Edwards coordinates for elliptic curves, part 1

Tanja Lange

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

joint work with Daniel J. Bernstein

19.10.2007

Discrete logarithm systems

Real world applications such as e-voting or digital signatures often apply discrete logarithm systems as a primitive.

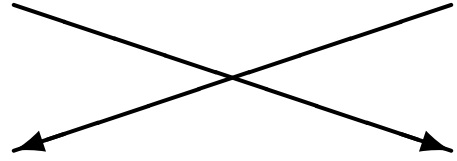
The discrete logarithm problem is the problem of finding a secret scalar, namely:

- given a group G generated by some P
- and a *scalar multiple* $Q = [n]P$ of P
- find n (modulo $\ell = \mathrm{ord}(P)$, the order of P).

n is called the Discrete Logarithm of Q to base P.

Within this talk, groups are written additively with group operation $P \oplus Q$ and $[n]P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n \text{ copies}}$.

Diffie-Hellman Key exchange

Alice		**B**ob
1. secretly generates $a < \|\langle P \rangle\|$		1. secretly generates $b < \|\langle P \rangle\|$
2. computes $Q_1 = [a]P$		2. computes $Q_2 = [b]P$
3. transmits Q_1		3. transmits Q_2
4. computes $[a]Q_2$	$= [ab]P =$	4. computes $[b] \cdot Q_1$

Common Key: the group element $k = [(ab)]P \in G$.

Proposed groups

- $\mathbb{F}_p^*$, multiplicative group of prime field.
- $\mathbb{F}_q^*$ (same for arbitrary finite field).
- $E(\mathbb{F}_q)$, group of $\mathbb{F}_q$-rational points on elliptic curve E.
- $\mathrm{Pic}_C^0(\mathbb{F}_q)$, divisor class group of curve C over $\mathbb{F}_q$.

Difference in security:

- First two examples have algorithms subexponential in q

$$O(\exp(c(\log q)^{1/3}(\log\log q)^{2/3})),$$

- for elliptic and small genus hyperelliptic curves the best algorithms are exponential in group size l

$$\Theta(\exp((1/2)\log l)) = \Theta(l^{1/2}).$$

This talk is about elliptic curve cryptography . . .

This talk is about elliptic curve cryptography . . . forget everything you know about elliptic curves.

This talk is about elliptic curve cryptography . . . forget everything you know about elliptic curves.

Or save it

```
>mv elliptic_curve obsolete/Weierstrass_form
```

Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.

$$\{(x, y) \in k \times k | x^2 + y^2 = 1\}$$

Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.

$$\{(x, y) \in k \times k | x^2 + y^2 = 1\}$$

is a commutative group with
$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$, where

$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2.$$

- Polar coordinates and trigonometric identities readily show that the result is on the curve.
- Associativity of the addition boils down to associativity of addition of angles.
- Look, an addition law!
- But it's not elliptic; index calculus work efficiently.

Now add on an elliptic curve

An elliptic curve:

Now add on an elliptic curve

An elliptic curve:

$$x^2 + y^2 = a^2(1 + x^2y^2)$$

Now add on an elliptic curve

Let k be a field with $2 \neq 0$ and let $a \in k$ with $a^5 \neq a$.
There is an – almost everywhere defined – operation on the set

$$\{(x, y) \in k \times k | x^2 + y^2 = a^2(1 + x^2y^2)\}$$

as

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$$

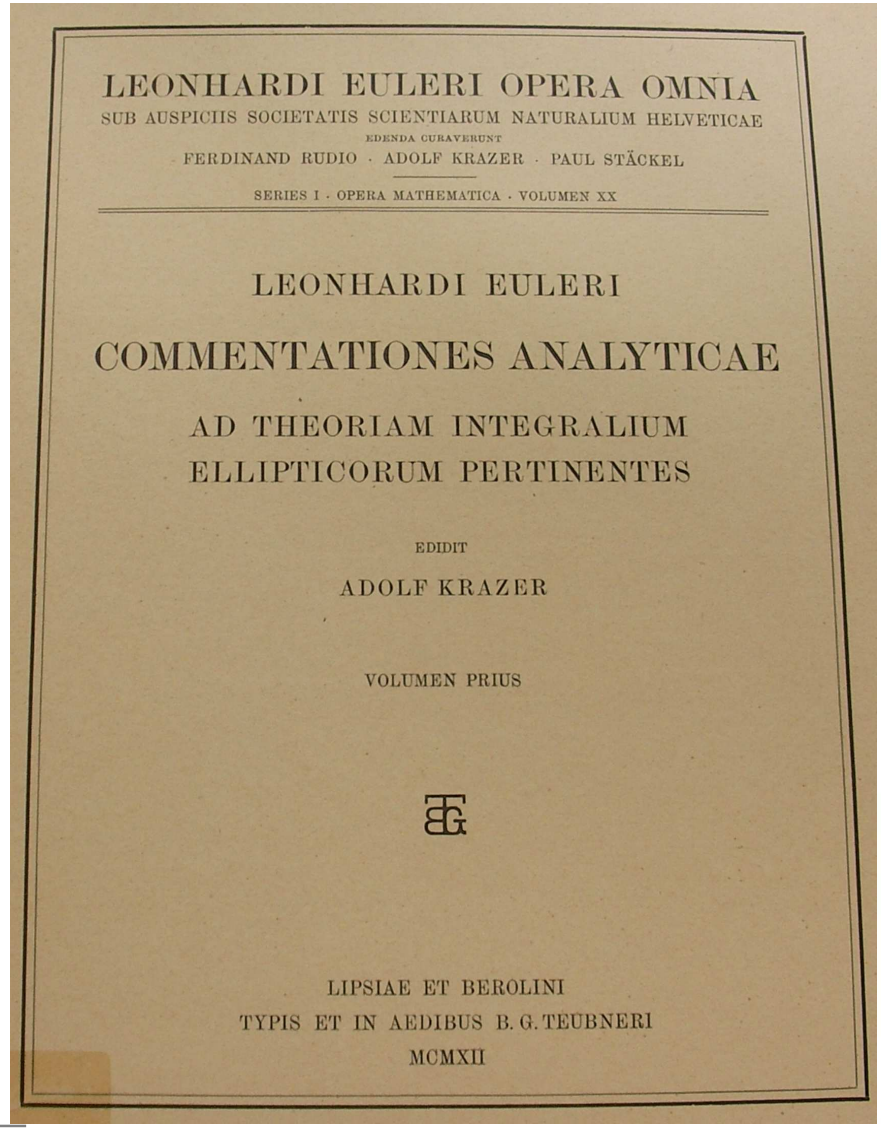
defined by the Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{a(1 + x_1x_2y_1y_2)} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)}.$$

Numerators like in addition on circle!

Where do these curves come from?

Long, long ago . . .



LEONHARDI EULERI OPERA OMNIA

SUB AUSPICIIS SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE

EDENDA CURAVERUNT

FERDINAND RUDIO · ADOLF KRAZER · PAUL STÄCKEL

SERIES I · OPERA MATHEMATICA · VOLUMEN XX

LEONHARDI EULERI

COMMENTATIONES ANALYTICAE

AD THEORIAM INTEGRALIUM
ELLIPTICORUM PERTINENTES

EDIDIT

ADOLF KRAZER

VOLUMEN PRIUS

LIPSIAE ET BEROLINI
TYPIS ET IN AEDIBUS B. G. TEUBNERI
MCMXII

Euler 1761

" Observationes de Comparatione Arcuum Curvarum Irrectificabilium"

I. DE ELLIPSI

1. Sit quadrans ellipticus ABC (Fig. 1), cuius centrum in C, eiusque semiaxes ponantur $CA=1$ et $CB=c$; sumta ergo abscissa quacunque $CP=x$ erit applicata ei respondens $PM=y=c\sqrt{(1-xx)}$; cuius differentiale cum sit $dy=-\frac{cxdx}{\sqrt{(1-xx)}}$, erit abscissae $CP=x$ arcus ellipticus respondens

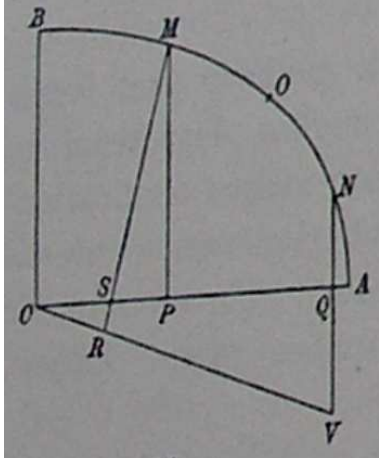


Fig. 1.

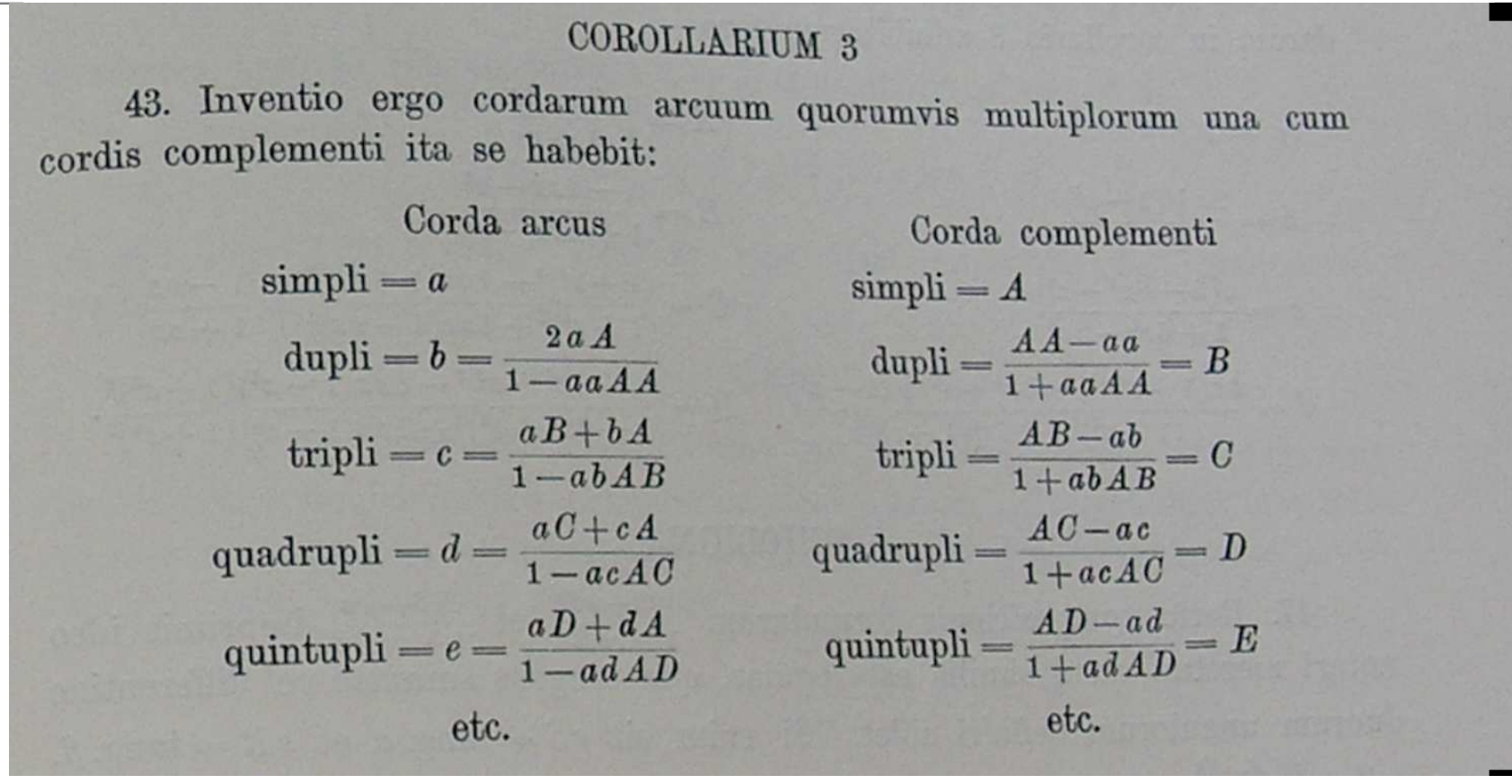
$$BM=\int\frac{dx\sqrt{(1-(1-cc)xx)}}{\sqrt{(1-xx)}}.$$

Ponatur brevitatis gratia $1-cc=n$, ut sit arcus

$$BM=\int dx\sqrt{\frac{1-nxx}{1-xx}},$$

$$\frac{1}{y^2}=\frac{1-nx^2}{1-x^2}\Leftrightarrow x^2+y^2=1+nx^2y^2.$$

Euler 1761



COROLLARIUM 3

43. Inventio ergo cordarum arcuum quorumvis multiplorum una cum cordis complementi ita se habebit:

Corda arcus	Corda complementi
simpli $= a$	simpli $= A$
dupli $= b = \frac{2aA}{1-aaAA}$	dupli $= \frac{AA-aa}{1+aaAA} = B$
tripli $= c = \frac{aB+bA}{1-abAB}$	tripli $= \frac{AB-ab}{1+abAB} = C$
quadrupli $= d = \frac{aC+cA}{1-acAC}$	quadrupli $= \frac{AC-ac}{1+acAC} = D$
quintupli $= e = \frac{aD+dA}{1-adAD}$	quintupli $= \frac{AD-ad}{1+adAD} = E$
etc.	etc.

Euler gives doubling and (special) addition for (a, A) on $a^2 + A^2 = 1 - a^2A^2$.

Gauss, posthumously

ELEGANTIORES INTEGRALIS $\int \frac{dx}{\sqrt{(1-x^4)}}$ PROPRIETATES.

[2.]

$1 = ss + cc + sscc$ sive $2 = (1+ss)(1+cc) = (\frac{1}{ss}-1)(\frac{1}{cc}-$

$$s = \sqrt{\frac{1-cc}{1+cc}}, \qquad c = \sqrt{\frac{1-ss}{1+ss}}$$

$$\sin \operatorname{lemn}(a \pm b) = \frac{sc' \pm s'c}{1 \mp scs'c'}$$

$$\cos \operatorname{lemn}(a \pm b) = \frac{cc' \mp ss'}{1 \pm ss'cc'}$$

$\sin \operatorname{lemn}(-a) = -\sin \operatorname{lemn} a$, $\cos \operatorname{lemn}(-a) = \cos \operatorname{lemn} a$

$\sin \operatorname{lemn} k\varpi = 0$ $\quad \sin \operatorname{lemn}(k+\frac{1}{2})\varpi = \pm 1$

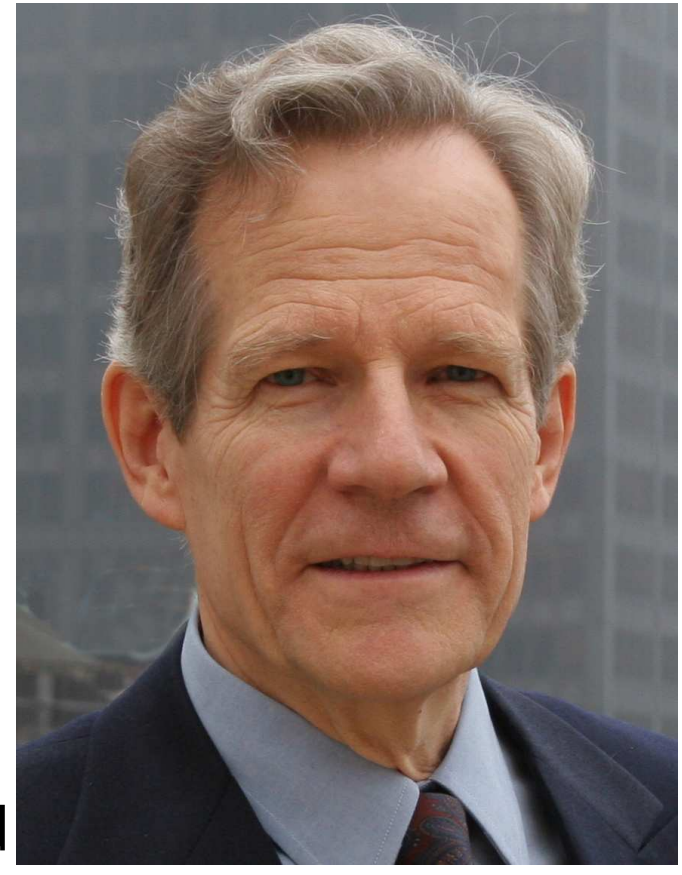
$\cos \operatorname{lemn} k\varpi = \pm 1$ $\quad \cos \operatorname{lemn}(k+\frac{1}{2})\varpi = 0$

Gauss gives general addition for arbitrary points on

$$1 = s^2 + c^2 + s^2c^2.$$

Ex uno plura

- Harold M. Edwards, Bulletin of the AMS, **44**, 393–422, 2007 $x^2 + y^2 = a^2(1 + x^2y^2), a^5 \neq a$ describes an elliptic curve.
- Every elliptic curve can be written in this form – over some extension field.
- Ur-elliptic curve
  $$x^2 + y^2 = 1 - x^2y^2$$
  needs $\sqrt{-1} \in k$ transform.
- Edwards gives above-mentioned addition law for this generalized form, shows equivalence with Weierstrass form, proves addition law, gives theta parameterization . . .



Edwards curves over finite fields

- We do not necessarily have $\sqrt{-1} \in k$! The example curve $x^2 + y^2 = 1 - x^2y^2$ from Euler and Gauss is not always an Edwards curve.
- Solution: change the definition of Edwards curves.
- Introduce further parameter d to cover more curves

$$x^2 + y^2 = c^2(1 + dx^2y^2),\ c, d \neq 0, dc^4 \neq 1.$$

- At least one of c, d small: if $c^4d = \bar{c}^4\bar{d}$ then $x^2 + y^2 = c^2(1 + dx^2y^2)$ and $x^2 + y^2 = \bar{c}^2(1 + \bar{d}x^2y^2)$ isomorphic.
  We can always choose $c = 1$ (and do so in the sequel).
- $\bar{c}^4\bar{d} = (c^4d)^{-1}$ gives quadratic twist (might be isomorphic).

Addition on Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

- Neutral element is

Addition on Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

- Neutral element is $(0, 1)$, this is an affine point!

Addition on Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_1, y_1) =$

Addition on Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_1, y_1) = (-x_1, y_1)$.

Addition on Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_1, y_1) = (-x_1, y_1)$.
- $(0, -1)$ has order 2, $(\pm 1, 0)$ have order 4,
  so not every elliptic curve can be transformed to an Edwards curve over k — but every curve with a point of order 4 can!
- Our Asiacrypt 2007 paper makes explicit the birational equivalence between a curve in Edwards form and in Weierstrass form.
  (And contains basically all results of this talk.)

Nice features of the addition law

- $P \oplus Q = \left(\dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$

Nice features of the addition law

- $P \oplus Q = \left(\dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\dfrac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \dfrac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$

Nice features of the addition law

- $P \oplus Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$
- No reason that the denominators should be 0.
- Addition law also works for doubling (compare that to your version in `obsolete/Weierstrass_form`!)
- Explicit formulas for addition/doubling:

Nice features of the addition law

- $P \oplus Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$
- No reason that the denominators should be 0.
- Addition law also works for doubling (compare that to your version in `obsolete/Weierstrass_form`!)
- Explicit formulas for addition/doubling:

$$\begin{aligned} A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2; \\ E &= (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D;\ F = d \cdot C \cdot D; \\ X_{P \oplus Q} &= A \cdot E \cdot (B - F);\ Y_{P \oplus Q} = A \cdot (D - C) \cdot (B + F); \\ Z_{P \oplus Q} &= (B - F) \cdot (B + F). \end{aligned}$$

Nice features of the addition law

- $P \oplus Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$
- No reason that the denominators should be 0.
- Addition law also works for doubling (compare that to your version in `obsolete/Weierstrass_form`!)
- Explicit formulas for addition/doubling:

$$\begin{aligned} A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2; \\ E &= (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D;\ F = d \cdot C \cdot D; \\ X_{P \oplus Q} &= A \cdot E \cdot (B - F);\ Y_{P \oplus Q} = A \cdot (D - C) \cdot (B + F); \\ Z_{P \oplus Q} &= (B - F) \cdot (B + F). \end{aligned}$$

Needs 10M + 1S + 1D + 7A.

Strongly unified group operations

- Addition formulas work also for doubling.
- Retrieve from `obsolete/Weierstrass_form` the equation $y^2 = x^3 + a_4x + a_6$, addition involves computation

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2, \\ (3x_1^2 + a_4)/(2y_1) & \text{else.} \end{cases}$$

  division by zero if first form is accidentally used for doubling.
- Strongly unified addition laws remove some checks from the code.
- Help against simple side-channel attacks. Attacker sees uniform sequence of identical group operations, no information on secret scalar given (assuming the field operations are handled appropriately).

Unified Projective coordinates

- Brier, Joye 2002
  Idea: unify how the slope is computed.
- improved in Brier, Déchène, and Joye 2004
- $$\lambda = \frac{(x_1+x_2)^2 - x_1x_2 + a_4 + y_1 - y_2}{y_1 + y_2 + x_1 - x_2}$$
  $$= \begin{cases} \frac{y_1-y_2}{x_1-x_2} & (x_1,y_1) \neq \pm(x_2,y_2) \\ \frac{3x_1^2+a_4}{2y_1} & (x_1,y_1) = (x_2,y_2) \end{cases}$$

  Multiply numerator & denominator by $x_1 - x_2$ to see this.
- Proposed formulae can be generalized to projective coordinates.
- Some special cases may occur, but with very low probability, e. g. $x_2 = y_1 + y_2 + x_1$. Alternative equation for this case.

Jacobi intersections

- Chudnovsky and Chudnovsky 1986; Liardet and Smart CHES 2001
- Elliptic curve given as intersection of two quadratics

$$s^2 + c^2 = 1 \text{ and } as^2 + d^2 = 1.$$

- Points $(S : C : D : Z)$ with $(s, c, d) = (S/Z, C/Z, D/Z)$.
- Neutral element is $(0, 1, 1)$.

$$\begin{aligned} S_3 &= (Z_1C_2 + D_1S_2)(C_1Z_2 + S_1D_2) - Z_1C_2C_1Z_2 - D_1S_2S_1D_2 \\ C_3 &= Z_1C_2C_1Z_2 - D_1S_2S_1D_2 \\ D_3 &= Z_1D_1Z_2D_2 - aS_1C_1S_2C_2 \\ Z_3 &= Z_1C_2^2 + D_1S_2^2. \end{aligned}$$

- Unified formulas need 13M + 2S + 1D.

Jacobi quartics

- Billet and Joye AAECC 2003

$$E_J : Y^2 = \epsilon X^4 - 2\delta X^2 Z^2 + Z^4.$$

$$\begin{aligned} X_3 &= X_1 Z_1 Y_2 + Y_1 X_2 Z_2 \\ Z_3 &= (Z_1 Z_2)^2 - \epsilon (X_1 X_2)^2 \\ Y_3 &= (Z_3 + 2\epsilon (X_1 X_2)^2)(Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2) + \\ &\quad 2\epsilon X_1 X_2 Z_1 Z_2 (X_1^2 Z_2^2 + Z_1^2 X_2^2). \end{aligned}$$

- Unified formulas need 10M+3S+D+2E
- Can have ϵ or δ small
- Needs point of order 2; for $\epsilon = 1$ the group order is divisible by 4.
- Some recent speed ups due to Duquesne and to Hisil, Carter, and Dawson.

Hessian curves

$$E_H : X^3 + Y^3 + Z^3 = cXYZ.$$

Addition: $P \neq \pm Q$	Doubling $P = Q \neq -P$
$X_3 = X_2Y_1^2Z_2 - X_1Y_2^2Z_1$	$X_3 = Y_1(X_1^3 - Z_1^3)$
$Y_3 = X_1^2Y_2Z_2 - X_2^2Y_1Z_1$	$Y_3 = X_1(Z_1^3 - Y_1^3)$
$Z_3 = X_2Y_2Z_1^2 - X_1Y_1Z_2^2$	$Z_3 = Z_1(Y_1^3 - X_1^3)$

- Curves were first suggested for speed
- Joye and Quisquater show

$$[2](X_1 : Y_1 : Z_1) = (Z_1 : X_1 : Y_1) \oplus (Y_1 : Z_1 : X_1)$$

- Unified formulas need 12M.
- Doubling is done by an addition, but not automatically – only unified, not strongly unified.

Unified addition law

- Unified formulas introduced as countermeasure against side-channel attacks – but useful in general.
- Strongly unified addition laws indeed remove the check for $P \neq Q$ before addition.
- Some systems allow to omit the check $P \neq -Q$ before addition.
- Most systems still have exceptional cases.
- No surprise:
  "The smallest cardinality of a complete system of addition laws on E equals two."
  (Theorem 1 in Wieb Bosma, Hendrik W. Lenstra, Jr., J. Number Theory **53**, 229–240, 1995)
- Bosma/Lenstra give such system; similar to unified projective coordinates.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Intuitive explanation:
The points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ are singular. They correspond to four points on the desingularization of the curve; but those four points are defined over $k(\sqrt{d})$.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$. Write $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $dx_1^2y_1^2(x_2^2 + y_2^2) = dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$. Write $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 \end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$. Write $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 \\ &= 1 + dx_1^2y_1^2 = x_1^2 + y_1^2 \end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$. Write $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $dx_1^2y_1^2(x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$. Write $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $dx_1^2y_1^2(x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

$$\begin{aligned}(x_1 + \epsilon y_1)^2 &= x_1^2 + y_1^2 + 2\epsilon x_1y_1 = dx_1^2y_1^2(x_2^2 + y_2^2) + 2x_1y_1dx_1x_2y_1y_2 \\ &= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) = dx_1^2y_1^2(x_2 + y_2)^2.\end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$. Write $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $dx_1^2y_1^2(x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

$$(x_1 + \epsilon y_1)^2 = x_1^2 + y_1^2 + 2\epsilon x_1y_1 = dx_1^2y_1^2(x_2^2 + y_2^2) + 2x_1y_1dx_1x_2y_1y_2$$

$$= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) = dx_1^2y_1^2(x_2 + y_2)^2.$$

$x_2 + y_2 \neq 0 \Rightarrow d = ((x_1 + \epsilon y_1)/x_1y_1(x_2 + y_2))^2 \Rightarrow d = \square$

$x_2 - y_2 \neq 0 \Rightarrow d = ((x_1 - \epsilon y_1)/x_1y_1(x_2 - y_2))^2 \Rightarrow d = \square$

If $x_2 + y_2 = 0$ and $x_2 - y_2 = 0$ then $x_2 = y_2 = 0$, contradiction.

Complete addition law

- For d not a square in k, the Edwards addition law is complete, there are no exceptional cases.
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on curve.
  - Addition works to add P and P.
  - Addition works to add P and $-P$.
  - Addition just works to add P and any Q.
- Only complete addition law in the literature.
- Bosma/Lenstra strikes over quadratic extension. "Pointless exceptional divisor!"

Fastest unified addition-or-doubling formula

System	Cost of unified addition-or-doubling
Projective	11M+6S+1D; see Brier/Joye '03
Projective if $a_4 = -1$	13M+3S; see Brier/Joye '02
Jacobi intersection	13M+2S+1D; see Liardet/Smart '01
Jacobi quartic ($\epsilon = 1$)	10M+3S+1D; see Billet/Joye '01
Hessian	12M; see Joye/Quisquater '01
Edwards	10M+1S+1D

- Exactly the same formulae for doubling (no re-arrangement like in Hessian; no if-else)
- No exceptional cases if d is not a square.
- Operation counts as in Asiacrypt'07 paper.
- See EFD `hyperelliptic.org/EFD`.

What if we know that we double?

How about non-unified doubling?

$$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$

$$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$

How about non-unified doubling?

$$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$

$$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$

Use curve equation $x^2 + y^2 = 1 + dx^2y^2$.

How about non-unified doubling?

$$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$

$$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$

$$= \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)}\right)$$

How about non-unified doubling?

$$[2]P = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$

$$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$

$$= \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)}\right)$$

$$\begin{aligned} B &= (X_1 + Y_1)^2;\ C = X_1^2;\ D = Y_1^2;\ E = C + D;\ H = (c \cdot Z_1)^2; \\ J &= E - 2H;\ X_3 = c \cdot (B - E) \cdot J;\ Y_3 = c \cdot E \cdot (C - D);\ Z_3 = E \cdot \end{aligned}$$

Inversion-free version needs 3M + 4S + 6A.

Very fast doubling formulae

System	Cost of doubling
Projective	5M+6S+1D; EFD
Projective if $a_4 = -3$	7M+3S; EFD
Hessian	7M+1S; see Hisil/Carter/Dawson '07
Doche/Icart/Kohel-3	2M+7S+2D; see Doche/Icart/Kohel '06
Jacobian	1M+8S+1D; EFD
Jacobian if $a_4 = -3$	3M+5S; see DJB '01
Jacobi quartic	2M+6S+2D; see Hisil/Carter/Dawson '07
Jacobi intersection	3M+4S; see Liardet/Smart '01
Edwards	3M+4S;
Doche/Icart/Kohel-2	2M+5S+2D; see Doche/Icart/Kohel '06

- Edwards fastest for general curves, no D.
- Operation counts as in our Asiacrypt paper.

Fastest addition formulae

System	Cost of addition
Doche/Icart/Kohel-2	12M+5S+1D; see Doche/Icart/Kohel ’06
Doche/Icart/Kohel-3	11M+6S+1D; see Doche/Icart/Kohel ’06
Jacobian	11M+5S; EFD
Jacobi intersection	13M+2S+1D; see Liardet/Smart ’01
Projective	12M+2S; HECC
Jacobi quartic	10M+3S+1D; see Billet/Joye ’03
Hessian	12M; see Joye/Quisquater ’01
Edwards	10M+1S+1D

- EFD and full paper also contain costs for mixed addition (mADD) and re-additions (reADD).
- reADD: non-mixed ADD where one point has been added before and computations have been cached.

Single-scalar multiplication using NAF

System	1 DBL, 1/3 mADD
Projective	8M+6.67S+1D
Projective if $a_4 = -3$	10M+3.67S
Hessian	10.3M+1S
Doche/Icart/Kohel-3	4.33M+8.33S+2.33D
Jacobian	3.33M+9.33S+1D
Jacobian if $a_4 = -3$	5.33M+6.33S
Jacobi intersection	6.67M+4.67S+0.333D
Jacobi quartic	4.67M+7S+2.33D
Doche/Icart/Kohel-2	4.67M+6.33S+2.33D
Edwards	6M+4.33S+0.333D

For comparison: Montgomery arithmetic takes 5M+4S+1D per bit.

Signed width-4 sliding windows

These counts include the precomputations.

System	0.98 DBL, 0.17 reADD, 0.025 mADD, 0.0035 A
Projective	7.17M+6.28S+0.982D
Projective if $a_4 = -3$	9.13M+3.34S
Doche/Icart/Kohel-3	3.84M+7.99S+2.16D
Hessian	9.16M+0.982S
Jacobian	2.85M+8.64S+0.982D
Jacobian if $a_4 = -3$	4.82M+5.69S
Doche/Icart/Kohel-2	4.2M+5.86S+2.16D
Jacobi quartic	3.69M+6.48S+2.16D
Jacobi intersection	5.09M+4.32S+0.194D
Edwards	4.86M+4.12S+0.194D

Montgomery takes 5M+4S+1D per bit. Edwards solidly faster!

Inverted Edwards coordinates

- Latest news (Bernstein/Lange, to appear at AAECC 2007):
  inverted Edwards coordinates are even faster strongly unified system – but not complete.
- Using the representation $(X_1 : Y_1 : Z_1)$ for the affine point $(Z_1/X_1, Z_1/Y_1)$ ($X_1Y_1Z_1 \neq 0$) gives operation counts:
  - Doubling takes $3M + 4S + 1D$.
  - Addition takes $9M + 1S + 1D$.
- This saves $1M$ for each addition compared to standard Edwards coordinates.
- New speed leader: inverted Edwards coordinates.

Different coordinate systems

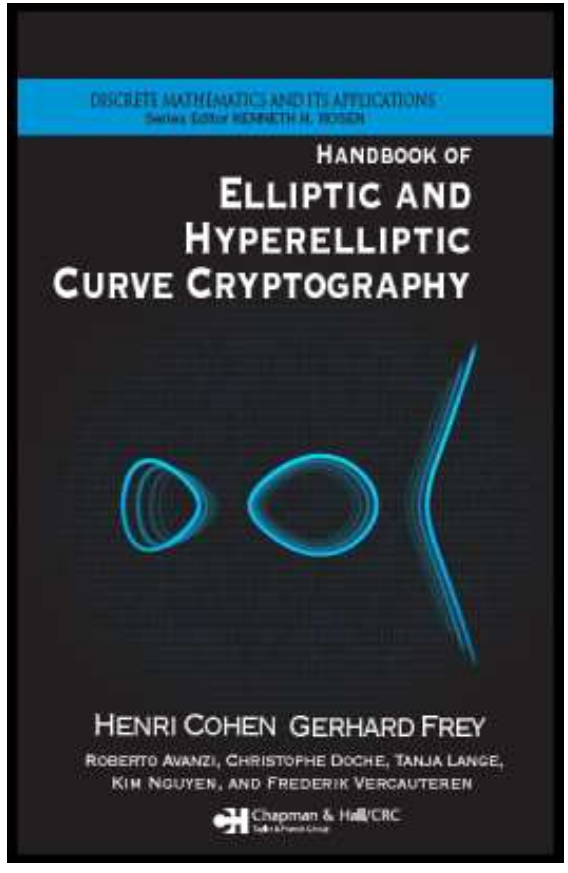
For coordinate systems we could find, the group law, operation counts (and improvements) for the explicit formulas, MAGMA-based proofs (sorry, not Pari) of their correctness, lots of entertainment visit the

Explicit Formulas Database

`http://www.hyperelliptic.org/EFD`

More halftime Advertising

Buy also Henri's "other" book! :–)



Handbook of Elliptic
and Hyperelliptic Curve Cryptography

R. Avanzi, H. Cohen, C. Doche,
G. Frey, T. Lange, K. Nguyen,
F. Vercauteren

CRC Press 2005

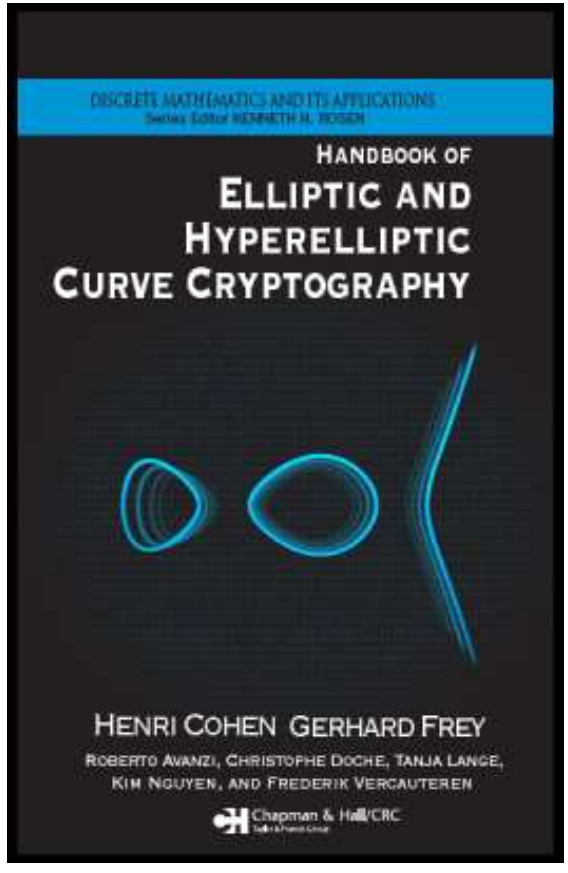
Sample chapter and more information
now available at

`www.hyperelliptic.org/HEHCC`

Please notify us about typos and omissions!

More halftime Advertising

Buy also Henri's "other" book! :–)



Handbook of Elliptic
and Hyperelliptic Curve Cryptography

R. Avanzi, H. Cohen, C. Doche,
G. Frey, T. Lange, K. Nguyen,
F. Vercauteren

CRC Press 2005

Sample chapter and more information
now available at

`www.hyperelliptic.org/HEHCC`

Please notify us about typos and omissions! (We know that the elliptic curve shape is obsolete. . .)