Cryptographic Applications of Trace Zero Varieties

Tanja Lange

ITSC - Information-Security and Cryptography

Ruhr-University of Bochum

lange@itsc.ruhr-uni-bochum.de

21.05.2004

Hyperelliptic curve

$$C : y^2 + h(x)y = f(x)$$

$h(x), f(x) \in \mathbb{F}_q[x]$, q prime power,
f monic, $\deg f = 2g + 1, \deg h \leq g$
nonsingular, i. e. not both partial derivatives zero for
$(a, b) \in C/\bar{\mathbb{F}}_q$

C hyperelliptic curve of genus g

with at least one $\mathbb{F}_q$-rational Weierstraß point
(elliptic curves are seen here as curves of genus 1)

This talk

Elliptic curves (genus $g = 1$)

$$y^2 = x^3 + a_4 x + a_6$$

Curves of genus $g = 2$

$$y^2 = x^5 + f_3 x^3 + f_2 x^2 + f_1 x + f_0$$

fields of odd characteristic $\mathbb{F}_{p^n}, p$ prime.

For cryptographic applications $g < 4$ is required, see Thériault'03

Divisor Class Group

Use divisors, i. e. sums of points, of degree zero and reduce modulo principal divisors (divisors arising from functions):

$$\mathrm{Pic}^0(C/\mathbb{F}_q) = Div^0(\mathbb{F}_q)/P(\mathbb{F}_q)$$

each class represented by degree zero divisor with $m \leq g$

$$\sum_{\substack{i=1 \\ P_i \in C\setminus\{P_\infty\}}}^{m} P_i - mP_\infty$$

most common case: $m = g$.

Mumford Representation

Use

$$\mathrm{Pic}^0(C/\mathbb{F}_q) \cong \mathbf{Cl}(C/\mathbb{F}_q)$$

to get representation

$$D = [u(x), v(x)]; u, v \in \mathbb{F}_q[x],$$

u monic, $\deg v < \deg u \leq g, \quad u | v^2 + vh - f.$

Isomorphism

$P_i = (x_i, y_i) \Leftrightarrow u(x_i) = 0, v(x_i) = y_i$ with correct multiplicity,

arithmetic uses $[u, v]$ only

Koblitz curves (subfield curves)

Hyperelliptic curve

$$C : y^2 + h(x)y = f(x),$$

with $h(x), f(x) \in \mathbb{F}_p[x]$, p small,

consider curve over $\mathbb{F}_{p^n}$, n sufficiently large.

Example:

$$C : y^2 + xy = x^5 + x^2 + 1$$

hyperelliptic curve of genus 2 over $\mathbb{F}_2$
hyperelliptic curve of genus 2 over $\mathbb{F}_{2^n}$

History: Koblitz '89; Günther, L., Stein '00; L. 01 (Ph.D.)

Frobenius endomorphism

- Operates on ideal classes $D = [u(x), v(x)]$ via
$$\sigma(D) = [\sigma(u(x)), \sigma(v(x))],$$
where $\sigma(\sum d_i x^i) = \sum d_i^q x^i$.
- Execution of Frobenius endomorphism is much faster than one group operation.
- σ satisfies characteristic polynomial
$$P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + a_1 p^{g-1} T + p^g$$
with integer coefficients, degree $2g$
- Use σ for faster scalar multiplication, repeatedly replacing

$$p^g(D) = -(\sigma^{2g}(D) + a_1 \sigma^{2g-1}(D) + \cdots + a_g \sigma^g(D) + \cdots + a_1 p^{g-1} \sigma(D)).$$

Trace Zero Subgroup G

Use idea of Koblitz curves with a small extension $n = 3, 5$ (should be prime) and large enough p

Trace Zero Subgroup G:

- $\{D | \sigma^{n-1}(D) + \sigma^{n-2}(D) + \cdots + \sigma(D) + D = 0\}$

Parameter:

- $n \in \{3, 5\}$ for $g = 1$.
- $n = 3$ for $g = 2$

History: Frey '98, Naumann '99 ($g = 1$), Diem '01
L. '01 ($g = 2$), Blady '02 ($g = 1$), (Weimerskirch '02)
Silverberg/Rubin '02 (supersingular curves)
Avanzi, Diem, Frey, L., Scholten '03

Geometric construction I

Example: elliptic curve

$$y^2 = x^3 + Ax + B \text{ over } \mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$$

write $x = \sum_{i=0}^{n-1} x_i \alpha^i$, $y = \sum_{i=0}^{n-1} y_i \alpha^i$

sort according to powers of α

$$\Rightarrow n\text{-dimensional variety over } \mathbb{F}_p.$$

in general $\Rightarrow ng$-dimensional variety over $\mathbb{F}_p$.

(in mathematical terms: do Weil descent on $\mathbb{F}_p$)

Geometric construction II

Trace condition (broken down to this g-dimensional variety over $\mathbb{F}_p$) cuts out subvariety $\mathcal{G}$

- $\mathcal{G}$ isomorphic to G (as groups)
- $\dim \mathcal{G} = g(n-1)$.
- group size computable from $P(T)$

$$\#\mathcal{G} = \#G \sim \#\mathbf{Cl}(C/\mathbb{F}_{p^n})/\#\mathbf{Cl}(C/\mathbb{F}_p) \sim p^{(n-1)g}$$

Security – Idea

Look for curves over $\mathbb{F}_p$ with Jacobian a subvariety of this $g(n-1)$ dimensional variety $\Rightarrow$ if it has too small genus then this is susceptible to attacks.

Example:

For $g = 1, n = 3$ one could find $J_{\tilde{C}}$ such that $\mathcal{G} \subseteq J_{\tilde{C}}$. By comparing sizes we get genus$(\tilde{C}) \geq 2 \Rightarrow$ security at least p – same as with classical squareroot-attacks (rho, kangaroo, baby-step-giant-step)

Results

(Diem/Scholten 03, building on Howe).

- $g = 2, n = 3$: one can easily exclude resulting genus $g < 5$, by checking that there are no points of order 3 over $\mathbb{F}_{p^2}$ (the quadratic extension field).
- $g = 1, n = 5$: same, look for 5-torsion points
- ($g = 1, n = 7$: family of curves of genus 8, not proposed)

Representations $g = 2$

(Interesting from mathematics point of view, necessary for implementations using explicit formulae)

Theorem

Put $g = 2, n = 3$. *Let* $2, 3 \nmid \#\mathbf{Cl}(C/\mathbb{F}_{p^3})$. *The nontrivial elements in the subgroup of order* l *of the trace zero variety* G *are the divisor classes represented by*

$$P_1 + P_2 - 2\infty \notin \mathrm{Div}(C/\mathbb{F}_p)^0,$$

where $P_1 \neq P_2, \sigma(P_2), \sigma^2(P_2)$.

Scalar multiples in G

Frobenius endomorphism satisfies characteristic polynomial

$P(T) = T^2 + a_1 T + p$ resp. $P(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 p T + p^2$

and trace relation

$$T^2 + T + 1 \text{ resp. } T^4 + T^3 + T^2 + T + 1.$$

Instead of computing mD for $0 \leq m < l$, $l \sim p^{(n-1)g}$ group oder $\langle D \rangle \subseteq G$ use

$$r_0 D + \cdots + r_{n-2} \sigma(D), \ |r_i| \sim \sqrt[n]{m}.$$

and (pairwise) Joint Sparse Form (JSF) of r_i

and/or start with random r_i.

Joint Sparse Form (JSF)

- (JSF 1) Of any three consecutive columns at least one is a zero column.
- (JSF 2) It is never the case that $u_{i,j+1}u_{i,j} = -1$.
- (JSF 3) If $u_{i,j+1}u_{i,j} \neq 0$ then $u_{1-i,j+1} = \pm 1$ and $u_{1-i,j} = 0$.

Example: $k_0 = 403, k_1 = 334$

$$\begin{array}{lcl} k_0 & = & \langle\ 1\ \ 0\ \ \text{-}1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ \text{-}1\ \rangle \\ k_1 & = & \langle\ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ \text{-}1\ \ 0\ \rangle \end{array}$$

$$\begin{array}{lcl} k_0 & = & \langle\ 1\ \ 0\ \ \text{-}1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \rangle \\ k_1 & = & \langle\ 1\ \ 0\ \ \text{-}1\ \ \text{-}1\ \ 0\ \ 1\ \ 0\ \ 0\ \ \text{-}1\ \ 0\ \rangle \end{array}$$

Avoid collisions I

(necessary when choosing random $r_i, i = 1, \ldots, g-1$)

Theorem

C elliptic curve over $\mathbb{F}_p$, $P(T) = T^2 + a_1 T + p$. D generator of subgroup of prime order l in G for $n = 3$.

$$\mathbf{r} := \min\{\frac{l}{p - a_1}, \frac{p-1}{\gcd(p-1, a_1 - 1)}\}.$$

The $\mathbf{r}^2$ classes $r_0 D + r_1 \sigma(D),\ 0 \leq r_i < \mathbf{r}$ are distinct.

Avoid collisions II

Theorem

C genus 2 hyperelliptic curve over $\mathbb{F}_p$,
$P(T) = T^4 + a_1T^3 + a_2T^2 + a_1pT + p^2$. D generator of subgroup of prime order l in G for $n = 3$.

$$\mathbf{r} := \min\left\{\left\lfloor\frac{l}{m}\right\rfloor, \frac{p^2 - a_2 + a_1}{\gcd(p^2 - a_2 + a_1, a_1p - a_2 + 1)}\right\},$$

where $m = \max\{p^2 + a_1p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1p - 1\}$.
The $\mathbf{r}^2$ classes $r_0D + r_1\sigma(D),\ 0 \le r_i < \mathbf{r}$ are distinct.

Avoid collisions III

Theorem

C elliptic curve over $\mathbb{F}_p$,
$P(T) = T^2 + a_1 T + p$, D generator of a subgroup of prime order l in G for $n = 5$.

$$\mathbf{r} := \min\left\{ \frac{l}{(1+p+|a_1|p)M}, \frac{|p^2 - a_1^2 p + a_1 p - p + 1|}{\gamma} \right\} ,$$

where

$M = \max\{|p^2 - a_1^2 p + 3a_1 p - 2p - a_1^3 + a_1^2 - a_1 + 2|, |p^2 - a_1^2 p - a_1 p + a_1^3 - a_1^2 + a_1|\}$

and $\gamma = \gcd(p^2 - a_1^2 p + a_1 p - p + 1, 2a_1 p - p - a_1^3 + a_1^2 - a_1 + 1)$.

The $\mathbf{r}^4$ classes $r_0 D + r_1 \sigma(D) + r_2 \sigma^2(D) + r_3 \sigma^3(D),\ 0 \le r_i < \mathbf{r}$ are distinct.

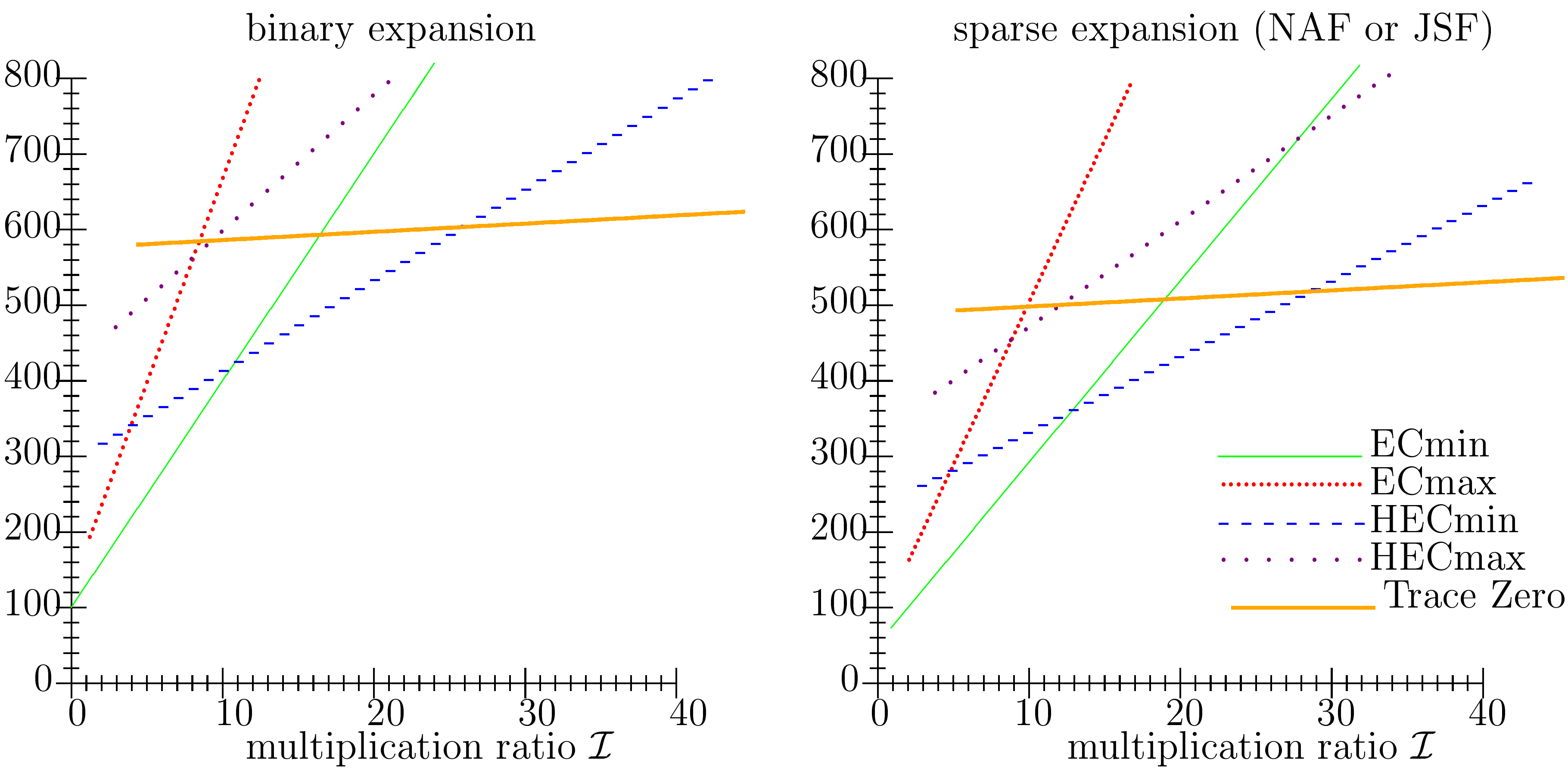
Comparison I, $g = 2, n = 3$

	Elliptic, in $\mathbb{F}_{p''}$			Genus 2, in $\mathbb{F}_{p'}$			G $(g=2)$, in $\mathbb{F}_p$		
	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.
Add.	1	1	2	1	3	22	1	21	141
Doub.	1	2	2	1	5	22	1	33	141
m-fold	6λ	10λ	12λ	6λ	26λ	132λ	3.5λ	97.5λ	501.5λ
NAF/ JSF	4.8λ	8.8λ	9.6λ	4.8λ	22.4λ	105.6λ	3λ	87λ	423λ

using efficient arithmetic in $\mathbb{F}_{p^3}$

(NAF includes same number of precomputations)

Comparison ($g = 2, n = 3$, worst case!)



Implementation – very preliminary ...

(Joint work with R. Avanzi)

bits		$E/\mathbb{F}_{p'}$, $g=1$	$\mathbf{Cl}(C/\mathbb{F}_{p''})$, $g=2$	$G, n=3$, $g=1$	$G, n=5$, $g=1$	$G, n=3$, $g=2$
160	unsig.	1,6ms	1,71ms	1,48ms	1,3ms	3,18ms
	prec.			1,38ms	1,22ms	2,98ms
192	unsig.	2ms	2,1ms	1,94ms	1,76ms	3,7ms
	prec.			1,86ms	1,68ms	3,3ms
256	unsig.	–	4,4ms	4,3ms	2,74ms	5,86ms
	prec.			3,96ms	2,6ms	5,38ms