EFFICIENT IMPLEMENTATION OF KOBLITZ CURVES AND GENERALIZED MERSENNE ARITHMETIC

Jerome A. Solinas

National Security Agency, Ft. Meade, MD, USA

jasolin@orion.ncsc.mil

CACR Visitor Jan.-June 1999

ECC '99

3 November 1999

PART I: OVERVIEW

- An advantage of elliptic curves:

  can choose the domain parameters to
  improve implementation performance

- Can choose

  → the **underlying finite field**

  → the **specific elliptic curve** (*vs. random* curve)

COMMON CHOICES

	Characteristic $p > 3$	Characteristic $p = 2$
Special Fields	*Pseudo-Mersenne Primes, Optimal Extension Fields, Generalized Mersenne Numbers*	*Optimal Bases, Field Towers, Silverman Fields*
Special Curves	*Gallant Curves*	*Koblitz Curves*

PART II: GENERALIZED MERSENNE PRIMES

- *Modular Multiplication:*

  → To multiply modulo p, do the integer multiplication and reduce the result modulo p.

  → This requires efficient modular reduction of integers less than p^2.

MERSENNE REDUCTION

- *Old trick:*

  → Let $p := 2^{521} - 1$. To reduce $n < p^2$ modulo p, write

  $$\boxed{n = 2^{521} \cdot T + U}$$

  where T and U are 521-bit integers.

  → Then

  $$\boxed{n \equiv T + U \pmod{p}}$$

  → Replaces ordinary modular reduction (integer division) by one addition (mod p).

DRAWBACKS

- Requires a 521-*bit shift*

  $\rightarrow$ Better to shift by a **multiple of the word size** w.

- Mersenne primes are **rare**.

  $\rightarrow$ None between 127 and 521.

- Crandall's fix:

  $\rightarrow$ Let $p = 2^m - k$ where m is a multiple of w and $k < 2^w$.

- Alternatively, have *Generalized Mersenne Primes.*

GENERALIZED MERSENNE PRIMES

- *Example*: $p = 2^{192} - 2^{64} - 1$.

→ Each integer $A < p^2$ can be represented via

$$A = \sum_{i=0}^{5} A_i \cdot 2^{64 \cdot i}$$

where each $A_i < 2^{64}$.

→ As bit strings, A is represented by six 64-bit words:

$$A = (\ A_5 \ \| \ A_4 \ \| \ A_3 \ \| \ A_2 \ \| \ A_1 \ \| \ A_0\,)$$

→ Reduce A modulo p via

$$\boxed{A \equiv T + S_1 + S_2 + S_3 \pmod{p}}$$

where

$$\begin{aligned}
T &= A_2 \cdot 2^{128} + A_1 \cdot 2^{64} + A_0 \\
S_1 &= A_3 \cdot 2^{64} + A_3 \\
S_2 &= A_4 \cdot 2^{128} + A_4 \cdot 2^{64} \\
S_3 &= A_5 \cdot 2^{128} + A_5 \cdot 2^{64} + A_5.
\end{aligned}$$

(Three modular additions)

COMMON GENERALIZED MERSENNE PRIMES

- $p = 2^{192} - 2^{64} - 1$ requires 3 modular additions.
- $p = 2^{224} - 2^{96} + 1$ requires 2 modular additions and 2 modular subtractions.
- $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ requires 6 modular additions and 4 modular subtractions.
- $p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$ requires 7 modular additions and 3 modular subtractions.
- $p = 2^{521} - 1$ requires 1 modular addition.

FINDING GENERALIZED MERSENNE PRIMES

- A generalized Mersenne prime p can be written $p = f(2^w)$ where w is the word size and the polynomial $f(t)$ has small degree d.

- The *modular reduction weight* of $f(t)$ is the number of modular additions and subtractions needed to reduce modulo p.

- *The problem:* given a multiple m of the word size w, find a polynomial $f(t)$ of degree m/w, with smallest possible modular reduction weight, such that $p = f(2^w)$ is prime.

- *The solution*:

  → Search over all integral polynomials of appropriate degrees with small coefficients.

  → Record all polynomials with small modular reduction weight. Sort by weight.

  → Starting with the smallest weight, check primality of $p = f(2^w)$ until a prime p is found.

- *Needed:* an efficient method for computing the modular reduction weight.

FINDING THE MODULAR REDUCTION WEIGHT

<u>*Example*</u>: $f(t) := t^3 - t + 1$.

$$t^3 \equiv -1 + t \pmod{f(t)}$$
$$t^4 \equiv -t + t^2 \pmod{f(t)}$$
$$t^5 \equiv -1 + t - t^2 \pmod{f(t)}$$

$$\begin{pmatrix} t^3 \\ t^4 \\ t^5 \end{pmatrix} \equiv \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ t \\ t^2 \end{pmatrix}$$

Positive entries:

$$\begin{pmatrix} -1 & \boxed{1} & 0 \\ 0 & -1 & \boxed{1} \\ -1 & \boxed{1} & -1 \end{pmatrix}$$

$$\max(0, 2, 1) = 2 \text{ modular additions.}$$

Negative entries:

$$\begin{pmatrix} \boxed{-1} & 1 & 0 \\ 0 & \boxed{-1} & 1 \\ \boxed{-1} & 1 & \boxed{-1} \end{pmatrix}$$

$$\max(2, 1, 1) = 2 \text{ modular subtractions.}$$

Modular reduction weight is $2 + 2 = 4$.

LOW MODULAR REDUCTION WEIGHTS

- $f(t) = t - b$ has weight $w = |b|$.
- $f(t) = t^d - t^c - 1$ has weight
$$w = 1 + \left\lceil \frac{d}{d-c} \right\rceil .$$
- $f(t) = t^d - t^c + 1$ has weight
$$w = 3 \left\lceil \frac{d}{d-c} \right\rceil - \left\lfloor \frac{d}{d-c} \right\rfloor - 1.$$
- $f(t) = t^d - t^{d-1} + t^{d-2} - \cdots 1$ has weight $w = 3$.
- $f(t) = t^4 - t^3 + t^2 + 1$ has weight $w = 4$.

GENERALIZED MERSENNE NUMBERS

- *Example:*

$$19\,p = 2^{384} - 2^{320} - 1$$

has reduction weight 7.

- To implement ECC modulo p, perform EC operations modulo $19\,p$. At the end, reduce (mod p) by repeated subtraction.

PART III: KOBLITZ CURVES

- The curves E_0 and E_1 given by

$$E_a : y^2 + xy = x^3 + a\,x^2 + 1.$$

- The group $\mathcal{G}$ of points with coordinates in $GF(2^m)$ has $\sim 2^m$ elements.

- ECC is done on the **main subgroup:** a prime-order subgroup $\mathcal{M}$ of $\mathcal{G}$ having index 2 (if $a = 1$) or 4 (if $a = 0$). Has order

$$r \sim 2^{m-2+a}.$$

SCALAR MULTIPLICATION

- *Complex Multiplication by* $\tau := (\sqrt{-7} - (-1)^a)/2$:

$$\tau\,(x, y) = (x^2, y^2)$$

- **Very efficient** to implement (esp. using normal bases).

- **Scalar multiplication** via the $\tau-$adic analogue of the binary method, using the $\tau-$adic nonadjacent expansion.

- *Example* : if $a = 1$, then TNAF of 9 is $\tau^5 - \tau^3 + 1$.

- Replaces **elliptic doubles** by **bit shifts**.

REDUCED TNAF's

- Let $\delta := (\tau^m - 1)/(\tau - 1)$. If $\alpha \equiv \beta \pmod{\delta}$, then
$$\alpha P = \beta P \text{ for } P \in \mathcal{M}.$$

- The *reduced τ−adic NAF* (or *RTNAF*) defined via
$$\text{RTNAF}(n) = \text{TNAF}(\rho),$$
where $\rho := n \bmod \delta$.

- RTNAF has length $\sim m$ and Hamming weight $\sim m/3$.

  $\rightarrow$ RTNAF-based scalar multiplication requires $\sim m/3$ elliptic adds.

MODULAR REDUCTION IN $\mathbb{Z}[\tau]$

- Reducing n modulo δ requires a *ring division* in $\mathbb{Z}[\tau]$

  $\rightarrow$ Requires two integer divisions by r

  $\rightarrow$ Potentially very expensive

- Use <u>*partial modular reduction*</u> instead

  $\rightarrow$ Since $r \approx 2^{m-2+a}$, can replace divisions by r with divisions by 2^{m-2+a} and 4 integer multiplications

  $\rightarrow$ Slight loss of precision may occasionally yield slightly bigger remainder than $n \bmod \delta$

ORDINARY RTNAF

- Signed τ-adic expansion (coefficients $0, \pm 1$)
- Of any two adjacent coefficients, at most one nonzero
- Length $\sim m$, Hamming weight $\sim m/3$
- Corresponding binary method:

  $\rightarrow$ No extra memory required

  $\rightarrow$ Work required:

  $\sim m/3$ elliptic adds

  $\sim 2\,m$ squarings (bit shifts)

  8 integer multiplications

WIDTH$-w$ RTNAF

- Coefficients are 0 and the odd numbers u with $|u| < 2^{w-1}$
- Of any w adjacent coefficients, at most one nonzero
- Length $\sim m$, Hamming weight $\sim m/(w+2)$
- Corresponding binary method requires:

  $\rightarrow$ Storing 2^{w-2} points

  $\rightarrow$ Work required:

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

  $\sim 4\,m$ squarings (bit shifts)

  8 integer multiplications

COMPUTING THE WIDTH$-w$ TNAF

- Given an odd integer u with $|u| < 2^{w-1}$, let

$$\alpha_u := u \bmod \tau^w$$

- Let t be the even root of the equation

$$t^2 + (-1)^a t + 2 \equiv 0 \pmod{2^w} \; .$$

- If z_0 odd and

$$u := z_0 + z_1 t \text{ mods } 2^w$$

then

$$\alpha_u = z_0 + z_1 \tau \bmod \tau^w$$

→ *Reduce modulo τ^w by looking up precomputed values*

```
Input $\rho$

Set $\mathcal{S} \leftarrow \langle \, \rangle$

Set $\zeta \leftarrow \rho$

While $\zeta \neq 0$

      If $\zeta$ odd then set $\alpha \leftarrow \zeta$ mod $\tau^w$

                          set $\zeta \leftarrow \zeta - \alpha$

                     else set $\alpha \leftarrow 0$

      Prepend $\alpha$ to $\mathcal{S}$

      Set $\zeta \leftarrow \zeta / \tau$

EndWhile

Output $\mathcal{S}$
```

ANALOGUES OF KOBLITZ CURVES

- Müller ('98) extended Koblitz curves to ground fields
  $\to$ $GF(2^2)$, CM by $(1+\sqrt{-15})/2$
  $\to$ $GF(2^3)$, CM by $(1+\sqrt{-23})/2$ or $(1+\sqrt{-31})/2$
  etc.

- Koblitz ('98) found analogous curves over $GF(3^m)$ and $GF(7^m)$

- Günther and Stein ('99) found analogous hyperelliptic curves