ANOMALOUS BINARY CURVES

Jerome A. Solinas

NSA, Ft. Meade, MD, USA

jasolin@orion.ncsc.mil

ECC '98

September 1998

OVERVIEW

- An advantage of elliptic curves:

  can choose underlying field to improve implementation performance

  $\rightarrow$ *Example:* Mersenne prime arithmetic

- Following is a family of very fast curves over $GF(2^m)$ (m odd)

NORMAL BASES

- If θ is a root of $p(t)$, then the full set of roots is

$$\mathcal{B} := \{\theta,\, \theta^2,\, \theta^{2^2},\, \ldots,\, \theta^{2^{m-1}}\}.$$

- If roots are linearly independent over $GF(2)$, then

$\rightarrow$ $p(t)$ is a *normal polynomial*

$\rightarrow$ $\mathcal{B}$ is a *normal basis* for $GF(2^m)$

- Bit string $\quad (c_0\, c_1\, c_2\, \cdots\, c_{m-1}) \quad$ represents

$$\gamma = c_0\,\theta + c_1\,\theta^2 + c_2\,\theta^{2^2} + \cdots + c_{m-1}\,\theta^{2^{m-1}}$$

SQUARING

- Since $\theta^{2^m} = \theta$, then

$$\left(c_0\,\theta + c_1\,\theta^2 + c_2\,\theta^{2^2} + \cdots + c_{m-1}\,\theta^{2^{m-1}}\right)^2$$

$$= c_0\,\theta^2 + c_1\,\theta^{2^2} + \cdots + c_{m-2}\,\theta^{2^{m-1}} + c_{m-1}\,\theta.$$

★ So: *can implement field squaring by a right cyclic shift of bit string.* If

$$\gamma = (c_0\,c_1\,c_2\,\cdots\,c_{m-1})$$

then

$$\gamma^2 = (c_{m-1}\,c_0\,c_1\,\cdots\,c_{m-2}).$$

FIELD MULTIPLICATION (Special Case)

- $p = Tm + 1$ prime (T small)
- Let $\psi \in GF(2^{Tm})$ have order p
- Let θ be the trace of ψ over $GF(2^m)$
- If $\mathcal{B} := \{\theta, \theta^2, \theta^{2^2}, \ldots, \theta^{2^{m-1}}\}$ forms a basis, then $\mathcal{B}$ is a normal basis (of "Type T") for which multiplication is especially simple.
- The smaller T is, the simpler the multiplication

MULTIPLICATION RULE

- Each Type T normal basis has a **multiplication rule.**

- *Example* (Type 4 basis over $GF(2^7)$):

$$
\begin{aligned}
F(\underline{u},\underline{v}) = {} & u_0\,v_1 + u_1\,(v_0 + v_2 + v_5 + v_6) \\
& + u_2\,(v_1 + v_3 + v_4 + v_5) \\
& + u_3\,(v_2 + v_5) + u_4\,(v_2 + v_6) \\
& + u_5\,(v_1 + v_2 + v_3 + v_6) + u_6\,(v_1 + v_4 + v_5 + v_6)
\end{aligned}
$$

FIELD MULTIPLICATION

Example (Type 4 basis over $GF(2^7)$):

$$(c_0\, c_1 \ldots c_{m-1}) = (1\,0\,1\,0\,1\,1\,1) \times (1\,1\,0\,0\,0\,0\,1)$$

$$\begin{cases} c_0 & = F(\,(1\,0\,1\,0\,1\,1\,1), (1\,1\,0\,0\,0\,0\,1)\,) = 1, \\ c_1 & = F(\,(0\,1\,0\,1\,1\,1\,1), (1\,0\,0\,0\,0\,1\,1)\,) = 0, \\ & \vdots \\ c_6 & = F(\,(1\,1\,0\,1\,0\,1\,1), (1\,1\,1\,0\,0\,0\,0)\,) = 1, \end{cases}$$

so that $c = (1\,0\,1\,1\,0\,0\,1)$.

FIELD MULTIPLICATION

- Multiplication simplest when θ given by a Gaussian period over $GF(2^{Tm})$, where

  $\rightarrow$ $p := T\,m + 1$ prime

  $\rightarrow$ m relatively prime to index in $GF(p)^{\times}$ of subgroup generated by 2

- *Example:* $T = 4$ over $GF(2^7)$ ("Type 4" normal basis)

Multiplication Rule :

Let $u :=$ order T element modulo p.

Define the sequence $F(1), \ldots, F(Tm)$ as follows.

```
Set w ← 1
For j from 0 to T − 1 do
    Set n ← w
    For i from 0 to m − 1 do
        Set F(n) ← i
        Set n ← 2n mod p
    Set w ← uw mod p
```

Example: $T = 4$ over $GF(2^7)$ $(p = 29,\ u = 12)$

$F(1) = 0$	$F(8) = 3$	$F(15) = 6$	$F(22) = 5$
$F(2) = 1$	$F(9) = 3$	$F(16) = 4$	$F(23) = 6$
$F(3) = 5$	$F(10) = 2$	$F(17) = 0$	$F(24) = 1$
$F(4) = 2$	$F(11) = 4$	$F(18) = 4$	$F(25) = 2$
$F(5) = 1$	$F(12) = 0$	$F(19) = 2$	$F(26) = 5$
$F(6) = 6$	$F(13) = 4$	$F(20) = 3$	$F(27) = 1$
$F(7) = 5$	$F(14) = 6$	$F(21) = 3$	$F(28) = 0$

Let

$$F(\underline{u}, \underline{v}) := \sum_{k=1}^{p-2} u_{F(k+1)} \, v_{F(p-k)}$$

Example:

$$\begin{aligned} F(\underline{u}, \underline{v}) = {} & u_0 \, v_1 + u_1 \, (v_0 + v_2 + v_5 + v_6) \\ & + u_2 \, (v_1 + v_3 + v_4 + v_5) \\ & + u_3 \, (v_2 + v_5) + u_4 \, (v_2 + v_6) \\ & + u_5 \, (v_1 + v_2 + v_3 + v_6) + u_6 \, (v_1 + v_4 + v_5 + v_6) \end{aligned}$$

$$(c_0\, c_1 \ldots c_{m-1}) = (a_0\, a_1 \ldots a_{m-1}) \times (b_0\, b_1 \ldots b_{m-1})$$

If

$$a = (1\,0\,1\,0\,1\,1\,1) \qquad \text{and} \qquad b = (1\,1\,0\,0\,0\,0\,1),$$

then

$$\begin{aligned}
c_0 &= F(\,(1\,0\,1\,0\,1\,1\,1),\,(1\,1\,0\,0\,0\,0\,1)\,) = 1,\\
c_1 &= F(\,(0\,1\,0\,1\,1\,1\,1),\,(1\,0\,0\,0\,0\,1\,1)\,) = 0,\\
&\;\vdots\\
c_6 &= F(\,(1\,1\,0\,1\,0\,1\,1),\,(1\,1\,1\,0\,0\,0\,0)\,) = 1,
\end{aligned}$$

so that $c = ab = (1\,0\,1\,1\,0\,0\,1)$.

DIVISION

- By Fermat's theorem, $\beta^{-1} = \beta^{2^m - 2}$

- Special method for exponentiating by $2^m - 2$

  $\rightarrow$ Let $B_k := \beta^{2^k - 1}$

  $\rightarrow$ Then $B_1 = \beta, \quad B_{m-1}^2 = \beta^{-1}$

  $\rightarrow$ "Binary method"

$$B_{2k} = B_k^{2^k} \cdot B_k$$

$$B_{k+1} = B_k^2 \cdot \beta$$

SOLVING QUADRATICS

- To find points on the elliptic curve

$$y^2 + xy = x^3 + A\,x^2 + B$$

need to solve

$$z^2 + z = \beta$$

(where $z = y\,x^{-1}$ and $\beta = x + A + B\,x^{-2}$)

- If $\beta_0 + \beta_1 + \cdots + \beta_{m-1} = 0$ then

$$z^2 + z = \beta = (\beta_0 \ \beta_1 \ \cdots \ \beta_{m-1})$$

has solutions z, $z+1$ where

$$\begin{aligned}
&z_0 \text{ arbitrary} \\
&z_1 := z_0 \oplus \beta_1 \\
&z_2 := z_1 \oplus \beta_2 \\
&\quad \vdots \\
&z_{m-1} := z_{m-2} \oplus \beta_{m-1}, \\
&z := (z_0 \ z_1 \ \cdots \ z_{m-1})
\end{aligned}$$

ELLIPTIC SCALAR MULTIPLICATION

- Efficient computation of kP for $k \approx 2^m$ and P a point on the elliptic curve $y^2 + xy = x^3 + a_2\,x^2 + a_6$.

- <u>*Binary Method*</u> : $k = 29 = 11101_{\text{TWO}}$

1	Start with P	P	$1 = 1$
1	Double, Add	$3P$	$3 = 11$
1	Double, Add	$7P$	$7 = 111$
0	Double	$14P$	$14 = 1110$
1	Double, Add	$29P$	$29 = 11101$

- Average **cost** for m-bit scalar multiplication:

  $\sim m$ elliptic doubles and $m/2$ elliptic adds

SIGNED BINARY EXPANSIONS

- *Subtraction* as efficient as addition on elliptic curves

$$-(x, y) = (x, x + y)$$

- So can use binary method with *signed binary expansions*

- Example: $k = 29 = 32 - 4 + 1 = \langle 1, 0, 0, -1, 0, 1 \rangle$

1	Start with P	P	$1 = \langle 1 \rangle$
0	Double	$2P$	$2 = \langle 1, 0 \rangle$
0	Double	$4P$	$4 = \langle 1, 0, 0 \rangle$
-1	Double, Subtract	$7P$	$7 = \langle 1, 0, 0, -1 \rangle$
0	Double	$14P$	$14 = \langle 1, 0, 0, -1, 0 \rangle$
1	Double, Add	$29P$	$29 = \langle 1, 0, 0, -1, 0, 1 \rangle$

THE NONADJACENT FORM (NAF)

- Signed binary expansion **not unique**

- **Every positive integer has a unique NAF** (signed binary expansion with no two consecutive coefficients nonzero)

- *Example:*

$$\mathrm{NAF}(29) = \langle 1, 0, 0, -1, 0, 1 \rangle$$

- The NAF has the **minimal number of nonzero coefficients** among all signed binary expansions and nearly **minimal length**

COMPUTING THE NAF

- Divide by 2 repeatedly, choosing nonzero remainders so that quotient is even

- *Example:* $k = 29$

$$
\begin{array}{ll}
29 = 2 \cdot 14 + 1 & \quad 4 = 2 \cdot 2 + 0 \\
14 = 2 \cdot 7 + 0 & \quad 2 = 2 \cdot 1 + 0 \\
7 = 2 \cdot 4 - 1 & \quad 1 = 1
\end{array}
$$

$\rightarrow$ $\mathrm{NAF}(29) = \langle 1, 0, 0, -1, 0, 1 \rangle$

- Only integer operations: addition/subtraction by 1

ADDITION-SUBTRACTION METHOD

- The **average density** of nonzero coefficients in a NAF is 1/3 (vs. 1/2 for the binary expansion)

- **Length** of NAF(n) $\approx$ bit length of n

- *Addition-Subtraction Method*

  = binary method using NAF

- Average **cost** for m-bit scalar multiplication:

  $\sim m$ elliptic doubles and $m/3$ elliptic adds

PRECOMPUTATION SPEEDUP

- *Width-3 NAF's:* binary expansion with nonzero coefficients $\pm 1, \pm 3$ and at most 1 nonzero coefficient among any 3 consecutive coefficients
- Always exists, unique, easy to compute
- Average density $1/4$
- *Example:* $83 = \langle 1, 0, 0, -3, 0, 0, 0, 3 \rangle$
- To compute $83P$ in this way, precompute and store $3P$
- Average cost $\approx m$ elliptic doubles and $m/4$ elliptic adds

WIDTH w NAF's

- A binary expansion with nonzero coefficients

$$\pm 1, \pm 3, \ldots, \pm(2^{w-1} - 1)$$

  and at most 1 nonzero coefficient among any w consecutive coefficients

- Always exists, unique, easy to compute

- Average density $1/(w+1)$

- *Example* (width 4):

$$359 = \langle 1, 0, 0, 0, -5, 0, 0, 0, 0, 7 \rangle$$

TIME-MEMORY TRADEOFF

- Using a width-w NAF for an m-bit scalar multiplication,

  $\rightarrow$ Need to precompute and store $2^{w-2}-1$ extra points

  $\rightarrow$ *Total cost:*

  $\sim m + 2^{w-3}$ doubles

  $\sim m/(w+1) + 2^{w-2}$ adds

  $\sim 2^{w-2}$ memory

- *Bottleneck*: the m elliptic doubles

ANOMALOUS BINARY CURVES

[Koblitz, CRYPTO '91]

- The ABC's are the curves

$$E_a : \; y^2 + xy = x^3 + ax^2 + 1$$

over $GF(2^m)$, where $a = 0$ or 1 (any m)

- Have the property that the *Frobenius map*

$$\phi : \; (x, y) \mapsto (x^2, y^2)$$

takes points on E_a to other points on E_a

- Implementing ϕ is essentially **cost-free**

(using normal basis representation)

ORDERS OF ABC's

- Easy to **compute** $N_m = \#E_a(GF(2^m))$ via **recursion**

  → If $a = 0$, then $N_1 = 4$, $N_2 = 8$,

  $$N_m = -N_{m-1} - 2\,N_{m-2} + 2^{m+1} + 4$$

  → If $a = 1$, then $N_1 = 2$, $N_2 = 8$,

  $$N_m = N_{m-1} - 2\,N_{m-2} + 2^m + 2$$

- For cryptographic purposes, want N_m **almost prime**

  → Only happens if m is **prime**

If $a = 0$, then $\boxed{N_m = 4 \cdot \text{prime}}$ for

$$m = 3, 5, 7, 11, 17, 19, 23, 101, 107, 109,$$
$$113, 163, 283, 311, 331, 347, 359$$

If $a = 1$, then $\boxed{N_m = 2 \cdot \text{prime}}$ for

$$m = 5, 7, 13, 19, 23, 41, 83, 97, 103, 107,$$
$$131, 233, 239, 277, 283, 349, 409$$

These are the only almost-prime values for $m \leq 512$.

- *Best situation:* **if** there were a curve E for which

$$\phi P = 2P \qquad \text{for all } P,$$

  then *doubling would be cost-free* (so that the bottleneck would disappear completely).

- Unfortunately, there is no such curve   : (

- *But* - still want to use ϕ somehow

- Describe its action on E via complex multiplication.

COMPLEX MULTIPLICATION

- If $P = (x, y)$ is a point on E, then

  $$(x^4, y^4) + 2\,(x, y) = (-1)^{1-a}\,(x^2, y^2)$$

  Symbolically,

  $$(\phi^2 + 2)\,P = (-1)^{1-a}\phi\,P$$

- Thus the Frobenius map ϕ acts on E like multiplication by the complex number τ, where

  $$\tau^2 + 2 = (-1)^{1-a}\tau$$

  Explicitly,

  $$\tau = ((-1)^{1-a} + \sqrt{-7})/2$$

τ-ADIC EXPANSIONS

- Replace *binary expansions* (powers of 2) by τ*-adic expansions* (sums and differences of powers of τ)

- **More efficient** since multiplication by τ is free

Example: $a = 0$, $k = 9 = \tau^5 - \tau^3 + 1 = \langle 1, 0, -1, 0, 0, 1 \rangle$

1	Start with P	(x, y)
0	Shift	(x^2, y^2)
-1	Shift, Subtract	$(x^4, y^4) - (x, y)$
0	Shift	$(x^8, y^8) - (x^2, y^2)$
0	Shift	$(x^{16}, y^{16}) - (x^4, y^4)$
1	Shift, Add	$(x^{32}, y^{32}) - (x^8, y^8) + (x, y)$
		$= 9P$

THE τ-ADIC NAF

- **Every positive integer has a unique τ-adic NAF** (τ-adic expansion with no two consecutive coefficients nonzero)

- *Example:*

$$\tau\mathrm{NAF}(9) = \langle 1, 0, -1, 0, 0, 1 \rangle$$

- The τ-adic NAF has the **minimal number of nonzero coefficients** among all τ-adic expansions

COMPUTING THE τ-ADIC NAF

- $a + b\tau$ divisible by τ (in $\mathbb{Z}[\tau]$) if and only if a even

- Divide by τ repeatedly, choosing nonzero remainders so that the quotient is divisible by τ

- *Example* $(a = 0)$

$$
\begin{aligned}
9 &= \tau \cdot (4 - 4\tau) + 1 & \qquad -2 + \tau &= \tau \cdot \tau - 1 \\
4 - 4\tau &= \tau \cdot (-2 - 2\tau) + 0 & \tau &= \tau \cdot 1 + 0 \\
-2 - 2\tau &= \tau \cdot (-2 + \tau) + 0 & 1 &= 1
\end{aligned}
$$

$\rightarrow \ \tau\mathrm{NAF}(9) = \langle 1, 0, -1, 0, 0, 1 \rangle$

- Only integer operations: addition/subtraction by 1

THE τ-ADIC METHOD

- The **average density** of nonzero coefficients in a τ-adic NAF is 1/3

- Length of $\tau\mathrm{NAF}(n) \approx$ <u>twice</u> the bit length of n *(Uh-oh!)*

- <u>*τ-adic Method*</u>*:*

  use τ-adic NAF on ABC's

- Average **cost** for m-bit scalar multiplication:

  <u>*no*</u> elliptic doubles and $\sim 2m/3$ elliptic adds

REDUCED τ-ADIC NAF

[Meier-Staffelbach, CRYPTO '92]

- The τ-adic NAF has length $2m$; want length m

- Multiplication by the complex number τ^m is the **identity mapping** on E_a over $GF(2^m)$

  (represents m-fold cyclic shift of m-long bit string)

- Thus $\alpha P = \beta P \quad \text{if} \quad \alpha \equiv \beta \pmod{\tau^m - 1}$

- *So:* divide k by $\tau^m - 1$ and take τ-adic NAF of remainder

- Length of result is $\sim m$, so $\sim m/3$ elliptic operations

$$\begin{aligned}
\alpha &= \tau^{15} - \tau^{13} - \tau^{11} - \tau^{8} + \tau^{5} + \tau^{3} - \tau \\
&= \langle 1, 0, -1, 0, -1, 0, 0, -1, 0, 0, 1, 0, 1, 0, -1, 0 \rangle \\
&= \langle 1, 0, 0, 0, -5, 0, 0, 0, 0, 0, -7, 0, 0, 0, 3, 0 \rangle \\
&= \tau^{15} - \beta_5 \cdot \tau^{11} - \beta_7 \cdot \tau^{5} + \beta_3 \cdot \tau
\end{aligned}$$

where

$$\beta_3 = \tau^2 - 1, \quad \beta_5 = \tau^2 + 1, \quad \beta_7 = \tau^3 - 1$$

Thus

$$\alpha P = \tau^{15} P - \tau^{11} P_5 - \tau^{5} P_7 + \tau P_3$$

where $P_i = \beta_i P$.

WIDTH w τ-ADIC NAF

- The width-w τ-adic NAF has density $(w+1)^{-1}$
- Need to precompute and store $(2^w - (-1)^w)/3$ points
- *Total work:*

$$\sim \frac{2^w}{3} + \frac{m}{w+1}$$

PERFORMANCE AT VARIOUS WIDTHS

Number of Elliptic Operations for E_1 over $GF(2^{163})$

	Precomputation	Real Time (avg)	Total (avg)
2	0	53.3	53.3
3	2	40	42
4	4	32	36
5	10	26.7	36.7
6	20	22.9	42.9
7	42	20	62