The EFD thing

Daniel J. Bernstein — University of Illinois at Chicago — djb@cr.yp.to

and

Tanja Lange — Technische Universiteit Eindhoven — tanja@hyperelliptic.org

and Nigel for the title

Ever found too many coordinate systems?

Which elliptic curve coordinate system

- is the fastest for addition, doubling, . . . ?

Ever found too many coordinate systems?

Which elliptic curve coordinate system

- is the fastest for addition, doubling, . . . ?
- is the slowest for addition, doubling,. . . ?

Ever found too many coordinate systems?

Which elliptic curve coordinate system

- is the fastest for addition, doubling, . . . ?
- is the fastest for re-addition?
- is the fastest for unified group operations?
- needs the fewest registers?
- is the best for single-scalar multiplication?
- is the best for multi-scalar multiplication?
- is the best for batch verification of signatures?
- etc.

. . . and which formulas are the best for a given system?

Projective Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P \oplus Q = (X_3 : Y_3 : Z_3)$
on $E : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$; $(x, y) \sim (X/Z, Y/Z)$

Addition: $P \neq \pm Q$

$A = Y_2Z_1 - Y_1Z_2, B = X_2Z_1 - X_1Z_2,$
$C = A^2Z_1Z_2 - B^3 - 2B^2X_1Z_2$
$X_3 = BC, Z_3 = B^3Z_1Z_2$
$Y_3 = A(B^2X_1Z_2 - C) - B^3Y_1Z_2,$

Doubling $P = Q \neq -P$

$A = a_4Z_1^2 + 3X_1^2, B = Y_1Z_1,$
$C = X_1Y_1B, D = A^2 - 8C$
$X_3 = 2BD, Z_3 = 8B^3$.
$Y_3 = A(4C - D) - 8Y_1^2B^2$

- No inversion is needed – good for most implementations
- General ADD: 12M+2S
- DBL: 7M+5S
- Fast . . . but very different performance of ADD and DBL

Jacobian Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P \oplus Q = (X_3 : Y_3 : Z_3)$
on $Y^2 = X^3 + a_4 X Z^4 + a_6 Z^6$; $(x, y) \sim (X/Z^2, Y/Z^3)$

Addition: $P \neq \pm Q$

$A = X_1 Z_2^2, B = X_2 Z_1^2, C = Y_1 Z_2^3,$
$D = Y_2 Z_1^3, E = B - A, F = D - C$
$X_3 = 2(-E^3 - 2AE^2 + F^2)$
$Z_3 = E(Z_1 + Z_2)^2 - Z_1^2 - Z_2^2$
$Y_3 = 2(-CE^3 + F(AE^2 - X_3)),$

Doubling $P = Q \neq -P$

$A = Y_1^2, B = Z_1^2$
$C = 4X_1 A, D = 3X_1^2 + a_4 B^2$
$X_3 = -2C + D^2$
$Z_3 = (Y_1 + Z_1)^2 - A - B$
$Y_3 = -8A^2 + D(C - X_3)$.

- General ADD: 11M+5S
- mixed ADD ($\mathcal{J} + \mathcal{A} = \mathcal{J}$): 8M+3S
- DBL: 3M+7S (one M by a_4); for $a_4 = -3$: 3M+5S

Chudnovsky Jacobian Coordinates

$P = (X_1 : Y_1 : Z_1 : Z_1^2 : Z_1^3)$, $Q = (X_2 : Y_2 : Z_2 : Z_2^2 : Z_2^3)$,
$P \oplus Q = (X_3 : Y_3 : Z_3 : Z_3^2 : Z_3^3)$ on $Y^2 = X^3 + a_4 X Z^4 + a_6 Z^6$;
$(x, y) \sim (X/Z^2, Y/Z^3)$

Addition: $P \neq \pm Q$

$A = X_1 Z_2^2, B = X_2 Z_1^2, C = Y_1 Z_2^3,$
$D = Y_2 Z_1^3, E = B - A, F = D - C$
$X_3 = 2(-E^3 - 2AE^2 + F^2)$
$Z_3 = E(Z_1 + Z_2)^2 - Z_1^2 - Z_2^2$
$Y_3 = 2(-CE^3 + F(AE^2 - X_3)),$
$Z_3^2, Z_3^3,$

Doubling $P = Q \neq -P$

$A = Y_1^2,$
$C = 4X_1 A, D = 3X_1^2 + a_4(Z_1^2)^2$
$X_3 = -2C + D^2$
$Z_3 = (Y_1 + Z_1)^2 - A - Z_1^2$
$Y_3 = -8A^2 + D(C - X_3)$
Z_3^2, Z_3^3

- General ADD: 10M+4S
- mixed ADD ($\mathcal{J} + \mathcal{A} = \mathcal{J}$): 8M+3S
- DBL: 3M+7S (one M by a_4)

. . . and with extra feature:

SCA resistance . . .

Montgomery Form

Generalized to arbitrary multiples $[n]P = (X_n : Y_n : Z_n), [m]P = (X_m : Y_m : Z_m)$ with known difference $[m-n]P$ on

$$E_M : By^2 = x^3 + Ax^2 + x$$

Addition: $n \neq m$

$$\begin{aligned} X_{m+n} &= Z_{m-n}\big((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)\big)^2, \\ Z_{m+n} &= X_{m-n}\big((X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)\big)^2 \end{aligned}$$

Doubling: $n = m$

$$\begin{aligned} 4X_nZ_n &= (X_n + Z_n)^2 - (X_n - Z_n)^2, \\ X_{2n} &= (X_n + Z_n)^2(X_n - Z_n)^2, \\ Z_{2n} &= 4X_nZ_n\big((X_n - Z_n)^2 + \big((A+2)/4\big)(4X_nZ_n)\big). \end{aligned}$$

An addition takes 4M and 2S whereas a doubling needs only 3M and 2S. Order is divisible by 4.

Side-channel atomicity

- Chevallier-Mames, Ciet, Joye 2004
  Idea: build group operation from identical blocks.
- Each block consists of:

  1 multiplication, 1 addition, 1 negation, 1 addition;

  fill with cheap dummy additions and negations

  ADD $(\mathcal{A}+\mathcal{J})$ needs 11 blocks
  DBL $(2\mathcal{J})$ needs 10 blocks

…	ADD$_9$	ADD$_{10}$	ADD$_{11}$	DBL$_1$	DBL$_2$	DBL$_3$	DBL$_4$	DBL$_5$	…

- Requires that M and S are indistinguishable from their traces.
- No protection against fault attacks.

Unified Projective coordinates

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

  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 intersection and quartic

- Liardet and Smart CHES 2001: Jacobi intersection
- Billet and Joye AAECC 2003: Jacobi-Model

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

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

- 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.

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 suggested Hessian Curves for unified group operations using

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

- Unified formulas need 12M.
- Needs point of order 3.

There is help!

Explicit-Formulas Database

`www.hyperelliptic.org/EFD`

Explicit-Formulas Database

System	Cost of doubling
Projective	5M+6S+1D; EFD
Projective if $a_4 = -3$	7M+3S; EFD
Hessian	6M+3S; see Joye/Quisquater '01
Jacobi quartic	1M+9S+1D; see Billet/Joye '01
Jacobian	1M+8S+1D; EFD
Jacobian if $a_4 = -3$	3M+5S; see DJB '01
Jacobi intersection	3M+4S; see Liardet/Smart '01
Doche/Icart/Kohel	2M+5S+2D; see Doche/Icart/Kohel '06

- All formulas human readable and computer verifiable.
- Several speed-ups only in EFD!
- Correct formulas only in EFD!
- Will extend EFD to characteristic 2 soon.

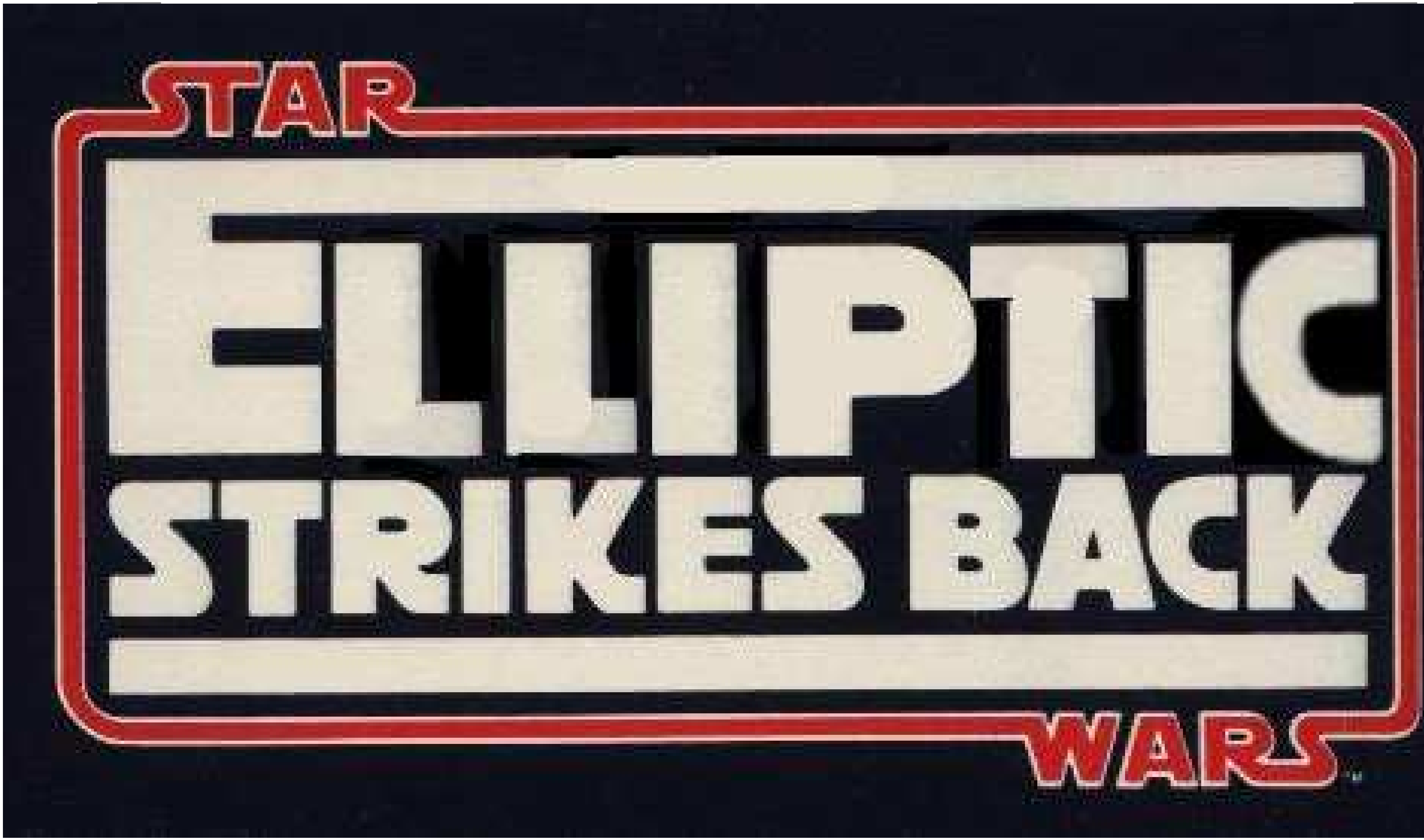
Elliptic vs Hyperelliptic

More and more papers say: Genus-2 hyperelliptic curves are better than elliptic curves!

- Special families of genus-2 curves in characteristic 2 faster than ECC.
- Generalization of Montgomery in odd characteristic
  - Gaudry: Genus-2 Montgomery-style formulas for nP in large characteristic.
  - Bernstein ECC 2006 “New Diffie-Hellman speed record” (with HECC)
  - Gaudry, ECC 2007: “Important speed-up.”
- Special base points for pairings.

Plan to include hyperelliptic curves in EFD.

But time has come . . .



Edwards curves

k field of odd characteristic.

$$x^2 + y^2 = 1 + dx^2y^2$$

is an elliptic curve for $d \neq 0, 1$.

- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{1 + d x_P x_Q y_P y_Q}, \frac{y_P y_Q - x_P x_Q}{1 - d x_P x_Q y_P y_Q} \right).$
- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.

Edwards curves

k field of odd characteristic.

$$x^2 + y^2 = 1 + dx^2y^2$$

is an elliptic curve for $d \neq 0, 1$.

- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{1 + d x_P x_Q y_P y_Q}, \frac{y_P y_Q - x_P x_Q}{1 - d x_P x_Q y_P y_Q} \right).$
- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $[2]P = \left(\frac{x_P y_P + y_P x_P}{1 + d x_P x_P y_P y_P}, \frac{y_P y_P - x_P x_P}{1 - d x_P x_P y_P y_P} \right).$

Edwards curves

k field of odd characteristic.

$$x^2 + y^2 = 1 + dx^2y^2$$

is an elliptic curve for $d \neq 0, 1$.

- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{1 + d x_P x_Q y_P y_Q}, \frac{y_P y_Q - x_P x_Q}{1 - d x_P x_Q y_P y_Q} \right).$
- Neutral element is $(0, 1)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $[2]P = \left(\frac{x_P y_P + y_P x_P}{1 + d x_P x_P y_P y_P}, \frac{y_P y_P - x_P x_P}{1 - d x_P x_P y_P y_P} \right).$
- Unified group operations!

Edwards curves

k field of odd characteristic.

$$x^2 + y^2 = 1 + dx^2y^2$$

is an elliptic curve for $d \neq 0, 1$.

- $$P + Q = \left(\frac{x_P y_Q + y_P x_Q}{1 + d x_P x_Q y_P y_Q}, \frac{y_P y_Q - x_P x_Q}{1 - d x_P x_Q y_P y_Q} \right).$$

$$\begin{aligned}
A &= Z_P \cdot Z_Q;\ B = A^2;\ C = X_P \cdot X_Q;\ D = Y_P \cdot Y_Q; \\
E &= d \cdot C \cdot D;\ F = B - E; G = B + E; \\
X_{P+Q} &= A \cdot F \cdot ((X_P + Y_P) \cdot (X_Q + Y_Q) - C - D); \\
Y_{P+Q} &= A \cdot G \cdot (D - C);\ Z_{P+Q} = F \cdot G.
\end{aligned}$$

Edwards curves

k field of odd characteristic.

$$x^2 + y^2 = 1 + dx^2y^2$$

is an elliptic curve for $d \neq 0, 1$.

- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{1 + d x_P x_Q y_P y_Q}, \frac{y_P y_Q - x_P x_Q}{1 - d x_P x_Q y_P y_Q} \right).$

$$\begin{aligned} A &= Z_P \cdot Z_Q;\ B = A^2;\ C = X_P \cdot X_Q;\ D = Y_P \cdot Y_Q; \\ E &= d \cdot C \cdot D;\ F = B - E; G = B + E; \\ X_{P+Q} &= A \cdot F \cdot ((X_P + Y_P) \cdot (X_Q + Y_Q) - C - D); \\ Y_{P+Q} &= A \cdot G \cdot (D - C);\ Z_{P+Q} = F \cdot G. \end{aligned}$$

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

Fastest unified formulae

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	10M+3S+1D; see Billet/Joye ’01
Hessian	12M; see Joye/Quisquater ’01
Edwards ($c = 1$)	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. Formulae correct for all affine inputs (incl. $(0, c)$, $P + (-P)$); formulae are complete!

Very fast doubling formulae

System	Cost of doubling
Projective	5M+6S+1D; EFD
Projective if $a_4 = -3$	7M+3S; EFD
Hessian	6M+3S; see Joye/Quisquater '01
Jacobi quartic	1M+9S+1D; see Billet/Joye '01
Jacobian	1M+8S+1D; EFD
Jacobian if $a_4 = -3$	3M+5S; see DJB '01
Jacobi intersection	3M+4S; see Liardet/Smart '01
Edwards ($c = 1$)	3M+4S;
Doche/Icart/Kohel	2M+5S+2D; see Doche/Icart/Kohel '06

- Edwards fastest for general curves, no D.

Fastest addition formulae

System	Cost of addition
Doche/Icart/Kohel	12M+5S+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 ($c = 1$)	10M+1S+1D

- Faster than Jacobian-3 etc. for single-scalar multiplication, multi-scalar multiplication, etc.
- Complete addition formulas: code-size advantage and SCA resistance.
- More at Asiacrypt 2007.