Unified addition formulae for elliptic curves

Daniel J. Bernstein | Tanja Lange (speaker)

University of Illinois at Chicago and Technische Universiteit Eindhoven

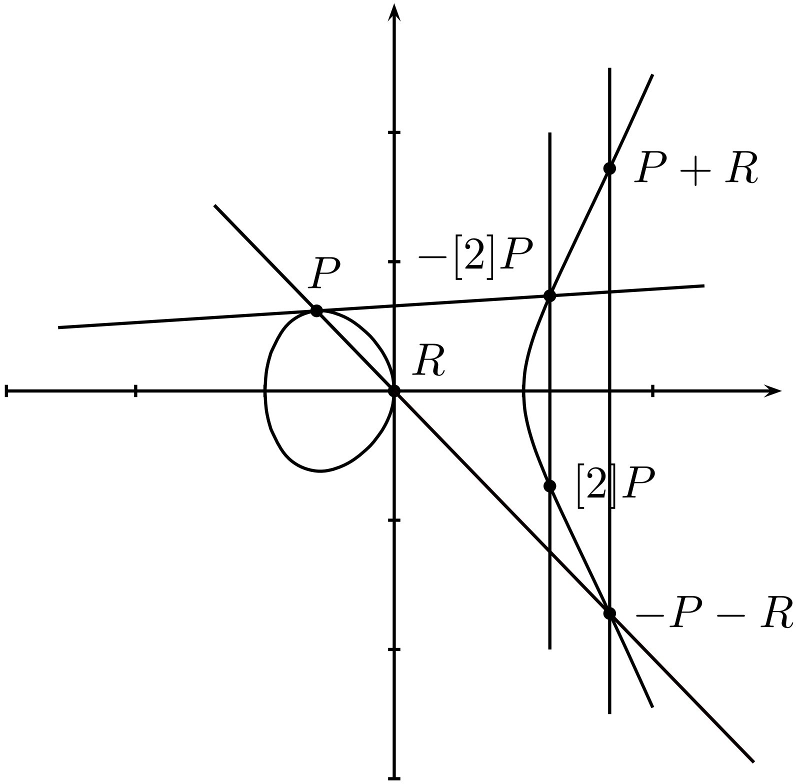
djb@cr.yp.to | tanja@hyperelliptic.org

15.04.2007

Addition on Elliptic Curves

At Mathematics: Algorithms and Proofs in Leiden, January 2007, Harold M. Edwards gave a talk on Addition on Elliptic Curves

So we expected . . .



Addition on Elliptic Curves

At Mathematics: Algorithms and Proofs in Leiden, January 2007, Harold M. Edwards gave a talk on Addition on Elliptic Curves

But there it was – the elliptic curve:

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

Addition on Elliptic Curves

At Mathematics: Algorithms and Proofs in Leiden, January 2007, Harold M. Edwards gave a talk on Addition on Elliptic Curves

But there it was – the elliptic curve:

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

Nonsingular if and only if $a^5 \neq a$.

Addition on Elliptic Curves

At Mathematics: Algorithms and Proofs in Leiden, January 2007, Harold M. Edwards gave a talk on Addition on Elliptic Curves

But there it was – the elliptic curve:

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

Nonsingular if and only if $a^5 \neq a$.
To see that this is indeed an elliptic curve, use $z = y(1 - a^2x^2)/a$ to obtain

$$z^2 = x^4 - (a^2 + 1/a^2)x^2 + 1.$$

Edwards' Addition Formulae

- $P = (x_P, y_P), Q = (x_Q, y_Q)$ on $x^2 + y^2 = a^2(1 + x^2y^2)$.
- $$P + Q = \left(\frac{x_P y_Q + y_P x_Q}{a(1 + x_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{a(1 - x_P x_Q y_P y_Q)}\right).$$
- $$\begin{aligned} [2]P &= \left(\frac{x_P y_P + y_P x_P}{a(1 + x_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{a(1 - x_P x_P y_P y_P)}\right) \\ &= \left(\frac{2x_P y_P}{a(1 + (x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{a(1 - (x_P y_P)^2)}\right). \end{aligned}$$
- For much more information on elliptic curves in this shape see Edwards 2007 paper in Bull. AMS., electronic April 9.

Why unified addition formulae?

Side Channels

Attacker can measure

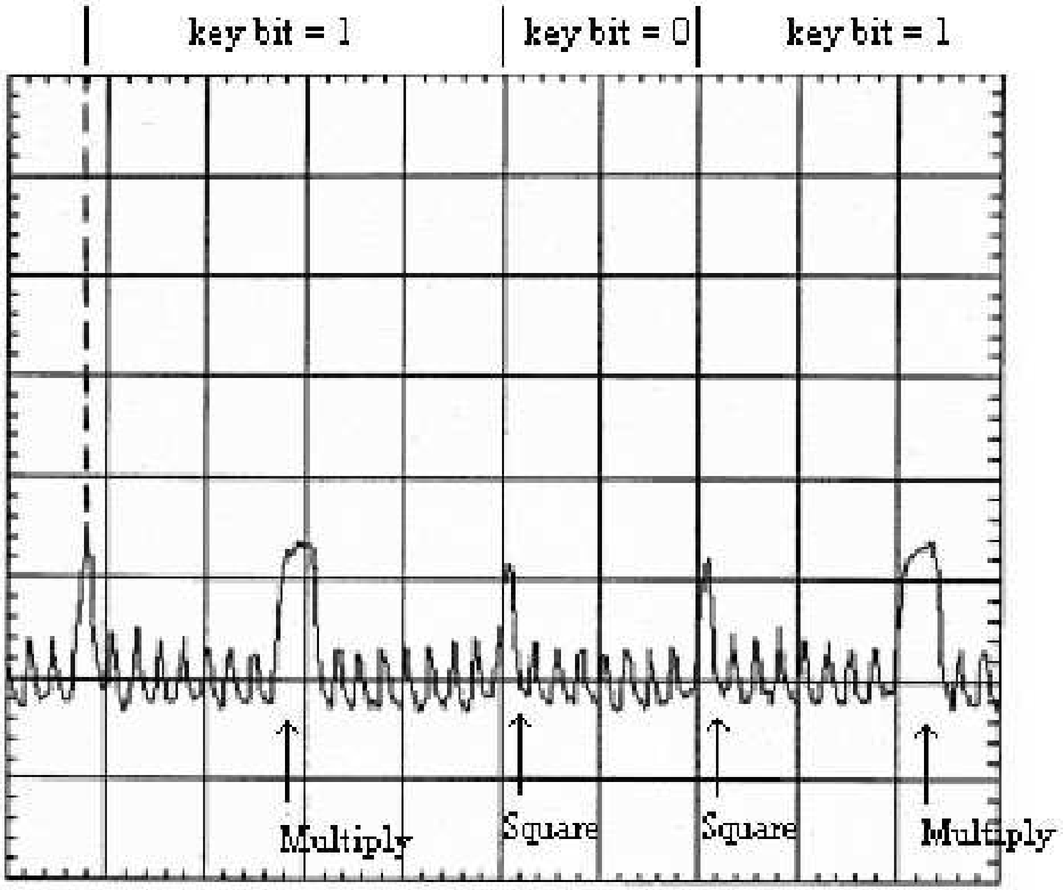
- Time to perform operations,
- Power consumption during operations,
- Electro-magnetic radiation during computation,
- Noise produced during computation.
- ...

Obviously, integer addition is cheaper than multiplication
$\Rightarrow$ needs more clock cycles, different characteristics of power trace.

Attacker might be able to reconstruct sequence of operations (power & EM) or at least learn how many of each kind were performed (timing).

Consequences

If sequence of operations depends on the secret key
and this is directly translated to the observed data, one can reconstruct the key



⇒ Simple Side-Channel Analysis (SSCA)
(often SPA= Simple Power Analysis).

(e. g. in binary square-and-multiply one has

S M S S M $\sim$ $(1101)_2 = 13$).

Scalar Multiplication – Double-and-Add

IN: $P \in E(\mathbb{F}_q)$, $n \in \mathbb{Z}$, $n = \sum_{i=0}^{l} n_i 2^i$
OUT: $Q = nP$

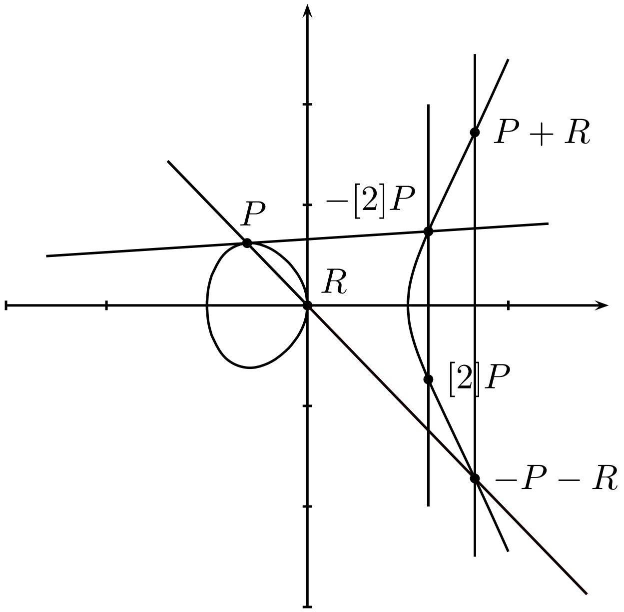
1. $Q = P$
2. for $i = l - 1$ down to 0 do
3. $\quad Q = 2Q$
4. $\quad$ if $(n_i = 1)$ then $Q = Q + P$
5. output Q

If ADD $\neq$ DBL one can easily determine n from the sequence of ADD and DBL:

DBL DBL ADD DBL ADD DBL DBL $\Leftrightarrow (101100)_2 = 44$

Weierstrass form (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



$$(x_1, y_1) + (x_2, y_2) =$$
$$= (x_3, y_3) =$$
$$= (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

where

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

$\Rightarrow$ Addition and Doubling differ considerably.

ADD: 1 I, 2M, 1S vs. DBL: 1 I, 2M, 2S

Unprotected arithmetic prone to SSCA.

Other coordinate systems

(Optimized for speed . . .

system	points	correspondence
affine ($\mathcal{A}$)	(x, y)	
projective ($\mathcal{P}$)	(X, Y, Z)	$(X/Z, Y/Z)$
Jacobian ($\mathcal{J}$)	(X, Y, Z)	$(X/Z^2, Y/Z^3)$
Chudnovsky Jacobian ($\mathcal{J}^C$)	(X, Y, Z, Z^2, Z^3)	$(X/Z^2, Y/Z^3)$
modified Jacobian ($\mathcal{J}^m$)	(X, Y, Z, aZ^4)	$(X/Z^2, Y/Z^3)$

system	addition			doubling		
affine ($\mathcal{A}$)	2M	1S	1I	2M	2S	1I
projective ($\mathcal{P}$)	12M	2S	–	7M	5S	–
Jacobian ($\mathcal{J}$)	11M	5S	–	3M	7S	–
Chudnovsky Jacobian ($\mathcal{J}^C$)	10M	4S	–	4M	7S	–
modified Jacobian ($\mathcal{J}^m$)	13M	6S	–	4M	4S	–

. . . considerably different!)

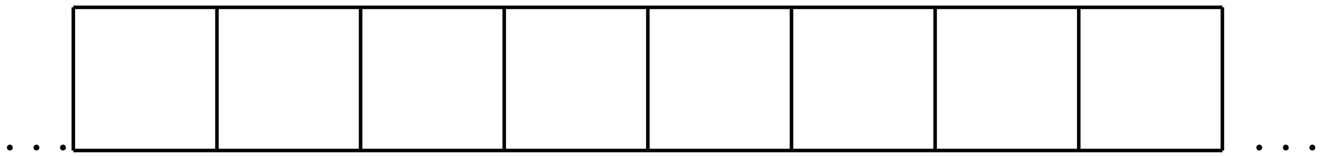
Common countermeasures

- Double-and-always-add
  very inefficient
- Side-channel atomicity (Chevallier-Mames, Ciet, Joye)
  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 $(\mathcal{A}+\mathcal{P})$ needs 11 blocks
  DBL $(2\mathcal{P})$ needs 10 blocks



- Brier and Joye, uniform Jacobian coordinates

Common countermeasures

- Double-and-always-add
  very inefficient
- Side-channel atomicity (Chevallier-Mames, Ciet, Joye)
  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 $(\mathcal{A}+\mathcal{P})$ needs 11 blocks
  DBL $(2\mathcal{P})$ needs 10 blocks

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

- Brier and Joye, uniform Jacobian coordinates

Uniform Group Operations

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

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

- Joye and Quisquater suggested Hessian Curves

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

They achieve uniformity by

$$[2](X_1 : Y_1 : Z_1) = (Z_1 : X_1 : Y_1) + (Y_1 : Z_1 : X_1)$$

and $(Z_1 : X_1 : Y_1) \neq (Y_1 : Z_1 : X_1)$.

Our contribution

Edwards form

- Slightly generalized shape:

$$E_E : x^2 + y^2 = c^2(1 + dx^2y^2)$$

  is elliptic curve for $c, d \neq 0$ and $dc^4 \neq 1$.
- Affine formulae

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

- Projective version takes

  10M + 1S + 1C + 1D + 7A,

  where C is the cost of multiplying by c, D is the cost of multiplying by d, and A abbreviates addition.

Comparison of unified formulae

System	Cost of unified addition-or-doubling
Jacobian	11M+6S+1C; see Brier/Joye '03
Jacobian if $a_4 = -1$	13M+3S; see Brier/Joye '02
Jacobi intersection	13M+2S+1C; see Liardet/Smart '01
Jacobi quartic	10M+3S+3C; see Billet/Joye '01
Hessian	12M; see Joye/Quisquater '01
This paper	10M+1S+1C

- Fastest unified addition-or-doubling formulae.
- Exactly the same formulae for doubling (no re-arrangement like in Hessian)
- No exceptional cases – affine input produces correct affine output – if d is not a square, i.e. no points with $dx_1x_2y_1y_2 = \pm 1$.

Multi-scalar multiplication I

- To compute $[n_1]P_1 + [n_2]P_2 + \cdots [n_m]P_m$ compute the doublings together, i.e. write scalars n_i in binary:

$$
\begin{array}{cccccccc}
n_1 & = & n_{1,l-1}2^{l-1} & +n_{1,l-2}2^{l-2} & +n_{1,l-3}2^{l-3} & \ldots & +n_{1,1}2 & +n_{1,0} \\
n_2 & = & n_{2,l-1}2^{l-1} & +n_{2,l-2}2^{l-2} & +n_{2,l-3}2^{l-3} & \ldots & +n_{2,1}2 & +n_{2,0} \\
\vdots & = & \vdots & \vdots & \vdots & & \vdots & \vdots \\
n_m & = & n_{m,l-1}2^{l-1} & +n_{m,l-2}2^{l-2} & +n_{m,l-3}2^{l-3} & \ldots & +n_{m,1}2 & +n_{m,0}
\end{array}
$$

- Compute as
$[2]\left([2](n_{1,l-1}P_1 + n_{2,l-1}P_2 + n_{3,l-1}P_3 + \cdots + n_{m,l-1}P_m) + \right.$
$\left.(n_{1,l-2}P_1 + n_{2,l-2}P_2 + n_{3,l-2}P_3 + \cdots + n_{m,l-2}P_m\right) + \cdots$
etc.

Multi-scalar multiplication II

- Needs many more additions than doublings, even with precomputations.
- Most coordinate systems optimized for many doublings, few additions (single scalar multiplication with windowing).
- Projective Edwards formulae offer best speed for addition and are not bad for doubling either.
- Applications in verification in accelerated ECDSA – 6 scalars.
- Applications in batch verification of signatures – many scalars – by taking random linear combinations.

The end

http://cr.yp.to/papers.html#newelliptic