Katherine Stange

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

> ECC 2007, Dublin, Ireland

> > ◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 のへで

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Outline

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets

Upping the Dimension Definitions Properties

Pairings

Pairings in ECC Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ○ □ ○ ○ ○ ○

Outline

Elliptic Divisibility Sequences Mathematics

Applications

Elliptic Nets

Upping the Dimension Definitions Properties

Pairings

Pairings in ECC Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本・山田・山田・山

Definition

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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲ロト ▲周 ト ▲ ヨ ト ▲ ヨ ト つのの

Definition

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

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

・ コ ト ・ 厚 ト ・ ヨ ト ・ ヨ ト ・ ヨ ・

• Generated by W_1, \ldots, W_4 via the recurrence.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Definition

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

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

・ロト ・ 雪 ト ・ ヨ ト ・ ヨ ト

- Generated by W_1, \ldots, W_4 via the recurrence.
- Example: 1,2,3,4,5,6,7,8,9,10,...

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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, ...
- Example: 1,3,8,21,55,144,377,987,2584,6765,...

・ロト ・ 雪 ト ・ ヨ ト ・ ヨ ト

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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,...
- Example: 1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, ...
- Example: 1, 1, -3, 11, 38, 249, -2357, 8767, 496036, -3769372, -299154043, -12064147359, ...

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

P = (0, 0)

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本 小田 ・ 小田 ・ 今日 ・

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

P = (0, 0)

[2]P = (3,5)

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本 小田 ・ 小田 ・ 今日 ・

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

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶ ▲□▶ ▲ □▶ ▲ □▶ ▲ □ ● のへで

P = (0,0) [2]P = (3,5) $[3]P = \left(-\frac{11}{9}, \frac{28}{27}\right)$

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

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

◆□▶ ◆□▶ ◆ □▶ ★ □▶ = □ ● ○ ○ ○

$$P = (0,0)$$

$$[2]P = (3,5)$$

$$[3]P = \left(-\frac{11}{9}, \frac{28}{27}\right)$$

$$[4]P = \left(\frac{114}{121}, -\frac{267}{1331}\right)$$

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

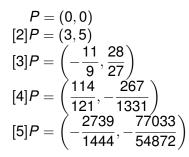
Elliptic Divisibility Sequences Mathematics

Elliptic Nets in

tange

Elliptic Nets

・ロト ・ 雪 ト ・ ヨ ト ・ ヨ ト



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

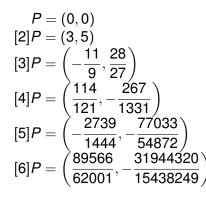
Elliptic Divisibility Sequences Mathematics

Elliptic Nets in

tange

Elliptic Nets

・ロト ・雪 ト ・ ヨ ト ・ ヨ ト



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

$$P = (0,0)$$

$$[2]P = (3,5)$$

$$[3]P = \left(-\frac{11}{9}, \frac{28}{27}\right)$$

$$[4]P = \left(\frac{114}{121}, -\frac{267}{1331}\right)$$

$$[5]P = \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right)$$

$$[6]P = \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right)$$

$$[7]P = \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right)$$

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

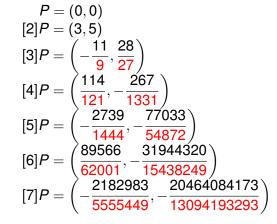
Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets





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

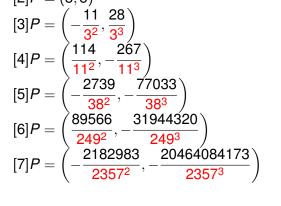
Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

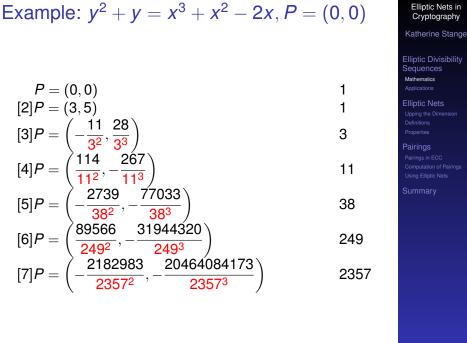
Summary



P = (0, 0)

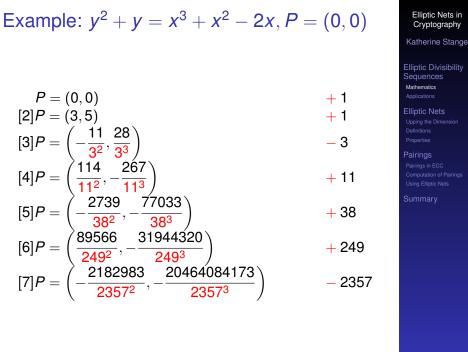
[2]P = (3,5)

▲□▶▲□▶▲□▶▲□▶ ■ のへの

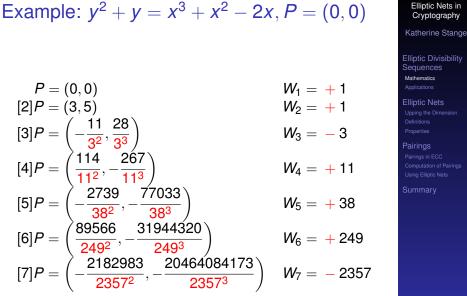


◆□▶ ◆□▶ ◆□▶ ◆□▶ □ ● ●

Elliptic Nets in Cryptography



◆□▶ ◆□▶ ◆□▶ ◆□▶ □ ● ●



Sequences Mathematics

Elliptic Nets

Pairings

◆□▶ ◆□▶ ◆□▶ ◆□▶ □ ● ●

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

 $P, [2]P, [3]P, [4]P, \dots$

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

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

$$\begin{split} \Psi_1 &= 1, \qquad \Psi_2 = 2y, \\ \Psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\ \Psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \end{split}$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

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

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

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

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

It gives an elliptic divisibility sequence!

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

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*.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本・日本・日本・日本・日本

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.

・ コ ト ・ 厚 ト ・ ヨ ト ・ ヨ ト ・ ヨ ・

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本・モート ほう うくぐ

 Using the formulae, we can consider divison polynomials over finite fields (where "denominator" has no meaning).

・ コ ト ・ 厚 ト ・ ヨ ト ・ ヨ ト ・ ヨ ・

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

- 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 $W_n = 0$.

・ コ ト ・ 厚 ト ・ ヨ ト ・ ヨ ト ・ ヨ ・

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

- 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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

- 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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

- 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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

- 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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

- 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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Outline

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets

Upping the Dimension Definitions Properties

Pairings

Pairings in ECC Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本・山田・山田・山

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*. Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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. Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Outline

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets

Upping the Dimension Definitions

Pairings

Pairings in ECC Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶▲□▶▲□▶▲□▶ □ ● ● ●

The Question - Upping the Dimension

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

$$[n]P \leftrightarrow W_n$$

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

The Question - Upping the Dimension

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

$$[n] P \leftrightarrow W_n$$

We might dream of ...

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

・ コ ト ・ 同 ト ・ ヨ ト ・ ヨ ト

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

The Question - Upping the Dimension

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

$$[n]P \leftrightarrow W_n$$

We might dream of ...

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

Or even ...

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

・ コ ト ・ 厚 ト ・ ヨ ト ・ ヨ ト ・ ヨ ・

etc.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Outline

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets

Upping the Dimension Definitions Properties

Pairings

Pairings in ECC Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・西ト・山田・山田・山下

Definition (KS)

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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

Definition (KS)

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

$$egin{aligned} &\mathcal{W}(p+q+s)\mathcal{W}(p-q)\mathcal{W}(r+s)\mathcal{W}(r)\ &+\mathcal{W}(q+r+s)\mathcal{W}(q-r)\mathcal{W}(p+s)\mathcal{W}(p)\ &+\mathcal{W}(r+p+s)\mathcal{W}(r-p)\mathcal{W}(q+s)\mathcal{W}(q)=0 \end{aligned}$$

Elliptic divisibility sequences are a special case
 (A = Z)

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

Definition (KS)

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

$$\begin{split} \mathcal{W}(p+q+s)\mathcal{W}(p-q)\mathcal{W}(r+s)\mathcal{W}(r) \\ &+\mathcal{W}(q+r+s)\mathcal{W}(q-r)\mathcal{W}(p+s)\mathcal{W}(p) \\ &+\mathcal{W}(r+p+s)\mathcal{W}(r-p)\mathcal{W}(q+s)\mathcal{W}(q) = 0 \end{split}$$

- Elliptic divisibility sequences are a special case
 (A = Z)
- ▶ In this talk, we will mostly discuss rank 2: $A = \mathbb{Z}^2$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Definition (KS)

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

$$\begin{split} \mathcal{W}(p+q+s)\mathcal{W}(p-q)\mathcal{W}(r+s)\mathcal{W}(r) \\ &+\mathcal{W}(q+r+s)\mathcal{W}(q-r)\mathcal{W}(p+s)\mathcal{W}(p) \\ &+\mathcal{W}(r+p+s)\mathcal{W}(r-p)\mathcal{W}(q+s)\mathcal{W}(q) = 0 \end{split}$$

- Elliptic divisibility sequences are a special case
 (A = 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 Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

$$_{\circ}$$
 [3]*Q* $_{\circ}$ [1]*P* + [3]*Q* $_{\circ}$ [2]*P* + [3]*Q*

$$_{\circ}$$
 [2] Q $_{\circ}$ [1] P + [2] Q $_{\circ}$ [2] P + [2] Q

$$[1]Q$$
 $[1]P + [1]Q$ $[2]P + [1]Q$

・ロト ・個ト ・ヨト ・ヨト ・ヨー

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

$$(\frac{56}{25}, \frac{371}{125}) (-\frac{95}{64}, \frac{495}{512}) (\frac{328}{361}, -\frac{2800}{6859})$$

$$\circ \quad \begin{pmatrix} 6\\1 \end{pmatrix}, -\frac{16}{1} \end{pmatrix} \qquad \circ \quad \begin{pmatrix} 1\\9 \end{pmatrix}, -\frac{19}{27} \end{pmatrix} \qquad \circ \quad \begin{pmatrix} 39\\1 \end{pmatrix}, \frac{246}{1} \end{pmatrix}$$

$$\circ \quad \left(\frac{1}{1}, \frac{0}{1}\right) \qquad \circ \quad \left(-\frac{2}{1}, -\frac{1}{1}\right) \quad \circ \quad \left(\frac{5}{4}, -\frac{13}{8}\right)$$

$$_{\circ} \infty \qquad \qquad _{\circ} \left(\frac{0}{1}, \frac{0}{1} \right) \qquad _{\circ} \left(\frac{3}{1}, \frac{5}{1} \right)$$

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・国ト・ヨト・ヨト のへの

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

$$_{\circ} \quad \left(\frac{56}{5^2}, \frac{371}{5^3}\right) \quad _{\circ} \quad \left(-\frac{95}{8^2}, \frac{495}{8^3}\right) \quad _{\circ} \quad \left(\frac{328}{19^2}, -\frac{2800}{19^3}\right)$$

$$\ \ \, \left(\frac{6}{1^2},-\frac{16}{1^3}\right) \quad \ \ \, _{\circ} \quad \left(\frac{1}{3^2},-\frac{19}{3^3}\right) \quad \ \ \, _{\circ} \quad \left(\frac{39}{1^2},\frac{246}{1^3}\right)$$

$$\circ \quad \left(\frac{1}{1^2}, \frac{0}{1^3}\right) \qquad \circ \quad \left(-\frac{2}{1^2}, -\frac{1}{1^3}\right) \quad \circ \quad \left(\frac{5}{2^2}, -\frac{13}{2^3}\right)$$

$$_{\circ} \infty \qquad \qquad _{\circ} \left(\frac{0}{1^2}, \frac{0}{1^3} \right) \qquad _{\circ} \left(\frac{3}{1^2}, \frac{5}{1^3} \right)$$

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

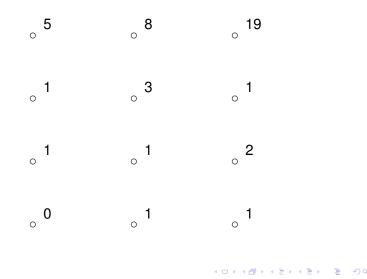
Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・国ト・ヨト・ヨト のへの

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



Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

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

。 - 5	。 + 8	_ 19
。 + 1	。+ 3	• – 1
。 + 1	。+ 1 。	→ + 2
。 + 0	° +1	• + 1
		(日)、(四)、(注)、(注)、(注)、(注)

Elliptic Nets in Cryptography

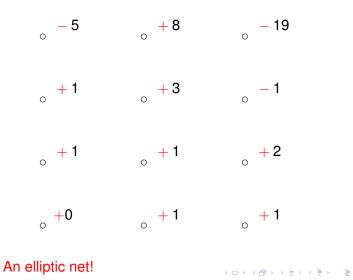
Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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



Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

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

・ コ ト ・ 同 ト ・ ヨ ト ・ ヨ ト

is an elliptic net.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

ふして 前 ふぼとうぼう (日)

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:

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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:

$$\Psi_{m,n}(P,Q) = 0$$
 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 $\mathbf{e}_i \neq \mathbf{e}_j$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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:

$$\Psi_{m,n}(P,Q) = 0$$
 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, P₁,..., P_n, and write W_{E,P}.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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:

$$\Psi_{m,n}(P,Q) = 0$$
 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, P₁,..., P_n, and write W_{E,P}.
- We call P_1, \ldots, P_n the basis of $W_{E,\mathbf{P}}$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

うせん 前 (本語) (語) (語) (日)

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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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

$$\begin{split} \Psi_{-1,1} &= x_1 - x_2 \ , \\ \Psi_{2,1} &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \ , \\ \Psi_{2,-1} &= (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ , \\ \Psi_{1,1,1} &= \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ , \end{split}$$

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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

$$\begin{split} \Psi_{-1,1} &= x_1 - x_2 \ , \\ \Psi_{2,1} &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \ , \\ \Psi_{2,-1} &= (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ , \\ \Psi_{1,1,1} &= \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ , \end{split}$$

Can calculate more via the recurrence...

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Call'INGS Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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

$$\begin{split} \Psi_{-1,1} &= x_1 - x_2 \ , \\ \Psi_{2,1} &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \ , \\ \Psi_{2,-1} &= (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ , \\ \Psi_{1,1,1} &= \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ , \end{split}$$

Can calculate more via the recurrence...

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

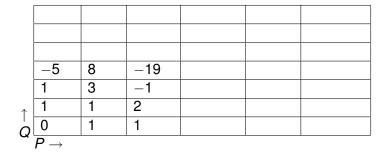
Elliptic Nets Upping the Dimension Definitions Properties

Computation of Pairings Using Elliptic Nets

Summary

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 のへで

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



Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

◆□ ▶ ◆□ ▶ ◆ 臣 ▶ ◆ 臣 ▶ ○ 臣 ● のへで

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

	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
O^{+}	0	1	1	-3	11	38
9	$\overline{P} \rightarrow$					

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

	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
O^{-}	0	1	1	-3	11	38
9	$\overline{P} \rightarrow$		-			

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

	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
$\stackrel{ }{Q}$	0	1	1	-3	11	38
a	$\overline{P} \rightarrow$			-	-	

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

	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
\overline{O}	0	1	1	-3	11	38
Q,	$\overline{P} \rightarrow$				·	

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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
$\stackrel{ }{Q}$	0	1	1	-3	11	38
9	$\overline{P} \rightarrow$					

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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				
\dot{o}	0	1	1	2	1	3	4				
G	$\overline{P} \rightarrow$										

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

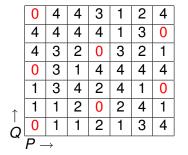
Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

◆□▶ ◆□▶ ◆ □▶ ★ □▶ = □ ● ○ ○ ○

Example over \mathbb{F}_5

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



• The polynomial $\Psi_{\mathbf{v}}(\mathbf{P}) = 0$ if and only if $\mathbf{v} \cdot \mathbf{P} = 0$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

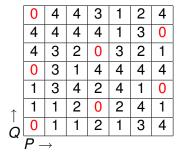
Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本・日本・日本・日本・日本

Example over \mathbb{F}_5

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



• 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). Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Outline

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets

Upping the Dimension Definitions

Properties

Pairings

Pairings in ECC Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

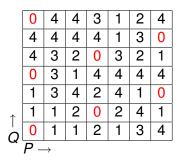
Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲ロト ▲周 ト ▲ ヨ ト ▲ ヨ ト つのの



Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

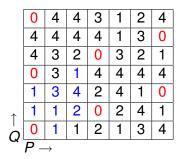
Elliptic Nets Upping the Dimension Definitions

Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・四ト・山田・山田・山口・



Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

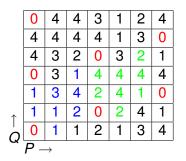
Elliptic Nets Upping the Dimension Definitions

Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・西ト・山田・山田・



Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

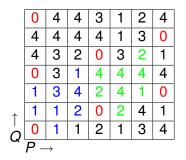
Elliptic Nets Upping the Dimension Definitions

Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・西ト・山田・山田・



 The elliptic net is not periodic modulo the lattice of apparition.

・ロト ・雪 ト ・ ヨ ト ・ ヨ ト

3

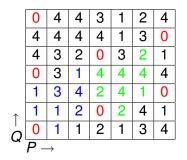
Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets



- 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.

・ コ ト ・ 西 ト ・ 日 ト ・ 日 ト

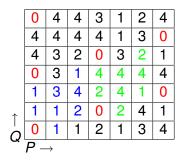
Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets



- 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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

There are such translation properties, and it is within these that the Tate pairing information lies.

Elliptic Nets and Linear Combinations of Points

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Ċ

Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

くしゃ 本語 そ 本語 を 本語 や スター

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

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

・ コ ト ・ 何 ト ・ ヨ ト ・ ヨ ト ・ ヨ ・

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions

Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

 $W_1(a_1, b_1)$ 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? Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Fioperile

Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

◆□▶ ◆□▶ ◆目▶ ◆目▶ → 目 → 今々ぐ

Assume E(K) is finitely generated. Let Ê be any finite rank free abelian group surjecting onto E(K).

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions

Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

うせん 前 (本語)(本語)(本語)(本語)(本語)

Assume E(K) is finitely generated. Let Ê be any finite rank free abelian group surjecting onto E(K).

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

・ コ ト ・ 何 ト ・ ヨ ト ・ ヨ ト ・ ヨ ・

► For a basis P_1 , P_2 , choose $p_i \in \hat{E}$ such that $\pi(p_i) = P_i$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions

Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Assume E(K) is finitely generated. Let Ê 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 $\mathbf{e}_i \mapsto p_i$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions

Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Assume E(K) is finitely generated. Let Ê 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, P₁, P₂ and defined on Z² is now identified with an elliptic net W' defined on Ê. Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Assume E(K) is finitely generated. Let Ê 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, P₁, P₂ and defined on Z² is now identified with an elliptic net W' defined on Ê.
- This allows us to compare elliptic nets associated to different bases.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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 **v**, then we say W_1 is equivalent to W_2 .

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲ロト ▲周 ト ▲ ヨ ト ▲ ヨ ト つのの

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 **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 Ê as explained in the previous slide.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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 **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 Ê as explained in the previous slide.
- ► In this way, we can associate an equivalence class to a subgroup of E(K).

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Outline

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets

Upping the Dimension Definitions Properties

Pairings

Pairings in ECC

Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲ロト ▲周 ト ▲ ヨ ト ▲ ヨ ト つのの

Bilinear Pairings

A bilinear pairing is a map

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

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

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

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲ロト ▲周 ト ▲ ヨ ト ▲ ヨ ト つのの

Pairing-Based Cryptographic Protocols

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 のへぐ

 $m \ge 1$ E/K an elliptic curve Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

くしゃ 本語 そ 本語 を 本語 や ふらく

$m \ge 1$ $P \in E(K)[m]$ E/K an elliptic curve $Q \in E(K)/mE(K)$

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・母 ト・モ ト・モー うくぐ

$m \ge 1$ $P \in E(K)[m]$ E/K an elliptic curve $Q \in E(K)/mE(K)$

 f_P with divisor $m(P) - m(\mathcal{O})$

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・西ト・日本・日本・日本・日本

 $m \ge 1$ E/K an elliptic curve $P \in E(K)[m]$ $Q \in E(K)/mE(K)$ f_P with divisor $m(P) - m(\mathcal{O})$ $D_Q \sim (Q) - (\mathcal{O})$ with support disjoint from div (f_P) Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

 $m \ge 1$ E/K an elliptic curve $Q \in E(K)/mE(K)$ f_P with divisor $m(P) - m(\mathcal{O})$ $D_Q \sim (Q) - (\mathcal{O})$ with support disjoint from div (f_P)

Define

$$au_m: E(K)[m] \times E(K)/mE(K) \rightarrow K^*/(K^*)^m$$

by

$$au_m(P,Q) = f_P(D_Q)$$
 .

It is well-defined, bilinear and Galois invariant.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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

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

It is bilinear, alternating, and non-degenerate.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

Outline

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets

Upping the Dimension Definitions Properties

Pairings

Pairings in ECC Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲ロト ▲周 ト ▲ ヨ ト ▲ ヨ ト つのの

Computing the Tate Pairing

• We must calculate $f_P(D_Q)$, where $\operatorname{div}(f_P) = m(P) - m(\mathcal{O})$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

うせん 前 (本語) (語) (語) (日)

Computing the Tate Pairing

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

Computing the Tate Pairing

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

- (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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

- We must calculate $f_P(D_Q)$, where $\operatorname{div}(f_P) = m(P) m(\mathcal{O})$.
- There are functions f_i for each i = 1, 2, ... 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)(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 2*i* or 2*i* + 1 (one or two steps respectively).

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

- We must calculate $f_P(D_Q)$, where $\operatorname{div}(f_P) = m(P) m(\mathcal{O})$.
- There are functions f_i for each i = 1, 2, ... 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)(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 2*i* or 2*i* + 1 (one or two steps respectively).
- Miller's algorithm: calculate f_m = f_P via double-and-add, and evaluate at D_Q.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Of course, this has since been optimised extensively.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶▲□▶▲□▶▲□▶ □ のQ@

- 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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本・日本・日本・日本

Outline

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets

Upping the Dimension Definitions Properties

Pairings

Pairings in ECC Computation of Pairings Using Elliptic Nets Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

Statement of Theorem

 $m \ge 1$ $P \in E(K)[m]$ E/K an elliptic curve $Q \in E(K)/mE(K)$ Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

くしゃ 本語 そ 本語 を 本語 や スター

Statement of Theorem

 $m \ge 1$ $P \in E(K)[m]$ E/K an elliptic curve $Q \in E(K)/mE(K)$

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

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

is the Tate pairing.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Choosing an Elliptic Net

Corollary In particular,

$$au_m(P,P) = rac{W_{E,P}(m+2)W_{E,P}(1)}{W_{E,P}(m+1)W_{E,P}(2)} \; ,$$

and

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

イロト 不得 ト イヨト イヨト 三日 -

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Example

$$E: y^2 + y = x^3 + x^2 - 2x$$
 over \mathbb{F}_{73} .
 $P = (0, 0)$ has order $m = 9$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

ふして 前 ふぼとうぼう (日)

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, ...

・ロト ・ 雪 ト ・ ヨ ト ・ ヨ ト

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Example

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

・ロト ・ 雪 ト ・ ヨ ト ・ ヨ ト

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Example

・ロト ・ 雪 ト ・ ヨ ト ・ ヨ ト

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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, ...

- 日本 - 4 日本 - 4 日本 - 日本

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Example

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

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

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 Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Algorithm Outline

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

ふして 前 ふぼとうぼう (日)

Algorithm Outline

Given *E*, *P*, *Q* with [*m*]*P* = 0, calculate the initial terms of *W*_{*E*,*P*,*Q*}.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

うせん 御 ・ (明・ (明・ (日・

Algorithm Outline

- 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).

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

Algorithm Outline

- 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 $\tau_m(P, Q) = W(m+1, 1)/W(m+1, 0)$.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶▲□▶▲□▶▲□▶ □ のQ@

Algorithm Outline

- 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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

Algorithm Outline

- 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:

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

Algorithm Outline

- 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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Algorithm Outline

- 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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Algorithm Outline

- 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}.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

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

◆□▶ ◆□▶ ◆□▶ ◆□▶ □ のQ@

Elliptic Nets in Cryptography

Katherine Stange

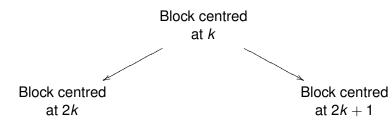
Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

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

Double and add algorithm:



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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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: DoubleAdd:	$\frac{6S + (6k + 26)M + S_k + \frac{3}{2}M_k}{6S + (6k + 26)M + S_k + 2M_k}$	
Algorithm:	Optimised Miller's ¹	
3	optimiood millor o	

¹Koblitz N., Menezes A., *Pairing-based cryptography at high* security levels, 2005 Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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]

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のの⊙

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

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・日本・日本・日本・日本

Naturally inversion-free.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

・ロト・母 ト・モ ト・モー うくぐ

- Naturally inversion-free.
- Naturally deterministic.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

うせん 御 ・ (明・ (明・ (日・

- Naturally inversion-free.
- Naturally deterministic.
- Since Double and DoubleAdd steps are similar or the same, is independent of hamming weight.

・ロト ・ 雪 ト ・ ヨ ト ・ ヨ ト

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

- 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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

- 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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

◆□▶ ◆□▶ ◆□▶ ◆□▶ □ ● ●

To compute a given pairing, we have many choices:

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

くしゃ 本語 そ 本語 を 本語 や スター

To compute a given pairing, we have many choices:

► Choice of a point S.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

うせん 前 (本語)(本語)(本語)(本語)(本語)

To compute a given pairing, we have many choices:

- Choice of a point S.
- Choice of lifts of P, Q, S.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

Summary

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.

▲ロト ▲周 ト ▲ ヨ ト ▲ ヨ ト つのの

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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.

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets

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. Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings in ECC Computation of Pairings Using Elliptic Nets

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/

Elliptic Nets in Cryptography

Katherine Stange

Elliptic Divisibility Sequences Mathematics Applications

Elliptic Nets Upping the Dimension Definitions Properties

Pairings Pairings in ECC Computation of Pairings Using Elliptic Nets