

**SOME COMPUTATIONAL SPEEDUPS
AND BANDWIDTH IMPROVEMENTS
FOR CURVES OVER PRIME FIELDS**

Jerome A. Solinas

National Security Agency, Ft. Meade, MD, USA

`jasolin@orion.ncsc.mil`

ECC '01

29 October 2001

First Topic:

TWIN SCALAR MULTIPLICATION ON ELLIPTIC CURVES

- Expressions of the form $aP + bQ$ appear in elliptic curve based cryptographic protocols such as ECDSA, MQV, etc.
- We present an optimized algorithm for the elliptic curve case.

(Left-to-Right) BINARY METHOD

Evaluate aP

53 =	1	1	0	1	0	1
$\times 2$	\mathcal{O}	$2P$	$6P$	$12P$	$26P$	$52P$
$+P$	P	$3P$		$13P$		$53P$

Cost of m -bit scalar multiplication:

$\sim m$ doubles, $\sim m/2$ general additions (avg.)

ADDITION-SUBTRACTION METHOD

- Since $-(x, y) = (x, -y)$, **subtracting** a point as efficient as **adding**
- So use **signed binary expansions**

$29 =$	1	0	0	-1	0	1
$\times 2$	\mathcal{O}	$2P$	$4P$	$8P$	$14P$	$28P$
$\pm P$	P			$7P$		$29P$

NONADJACENT FORM

An optimal signed binary expansion is the NAF (no two consecutive nonzero entries).

- A NAF representation **exists** for every positive n .
- The NAF of n is **unique**.
- Easy to **calculate** NAF of n .
- NAF of n has **minimal Hamming weight** (fewest non-zero entries) among all signed binary expansions of n .
- Average Hamming density is $1/3$.

ORDINARY STRAUS-SHAMIR METHOD

$9 =$	1	0	0	1
$5 =$	0	1	0	1
$\times 2$	\mathcal{O}	$2P$	$4P + 2Q$	$8P + 4Q$
$+P$	P			
$+Q$		$2P + Q$		
$+(P + Q)$				$9P + 5Q$

Costs $\sim m$ doubles, $\sim 3m/4$ general additions (avg.)

ELLIPTIC STRAUS-SHAMIR METHOD

	1	0	0	-1	0	1	0	-1
	1	0	1	0	0	-1	0	-1
$\times 2$	\mathcal{O}	✓	✓	✓	✓	✓	✓	✓
P				-				
Q			+					
$P + Q$	+							-
$P - Q$						+		

COST OF ELLIPTIC STRAUS-SHAMIR METHOD

- ESSM uses *joint signed binary expansions*
- *Joint Hamming weight* = number of non-zero columns
- *Cost of m -bit ESSM:*
 - $\sim m$ Point Doublings, $\sim hm$ Point Additionswhere h = Joint Hamming density
(proportion of non-zero columns)
- *Problem*: find a representation with minimal h .

JOINT SPARSE FORM

Joint Sparse form = a joint signed binary expansion with:

- any 3 consecutive columns includes a zero column
- if two adjacent entries in a row are nonzero, then they are $(1 \quad 1)$ or $(-1 \quad -1)$, and the corresponding entries from the other row are $(\pm 1 \quad 0)$

Example:

1	1	0	-1	0	1	0	0	-1	0	0	1
1	0	0	0	0	-1	-1	0	1	0	1	0

JOINT SPARSE FORM: PROPERTIES

- A JS representation **exists** for every positive n_0, n_1 .
- The JS form of n_0 and n_1 is **unique**.
- Easy to **calculate** JS form of n_0 and n_1 .
- The JS form of n_0 and n_1 has **minimal joint Hamming weight** among all joint signed binary expansions of n_0 and n_1 .
- **Average joint Hamming density** is $1/2$.

ELLIPTIC STRAUS-SHAMIR METHOD

- By “the elliptic Straus-Shamir method” we mean using the JS form.
- An m -bit twin scalar multiplication via the ESSM costs $\sim m$ doublings, $\sim m/2$ general additions (*avg.*)
- Need to precompute and store the sum and difference of the two points.

APPLICATION OF ESSM TO ELLIPTIC SCALAR MULTIPLICATION

Idea: write the $2k$ -bit integer n as

$$n = a + b\lambda$$

where a, b are each k bits long. Then use ESSM to compute

$$nP = aP + bQ$$

where $Q = \lambda P$.

COST OF ESSM METHOD

- Addition-Subtraction method costs

$2k$ doubles, $2k/3$ general additions.

- ESSM method costs

k doubles, $k/2$ general additions

plus

cost of computing a and b from n

plus

cost of computing Q from λ and P .

Example 1 (Lim-Lee, Crypto '94):

- $\lambda = 2^k$
- No cost computing a, b from $a + b \cdot 2^k$
- Computing Q requires k doubles
- First multiplication of a given P costs
 - $\sim 2k$ doubles, $\sim k/2$ general additions
 - (saves $\sim k/6$ gen. additions over Add.-Subt. Method)
- If Q saved, each subsequent multiplication of P costs
 - $\sim k$ doubles, $\sim k/2$ general additions

Example 2 (Gallant-Lambert-Vanstone, Crypto '01):

- $\lambda \in \text{End}(E)$, small complex integer (e.g., i or ω)
- $Q = [\lambda]P$ (cheap complex multiplication)
- $a + b\lambda$ is n reduced modulo some fixed ρ (complex integer whose norm is the order of the subgroup)
- Costs
 - $\sim k$ doubles, $\sim k/2$ general additions
 - plus cost of modular reduction
- Faster, but requires special curves

Example 3:

- $p = 2^{390} + 3$ (prime)
- E is the curve $y^2 = x^3 - 2$ over \mathbb{F}_p
- $\#E(\mathbb{F}_p) = 2^{390} - 2^{195} + 7 = 63r$ (r prime)
- In the order- r subgroup,

$$(2^{195} \cdot c + d)(x, y) = (2c + d)(x, y) + 3c \left((2^{389} + 2^{194} + 1)x, y \right)$$

- No precomputation of Q or modular reduction required

Second Topic:

**MINIMIZING BANDWIDTH
IN EC PARAMETERS**

- Specifying EC parameters can require significant bandwidth
- We introduce a family of “compact curves” whose parameters can be compute efficiently from the domain ID.

AUTHENTICATION ACROSS DOMAINS

- Suppose a network is divided into **domains**
- Want **authentication** throughout the network, but **confidentiality** (*i.e.*, key agreement) only within domains
- Simple cryptographic solution: **different parameters** for each domain

THE PARAMETER SPECIFICATION PROBLEM

- If many domains exist (or if they change frequently), users won't know the parameters of every domain
- So digital signatures must be accompanied by parameter information
- This adds significant bandwidth to signatures
- Solution: ID-based parameters

COMPACT CURVES

Let $f \equiv 2 \pmod{3}$ and $g \equiv 3 \pmod{6}$ and suppose that

$$p := f^2 - fg + g^2,$$

$$r := p + 1 - (2f - g)$$

are prime with $p \equiv \pm 3 \pmod{8}$. The compact curve $C_{f,g}$ is

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

over \mathbb{F}_p , with base point $(-1, 1)$.

- Group order is $\#C_{f,g}(\mathbb{F}_p) = r$.

ID-BASED PARAMETERS

- The parameters for $C_{f,g}$ are all easily computed from f and g
- Take $f = \text{Hash}(ID_{\text{domain}})$ and let g be smallest positive integer for which p and r are both prime
- Then the parameters are a deterministic function of ID_{domain}
- To save verification time, can send g along with ID_{domain}

GALLANT-LAMBERT-VANSTONE SPEEDUP ON COMPACT CURVES

- Let δ be the norm- r complex integer

$$\delta = 1 - f - g\omega$$

and let

$$u + v\omega = n \pmod{\delta}$$

in $\mathbb{Z}[\omega]$. Then

$$n(x, y) = u(x, y) + v(-fg^{-1}x, y).$$

G-L-V ON COMPACT CURVES (*cont'd*)

$$n \bmod \delta := n - \delta \cdot \text{Round}[n/\delta]$$

where

$$\text{Round}[x + y\omega] = [a] + [b]\omega$$

where

$$3a = [x + y] + [2x - y] + 2$$

$$3b = [x + y] + [x - 2y] + 2$$

COMPACT HYPERELLIPTIC CURVES

For appropriate $p \equiv 1 \pmod{10}$, let C be the genus-2 curve

$$y^2 = x^5 + 8$$

over \mathbb{F}_p , with base point $(1, 3)$.

Then have:

- Closed-form evaluation of r (large prime order of Jacobian group), and so compact representation of parameters
- Explicit Gallant-Lambert-Vanstone speedup