Trace-Zero Subvariety for Cryptosystems

Tanja Lange

ITSC - Information-Security
and Cryptography

Ruhr-University of Bochum
lange@itsc.ruhr-uni-bochum.de

04.06.2002

Group G suitable

1. scalar multiplication is fast,
   $\Rightarrow$ key-exchange is fast

2. group order can be computed efficiently,
   (avoid Chinese remaindering, ...)

3. discrete logarithm problem is computationally hard,

4. representation is easy and compact.

Examples (group)

1. Diffie, Hellman (1976): $G = \mathbf{F}_p^*$, i.e.

$$G = \{\, 1,\, 2,\, \ldots,\, p-1 \}$$

2. $G = \mathbf{F}_q^*$, $q = p^l$

3. Miller/Koblitz (1985): $G = E(\mathbf{F}_q)$, i.e.

$$G = \{\, (x, y) \in \mathbf{F}_q^2 \;:\; y^2 = x^3 + ax + b \,\} \cup \{\, \infty \,\}$$

4. **Koblitz** (1989): $G = \mathbf{Cl}(C/\mathbf{F}_q)$, ideal class group of a **hyperelliptic** curve C over $\mathbf{F}_q$

Hyperelliptic Curve

$$C : v^2 + h(u)v = f(u)$$

$h(u), f(u) \in \mathbf{F}_q[u]$, q prime power

f monic, $\deg f = 2g + 1, \deg h \leq g$

nonsingular, i. e. not both partial derivatives zero for $(x, y) \in C/\bar{\mathbf{F}}_q$

C **hyperelliptic curve of genus** g

(elliptic curves are curves of genus 1)

Group

Points do **not** form a group

use **ideal class group** $\mathrm{Cl}(C/\mathbf{F}_q)$ of $\mathbf{F}_q[x,y]/(C)$.

Elements D represented by two polynomials

$$D = [a(u), b(u)]; a, b \in \mathbf{F}_{q^n}[u],$$

$\deg b < \deg a \leq g, \quad a | b^2 + bh - f.$

$\Rightarrow$ compact representation

Background

Divisor of degree 0

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

ideal class group isomorphic to **divisor class group**

$$\mathrm{Pic}^0(C/\mathbf{F}_{q^n}) = Div^0(\mathbf{F}_{q^n})/P(\mathbf{F}_{q^n})$$

class represented by degree zero divisor with $m \le g$

isomorphic to Jacobian – g-dimensional abelian variety over $\mathbf{F}_q$

Weil descent

Example elliptic curve

$$y^2 = x^3 + Ax + B \text{ over } \mathbf{F}_{q^n} = \mathbf{F}_q[\alpha]$$

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 $\alpha \Rightarrow n$-dimensional variety over $\mathbf{F}_q$.

in general do this with Jacobian $\Rightarrow n \cdot g$-dimensional variety over $\mathbf{F}_q$.

Trace-zero subvariety G I

genus 1 or 2 curve defined over $\mathbf{F}_p$, considered over F_{p^3}

$$D \in G \Leftrightarrow D \in \mathbf{Cl}(C/\mathbf{F}_{p^3}) \text{ and } D + \sigma(D) + \sigma^2(D) = 0,$$

σ Frobenius endomorphism, satisfies characteristic polynomial

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

$$D = [x^m + \sum_{i=0}^{m-1} u_i x^i, \sum_{i=0}^{m-1} v_i x^i] \Rightarrow \sigma(D) = [x^m + \sum_{i=0}^{m-1} u_i^p x^i, \sum_{i=0}^{m-1} v_i^p x^i]$$

Trace-zero subvariety G II

dimension 2g, group size from $P(T)$,

$$\#G \sim \#\mathrm{Cl}(C/\mathbf{F}_{p^3})/\#\mathrm{Cl}(C/\mathbf{F}_p) \sim p^{2g}$$

elements $[1,0]$ and $[u,v]$, $\deg u = 2$,

for corresponding points

Theorem 1 *Let* $2,3 \not| \; l|\#\mathrm{Cl}(C/\mathbf{F}_{p^3})$. *Then the nontrivial elements in the subgroup of order* l *of the trace zero variety* G *are the divisor classes represented by*

$$P_1 + P_2 - 2\infty,$$

where $P_1 \neq P_2, \sigma(P_2), \sigma^2(P_2)$ *and not both* $P_1, P_2 \in C(\mathbf{F}_p)$.

Arithmetic in $\mathrm{Cl}(C/\mathbf{F}_q)$

hyperelliptic curve, genus 2 (Takahashi)

addition:	1 I, 2 S, 23 M
doubling:	1 I, 5 S, 22 M

in $\mathbf{F}_q$.

On general elliptic curve

addition:	1 I, 1 S, 1 M
doubling:	1 I, 2 S, 1 M

in $\mathbf{F}_{q'}$. For equal group-size $q' \sim q^2$.

Do better in G

instead of computing mD for $0 \le m < l$, $l \sim p^{2g}$ group oder $\langle D \rangle \subseteq G$ use

$$r_0 D + r_1 \sigma(D),\ |r_i| \sim \sqrt{m}.$$

simultaneously scan bits of r_0 and r_1.

$$\begin{aligned} r_0 &= 10011100\ldots 00110 \\ r_1 &= 01110010\ldots 00000 \end{aligned}$$

use $D + \sigma(D) = -\sigma^2(D)$

binary expansions density 3/4
Joint Sparse Form (JSF) (digits $\in \{0, \pm 1\}$) density 1/2

Avoid collisions

Theorem 2 *C elliptic curve over $\mathbf{F}_p$, $P(T) = T^2 + a_1 T + p$. D generator of subgroup of prime order l in trace zero variety G.*

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

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

Theorem 3 *C genus 2 hyperelliptic curve over $\mathbf{F}_p$, $P(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 p T + p^2$. D generator of subgroup of prime order l in trace zero variety G.*

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

where $m = \max\{p^2 + a_1 p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1 p - 1\}$.
The $\mathbf{r}^2$ classes $r_0 D + r_1 \sigma(D)$, $0 \le r_i < \mathbf{r}$ are distinct.

Arithmetic in $\mathbb{F}_{p^3}$ I

$(b_2\xi^2 + b_1\xi + b_0)(c_2\xi^2 + c_1\xi + c_0) =$
$(b_1c_1 + (b_0 + b_2)(c_0 + c_2) - b_0c_0 - b_2c_2)\xi^2 + ((b_0 + b_1)(c_0 + c_1) -$
$b_0c_0 - b_1c_1 + b_2c_2\alpha)\xi$
$+ b_0c_0 + ((b_1 + b_2)(c_1 + c_2) - b_1c_1 - b_2c_2)\alpha.$

$\Delta = b_2^3\alpha^2 + b_1^3\alpha + b_0^3 - 3b_0b_1b_2\alpha.$
$\Rightarrow (b_2\xi^2 + b_1\xi + b_0)^{-1} =$
$((b_1^2 - b_2b_0)\xi^2 + (b_2^2\alpha - b_1b_0)\xi + b_0^2 - b_2b_1\alpha)/\Delta.$

Arithmetic in $\mathbf{F}_{p^3}$ II

	i	s	m
M			6(8)
S		6	(2)
I	1	3(2)	9(12)

Arithmetic in G

addition: 153 (206)m, 9 (8)s, 1i
doubling: 141 (198)m, 33 (32)s, 1i

in $\mathbf{F}_p$

Comparison

	Elliptic, in $\mathbf{F}_{p''}$			Genus 2, in $\mathbf{F}_{p'}$			G, in $\mathbf{F}_p$		
	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.	Inv.	Sqr.	Mult.
Add.	1	1	2	1	2	23	1	9	153
Doub.	1	2	2	1	5	22	1	33	141
m-fold	6λ	10λ	12λ	6λ	24λ	134λ	3.5λ	79.5λ	517.5λ
NAF	4.8λ	8.8λ	9.6λ	4.8λ	21.6λ	106.6λ	3λ	75λ	435λ

Timings

so far only ....

Comparison in clock-cycles

Elliptic Curve	5722
Genus 2 Curve	9267
Trace-Zero Group	7413

using high level GMP v 4.0.1