\mathrm{Jac}(C)$: (Mumford)

An element (= a divisor) of $\mathrm{Jac}(C)$ is

$$D = < u(z), v(z) >, \deg(u) \leq g, \deg(v) < \deg(u),$$

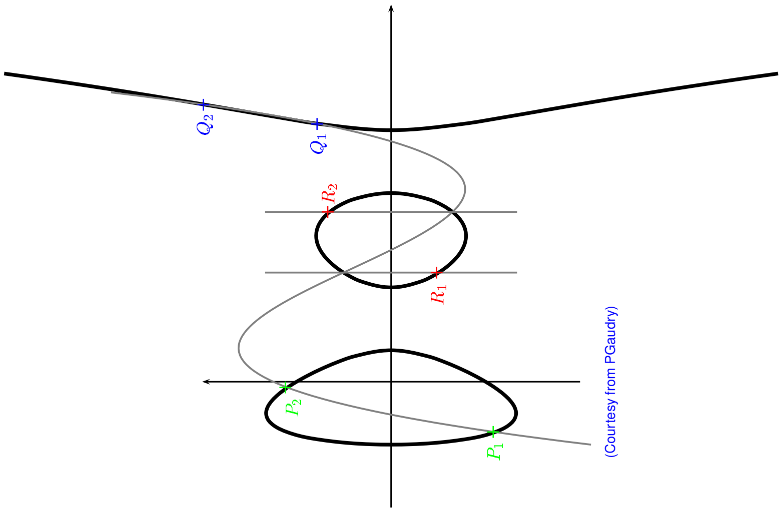
defined by (if $P_i = (x_i, y_i)$),

$$u(z) = \prod_{i=1}^{g} (z - x_i), \text{ and } v(x_i) = y_i, \ \forall i.$$

Rem. If $D = < u(z), v(z) >$, then $-D = < u(z), -v(z) >$.

Group law: Cantor's algorithm (or special formulae for fixed g *à la* Spallek, Harley, Nagao).

Slide 9



Slide 10

Cardinality

$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^n}$; $N_r = \#C(\mathbb{K}_r)$ where $[\mathbb{K}_r : \mathbb{K}] = r$:

$$Z(T) = \exp\left(\sum_{r \geq 1} N_r \frac{T^r}{r}\right).$$

Ex. $\mathbb{P}^1(\mathbb{F}_{q^r}) = \{(x_0, x_1) \neq (0,0) \in \mathbb{F}_{q^r}^2\}/\sim$.

$$\#\mathbb{P}^1(\mathbb{F}_{q^r}) = 1 + q^r$$

$$Z(T) = \frac{1}{(1-T)(1-qT)}.$$

Thm. (Weil) $Z(T) \in \mathbb{Q}[T]$

$$Z(T) = \frac{L(T)}{(1-T)(1-qT)}$$

(i) $L(T) = 1 + a_1 T + \cdots + q^g T^{2g}$, $a_i \in \mathbb{Z}$;

(ii) $a_{2g-i} = q^{g-i} a_i$ for $0 \leq i \leq g$;

(iii) if $L(T) = \prod(1 - \alpha_i T)$, then $\alpha_i \alpha_{g+i} = q$ and $|\alpha_i| = \sqrt{q}$.

Thm. $\#\mathrm{Jac}(C) = L(1)$.

Coro. $|\#C - (q+1)| \leq 2g\sqrt{q}$;
$(\sqrt{q} - 1)^{2g} \leq \#\mathrm{Jac}(C) \leq (\sqrt{q} + 1)^{2g}$.

Slide 11

ℓ-torsion

Def. $\mathrm{Jac}[n] = \{P \in \mathrm{Jac}(\overline{\mathbb{K}}), [n]P = O_J\}$.

Thm. If $(n, \mathrm{char}(\mathbb{K})) = 1, \mathrm{Jac}[n] \sim (\mathbb{Z}/n\mathbb{Z})^{2g}$;
$\mathrm{Jac}[p^r] = (\mathbb{Z}/p\mathbb{Z}^r)^k, 0 \leq k \leq g$.

Rem. In general $k = g$ (ordinary curves); when $g = 1$, the case $k = 0$ corresponds to *supersingular* curves.

Coro. $\mathrm{Jac}(C)/\mathbb{K}$ is at most $C_1 \times C_2 \times \cdots \times C_{2g}$.

Division polynomials for elliptic curves:

Take $E : y^2 = x^3 + Ax + B$:

$$[n](X, Y) = \left(\frac{\phi_n(X,Y)}{\psi_n(X,Y)^2}, \frac{\omega_n(X,Y)}{\psi_n(X,Y)^3}\right)$$

$$\phi_n = X\psi_n^2 - \psi_{n+1}\psi_{n-1}$$

$$4Y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$$

$$\phi_n, \psi_{2n+1}, \psi_{2n}/(2Y), \omega_{2n+1}/Y, \omega_{2n} \in \mathbb{Z}[A, B, X]$$

Rem. When $g > 1$, one can define analogous division polynomials (cf. Cantor).

Slide 12

$$f_n(X) = \begin{cases} \psi_n(X,Y) & \text{for } n \text{ odd} \\ \psi_n(X,Y)/(2Y) & \text{for } n \text{ even} \end{cases}$$

$$f_{-1} = -1, \quad f_0 = 0, \quad f_1 = 1, \quad f_2 = 1$$

$$f_3(X,Y) = 3X^4 + 6AX^2 + 12BX - A^2$$

$$f_4(X,Y) = X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3$$

$$f_{2n} = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2)$$

$$f_{2n+1} = \begin{cases} f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}(16Y^4) & \text{if } n \text{ is odd} \\ (16Y^4)f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1} & \text{otherwise.} \end{cases}$$

$$\deg(f_n(X)) = \begin{cases} (n^2-1)/2 & \text{if } n \text{ is odd} \\ (n^2-4)/2 & \text{otherwise.} \end{cases}$$

Thm. $P = (x, y)$ point of order ℓ in $E(\overline{\mathbb{K}})$ $\iff [2]P = O_E$ or $f_\ell(x) = 0$.

Rem. $f_3(X) = -A^2$ when $\mathrm{char}(\mathbb{K}) = 3$, so that all $Y^2 = X^3 + AX + B$ are supersingular in this case.

Slide 13

II. Generic methods

Input: a finite abelian group $(G, +)$ with $\#G \leq B$.

Output: $\#G$.

Enumeration: $O(\#G)$.

Use Lagrange's theorem: for random $x \in G$, find $\omega =$ order of x. Deduce from this the order of G (take care to small orders, group structure with SNF, etc.; see Cohen).

How to find ω:

- try increasing value of ω: $O(\omega) \leq O(B)$ (??).
- Shanks's *baby steps/giant steps method*: write $m = m_0 + m_1 b$ for some $b, 0 \leq m_0 < b$, $0 \leq m_1 \leq B/b$ and write

$$[m]x = 0 \iff [m_1]([-b]x) = [m_0]x.$$

1. **baby steps**: precompute $\mathcal{B} = \{[m_0]x, 0 \leq m_0 \leq b\}$;
2. **giant steps**: find all m_1 s.t. $[m_1]([-b]x) = [m_0]x$ for some m_0.

Slide 14

Cost: $b + B/b$ minimized with $b = \sqrt{B}$. Time and space are $O(\sqrt{B})$ group operations, **deterministic**.

Rem. membership must be tested very fast (hashing).

Rem. can be modified when $A \leq \#G \leq B$, yielding a method in $O(\sqrt{B-A})$.

• Using kangaroos (Stein-Teske, Gaudry-Harley): **probabilistic** method in $O(\sqrt{B-A})$ time and $O(1)$ space (see discrete logs in part III).

Slide 15

Application to elliptic curves

- **Enumeration:** find all $x \in \mathbb{F}_q$ s.t. $f(x)$ is a square.
- **Lagrange:** $[q+1]P = [\pm c]P$ for $0 \leq c \leq 2\sqrt{q}$.

  Rem. If $\mathrm{ord}(P)$ is large enough, then

  $$\#\{c \in [-2\sqrt{q}, 2\sqrt{q}], [q+1-c]P = O_E\} = 1$$

  and we can bypass the structure problem.
- **Kangaroos:** idem.
- **Shanks:**

  More precisely: $c = n_0 + n_1 W, 0 \leq n_0 < W$, $|n_1| \leq 2\sqrt{q}/W$. Write

  $$[q+1-n_0]P = [\pm n_1][W]P, 0 \leq n_1 \leq 2\sqrt{q}/W$$

  Cost: $W = \sqrt{2\sqrt{q}}$, so $O(2\sqrt{2\sqrt{q}})$.

Slide 16

Application to hyperelliptic curves

$$L(1) = 1 - s_1 + \cdots + (-1)^g s_g$$
$$+(-1)^{g+1} q s_{g-1} + \cdots - q^{g-1} s_1 + q^g,$$
$$|s_i| \leq \binom{2g}{i} q^{i/2}.$$

A) Enumeration

$g = 2$**:** compute $N_1(C)$ and $N_2(C)$ and deduce
$s_1 = q + 1 - N_1(C)$,
$s_2 = (s_1^2 + N_2(C) - (q^2 + 1))/2$.

$g = 3$**:** $s_3 = (s_1^3 - 3s_1 s_2 - N_3 + q^3 + 1)/3$.

Prop. Method in $O(q^g)$.

B) Lagrange

Hasse-Weil gives $w = (\sqrt{q}+1)^{2g} - (\sqrt{q}-1)^{2g} = \mathbf{4gq^{g-1/2}} + O(q^{g-1})$ (for fixed g, $q \to +\infty$).

Prop. Method in $O(q^{(2g-1)/2})$ (for fixed g).

Slide 17

C) Shanks/Kangaroos

Prop. Method in $O(q^{(2g-1)/4})$ (for fixed g).

Using partial information

Prop. (Elkies) If the $k-1$ first s_i's are known, then

$$w' = 2\binom{2g}{k} q^{g-k/2} + O(q^{g-(k+1)/2})$$

and with more work

$$w'' = \frac{4g}{k} q^{g-k/2} + O(q^{g-(k+1)/2}).$$

Cost: $O(q^{k-1}) + O(q^{(2g-k)/4})$ leading to $k = (2g+4)/5$ and $O(q^{(2g-1)/5})$.

Ex. $g = 3$ leads to a $O(q)$ method by computing s_1 instead of $O(q^{5/4})$.

Stein-Teske-Williams: use truncated Euler product of the L-function to approximate $L(1)$, get same type of bound $O(q^{\lfloor (2g-1)/5 \rceil})$. Record (1999): $q = 10^8 + 7$, $g = 3$, $\#\mathrm{Jac} \approx 10^{24}$ in 10 hours on a Pentium Pro/200 with SIMATH.

Slide 18

III. Particular curves

A) Supersingular curves

Supersingular elliptic curves: E s.t. $\#E = q + 1 - c, p \mid c$ (not every c, all is known).

For instance: when $n = 2m+1, q = 2^n$

E	c_n
$Y^2 + Y = X^3$	0
$Y^2 + Y = X^3 + X$	$-(2/n)\sqrt{2q}$
$Y^2 + Y = X^3 + X + 1$	$(2/n)\sqrt{2q}$

(See A. Menezes and S. Vanstone, *Utilitas Math.*, 38:135–153, 1990)

Pb: subject to the MOV reduction (see also Frey, Rück).

$g > 1$**:** can be generalized, but reductions still apply (see also Galbraith for security evaluation).

B) Weil-Koblitz

Build curves over $\mathbb{F}_q$ for q small and use $\mathrm{Jac}(C)/\mathbb{F}_{q^k}$.

Pb: ECDL might be a little easier.

Slide 19

C) CM curves

(complex multiplication)

$g = 1$**:**

Thm. (Katre) If $p = x^2 + 4y^2$ with $x \equiv 1 \bmod 4$ and $a \not\equiv 0 \bmod p$, then $E : Y^2 = X^3 + aX$ has cardinality

$$p+1-\begin{cases} 2x & \text{if } (a/p)_4 = 1, \\ -2x & \text{if } (a/p)_4 = -1, \\ -4y & \text{otherwise with } y \text{ s.t. } 2y(a/p)_4 = x. \end{cases}$$

There are 13 cases of curves defined over $\mathbb{Q}$ having such properties; in general, $4p = A^2 + DB^2$, $\#E = p + 1 - A$: basis for primality proving with elliptic curves (ECPP, Atkin, M.).

$g > 1$**:**

Spallek, Weng ($g = 2$); Buhler-Koblitz; Duursma-Sakurai; Chao, Matsuda, Nakamura, Tsujii.

Pb: too much structure?

D) Weil descent

Start from ec's to build hec's (Smart *et al.*).

Slide 20

IV. Schoof's algorithm

The Frobenius endomorphism

Ordinary:

$$\begin{array}{rccc} \varphi: & \overline{\mathbb{K}} & \to & \overline{\mathbb{K}} \\ & x & \mapsto & x^q \end{array}$$

Extension to C and $\mathrm{Jac}(C)$:

$$\begin{array}{rccc} \varphi: & C(\overline{\mathbb{K}}) & \to & C(\overline{\mathbb{K}}) \\ & (X, Y) & \mapsto & (X^q, Y^q) \end{array}$$

Fundamental thm. The minimal polynomial $\chi(T)$ of φ is the reciprocal of $L(T)$. Moreover $\#\mathrm{Jac}(C)/\mathbb{F}_q = \chi(1)$.

Consequence: computing $\#\mathrm{Jac}(C)/\mathbb{F}_q$ boils down to computing $\chi(T)$.

Slide 21

$g = 1$: for E with $\chi(T) = T^2 - cT + q$, $|c| \leq 2\sqrt{q}$.

φ restricted to $E[\ell]$ satisfies:

$$\varphi^2 - c\varphi + q \equiv 0 \bmod \ell$$

so we can find $c_\ell \equiv c \bmod \ell$ such that

$$(X^{q^2}, Y^{q^2}) \oplus [q](X, Y) = [c_\ell](X^q, Y^q)$$

in $\mathbb{K}[X, Y]/(E, f_\ell(X))$ and use CRT once $\prod \ell > 4\sqrt{q}$. Yields a $O(\log^8 q)$ **deterministic algorithm**.

Pb. $\deg(f_\ell) = O(\ell^2)$.

$g > 1$: general algorithm by Pila (1990), but impossible to implement; Kampkötter (1991) for any hyperelliptic, with precise equations for $g = 2$ (uses Gröbner bases).

Slide 22

2nd MAGC Workshop

November 18, 2000

II. Point counting algorithms: elaborate methods

F. Morain

http://www.lix.polytechnique.fr/Labo/Francois.Morain/

Slide 23

Plan

I. What we saw yesterday.

II. Isogenies and point counting: Elkies, Atkin, Couveignes, Lercier.

III. Satoh's algorithm.

IV. Generalization to genus 2.

V. Generating cryptographically strong elliptic curves.

Slide 24

I. What we saw yesterday

$$\begin{array}{rccc} \varphi: & C(\overline{\mathbb{K}}) & \to & C(\overline{\mathbb{K}}) \\ & (X,Y) & \mapsto & (X^q, Y^q) \end{array}$$

Fundamental thm. The minimal polynomial $\chi(T)$ of φ is the reciprocal of $L(T)$. Moreover $\#\mathrm{Jac}(C)/\mathbb{F}_q = \chi(1)$.

Consequence: computing $\#\mathrm{Jac}(C)/\mathbb{F}_q$ boils down to computing $\chi(T)$.

$g=1$: for E with $\chi(T) = T^2 - cT + q$, $|c| \leq 2\sqrt{q}$.

φ restricted to $E[\ell]$ satisfies:

$$\varphi^2 - c\varphi + q \equiv 0 \bmod \ell$$

so we can find $c_\ell \equiv c \bmod \ell$ such that

$$(X^{q^2}, Y^{q^2}) \oplus [q](X,Y) = [c_\ell](X^q, Y^q)$$

in $\mathbb{K}[X,Y]/(E, f_\ell(X))$ and use CRT once $\prod \ell > 4\sqrt{q}$. Yields a $O(\log^8 q)$ **deterministic algorithm**.

Pb. $\deg(f_\ell) = O(\ell^2)$.

Slide 25

II. Isogenies and point counting

A) Elements of theory

Def. $\phi : E \to E^*$, $\phi(O_E) = O_{E^*}$; induces a morphism of groups.

First examples

1.
$$[k](X,Y) = \left(\frac{A_k}{\psi_k^2}, \frac{B_k}{\psi_k^3}\right)$$

2. $[i](X,Y) = (-X, iY)$ on $E : Y^2 = X^3 - X$.

3. $\varphi(X,Y) = (X^q, Y^q)$, $\mathbb{K} = \mathbb{F}_q$.

Thm. (dual isogeny) There is a unique $\hat{\phi} : E^* \to E$, $\hat{\phi} \circ \phi = [m]$, $m = \deg\phi$.

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[dr, "{[m]}"'] & E^* \arrow[d, "\hat{\phi}"] \\ & E \end{tikzcd}$$

Slide 26

Isogenies and subgroups

Thm. If F is a finite subgroup of E, then there exists ϕ and E^* s.t.

$$\phi : E \to E^* = E/F, \quad \ker(\phi) = F.$$

Ex. $E : y^2 = x^3 + ax^2 + bx$, $F = <(0,0)>$;

$$E^* : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X,$$

$$\phi : (x,y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right).$$

More generally: Vélu's formulas give

$$\phi(X,Y) = \left(\frac{G(X)}{H(X)^2}, \frac{J(X,Y)}{H(X)^3}\right).$$

(case $\deg\phi$ odd.)

Slide 27

Application to point counting

Suppose F is a subgroup of order ℓ of E:

$$\begin{tikzcd} E \arrow[r, "I"] \arrow[dr, "{[\ell]}"'] & E^* \arrow[d, "\hat{I}"] \\ & E \end{tikzcd}$$

$$I(X,Y) = \left(\frac{G}{H^2}, \dots\right), \deg(H) = (\ell - 1)/2$$

$\ker(I) \subset E[\ell] \Rightarrow H(X) \mid f_\ell(X)$ in $\mathbb{K}[X]$.

Schoof's algorithm on a degree $O(\ell)$ polynomial.

Pb. When does such an F exist over $\mathbb{K}$?

Slide 28

B) Atkin and Elkies

Consider $\varphi : (X, Y) \mapsto (X^q, Y^q)$ and its restriction φ_ℓ to $E[\ell]$:

$$\varphi_\ell^2 - c\varphi_\ell + q = 0,$$
$$\Delta = c^2 - 4q.$$

If $(\Delta/\ell) = +1$, then over $\mathbb{F}_\ell$,

$$\mathrm{Mat}(\varphi_\ell) \simeq \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \Leftrightarrow \exists F, \varphi(F) = F \Leftrightarrow F$$

is a cyclic subgroup of order ℓ, defined over $\mathbb{K}$.

Clon. If $(\Delta/\ell) = +1$, f_ℓ has a factor of degree $(\ell - 1)/2$.

Pb. How do we know that $(\Delta/\ell) = +1$?

Slide 29

Modular polynomials

Thm. $\exists \Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ s.t. E and E^* are ℓ-isogenous over $\mathbb{K}$ only if $\Phi_\ell(j(E), j(E^*)) = 0$.

Rem. This polynomial comes from the theory of elliptic curves over $\mathbb{C}$.

Ex.

$$\Phi_2(X, Y) = X^3 + X^2\left(-Y^2 + 1488\,Y - 162000\right)$$
$$+X\left(1488\,Y^2 + 40773375\,Y + 8748000000\right)$$
$$+Y^3 - 162000\,Y^2 + 8748000000\,Y - 157464000000000.$$

Thm. $E/\mathbb{F}_q$:

$$\Phi_\ell(X, j(E)) = \begin{cases} (1)(1)(s)\cdots(s) & \text{if } (\Delta/\ell) = +1, \\ (s)\cdots(s) & \text{if } (\Delta/\ell) = -1 \end{cases}$$

and s is the order of λ_1/λ_2.

Atkin's idea: use the splitting of Φ_ℓ to deduce information on t and combine it via a clever match and sort algorithm.

Slide 30

Clon. $(\Delta/\ell) = +1$ iff $\Phi_\ell(X, j(E))$ has two distinct roots over $\mathbb{K}$.

Slide 31

Elkies's algorithm

repeat

1. factor $\Phi_\ell(X, j(E))$ over $\mathbb{K}$.
2. if type = $(1)(1)(r)\cdots(r)$:
   - 2.1 build E^*;
   - 2.2 build I;
   - 2.3 find $c \bmod \ell$;

until $\prod_{\ell \text{ good}} \ell > 4\sqrt{q}$.

Thm. $O(\log^6 q)$ probabilistic.

Rem. One can build Φ_ℓ using series operations: Φ^c, Φ^*, Φ^Θ (Atkin), Φ^M (Müller), for $\ell \leq 1000$.

Slide 32

More details

- $p \gg \ell$**:** (Elkies, Atkin, 1988–1992)
  - use the theory of elliptic curves and lattices over $\mathbb{C}$ (Weierstrass $\wp$ function); rational formulas for E^*;
  - computing I takes $O(\ell)$ steps and uses $O(\ell)$ memory;
  - very efficient in practice: p with 500 decimal digits (M. 1995).
- p **small:** Couveignes I (first efficient method, 1994), II.
- $p = 2$**:** Lercier (1996), most efficient method until Satoh (1999-2000).

Slide 33

C) Using formal groups

$$t = -X/Y, s = -1/Y$$

$$F(t,s) := t^3 + a_1 ts + a_2 t^2 s + a_3 s^2 + a_4 t s^2 + a_6 s^3 - s = 0.$$

$$s = \mathcal{S}(t) = t^3 + a_1 t^4 + (a_1^2 + a_2)t^5 + O(t^6).$$

$$Y = -\frac{1}{s} = -t^{-3} + a_1 t^{-2} + a_2 t^{-1} + a_3 + (a_1 a_3 + a_4)t + O(t^2)$$

$$X = \frac{t}{s} = -tY = t^{-2} - a_1 t^{-1} - a_2 - a_3 t - (a_1 a_3 + a_4)t^2 + O(t^3)$$

$$t_3 = F_a(t_1, t_2) = t_1 + t_2 - a_1 t_1 t_2 - a_2(t_1^2 t_2 + t_1 t_2^2)$$
$$-(2a_3 t_1^3 t_2 - (a_1 a_2 - 3a_3)t_1^2 t_2^2 + 2a_3 t_1 t_2^3) + \ldots$$

$$[2]t_1 = 2\,t_1 - a_1\,t_1^2 - 2\,a_2\,t_1^3 + (a_1\,a_2 - 7\,a_3)\,t_1^4 + \cdots$$

$$[n]t_1 = n\,t_1 + \cdots$$

Thm. $[p](t) = \Psi_{p,E}(t)^p = c_p(E)t^p + O(t^p)$.

Thm. $\mathrm{Norm}_{\mathbb{K}/\mathbb{F}_p}(c_p(E)) \equiv \mathrm{Tr}_{\mathbb{K}/\mathbb{F}_p}(\varphi) \bmod p$.

Ex. $c_2([a_1, a_2, a_3, a_4, a_6]) = a_1$, $c_3([a_2, a_6]) = a_2$.

Slide 34

CouveignesI

Looking for I is equivalent to searching for a morphism of formal groups $\mathcal{M} : \mathcal{E} \to \mathcal{E}^*$

$$\mathcal{M}(t(\tau), s(\tau)) = (\mathcal{U}(t(\tau)), \mathcal{S}^*(\mathcal{U}(t(\tau))))$$

s.t.

$$\mathcal{M}(P_1 \oplus P_2) = \mathcal{M}(P_1) \oplus \mathcal{M}(P_2)$$

or

$$\mathcal{U}(t_1 \oplus t_2(\tau)) = \mathcal{U}(t_1(\tau)) \oplus \mathcal{U}(t_2(\tau))$$

where $\mathcal{U}(t) = t + \sum_{i \geq 2} u_i t^i$. $\mathcal{U}$ is found incrementally using inderterminate coefficients.

Thm. time $O(\ell^3)$, space $O(\ell^2)$.

Rem. In real life, difficult to implement (huge series computations).

For more details, see Lercier & Morain, *Math. Comp.* 69, 2000.

Slide 35

D) Lercier's algorithm

Motivation: CouveignesI too slow, too much memory involved (huge series computations).

$$p = 2, E: Y^2 + XY = X^3 + a, E^*: Y^2 + XY = X^3 + b$$

Prop. $I(X) = XL(X)^2/H(X)^2$.

Ideas:

- send $P = (0, \sqrt{a})$ to $P^* = (0, \sqrt{b})$ and use:
$$P \oplus M = (0, \sqrt{a}) \oplus (X, Y) = (\sqrt{a}/X, \ldots);$$
- use
$$I(P \oplus M) = P^* \oplus I(M);$$
- use
$$I \circ [2] = [2] \circ I;$$
- translate all these equations in a (non linear) system of equations in coefficients of $L(X)$ and $H(X)$ and solve it.

Slide 36

Analysis: heuristically, time is $O(\ell^3)$ with a much better constant; space is $O(\ell)$.

In practice: considerably faster than Couveignes's first algorithm: 400 times faster for computing isogenies for $\mathbb{K} = \mathbb{F}_{2^{300}}$, resulting in a **speed-up of** 5 on the total running time for the complete SEA algorithm.

$\mathbb{F}_{2^{155}}$	86 sec
$\mathbb{F}_{2^{196}}$	308 sec
$\mathbb{F}_{2^{300}}$	2851 sec
$\mathbb{F}_{2^{1663}}$	330 days

(Alpha 266 MHz)

Rem. Vercauteren (October 1999) $\mathbb{F}_{2^{1999}}$ after 65 days of CPU time on 400 MHz PCs.

Slide 37

E) CouveignesII

Idea: $E[p]$ seems to be of first importance.

Prop.

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[dr, "{[p]}"'] & E^p \arrow[d, "\hat{\varphi}"] \\ & E \end{tikzcd}$$

$$[p](X, Y) = (F_p(X)^p, G_p(X, Y)^p)$$

Coro.

$$f_{p^i}(X) = \tilde{f}_{p^i}^{p^i}, \deg \tilde{f}_{p^i} = d_i = p^{i-1}(p-1)/2 \text{ or } 2^{i-1}$$

Idea: I maps $E[p^k]$ to $E^*[p^k]$:

$$I([m]P) = [m]P^*, \quad I(x_m) = x_m^*$$

Slide 38

Use interpolation: let $A(X)$ s.t. $A(x_m) = x_m^*$ for all $m, 1 \leq m \leq d_k$. Then

$$I(X) \equiv A(X) \bmod \tilde{f}_{p^k}(X)$$

Prop. If $d_k > 2\ell$, recover H via the euclidean algorithm.

Rem. In general, the p^k-division is not rational and the interpolation part must be done with some care.

Prop. Complexity should be time $O(\ell^{2+\epsilon})$, space $O(\ell)$.

Prop. Artin-Schreier approach of Couveignes: $O(n\mathcal{M}(\ell))$, see *Math. Comp.* 69, 2000.

Slide 39

III. Satoh's algorithm

Def. $\mathbb{Z}_p$ ring of p-adic integers $(x_1, x_2, \ldots, x_n, \ldots)$ s.t. $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ and $x_{n+1} \equiv x_n \bmod p^n$. Denote by $\pi : \mathbb{Z}_p \to \mathbb{F}_p$ sending x to x_1.

Def. Let $q = p^r$ and $f(t) \in \mathbb{Z}_p[t]$ s.t. $\pi(f)$ is irreducible in $\mathbb{F}_p[t]$. Then $\mathbb{Z}_q = \mathbb{Z}_p[t]/(f(t))$.

An element of $\mathbb{Z}_q$ is $\mathcal{A} = a_{r-1}t^{r-1} + \cdots + a_0$ with $a_i \in \mathbb{Z}_p$; $\mathbb{Z}_q$ contains $\mathbb{Z}_p$ as a subring.

$$\pi(\mathcal{A}) = \sum_i \pi(a_i)t^i.$$

Prop. Let σ be the *little* Frobenius sending x in $\mathbb{F}_q$ to x^p. There is a canonical way to lift σ to $\Sigma : \mathbb{Z}_q \to \mathbb{Z}_q$.

Extend σ to points $\sigma(x, y) = (\sigma(x), \sigma(y))$ and to curves: $\sigma(E) = [\sigma(a_i)]$, so that if $P \in E(\mathbb{K})$, then $\sigma(P) \in \sigma(E)(\mathbb{K})$.

Slide 40

Thm (Lubin-Serre-Tate) Let $E/\mathbb{F}_q$ with $j = j(E) \in \mathbb{F}_q - \mathbb{F}_{p^2}$. There is a unique $\mathcal{J}$ in $\mathbb{Z}_q$ s.t.

$$\Phi_p(\mathcal{J}, \Sigma(\mathcal{J})) = 0,$$

$\pi(\mathcal{J}) = j$; $\mathcal{J}$ is the invariant of the *canonical lift* $\mathcal{E}$ of E and $\mathrm{End}(\mathcal{E}) = \mathrm{End}(E)$.

Isogeny cycles:

$$\begin{array}{ccccccccc} \mathcal{E}_0 & \xrightarrow{\Sigma_{r-1}} & \mathcal{E}_{r-1} & \xrightarrow{\Sigma_{r-2}} & \cdots & \xrightarrow{\Sigma_1} & \mathcal{E}_1 & \xrightarrow{\Sigma_0} & \mathcal{E}_0 \\ \downarrow \pi & & \downarrow \pi & & & & \downarrow \pi & & \\ E_0 & \xrightarrow{\sigma_{r-1}} & E_{r-1} & \xrightarrow{\sigma_{r-2}} & \cdots & \xrightarrow{\sigma_1} & E_1 & \xrightarrow{\sigma_0} & E_0 \end{array}$$

Prop. $\varphi = \sigma_0 \circ \sigma_1 \circ \cdots \circ \sigma_{r-1}$,
$\mathcal{F} = \Sigma_0 \circ \Sigma_1 \circ \cdots \circ \Sigma_{r-1}$.

Thm. $\mathrm{Tr}(\varphi) = \mathrm{Tr}(\mathcal{F})$.

Slide 41

Computing $\mathrm{Tr}(\mathcal{F})$

Use the dual of Frobenius to get another isogeny cycle amenable to computations:

$$\begin{array}{ccccccccc} \mathcal{E}_0 & \xrightarrow{\hat{\Sigma}_0} & \mathcal{E}_1 & \xrightarrow{\hat{\Sigma}_1} & \cdots & \xrightarrow{\hat{\Sigma}_{r-2}} & \mathcal{E}_{r-1} & \xrightarrow{\hat{\Sigma}_{r-1}} & \mathcal{E}_0 \\ \downarrow \pi & & \downarrow \pi & & & & \downarrow \pi & & \\ E_0 & \xrightarrow{\hat{\sigma}_0} & E_1 & \xrightarrow{\hat{\sigma}_1} & \cdots & \xrightarrow{\hat{\sigma}_{r-2}} & E_{r-1} & \xrightarrow{\hat{\sigma}_{r-1}} & E_0 \end{array}$$

Prop. $\hat{\varphi} = \hat{\sigma}_{r-1} \circ \hat{\sigma}_{r-2} \circ \cdots \circ \hat{\sigma}_0$ (idem for $\hat{\mathcal{F}}$) and also $\mathrm{Tr}(\hat{\mathcal{F}}) = \mathrm{Tr}(\mathcal{F}) = \mathrm{Tr}(\varphi)$.

Let τ (resp. τ_i) denote the local parameter of $\mathcal{E}$ (resp. $\mathcal{E}_i$).

$$\mathcal{F}(\tau) = \sum_{k \geq 1} c_k \tau^k$$

Prop. (Satoh) $\mathrm{Tr}(\mathcal{F}) = c_1 + q/c_1$.

$$c_1 = \prod_{i=0}^{d-1} g_i$$

where (Vélu's formulas again)

$$\hat{\Sigma}_i(\tau_i) = g_i \tau_i + O(\tau_i^2)$$

Slide 42

Satoh's algorithm in brief

1. Compute the curves E_0, E_1, E_{r-1} and their invariants j_i.
2. Lift all the j_i's simultaneously by a Newton iteration to get $\mathcal{J}_i$:

   $\Theta((x_i)) = (\Phi_p(x_0, x_1), \Phi_p(x_1, x_2), \ldots, \Phi_p(x_{r-1}, x_0))$

   as

   $$(x_i) \leftarrow (x_i) - ((D\Theta)^{-1}\Theta)((x_i)).$$
3. Lift each E_i coefficient by coefficient.
4. Lift the p-torsion subgroup of E_i.
5. Compute the $\hat{\Sigma}_i$'s.
6. Compute the trace.

Thm. (Satoh-FGH) For fixed p, Satoh-FGH requires $O(r^3)$ memory and $O(r^{3+\varepsilon})$ bit-operations.

Slide 43

Results

Implementation details: too many of them, see [FGH] and the URL

`http://www.xent.com/~harley`

for a demo version of the ECPC program.

Record: $\mathbb{F}_{2^{8009}}$ in 313 hours on an Alpha EV6, 750 MHz, 16.9 Gb (in Cornell).

More timings: on Alpha 750 MHz

Degree	Time	Degree	Time
160	$2.5s$	1000	$22m$
200	$4.6s$	2000	$3h$
240	$7.1s$	4000	$29h$

Slide 44

IV. Generalization to genus 2

- **Division polynomials:** Cantor.
- **Schoof:** Pila; Kampkötter (Gröbner bases).
- **Modular equations:**
  - Siegel's modular forms; large output. On-going work by Gaudry and Harley.
  - Alternative equations by Gaudry and Schost (similar to Charlap, Coley and Robbins for elliptic curves): computed for $g = 2$, $\ell = 3$ (see PG's web page for the equation).
  - Factorization patterns: exist; cf. PG for $g = 2$.
- **Isogenies:** Vélu's formulas?
- **Satoh's algorithm:** LST valid. Need modular equation.

Slide 45

Current status

- **Genus $g > 2$:** Stein-Teske (1999): $q = 10^8 + 7$, $g = 3$, $\#\mathrm{Jac} \approx 10^{24}$ in 10 hours on a Pentium Pro/200 with SIMATH.
- **Genus 2:** Gaudry & Harley (ANTS IV)
  - find $\#\mathrm{Jac} \bmod \ell$ using Cartier-Manin ($\ell = p$) or Cantor's division polynomials;
  - find $\#\mathrm{Jac} \bmod 2^k$ by looking for solutions of $[2]D = D_0$;
  - combine all this to reduce the birthday paradox.
  - record: $p = 10^{19} + 51$;

    $$y^2 = x^5 + \ 3141592653589793238\, x^4 + \cdots$$

    $$\#\mathrm{Jac} = 99999999982871020671452277000281660080,$$

ℓ^n	2^{16}	3	5	7	11	13
time	$10h$	$1200s$	$300s$	$12h$	$19h$	$205h$

Width 2.5×10^{29}, 50 days on a 500 MHz Alpha.

Slide 46

V. Generating cryptographically strong curves

$\mathbb{F}_p$ with large p or $\mathbb{F}_{2^n}$ with n prime (Weil descent, see Menezes & Qu); subgroups of large prime order.

- **Supersingular curves:** too much structure (?).
- **CM curves:** quite efficient for $g = 1$ or $g = 2$, but who knows?
- **Fixed curves:** The NIST curves (?).
- **Random curves:**
  - $g > 1$ not efficient yet.
  - $g = 1$: use SEA for large p, Satoh for $p = 2$. Very efficient when combined to the early-abort approach in Lercier's EUROCRYPT'97 article. Experiments conducted by FGH combining SEA and Satoh show that it takes **5 min** on Alpha 750 MHz to build a good curve over $\mathbb{F}_{2^{233}}$.

Slide 47

2nd MAGC Workshop

November 19, 2000

III. Discrete log algorithms

F. Morain

Slide 48

Plan

I. The problem.

II. Generic methods.

III. Index calculus.

IV. Cryptographic implications.

Slide 49

I. The problem

$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^r}$

Input: $P \in \mathrm{Jac}(C)$ of order $n, Q \in < P >$.

Output: k s.t. $Q = [k]P$.

Ex. elliptic case

$C/\mathbb{K} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$

or hyperelliptic case:

$$C/\mathbb{K} : Y^2 + H(X)Y = X^{2g+1} + \cdots$$

Benchmark CERTICOM exercises (cf. `http://www.certicom.com/chal`).

Slide 50

General results

- **No (known) subexponential method for small** g (including $g = 1$); recover a subexp method when g increases.
- **Reduction** $\mathrm{Jac}(C)/\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^k}$ with k small:
  - Supersingular curves: *MOV* (Menezes, Okamoto, Vanstone using the Weil pairing); Frey & Rück (using the Tate pairing); Galbraith. See G. Frey's talks.
  - other cases: elliptic curves with $t = 2$ with the Tate pairing.
- Discrete logs in subgroups of order p^e of $\mathrm{Jac}(C)/\mathbb{F}_{p^r}$ can be found in **polynomial time**: $g = 1$ (anomalous curves) done by Satoh-Araki, Semaev, Smart; $g > 1$ by Rück.
- **Elliptic curves:** lifting points or *XEDNI*: Silverman *et al.*, Cheon *et al.*. Do not work in the present form.

Slide 51

II. Generic methods

A) Shanks

$$k \in [-(n-1)/2, (n-1)/2], \quad w = \sqrt{(n-1)/2}$$
$$k = uw + v, 0 \leq v < w, \quad |u| \leq w.$$
$$[k]P = Q \Longleftrightarrow [u]([w]P) = Q \ominus [v]P.$$

baby steps: compute the points $Q \ominus [v]P$ for all v's in $O(w)$ steps.

giant steps: find u in $O(w)$ steps.

Cost: $O(w) = O(\sqrt{n})$ in time and space, **deterministic**.

B) Pohlig-Hellman

$$n = \prod_i p_i^{\alpha_i}$$

Idea: finding $[x]P = Q$ is equivalent to finding $x \bmod n$, i.e., $x \bmod p_i^{\alpha_i}$ for all i (CRT). It reduces the discrete log $\bmod n$ to that $\bmod p_i^{\alpha_i}$ for all i.

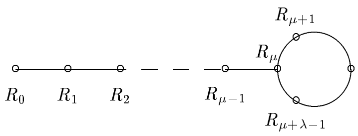
Cost: $O(\max(\alpha_i \mathrm{DL}(p_i)))$.

Slide 52

C) Pollard's ρ

Idea: use the properties of functional graphs.

Let f be a random function: $< P > \rightarrow < P >$, $R_0 \in < P >_R$ and build $R_{i+1} = f(R_i)$:



More precisely, one starts from $R_0 = [u_0]P + [v_0]Q$ with u_0 and v_0 in $\mathbb{Z}/n\mathbb{Z}_R$ and one builds the sequence $R_{i+1} = f(R_i)$, which also builds (u_i) and (v_i) modulo n s.t. $R_i = [u_i]P + [v_i]Q$.

Random mapping statistics; (Flajolet & Odlyzko, EUROCRYPT'89) a functional graph for a random f with n vertices should have $0.5 \log n$ components, $\overline{\mu}_n = \overline{\lambda}_n = \sqrt{\pi n/8}$, $\overline{\rho}_n = \sqrt{\pi n/2}$.

Slide 53

Clon: after $\approx \sqrt{\pi n/2}$ iterations, we should find a collision, that is i and j s.t. $R_i = R_j$:

$$[u_i - u_j]P + [v_i - v_j]Q = 0$$

hence k if $v_i \neq v_j$ (which happens with probability $1/n$).

Floyd's algorithm: there is an $e = O(\sqrt{\mu})$ s.t. $R_e = R_{2e}$:

- $R := R_0$, $S := R_0$;
- **repeat** $R := f(R)$, $S := f(f(S))$ **until** $R = S$.

Cost: time $O(\sqrt{n})$ and space $O(1)$.

Slide 54

D) Parallel collision search

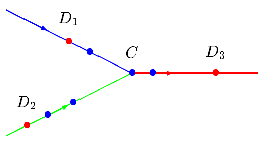
1) Distinguished points

(Quisquater & Delescaille, EUROCRYPT'89)

Idea: store points with a distinguishing property (e.g., $P = (x, y)$ and $x \equiv 0 \bmod 2^b$). If θ is the proportion of distinguished points, one should find a collision after having computed $\theta\sqrt{\pi n/2}$ distinguished points.

2) The algorithm

(van Oorschot & Wiener, *J. Cryptology*, 1999)



M processors run through the graph at the same time: one should find a collision after each processor has computed $\sqrt{\pi n/2}/M$ points, or $\theta\sqrt{\pi n/2}/M$ distinguished points.

Rem. All solved exercises of Certicom done this way.

Slide 55

Choosing f

- **additive random walk:**
  - precompute r points $(T^{(j)})_{0 \leq j < r}$ in $< P >$, e.g. $T^{(j)} = [u^{(j)}]P + [v^{(j)}]Q$.
  - $f(R) = R + T^{(j)}$, with $j = \mathcal{H}(R)$ where $\mathcal{H}$ sends $< P >$ to $\{0, 1, \ldots, r-1\}$. In other words: $R_i = [u_i]P + [v_i]Q$, with $u_{i+1} \equiv u_i + u^{(j)} \bmod n, \quad v_{i+1} \equiv v_i + v^{(j)} \bmod n$.
  - Satler & Schnorr: $r \geq 8$; Teske: $r \geq 20$ (+ Hildebrand's result on random walks $\bmod n$).
- **multiplicative random walk:** (Gallant *et al.*)
  - choose multipliers $(\mu_j)_{0 \leq j < r}$;
  - $f(R) = [\mu_j]R$, $j = \mathcal{H}(R)$, i.e.:

$$f(R) = \left[\prod_{j=0}^{r-1} \mu_j^{f_j}\right] R_0;$$

  - requires at least two processors;
  - computing $[\mu_j]R$ must be done quickly.

Slide 56

E) Adaptation to algebraic curves

Using equivalence classes

Idea: $\sim$ equivalence relation s.t. $\#(< P > / \sim) = n/m$. A random walk should find a collision after $\sqrt{\pi n/(2m)}$ iterations.

Finding $\sim$:

- Wiener, Zuccherato: $(x, y) \sim (x, -y)$.
- Gallant, Lambert et Vanstone; Harley: use little Frobenius on ABC curves.
- Duursma, Gaudry, M.: automorphism α of order m of C: $S \sim T \iff \exists i, S = \alpha^i T$.
  Ex1. $Y^2 = X^3 + aX$ with $[i](x, y) = (-x, iy)$ where $i^2 = -1$ (+ Frobenius).
  Ex2. On $Y^2 = X^5 - 1$, $\alpha(x, y) = (\zeta_5 x, y)$, where $\zeta_5^5 = 1$, $-\alpha$ has order 10; action on Jac as:
  $$[z^2 + u_1 z + u_0, v_1 z + v_0] \mapsto [z^2 + \zeta_5 u_1 z + \zeta_5^2 u_0, -\zeta_5^{-1} v_1 z - v_0].$$

Technical details: well defined f; short cycles.

Slide 57

ECC2K-108

(Harley *et al.*, taken from `http://cristal.inria.fr/~harley/`)

- 1300 individuals, 9500 machines, dec 1999 until april 2000.
- **200,000 days on a 450 MHz PC with MMX**, i.e. more than 500 years. For comparison, cracking a 56-bit DES key by exhaustive search would take about 110000 days.
- 2.8×10^{15} elliptic-curve operations of which 2.3×10^{15} led to distinguished points recorded at INRIA; 2.05 million distinguished points in 1.3 Gigabytes of email.

Slide 58

III. Index calculus methods

A) The basic scheme

Western and Miller; Pollard, Adleman, Merkle, etc. Methods in

$$L_N[\alpha, c] = \exp((c+o(1))(\log N)^\alpha (\log\log N)^{1-\alpha}).$$

Input: $G = \mathbb{F}_q^*, \mathrm{Jac}(C)$ of large genus; $G =< g >$, $a = g^z$.

Step 1: find the logarithms of the primes (resp. irreducible polynomials, prime divisors) of a factor basis $\mathcal{F} = \{p_1, p_2, \ldots, p_k\}$.

Step 2: look for b s.t. ag^b factors over $\mathcal{F}$:

$$ag^b = \prod_{j=1}^{k} p_j^{\alpha_j}$$

yields

$$z + b \equiv \sum_{j=1}^{k} \alpha_j \log_g p_j \bmod \#G.$$

Slide 59

How do we find the $\log_g p_j$?

Choose random integers b_i for which

$$g^{b_i} = \prod_{j=1}^{k} p_j^{\alpha_{i,j}}$$

or:

$$b_i \equiv \sum_{i=1}^{k} \alpha_{i,j} \log_g p_j \bmod \#G.$$

When enough relations have been gathered, solve the system.

Cost: $O(L_{\#G}[1/2, c])$ where c depends on G and/or $\#G$.

Best algorithm so far: *à la* NFS $O(L_p[1/3, c'])$ (Gordon, Schirokauer).

Record: Joux & Lercier (**100 digits**, 1999).

Slide 60

B) Discrete log on hyperelliptic curves

- Algorithm ADH from *Adleman, DeMarrais, Huang* (ANTS I):

$$\mathbf{L_{p^{2g+1}}[1/2, c]}$$

with $c \leq 2.181$ if $\log p \leq (2g+1)^{0.98}$ (heuristic using Lovorn's theorem on smooth polynomials); SNF.

- *Flassenberg & Paulus:* using sieving techniques; experiments with $y^2 = x^{2g+1} + 2x + 1$, faster than Shanks for $g \geq 6$.
- $y^2 = x^{2g+2} + \cdots$ (Müller-Stein-Thiel): proved $L_{p^{2g+2}}[1/2, 1.44]$.
- Extensions, proved analysis and optimizations by *Enge*:

$$\mathbf{L_{q^g}[1/2, c(\theta)]}$$

if $\theta \log q \leq g$, with $\lim_{\theta \to 0} c(\theta) = +\infty$; easier SNF. Smaller $c = \sqrt{2}$ by Enge and Gaudry.

- *Gaudry*'s variant: **fast, practical, implemented, breaks a lot of proposed systems**.

Slide 61

C) Gaudry's variant

Main features:

- *easy* to describe and to analyze.
- *index calculus* using a basis of S-smooth divisors, i.e. $\mathcal{F} = \{< u(z), v(z) > \in \mathrm{Jac}(C), u(z)$ is irreducible of degree $\leq S\}$, with $S = 1$ for $g \leq 8$.
- Finding relations using a *random walk*.
- Easier linear algebra.
- **exponential asymptotic complexity** but **very practical** and **breaks a lot of systems** proposed by various authors.

Slide 62

The algorithm

Input: $D_1, D_2 \in \mathrm{Jac}(C), n = \mathrm{ord}(D_1)$ **known**.

Output: λ s.t. $D_2 = [\lambda]D_1$.

1. [Initialisations:] Fix a smoothness bound S and build the basis $\mathcal{F} = \{g_1, g_2, \ldots, g_w\}$. Compute $T^{(j)} := [\alpha^{(j)}]D_1 + [\beta^{(j)}]D_2$ for $j \in [1..r]$ and set $R_0 := [\alpha_0]D_1 + [\beta_0]D_2$. Put $k := 1$.
2. [Main loop:]

   (a) Look for a smooth divisor:

   repeat

   $j := \mathcal{H}(R_0), R_0 := R_0 + T^{(j)}$,

   $\alpha_0 += \alpha^{(j)} \bmod n, \beta_0 += \beta^{(j)} \bmod n$.

   until $R_k := R_0 = [u_0(z), v_0(z)]$ is S-smooth.

   (b) [Write R_0 on $\mathcal{F}$:] factor $u_0(z)$ over $\mathbb{F}_q$, store $R_k = \sum m_{ik} g_i$ and $\alpha_k = \alpha_0, \beta_k = \beta_0$.

   (c) If $k < \#\mathcal{F} + 1$, then $k := k + 1$, go to 4.
3. [Linear algebra:] find (γ_k) in $\mathrm{Ker}({}^tM)$ on $\mathbb{Z}/n\mathbb{Z}$.
4. Return $\lambda = -(\sum \alpha_k \gamma_k)/(\sum \beta_k \gamma_k) \bmod n$.

Slide 63

Analysis for $S = 1$

(enough for $g \leq 8$)

Prop. The probability for $u(z) \in \mathbb{F}_q[z]$ of degree g to be 1-smooth is $1/g!$ ($\#\{g-$ sets of $P \in C\} \approx q^g/g!$).

- **building** $\mathcal{F}$**:** $\#\mathcal{F} = O(q) \Rightarrow O(q)$ computations of squareroots in $\mathbb{F}_q$.
- **random walk:** $O(g!q)$ additions on the jacobian and smoothness test of a degree g polynomial, followed by $O(q)$ EDF's of degree g polynomials (total $\leq O(gq)$).
- **linear algebra:** with Lanczos on a $q \times q$ matrix over $\mathbb{Z}/n\mathbb{Z}$, each row having $\leq g$ entries $\Rightarrow O(q(qg)(\log n)^2) = O(g^3 q^2 (\log q)^2)$ (since $n \approx q^g$).

Thm. Gaudry's variant takes time $O(q^2 \log^c q)$ for fixed g.

Fine points: smoothness test (use discriminant *à la* Swan), EDF, SGE for fast linear algebra ($\neq$ factorization, $\neq$ discrete log over $\mathbb{F}_{p^n}$).

Slide 64

More properties

Rem. The algorithm has **asymptotic exponential** complexity, but works very well in practice (see below), since it must factor polynomials of smaller degree than ADH. Provably (and practically) better than Pollard's ρ for $g > 4$.

Size of Jac **breakable**: $\#\mathrm{Jac} = q^g = (2\#\mathcal{F})^g$:

$\#\mathcal{F}\backslash g$	4	5	6	7	8
10^5	2^{70}	2^{88}	2^{105}	2^{123}	2^{140}
10^6	2^{83}	2^{104}	2^{125}	2^{146}	2^{167}

Crucial rem. An automorphism of order m reduces $\#\mathcal{F}$ by a factor m and the linear algebra by m^2.

Slide 65

Hyperelliptic cryptosystems

Author	equation	q	auto
Koblitz	$Y^2+Y=X^5+X^3$ $(*)$	2^ℓ	4ℓ
	$Y^2+Y=X^5+X^3+X$ $(*)$	2^ℓ	2ℓ
	$Y^2+Y=X^{2g+1}+X$	2^ℓ	2ℓ
	$Y^2+Y=X^{2g+1}$	2^ℓ	2ℓ
Spallek	$Y^2=X^5-140X^3-240X^2+3810X+6928$	p	2
Buhler Koblitz Chao et al.	$Y^2+Y=X^{2g+1}$ (+ twists)	p with $p\equiv 1\ (2g+1)$	$2(2g+1)$
Sakai Sakurai Smart	$Y^2+Y=X^{13}+X^{11}+X^9+X^5+1$	2^{29}	4×29
Duursma Sakurai	$Y^2=X^p-X+1$	p^ℓ	$2\ell p$

Slide 66

Timings

Magma 2.3 on Pentium II 450 MHz, 128 Mb.

Example 1:

field	$\mathbb{F}_{5026243}$
equation	$y^2+y=x^{13}$
genus	6
auto	13
$\#\mathrm{Jac}$	$\approx 10^{40}$
basis	$193,485$
matrix	$165,778\times 165,779$

construct. basis	1638 s
relations	6 days
SGE	1218
Lanczos	9 days

Slide 67

Example 2:

field	$\mathbb{F}_{2^{23}}$
equation	$y^2+(x+1)y=x^{13}+x^{11}+x^8+x^7+x^5+x^4+x+1$
genus	6
auto	2×23
$\#\mathrm{Jac}$	$\approx 10^{41}$
basis	$182,462$
matrix	$162,873\times 162,874$

construct. basis	6575 s
relations	9 days
SGE	880 s
Lanczos	12 days

Slide 68

Perspectives

Proven analyses: (Enge & Gaudry) unification of the methods used for finite fields and class groups.

Limiting factor: linear algebra stage, not the collection of relations ($\approx$ factorization). Wait for progress in distributed linear algebra.

Ex. (Sakai Sakurai Smart)
$y^2 + y = x^{13} + x^{11} + x^9 + x^5 + 1$ (genus 6) on $\mathbb{F}_{2^{29}}$ with an automorphism of order 4×29, $\#\mathrm{Jac} \approx 2^{174}$. Requires $\#\mathcal{F} \approx 4,500,000$.

Genus 4**:** rho and PG's are $O(q^2)$; dividing the size of the basis by $q^{1/5}$ yields a $q^{8/5}$ method.

Genus 2**:** (Gaudry) using a union-find type method for performing the linear algebra phase, same complexity as rho.

Genus 3**:** linear time linear algebra?

Important application: use this as a tool in the Weil descent.

Slide 69

Weil descent: an example

$$\mathbb{F}_{q^n} = \mathbb{F}_q[t]/(f(t))$$
$$E : Y^2 = X^3 + \alpha X + \beta$$

Write $\alpha = \sum_i a_i t^i$, $\beta = \sum_i b_i t^i$,

$$X = \sum_i x_i t^i, \quad Y = \sum_i y_i t^i,$$

$$0 = Y^2 - (X^3 + \alpha X + \beta) = \sum \varphi_j(a_i, b_i, x_i, y_i) t^i$$

Thm. $\{\varphi_i\}$ defines an **abelian variety of dimension** n, with law (and points) inherited from E. Moreover, $\chi_A(T) = \chi_E(T^n)$.

A nice case: $2 \mid q$, $\mathbb{F}_{q^n}$ with basis $\{\theta, \theta^2, \ldots, \theta^{2^{n-1}}\}$ and $\theta + \theta^2 + \ldots + \theta^{2^{n-1}} = 1$. On $E : Y^2 + XY = X^3 + \beta$, write $X = \sum_i x_i \theta^{2^i}, \ldots$ and find the equation of C on A s.t. $x_0 = x_1 = x_2 = \cdots = x_{n-1} = x$.

$$C : y^{2^n} + x^{2^n - 1} y + \sum_{i=0}^{n-1} x^{2^n + 2^i} + g(x) = 0$$

with $\deg(g) \le 2^n$.

Slide 70

Thm. $\exists m \in [1..n]$ s.t. C has an irreducible component which is hyperelliptic of genus 2^{m-1} or $2^{m-1} - 1$. Moreover, we have an homomorphism $E \to \mathrm{Jac}(C)$.

If n is small, solve DL on Jac by Gaudry's algorithm.

Ex. $\mathbb{F}_q = \mathbb{F}_{2^{21}}$, $E/\mathbb{F}_{q^4}$, $g = 4$.

Rem. m further analyzed by Menezes & Wu, $\mathbb{F}_{2^p}$ **not breakable**.

Rem. Recent computations of Smart: can break $E/\mathbb{F}_{q^4}$, $g = 8$, faster than ρ for $q > 2^{17}$.

Slide 71

IV. Cryptographic implications

- Be very **careful** when using curves with an automorphism of large order.
- Find curves with cardinality easy to compute but without automorphisms: use **random** curves or maybe $X_0(N)$ (which has only involutions).
- Low genus is 5 or maybe 4 or 3 (surely not 1)? Implies make the base field larger (bad news for smart cards).
- **buy random elliptic curves!**

Slide 72