Elliptic Nets in Cryptography

Katherine Stange

Department of Mathematics
Brown University
http://www.math.brown.edu/~stange/

ECC 2007,
Dublin, Ireland

Outline

Elliptic Divisibility Sequences

Definition

A integer sequence W is an *elliptic divisibility sequence* if for all positive integers $m > n$,

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 .$$

- Generated by $W_1, \ldots, W_4$ via the recurrence.
- Example: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$
- Example: $1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, \ldots$
- Example: $1, 1, -3, 11, 38, 249, -2357, 8767, 496036, -3769372, -299154043, -12064147359, \ldots$

Example: $y^2 + y = x^3 + x^2 - 2x$, $P = (0,0)$

$$\begin{aligned}
P &= (0,0) \\
[2]P &= (3,5) \\
[3]P &= \left(-\frac{11}{9}, \frac{28}{27}\right) \\
[4]P &= \left(\frac{114}{121}, -\frac{267}{1331}\right) \\
[5]P &= \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right) \\
[6]P &= \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right) \\
[7]P &= \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right)
\end{aligned}$$

$$\begin{aligned}
W_1 &= +1 \\
W_2 &= +1 \\
W_3 &= -3 \\
W_4 &= +11 \\
W_5 &= +38 \\
W_6 &= +249 \\
W_7 &= -2357
\end{aligned}$$

Sequences from Division Polynomials

Consider a point $P = (x, y)$ and its multiples on an elliptic curve $E : y^2 = x^3 + Ax + B$. Then

$$[n]P = \left(\frac{\phi_n(P)}{\Psi_n(P)^2}, \frac{\omega_n(P)}{\Psi_n(P)^3} \right)$$

where

$$\Psi_1 = 1, \qquad \Psi_2 = 2y,$$
$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$
$$\Psi_{m+n}\Psi_{m-n}\Psi_1^2 = \Psi_{m+1}\Psi_{m-1}\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\Psi_m^2 .$$

It gives an elliptic divisibility sequence!

Division Polynomials and Torsion Points

- When n is odd, Ψ_n is a polynomial in x.
- When n is even, $\Psi_n/2y$ is a polynomial in x.
- The roots of these polynomials are exactly the x-coordinates of the n-torsion points of E.

Division Polynomials and Sequences over Finite Fields

- Using the formulae, we can consider divison polynomials over finite fields (where "denominator" has no meaning).
- Here, the point P will always have finite order, say n. The associated sequence will have $W_n = 0$.

Example

$E : y^2 + y = x^3 + x^2 - 2x$ over $\mathbb{F}_5$.
$P = (0, 0)$ has order 9.
The associated sequence is
$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

Counting Points on an Elliptic Curve over a Finite Field

- The Schoof-Elkies-Atkin algorithm and the Satoh algorithm both depend on calculating certain (different) factors of the p-th division polynomial for certain primes p.

Shipsey's Attacks on the Elliptic Curve Discrete Log

- The elliptic curve discrete logarithm problem is known to be weak in certain cases, where the Menezes-Okamoto-Vanstone/Frey-Ruck attack can be used.
- Shipsey uses the computation of elliptic divisibility sequences to give simple attacks in these cryptographically weak cases.
- We will see later in this talk that there's an underlying explanation for the existence of Shipsey's attack which can be understood through the Tate pairing.

The Question - Upping the Dimension

The elliptic divisibility sequence is associated to the sequence of points $[n]P$ on the curve.

$$\boxed{[n]P \leftrightarrow W_n}$$

We might dream of . . .

$$\boxed{[n]P + [m]Q \leftrightarrow W_{n,m}}$$

Or even . . .

$$\boxed{[n]P + [m]Q + [t]R \leftrightarrow W_{n,m,t}}$$

etc.

Definition of an elliptic net

Definition (KS)

Let R be an integral domain, and A a finite-rank free abelian group. An *elliptic net* is a map $W : A \to R$ such that the following recurrence holds for all $p, q, r, s \in A$.

$$\begin{aligned}
&W(p+q+s)W(p-q)W(r+s)W(r) \\
&\qquad + W(q+r+s)W(q-r)W(p+s)W(p) \\
&\qquad\quad + W(r+p+s)W(r-p)W(q+s)W(q) = 0
\end{aligned}$$

- Elliptic divisibility sequences are a special case ($A = \mathbb{Z}$)
- In this talk, we will mostly discuss rank 2: $A = \mathbb{Z}^2$.
- The recurrence generates the net from finitely many initial values.

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

○ $\left(\frac{56}{25}, \frac{371}{125}\right)$	○ $\left(-\frac{95}{64}, \frac{495}{512}\right)$	○ $\left(\frac{328}{361}, -\frac{2800}{6859}\right)$
○ $\left(\frac{6}{1}, -\frac{16}{1}\right)$	○ $\left(\frac{1}{9}, -\frac{19}{27}\right)$	○ $\left(\frac{39}{1}, \frac{246}{1}\right)$
○ $\left(\frac{1}{1}, \frac{0}{1}\right)$	○ $\left(-\frac{2}{1}, -\frac{1}{1}\right)$	○ $\left(\frac{5}{4}, -\frac{13}{8}\right)$
○ 0	○ $\left(\frac{0}{1}, \frac{0}{1}\right)$	○ $\left(\frac{3}{1}, \frac{5}{1}\right)$

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

○ -5	○ +8	○ -19
○ +1	○ +3	○ -1
○ +1	○ +1	○ +2
○ 0	○ +1	○ +1

An elliptic net!

Curve + Points give Net

Theorem (KS)

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, there exist rational functions

$$\Psi_{\mathbf{v}} : E^n \to K$$

such that for any fixed $\mathbf{P} \in E^n$, the function $W : \mathbb{Z}^n \to K$ defined by

$$W(\mathbf{v}) = \Psi_{\mathbf{v}}(\mathbf{P})$$

is an elliptic net.

Functions $\Psi_{\mathbf{v}}$

The functions $\Psi_{\mathbf{v}}$ satisfy

1. $\Psi_{\mathbf{v}}(\mathbf{P})$ vanishes exactly when $\mathbf{v} \cdot \mathbf{P} = 0$ on E and has poles supported on a certain simple set. Example:

$$\Psi_{m,n}(P, Q) = 0 \text{ whenever } [m]P + [n]Q = 0$$

2. $\Psi_{\mathbf{v}} = 1$ whenever $\mathbf{v}$ is $\mathbf{e}_i$ or $\mathbf{e}_i + \mathbf{e}_j$ for some standard basis vectors $\mathbf{e}_i \neq \mathbf{e}_j$.

- We call W the elliptic net associated to $E, P_1, \ldots, P_n$, and write $W_{E,\mathbf{P}}$.
- We call $P_1, \ldots, P_n$ the basis of $W_{E,\mathbf{P}}$.

Net Polynomial Examples

In higher rank case, we also have such polynomial representations.

$$\Psi_{-1,1} = x_1 - x_2 \ ,$$

$$\Psi_{2,1} = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \ ,$$

$$\Psi_{2,-1} = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ ,$$

$$\Psi_{1,1,1} = \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ ,$$

Can calculate more via the recurrence...

$$\begin{aligned}\Psi_{3,1} = {} & (x_2 - x_1)^{-3}(4x_1^6 - 12x_2x_1^5 + 9x_2^2x_1^4 + 4x_2^3x_1^3 \\ & - 4y_2^2x_1^3 + 8y_1^2x_1^3 - 6x_2^4x_1^2 + 6y_2^2x_2x_1^2 - 18y_1^2x_2x_1^2 \\ & + 12y_1^2x_2^2x_1 + x_2^6 - 2y_2^2x_2^3 - 2y_1^2x_2^3 + y_2^4 - 6y_1^2y_2^2 \\ & + 8y_1^3y_2 - 3y_1^4) \ .\end{aligned}$$

Example over $\mathbb{Q}$

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0, 0), Q = (1, 0)$$

4335	5959	12016	−55287	23921	1587077
94	479	919	−2591	13751	68428
−31	53	−33	−350	493	6627
−5	8	−19	−41	−151	989
1	3	−1	−13	−36	181
1	1	2	−5	7	89
0	1	1	−3	11	38

$\uparrow$
Q

$P \rightarrow$

Example over $\mathbb{F}_5$

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

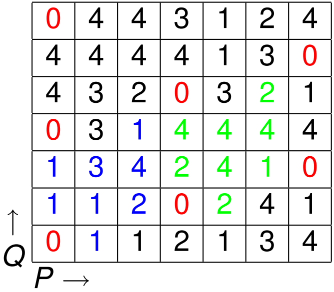
0	4	4	3	1	2	4
4	4	4	4	1	3	0
4	3	2	0	3	2	1
0	3	1	4	4	4	4
1	3	4	2	4	1	0
1	1	2	0	2	4	1
0	1	1	2	1	3	4

$\uparrow$ Q

$P \rightarrow$

- The polynomial $\Psi_{\mathbf{v}}(\mathbf{P}) = 0$ if and only if $\mathbf{v} \cdot \mathbf{P} = 0$.
- These zeroes lie in a lattice: the *lattice of apparition* associated to prime (here, 5).

Periodicity Property with Respect to Lattice of Apparition



0	4	4	3	1	2	4
4	4	4	4	1	3	0
4	3	2	0	3	2	1
0	3	1	4	4	4	4
1	3	4	2	4	1	0
1	1	2	0	2	4	1
0	1	1	2	1	3	4

- The elliptic net is not periodic modulo the lattice of apparition.
- The appropriate translation property should tell how to obtain the green values from the blue values.
- There are such translation properties, and it is within these that the Tate pairing information lies.

Elliptic Nets and Linear Combinations of Points

- If W_i is the elliptic net associated to E, P_i, Q_i for $i = 1, 2$, and

  $$[a_1]P_1 + [b_1]Q_1 = [a_2]P_2 + [b_2]Q_2$$

  then

  $$W_1(a_1, b_1) \text{ is not necessarily equal to } W_2(a_2, b_2) \ .$$

- So how do we propose to compare two elliptic nets supposedly associated to the same linear combinations, but using different bases?

Defining a Net on a Free Abelian Cover

- Assume $E(K)$ is finitely generated. Let $\hat{E}$ be any finite rank free abelian group surjecting onto $E(K)$.

$$\pi : \hat{E} \to E(K)$$

- For a basis P_1, P_2, choose $p_i \in \hat{E}$ such that $\pi(p_i) = P_i$.
- We specify an identification

$$\mathbb{Z}^2 \cong \langle p_1, p_2 \rangle$$

  via $\mathbf{e}_i \mapsto p_i$.
- The elliptic net W associated to E, P_1, P_2 and defined on $\mathbb{Z}^2$ is now identified with an elliptic net W' defined on $\hat{E}$.
- This allows us to compare elliptic nets associated to different bases.

Defining a Special Equivalence Class

Definition

Let $W_1, W_2 : A \to K$. Suppose $f : A \to K^*$ is a quadratic function. If

$$W_1(\mathbf{v}) = f(\mathbf{v}) W_2(\mathbf{v})$$

for all $\mathbf{v}$, then we say W_1 *is equivalent to* W_2.

- Elliptic nets associated to different bases are equivalent, when the elliptic nets are viewed as maps on $\hat{E}$ as explained in the previous slide.
- In this way, we can associate an equivalence class to a subgroup of $E(K)$.

Bilinear Pairings

A bilinear pairing is a map

$$e : G_1 \times G_2 \to G_3$$

where G_i are abelian groups and G_3 is cyclic, and for all $p_1, p_2 \in \mathbb{G}_1$, $q_1, q_2 \in \mathbb{G}_2$, we have

$$e(p_1 + p_2, q_1) = e(p_1, q_1)e(p_2, q_1)$$
$$e(p_1, q_1 + q_2) = e(p_1, q_1)e(p_1, q_2)$$

Pairing-Based Cryptographic Protocols

- tripartite Diffie-Hellman key exchange [Joux]
- identity-based encryption [Boneh-Franklin]
- many others...

Tate Pairing

$$\begin{array}{ll} m \geq 1 & P \in E(K)[m] \\ E/K \text{ an elliptic curve} & Q \in E(K)/mE(K) \end{array}$$

f_P with divisor $m(P) - m(\mathcal{O})$
$D_Q \sim (Q) - (\mathcal{O})$ with support disjoint from $\operatorname{div}(f_P)$

Define

$$\tau_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$$

by

$$\tau_m(P, Q) = f_P(D_Q) \ .$$

It is well-defined, bilinear and Galois invariant.

Weil Pairing

For $P, Q \in E(K)[m]$, the more well-known Weil pairing can be computed via two Tate pairings:

$$e_m(P, Q) = \tau_m(P, Q)\tau_m(Q, P)^{-1} \quad .$$

It is bilinear, alternating, and non-degenerate.

Computing the Tate Pairing

- We must calculate $f_P(D_Q)$, where $\mathrm{div}(f_P) = m(P) - m(\mathcal{O})$.
- There are functions f_i for each $i = 1, 2, \ldots$ such that

$$f_{i+j} = f_i f_j \frac{L}{V}$$

  where L and V are the lines used in the computation of the sum of points $[i]P$ and $[j]P$ on the elliptic curve.
- (The f_i have divisors $i(P) - ([i]P) - (i-1)(\mathcal{O})$.)
- Calculate $f_m = f_P$ by applying this step repeatedly, calculating the multiples of P as you go.
- Most efficient is double-and-add: at each step, go from i to either $2i$ or $2i+1$ (one or two steps respectively).
- Miller's algorithm: calculate $f_m = f_P$ via double-and-add, and evaluate at D_Q.

Computing the Tate Pairing

- Of course, this has since been optimised extensively.
- To obtain a unique value as the result of a Tate pairing (instead of an equivalence class), one usually performs a final exponentiation.

Statement of Theorem

$$\begin{array}{ll} m \geq 1 & P \in E(K)[m] \\ E/K \text{ an elliptic curve} & Q \in E(K)/mE(K) \end{array}$$

Theorem (KS)

Choose $S \in E(K)$ such that $S \notin \{\mathcal{O}, -Q\}$. Choose p, q, $s \in \hat{E}$ such that $\pi(p) = P$, $\pi(q) = Q$ and $\pi(s) = S$. Let W be an elliptic net in the equivalence class associated to a subgroup of $E(K)$ containing P, Q, and S. Then the quantity

$$\tau_m(P, Q) = \frac{W(s + mp + q)W(s)}{W(s + mp)W(s + q)}$$

is the Tate pairing.

Choosing an Elliptic Net

Corollary

In particular,

$$\tau_m(P,P) = \frac{W_{E,P}(m+2)W_{E,P}(1)}{W_{E,P}(m+1)W_{E,P}(2)} \ ,$$

and

$$\tau_m(P,Q) = \frac{W_{E,P,Q}(m+1,1)W_{E,P,Q}(1,0)}{W_{E,P,Q}(m+1,0)W_{E,P,Q}(1,1)} \ .$$

Tate Pairing and Periodicity Properties

Example

$E : y^2 + y = x^3 + x^2 - 2x$ over $\mathbb{F}_{73}$.
$P = (0, 0)$ has order $m = 9$.
The associated sequence is
$0, 1, 1, 70, 11, 38, 30, 52, 7, 0, 56, 30, 30, 61, 47, 3, 8, 9, 0, \ldots$
W(1),W(2) W(m+1),W(m+2)

$$\tau_m(P, P) = \left(\frac{W(m+2)}{W(m+1)}\right)\left(\frac{W(1)}{W(2)}\right) = \left(\frac{30}{56}\right)\left(\frac{1}{1}\right) = 24$$

Note: Result is in $\mathbb{F}_{73}^* / (\mathbb{F}_{73}^*)^9$ which is not trivial, since $9 | (73 - 1)$. For a field of q elements, the smallest integer k such that $m | q^k - 1$ is called the *embedding degree*.

Elliptic Net Algorithm

Algorithm Outline

1. Given E, P, Q with $[m]P = 0$, calculate the initial terms of $W_{E,P,Q}$.
2. Using the recurrence relation, calculate the terms $W(m+1,0)$, $W(m+1,1)$.
3. Calculate $\tau_m(P,Q) = W(m+1,1)/W(m+1,0)$.
4. Perform final exponentiation as in Miller's.

Remarks:

- There are polynomial formulae for the initial terms of Step 1.
- Step 4 is also performed in Miller's algorithm and the same efficient methods apply here.
- The challenge lies in efficient computation of large terms of the net $W_{E,P,Q}$.

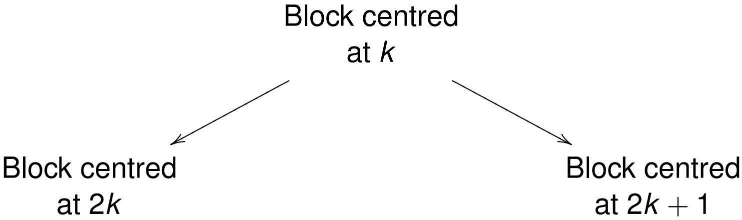
Computing Terms of $W_{E,P,Q}$

		(k-1,1)	(k,1)	(k+1,1)			
(k-3,0)	(k-2,0)	(k-1,0)	(k,0)	(k+1,0)	(k+2,0)	(k+3,0)	(k+4,0)

Figure: A block centred at k

Computing Terms of $W_{E,P,Q}$

Double and add algorithm:



Block centred at k

Block centred at $2k$

Block centred at $2k+1$

Each term of the new block requires one instance of the recurrence relation, i.e. several multiplications and an addition.

Complexity

Let k be the embedding degree. Let $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$.

S	squaring in $\mathbb{F}_q$
S_k	squaring in $\mathbb{F}_{q^k}$
M	multiplication in $\mathbb{F}_q$
M_k	multiplication in $\mathbb{F}_{q^k}$

Algorithm:	Elliptic Net
Double:	$6S + (6k + 26)M + S_k + \frac{3}{2}M_k$
DoubleAdd:	$6S + (6k + 26)M + S_k + 2M_k$

Algorithm:	Optimised Miller's [1]
Double:	$4S + (k + 7)M + S_k + M_k$
DoubleAdd:	$7S + (2k + 19)M + S_k + 2M_k$

---

[1] Koblitz N., Menezes A., *Pairing-based cryptography at high security levels*, 2005

In Practice

Thank you to Michael Scott, Augusto Jun Devigili and Ben Lynn for implementing the algorithm. A timing comparison program is bundled with Ben Lynn's Pairing-Based Cryptography Library at http://crypto.stanford.edu/pbc/

- **type a**: 512 bit base-field, embedding degree 2, 1024 bits security, $y^2 = x^3 + x$, group order is a Solinas prime.
- **type f**: 160 bit base-field, embedding degree 12, 1920 bits security, Barreto-Naehrig curves [*Pairing Friendly Elliptic Curves of Prime Order*, SAC 2005]

Algorithm:	Miller's	Elliptic Net
type a	19.8439 ms	40.6252 ms
type f	238.4378 ms	239.5314 ms

average time of a test suite of 100 randomly generated pairings in each of the two cases

Potential Advantages

- Naturally inversion-free.
- Naturally deterministic.
- Since Double and DoubleAdd steps are similar or the same, is independent of hamming weight.
- Lends itself to time-saving precomputation for repeated pairings $e_m(P, Q)$, e.g. where E, m, and P are fixed.
- Code is simple.

Improving the Algorithm

To compute a given pairing, we have many choices:

- Choice of a point S.
- Choice of lifts of P, Q, S.
- Choice of a subgroup of $E(K)$ containing P and Q, and S.
- Choice of an elliptic net in the given equivalence class.
- Choice of scaling of the chosen net.
- Choice of recurrences used to compute the terms of the net.
- Choice of order of operations for the computations.

In the algorithm I have given, I have made apparently convenient choices for these things. It is very probable significant improvement is possible.

Summary

- Elliptic nets provide an alternative computational model for elliptic curves.
- The terms of an elliptic net compute the Tate and Weil pairings.
- Other cryptographic applications?

Slides, Article, and Pari/GP scripts available at
http://www.math.brown.edu/~stange/