The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences

Katherine Stange[1] and Kristin Lauter[2]

[1]Department of Mathematics, Harvard University
and
[2]Microsoft Research, Redmond, Washington

Fields Cryptography Retrospective Meeting,
Toronto, May 14, 2009

-1cm-

1cm

Elliptic Curves in Cryptography

- Suggested by Victor Miller and Neil Koblitz in 1985
- Now implemented many places; part of NSA's Suite B
- Relies on Problem:
  - Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$. Determine k such that $Q = [k]P$.
- Seems safe since no one can think of a good way to do it (in subexponential time).

Elliptic Curves in Cryptography

- Suggested by Victor Miller and Neil Koblitz in 1985
- Now implemented many places; part of NSA's Suite B
- Relies on Problem:
  - Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$. Determine k such that $Q = [k]P$.
- Seems safe since no one can think of a good way to do it (in subexponential time).
- So... it is in the interests of world security that we keep failing to solve this problem in new and creative ways.

Generic attacks

Attacks which work in any group where group operation is easy to compute. This relies on the 'birthday paradox': selecting elements of a set of size n randomly, we expect to see a repeat after $O(\sqrt{n})$ selections.

Generic attacks

Attacks which work in any group where group operation is easy to compute. This relies on the 'birthday paradox': selecting elements of a set of size n randomly, we expect to see a repeat after $O(\sqrt{n})$ selections.
$Q = [k]P$; find k?

Generic attacks

Attacks which work in any group where group operation is easy to compute. This relies on the 'birthday paradox': selecting elements of a set of size n randomly, we expect to see a repeat after $O(\sqrt{n})$ selections.
$Q = [k]P$; find k?
Shanks baby-step-giant-step:

- Let $N = \lceil \sqrt{n} \rceil$.
- Create a list of elements $P, [2]P, \ldots, [N]P$.
- Create a list of elements $Q + R, Q + [2]R, \ldots, Q + [N]R$ where $R = [-N]P$.
- Find a collision between the two sets.

Generic attacks

Attacks which work in any group where group operation is easy to compute. This relies on the 'birthday paradox': selecting elements of a set of size n randomly, we expect to see a repeat after $O(\sqrt{n})$ selections.
$Q = [k]P$; find k?
Shanks baby-step-giant-step:

- Let $N = \lceil \sqrt{n} \rceil$.
- Create a list of elements $P, [2]P, \ldots, [N]P$.
- Create a list of elements $Q + R, Q + [2]R, \ldots, Q + [N]R$ where $R = [-N]P$.
- Find a collision between the two sets.

Pollard rho:

- Iterate a sufficiently 'mixing' function $f : G \to G$ (whose definition depends on Q) and wait for $f^{(i)}(P) = f^{(2i)}(P)$

Some Attacks

- Pohlig-Hellman: a method to reduce ECDLP to the case of prime order. Depends on the Chinese remainder theorem.

Some Attacks

- Pohlig-Hellman: a method to reduce ECDLP to the case of prime order. Depends on the Chinese remainder theorem.
- 'anomalous': curve has p points over $\mathbb{F}_p$; Samaev, Satoh-Araki, Smart, and Shipsey all give polynomial algorithms for discrete log in these cases. (These work via an isomorphism to the group $\mathbb{F}_p^+$.)

Some Attacks

- Pohlig-Hellman: a method to reduce ECDLP to the case of prime order. Depends on the Chinese remainder theorem.
- 'anomalous': curve has p points over $\mathbb{F}_p$; Samaev, Satoh-Araki, Smart, and Shipsey all give polynomial algorithms for discrete log in these cases. (These work via an isomorphism to the group $\mathbb{F}_p^+$.)
- Weil descent attacks are also isomorphism attacks over binary fields, this time to the Jacobian of a hyperelliptic curve.

Some Attacks

- Pohlig-Hellman: a method to reduce ECDLP to the case of prime order. Depends on the Chinese remainder theorem.
- 'anomalous': curve has p points over $\mathbb{F}_p$; Samaev, Satoh-Araki, Smart, and Shipsey all give polynomial algorithms for discrete log in these cases. (These work via an isomorphism to the group $\mathbb{F}_p^+$.)
- Weil descent attacks are also isomorphism attacks over binary fields, this time to the Jacobian of a hyperelliptic curve.
- Weil and Tate pairing attacks: more on this later.

Some Attacks

- Pohlig-Hellman: a method to reduce ECDLP to the case of prime order. Depends on the Chinese remainder theorem.
- 'anomalous': curve has p points over $\mathbb{F}_p$; Samaev, Satoh-Araki, Smart, and Shipsey all give polynomial algorithms for discrete log in these cases. (These work via an isomorphism to the group $\mathbb{F}_p^+$.)
- Weil descent attacks are also isomorphism attacks over binary fields, this time to the Jacobian of a hyperelliptic curve.
- Weil and Tate pairing attacks: more on this later.
- Many (mostly) failed attempts to do an index calculus for elliptic curves.

Some Attacks

- Pohlig-Hellman: a method to reduce ECDLP to the case of prime order. Depends on the Chinese remainder theorem.
- 'anomalous': curve has p points over $\mathbb{F}_p$; Samaev, Satoh-Araki, Smart, and Shipsey all give polynomial algorithms for discrete log in these cases. (These work via an isomorphism to the group $\mathbb{F}_p^+$.)
- Weil descent attacks are also isomorphism attacks over binary fields, this time to the Jacobian of a hyperelliptic curve.
- Weil and Tate pairing attacks: more on this later.
- Many (mostly) failed attempts to do an index calculus for elliptic curves.
- Recent success by Claus Diem: curves over a family of finite fields $\mathbb{F}_{q^n}$ where $n = O(\sqrt{\log q})$.

Division polynomials

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

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

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

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

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

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

Anything satsifying this recurrence relation I'll call an *elliptic divisibility sequence*.

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

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

Anything satsifying this recurrence relation I'll call an *elliptic divisibility sequence*. In particular, if we evaluate at P, we get the *elliptic divisibility sequence* associated to E and P.

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

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

Anything satsifying this recurrence relation I'll call an *elliptic divisibility sequence*. In particular, if we evaluate at P, we get the *elliptic divisibility sequence* associated to E and P.

Division polynomials and sequences over finite fields

- The point P will always have finite order, say n. The associated sequence will have $W_n = 0$.

Division polynomials and sequences over finite fields

- 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.

Division polynomials and sequences over finite fields

- 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
$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

Division polynomials and sequences over finite fields

- 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
$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

Division polynomials and sequences over finite fields

- 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
$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

Division polynomials and sequences over finite fields

- 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
$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

Division polynomials and sequences over finite fields

- 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
$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

Division polynomials and sequences over finite fields

- 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
$0, 1, 1, {\color{red}2}, 1, 3, 4, 3, 2, 0, 3, 2, {\color{red}1}, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

Translation properties

Theorem (Ward / Swart / Ayad)

Let W be an elliptic divisibility sequence such that $W(1) = 1, W(2)W(3) \neq 0$. Let $r \in \mathbb{Z}$ be such that $W(r) = 0$. Then there exist a, b such that

$$W(n + kr) = W(n)a^{nk}b^{k^2}.$$

Translation properties

Theorem (Ward / Swart / Ayad)

Let W be an elliptic divisibility sequence such that $W(1) = 1, W(2)W(3) \neq 0$. Let $r \in \mathbb{Z}$ be such that $W(r) = 0$. Then there exist a, b such that

$$W(n + kr) = W(n)a^{nk}b^{k^2}.$$

Example ($E : y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$ over $\mathbb{F}_5$)

$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$
$W(9k + n) \equiv W(n)4^{nk}2^{k^2} \mod 5$

Translation properties

Theorem (Ward / Swart / Ayad)

Let W be an elliptic divisibility sequence such that $W(1) = 1, W(2)W(3) \neq 0$. Let $r \in \mathbb{Z}$ be such that $W(r) = 0$. Then there exist a, b such that

$$W(n + kr) = W(n)a^{nk}b^{k^2}.$$

Example ($E : y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$ over $\mathbb{F}_5$)

$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

$W(9k + n) \equiv W(n)4^{nk}2^{k^2} \mod 5$

$W(10) \equiv 3W(1) \mod 5$

Translation properties

Theorem (Ward / Swart / Ayad)

Let W be an elliptic divisibility sequence such that $W(1) = 1, W(2)W(3) \neq 0$. Let $r \in \mathbb{Z}$ be such that $W(r) = 0$. Then there exist a, b such that

$$W(n + kr) = W(n)a^{nk}b^{k^2}.$$

Example ($E : y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$ over $\mathbb{F}_5$)

$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 2, 1, 3, 4, \ldots$

$W(9k + n) \equiv W(n)4^{nk}2^{k^2} \mod 5$

$W(10) \equiv 3W(1) \mod 5$

$k = 2 : W(18 + n) \equiv W(n)4^{2n}2^4 \equiv W(n) \mod 5$

Perfect periodicity

Perfect periodicity

- An elliptic divisibility sequence which is periodic with respect to its rank of apparition is *perfectly periodic*.

Perfect periodicity

- An elliptic divisibility sequence which is periodic with respect to its rank of apparition is *perfectly periodic*.

Theorem (Lauter,S.)

Suppose $(q-1, \mathrm{ord}(P)) = 1$. *Define* $\phi : E \to \mathbb{F}_q$ *by*

$$\phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+\mathrm{ord}(P))} \right)^{\frac{1}{\mathrm{ord}(P)^2}} .$$

Then $W(n) = \phi([n]P)$ *is a perfectly periodic elliptic divisibility sequence, and furthermore,*

$$\phi([n]P) = \phi(P)^{n^2} W_{E,P}(n).$$

Example of perfect periodicity

$E : y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$ over $\mathbb{F}_5$
The usual elliptic divisibility sequence $W_{E,P}(n)$ is...

$$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 1, 2, 1, 3, 4, \ldots$$

Example of perfect periodicity

$E : y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$ over $\mathbb{F}_5$
The usual elliptic divisibility sequence $W_{E,P}(n)$ is...

$$0, 1, 1, 2, 1, 3, 4, 3, 2, 0, 3, 2, 1, 2, 4, 3, 4, 4, 0, 1, 1, 1, 2, 1, 3, 4, \ldots$$

From the theorem,

$$\phi(P) = \left(\frac{1}{2}\right)^1 = 3.$$

Then the sequence $\phi([n]P)$ is... $(\phi([n]P) = 3^{n^2} W_{E,P}(n))$

$$0, 3, 1, 1, 1, 4, 4, 4, 2, 0, 3, 1, 1, 1, 4, 4, 4, 2, 0, 3, 1, 1, 1, 4, 4, \ldots$$

Problem

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$. Determine k such that $Q = [k]P$.

EDS Discrete Log

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W *and terms* $W(k)$, $W(k+1)$, $\ldots$, $W(k+s-1)$, *determine* k.

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W *and terms* $W(k)$, $W(k+1)$, $\ldots$, $W(k+s-1)$, *determine* k.

First posed by Rachel Shipsey:

EDS Discrete Log

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W *and terms* $W(k)$, $W(k+1)$, $\ldots$, $W(k+s-1)$, *determine* k.

First posed by Rachel Shipsey:

- Reduced it to $\mathbb{F}_q^*$ discrete logarithm problem.

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W and terms $W(k)$, $W(k+1)$, ..., $W(k+s-1)$, determine k.

First posed by Rachel Shipsey:

- Reduced it to $\mathbb{F}_q^*$ discrete logarithm problem.
- Used the solution to give an attack on ECDLP in case $\mathrm{ord}(P) = q - 1$.

EDS Discrete Log

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W and terms $W(k)$, $W(k+1)$, $\ldots$, $W(k+s-1)$, determine k.

First posed by Rachel Shipsey:

- Reduced it to $\mathbb{F}_q^*$ discrete logarithm problem.
- Used the solution to give an attack on ECDLP in case $\mathrm{ord}(P) = q - 1$.
- Gave algorithms for computing a block of seven terms at position $a + b$ from blocks at position a and b.

Problem (Width s EDS Discrete Log)

Given an elliptic divisibility sequence W *and terms* $W(k)$, $W(k+1)$, $\ldots$, $W(k+s-1)$, *determine* k.

First posed by Rachel Shipsey:

- Reduced it to $\mathbb{F}_q^*$ discrete logarithm problem.
- Used the solution to give an attack on ECDLP in case $\mathrm{ord}(P) = q - 1$.
- Gave algorithms for computing a block of seven terms at position $a + b$ from blocks at position a and b.
- One might attempt generic discrete log attacks for groups, e.g. Pollard ρ.

Hard problems for EDS

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\operatorname{ord}(P) \geq 4$.

Hard problems for EDS

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\operatorname{ord}(P) \geq 4$.

Problem (EDS Association)

Determine $W_{E,P}(k)$ *for the value of* $0 < k < \operatorname{ord}(P)$ *such that* $Q = [k]P$*.*

Hard problems for EDS

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\mathrm{ord}(P) \geq 4$.

Problem (EDS Association)

Determine $W_{E,P}(k)$ *for the value of* $0 < k < \mathrm{ord}(P)$ *such that* $Q = [k]P$.

Problem (EDS Residue)

Determine the quadratic residuosity of $W_{E,P}(k)$ *for the value of* $0 < k < \mathrm{ord}(P)$ *such that* $Q = [k]P$.

Hard problems for EDS

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. Suppose one is given points $P, Q \in E(K)$ such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\mathrm{ord}(P) \geq 4$.

Problem (EDS Association)

Determine $W_{E,P}(k)$ *for the value of* $0 < k < \mathrm{ord}(P)$ *such that* $Q = [k]P$.

Problem (EDS Residue)

Determine the quadratic residuosity of $W_{E,P}(k)$ *for the value of* $0 < k < \mathrm{ord}(P)$ *such that* $Q = [k]P$.

- The smallest positive value of k such that $[k]P = Q$ will be called the *minimal multiplier*.

Relating hard problems

$$
\begin{tikzcd}
\text{perfectly periodic} & {[k]P} \arrow[dl, shift right, "(\log q)^3"'] \arrow[dd, dashed, "ECDLP"] \arrow[dr, dashed, "\begin{matrix} EDS \\ Association \end{matrix}"] & \text{not perfectly periodic} \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right, "(\log q)^2"'] \arrow[dr, dashed, "\begin{matrix} Width\ 3 \\ EDS\ Discrete\ Log \end{matrix}"'] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, shift left, "\mathbb{F}_q^* DLP"] \\
& k \arrow[ur, shift left, "(\log q)^3"] &
\end{tikzcd}
$$

$[k]P \to \{\phi([i]P)\}_{i=k}^{k+2}$

- Perfectly periodic case.

$$\begin{tikzcd}
& {[k]P} \arrow[dl, squiggly, shift right] \arrow[dd, dashed] \arrow[dr, dashed] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right] \arrow[dr, dashed] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, shift left] \\
& k \arrow[ur, shift left] &
\end{tikzcd}$$

- Use
$$\phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+\mathrm{ord}(P))} \right)^{\frac{1}{\mathrm{ord}(P)^2}} .$$
- Use Shipsey algorithms to calculate W to distance q.
- $(\log q)^3$ time.

$\{\phi([i]P)\}_{i=k}^{k+2} \to [k]P$

$$\begin{tikzcd}
& {[k]P} \arrow[dl, shift right] \arrow[dr, dashed] \arrow[dd, dashed] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, squiggly, shift right] \arrow[dr, dashed] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, shift left] \\
& k \arrow[ur, shift left] &
\end{tikzcd}$$

- Perfectly periodic case.

- Use
$$x(P) - x([k]P) = \frac{\phi([k+1]P)\phi([k-1]P)}{\phi([k]P)^2}$$

- $(\log q)^2$ time.

$k \to \{W_{E,P}(i)\}_{i=k}^{k+2}$

$$
\begin{tikzcd}
 & {[k]P} \arrow[dl, shift right] \arrow[dr, dashed] \arrow[dd, dashed] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right] \arrow[dr, dashed] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, shift left] \\
 & k \arrow[ur, rightsquigarrow, shift left] &
\end{tikzcd}
$$

- Non-perfectly periodic case.

- Use Shipsey algorithms to calculate terms.
- $(\log q)^3$ time.

$\{W_{E,P}(i)\}_{i=k}^{k+2} \to k$

- Non-perfectly periodic case.

$$
\begin{tikzcd}
 & {[k]P} \arrow[dl, shift right] \arrow[dr, dashed] \arrow[dd, dashed] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right] \arrow[dr, dashed] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, squiggly, shift left] \\
 & k \arrow[ur, shift left] &
\end{tikzcd}
$$

- Use

$$\frac{\phi([k+1]P)}{\phi([k]P)} = \phi(P)^{2k+1}\frac{W_{E,P}(k+1)}{W_{E,P}(k)}.$$

$\{W_{E,P}(i)\}_{i=k}^{k+2} \to k$

- Non-perfectly periodic case.

$$\begin{tikzcd}
 & {[k]P} \arrow[dl, shift right] \arrow[dr, dashed] \arrow[dd, dashed] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right] \arrow[dr, dashed] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, squiggly, shift left] \\
 & k \arrow[ur, shift left] &
\end{tikzcd}$$

- Use
$$\frac{\phi([k+1]P)}{\phi([k]P)} = \phi(P)^{2k+1}\frac{W_{E,P}(k+1)}{W_{E,P}(k)}.$$

(which is from $\phi([k]P) = \phi(P)^{k^2} W_{E,P}(k)$ with $k, k+1$).

$\{W_{E,P}(i)\}_{i=k}^{k+2} \to k$

$$\begin{tikzcd}
 & {[k]P} \arrow[dl, shift right] \arrow[dr, dashed] \arrow[dd, dashed] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right] \arrow[dr, dashed] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, squiggly, twoheadrightarrow, shift left] \\
 & k \arrow[ur, shift left] &
\end{tikzcd}$$

- Non-perfectly periodic case.

- Use
$$\frac{\phi([k+1]P)}{\phi([k]P)} = \phi(P)^{2k+1}\frac{W_{E,P}(k+1)}{W_{E,P}(k)}.$$
(which is from $\phi([k]P) = \phi(P)^{k^2} W_{E,P}(k)$ with $k, k+1$).
- This $\mathbb{F}_q^*$ discrete log can be solved in sub-exponential time.

$\{W_{E,P}(i)\}_{i=k}^{k+2} \to k$

$$\begin{tikzcd}
& {[k]P} \arrow[dl, shift right] \arrow[dr, dashed] \arrow[dd, dashed] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right] \arrow[dr, dashed] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, Rightarrow, squiggly] \\
& k \arrow[ur] &
\end{tikzcd}$$

- Non-perfectly periodic case.

- Use
$$\frac{\phi([k+1]P)}{\phi([k]P)} = \phi(P)^{2k+1}\frac{W_{E,P}(k+1)}{W_{E,P}(k)}.$$
(which is from $\phi([k]P) = \phi(P)^{k^2} W_{E,P}(k)$ with $k, k+1$).
- This $\mathbb{F}_q^*$ discrete log can be solved in sub-exponential time.
- (This is a different method than Shipsey; similar result.)

Relating hard problems II

perfectly periodic

not perfectly periodic

$$
\begin{tikzcd}
 & {[k]P} \arrow[dl, shift right, "(\log q)^3"'] \arrow[dd, dashed, "ECDLP"] \arrow[dr, dashed, "\substack{EDS\\ Association}"] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right, "(\log q)^2"'] \arrow[dr, dashed, "\substack{Width\ 3\\ EDS\ Discrete\ Log}"'] & & \{W_{E,P}(i)\}_{i=k}^{k+2} \arrow[dl, shift left, "\mathbb{F}_q^* DLP"] \\
 & k \arrow[ur, shift left, "(\log q)^3"] &
\end{tikzcd}
$$

Relating hard problems II

perfectly periodic

not perfectly periodic

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
 & {[k]P} \arrow[dl, shift right, "(\log q)^3"'] \arrow[dd, dashed, "ECDLP"] \arrow[dr, dashed, "\substack{EDS\\ Association\\ Quotient}"] & \\
\{\phi([i]P)\}_{i=k}^{k+2} \arrow[ur, shift right, "(\log q)^2"'] \arrow[dr, dashed, "\substack{Width\ 3\\ EDS\ Discrete\ Log}"'] & & {\color{red}\frac{W_{E,P}(k+1)}{W_{E,P}(k)}} \arrow[dl, shift left, "\mathbb{F}_q^* DLP"] \\
 & k \arrow[ur, shift left, "(\log q)^3"] &
\end{tikzcd}
$$

It is enough to know parity of k

Suppose $\mathrm{ord}(P)$ is odd.
An algorithm for finding k such that $[k]P = Q$ and $0 < k < \mathrm{ord}(P)$.

It is enough to know parity of k

Suppose $\mathrm{ord}(P)$ is odd.
An algorithm for finding k such that $[k]P = Q$ and $0 < k < \mathrm{ord}(P)$.

1. If P = Q, stop.

It is enough to know parity of k

Suppose $\mathrm{ord}(P)$ is odd.
An algorithm for finding k such that $[k]P = Q$ and $0 < k < \mathrm{ord}(P)$.

1. If P = Q, stop.
2. Find parity of smallest positive k such that $[k]P = Q$.

It is enough to know parity of k

Suppose $\mathrm{ord}(P)$ is odd.
An algorithm for finding k such that $[k]P = Q$ and $0 < k < \mathrm{ord}(P)$.

1. If P = Q, stop.
2. Find parity of smallest positive k such that $[k]P = Q$.
3. If k is even, find Q' such that $[2]Q' = Q$. If k is odd, find Q' such that $[2]Q' = Q - P$.

It is enough to know parity of k

Suppose $\mathrm{ord}(P)$ is odd.
An algorithm for finding k such that $[k]P = Q$ and $0 < k < \mathrm{ord}(P)$.

1. If P = Q, stop.
2. Find parity of smallest positive k such that $[k]P = Q$.
3. If k is even, find Q' such that $[2]Q' = Q$. If k is odd, find Q' such that $[2]Q' = Q - P$.
4. Set $Q = Q'$ and return to step 1.

It is enough to know parity of k

Suppose $\mathrm{ord}(P)$ is odd.
An algorithm for finding k such that $[k]P = Q$ and $0 < k < \mathrm{ord}(P)$.

1. If P = Q, stop.
2. Find parity of smallest positive k such that $[k]P = Q$.
3. If k is even, find Q' such that $[2]Q' = Q$. If k is odd, find Q' such that $[2]Q' = Q - P$.
4. Set $Q = Q'$ and return to step 1.

- When we return to step 1, the new k' is $k/2$ or $(k-1)/2$ depending on parity in step 2.

It is enough to know parity of k

Suppose $\mathrm{ord}(P)$ is odd.
An algorithm for finding k such that $[k]P = Q$ and $0 < k < \mathrm{ord}(P)$.

1. If P = Q, stop.
2. Find parity of smallest positive k such that $[k]P = Q$.
3. If k is even, find Q' such that $[2]Q' = Q$. If k is odd, find Q' such that $[2]Q' = Q - P$.
4. Set $Q = Q'$ and return to step 1.

- When we return to step 1, the new k' is $k/2$ or $(k-1)/2$ depending on parity in step 2.
- To find k when the algorithm ends, count up the sequence of parities – gives binary expansion of k.

EDS Residue

- Suppose we could calculate the residuosity of $W_{E,P}(k)$ (non-perfectly-periodic case).

EDS Residue

- Suppose we could calculate the residuosity of $W_{E,P}(k)$ (non-perfectly-periodic case).
- Assume $\phi(P)$ is a non-residue.

EDS Residue

- Suppose we could calculate the residuosity of $W_{E,P}(k)$ (non-perfectly-periodic case).
- Assume $\phi(P)$ is a non-residue.
- We have the $\mathbb{F}_q^*$ discrete logarithm equation:

$$\phi([k]P) = \phi(P)^{k^2} W_{E,P}(k).$$

EDS Residue

- Suppose we could calculate the residuosity of $W_{E,P}(k)$ (non-perfectly-periodic case).
- Assume $\phi(P)$ is a non-residue.
- We have the $\mathbb{F}_q^*$ discrete logarithm equation:

$$\phi([k]P) = \phi(P)^{k^2} W_{E,P}(k).$$

- The parity of k can be calculated from the residuosity in polynomial time.

Can we solve EDS Residue?

No. Interestingly, we can calculate the residuosity of ratios of terms

$$\frac{W_{E,P}(k+1)}{W_{E,P}(k)}$$

but this doesn't help.

Theorem (Lauter, S.)

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. If any one of the following problems is solvable in sub-exponential time, then all of them are:

1. *ECDLP*
2. *EDS Association for non-perfectly periodic sequences*
3. *Width 3 EDS Discrete Log for perfectly periodic sequences*

If $|E(\mathbb{F}_q)|$ is odd and $\mathrm{char}(\mathbb{F}_q) \neq 2$, we can also include

4. *EDS Residue for non-perfectly periodic sequences*

Division polynomials of higher rank?

The n-th division polynomial is associated to the vanishing of $[n]P$ on the curve.

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

Division polynomials of higher rank?

The n-th division polynomial is associated to the vanishing of $[n]P$ on the curve.

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

We might dream of ...

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

Division polynomials of higher rank?

The n-th division polynomial is associated to the vanishing of $[n]P$ on the curve.

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

We might dream of ...

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

Or even ...

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

etc.

Definition (S)

Let K be a field. An *elliptic net* is a map $W : A \to K$ such that the following recurrence holds for all p, q, r, $s \in \mathbb{Z}^n$.

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

Definition (S)

Let K be a field. An *elliptic net* is a map $W : A \to K$ such that the following recurrence holds for all p, q, r, $s \in \mathbb{Z}^n$.

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

- Elliptic divisibility sequences are a special case ($n = 1$)

Definition (S)

Let K be a field. An *elliptic net* is a map $W : A \to K$ such that the following recurrence holds for all p, q, r, $s \in \mathbb{Z}^n$.

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

- Elliptic divisibility sequences are a special case $(n = 1)$
- In this talk, we will mostly discuss rank $n = 2$.

Definition of an elliptic net

Definition (S)

Let K be a field. An *elliptic net* is a map $W : A \to K$ such that the following recurrence holds for all p, q, r, $s \in \mathbb{Z}^n$.

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

- Elliptic divisibility sequences are a special case $(n = 1)$
- In this talk, we will mostly discuss rank $n = 2$.
- The recurrence generates the net from finitely many initial values.

Net polynomial examples

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

Net polynomial examples

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

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

Net polynomial examples

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

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

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

Net polynomial examples

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

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

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

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

Net polynomial examples

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

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

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

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

Can calculate more via the recurrence...

Net polynomial examples

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

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

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

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

Can calculate more via the recurrence...

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

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{\begin{array}{c} \textit{elliptic net} \\ W : \mathbb{Z}^n \to K \\ \textit{modulo scale} \\ \textit{equivalence} \end{array}\right\} \quad \leftrightarrow \quad \left\{\begin{array}{c} \textit{cubic Weierstrass curve } C \textit{ over } K \\ \textit{together with } m \textit{ points in } C(K) \\ \textit{modulo change of variables} \\ x' = x + r, y' = y + sx + t \end{array}\right\}$$

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{\begin{array}{c}\textit{elliptic net}\\ W:\mathbb{Z}^n\to K\\ \textit{modulo scale}\\ \textit{equivalence}\end{array}\right\} \quad \leftrightarrow \quad \left\{\begin{array}{c}\textit{cubic Weierstrass curve } C \textit{ over } K\\ \textit{together with } m \textit{ points in } C(K)\\ \textit{modulo change of variables}\\ x'=x+r, y'=y+sx+t\end{array}\right\}$$

- $n=m$ and $W(\mathbf{v})=\Psi_{\mathbf{v}}(P_1,\ldots,P_m,C)$

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{\begin{array}{c}\textit{elliptic net}\\ W:\mathbb{Z}^n\to K\\ \textit{modulo scale}\\ \textit{equivalence}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\textit{cubic Weierstrass curve } C \textit{ over } K\\ \textit{together with } m \textit{ points in } C(K)\\ \textit{modulo change of variables}\\ x'=x+r, y'=y+sx+t\end{array}\right\}$$

- $n = m$ and $W(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \ldots, P_m, C)$
- explicit equations to go back and forth!

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{\begin{array}{c}\textit{elliptic net}\\ W:\mathbb{Z}^n\to K\\ \textit{modulo scale}\\ \textit{equivalence}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\textit{cubic Weierstrass curve } C \textit{ over } K\\ \textit{together with } m \textit{ points in } C(K)\\ \textit{modulo change of variables}\\ x'=x+r, y'=y+sx+t\end{array}\right\}$$

- $n = m$ and $W(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \ldots, P_m, C)$
- explicit equations to go back and forth!
- singular cubics correspond to Lucas sequences or integers

Curve-net bijection

Theorem (S.)

There is a bijection of partially ordered sets:

$$\left\{\begin{array}{c}\textit{elliptic net}\\ W:\mathbb{Z}^n\to K\\ \textit{modulo scale}\\ \textit{equivalence}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\textit{cubic Weierstrass curve } C \textit{ over } K\\ \textit{together with } m \textit{ points in } C(K)\\ \textit{modulo change of variables}\\ x'=x+r, y'=y+sx+t\end{array}\right\}$$

- $n=m$ and $W(\mathbf{v})=\Psi_{\mathbf{v}}(P_1,\dots,P_m,C)$
- explicit equations to go back and forth!
- singular cubics correspond to Lucas sequences or integers
- scale equivalence: $W\sim W' \iff W(\mathbf{v})=f(\mathbf{v})W'(\mathbf{v})$ for $f:\mathbb{Z}^n\to K^*$ quadratic
- on left, remove nets with zeroes too close to the origin
- on right, remove cases with small torsion points or pairs which are equal or inverses
- consider only nets with $W(\mathbf{v})=1$ for $\mathbf{v}=\mathbf{e}_i$ or $\mathbf{v}=\mathbf{e}_i+\mathbf{e}_j$

Example over $\mathbb{Q}$

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

	-5	8	-19			
	1	3	-1			
$\uparrow$	1	1	2			
Q	0	1	1			
	$P \rightarrow$					

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

$\uparrow Q$ $\quad P \rightarrow$

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
$\uparrow$	1	1	2	−5	7	89
Q	0	1	1	−3	11	38
	$P \rightarrow$					

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 $\mathbb{Q}$

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

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 $\mathbb{Q}$

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

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

$P \rightarrow$

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
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \rightarrow$						

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

Example over $\mathbb{F}_5$

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

$$\begin{array}{cc|c|c|c|c|c|c|c|}
\hline
 & & \color{red}{0} & 4 & 4 & 3 & 1 & 2 & 4 \\
\hline
 & & 4 & 4 & 4 & 4 & 1 & 3 & \color{red}{0} \\
\hline
 & & 4 & 3 & 2 & \color{red}{0} & 3 & 2 & 1 \\
\hline
 & & \color{red}{0} & 3 & 1 & 4 & 4 & 4 & 4 \\
\hline
 & & 1 & 3 & 4 & 2 & 4 & 1 & \color{red}{0} \\
\hline
 & \uparrow & 1 & 1 & 2 & \color{red}{0} & 2 & 4 & 1 \\
\hline
 & Q & \color{red}{0} & 1 & 1 & 2 & 1 & 3 & 4 \\
\hline
\multicolumn{2}{c}{} & \multicolumn{7}{l}{P \rightarrow}
\end{array}$$

- 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
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4

$P \rightarrow$

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
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \rightarrow$						

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
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \rightarrow$						

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

$\uparrow Q$

$P \rightarrow$

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

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
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \rightarrow$						

- 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.

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

$\uparrow Q$

$P \rightarrow$

- 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.

Translation properties

Let Γ be the lattice of apparition for an elliptic net W. Define $g : \Gamma \times \mathbb{Z}^n \to K^*$ by

$$g(\mathbf{r}, \mathbf{m}) = \frac{W(\mathbf{m} + \mathbf{r})}{W(\mathbf{m})}.$$

Translation properties

Let Γ be the lattice of apparition for an elliptic net W. Define $g : \Gamma \times \mathbb{Z}^n \to K^*$ by

$$g(\mathbf{r}, \mathbf{m}) = \frac{W(\mathbf{m} + \mathbf{r})}{W(\mathbf{m})}.$$

Theorem (Ward $n = 1$; S., $n > 1$)

The function g is quadratic and affine linear in 2nd variable.

Translation properties

Let Γ be the lattice of apparition for an elliptic net W. Define $g : \Gamma \times \mathbb{Z}^n \to K^*$ by

$$g(\mathbf{r}, \mathbf{m}) = \frac{W(\mathbf{m} + \mathbf{r})}{W(\mathbf{m})}.$$

Theorem (Ward $n = 1$; S., $n > 1$)

The function g is quadratic and affine linear in 2nd variable.

Example

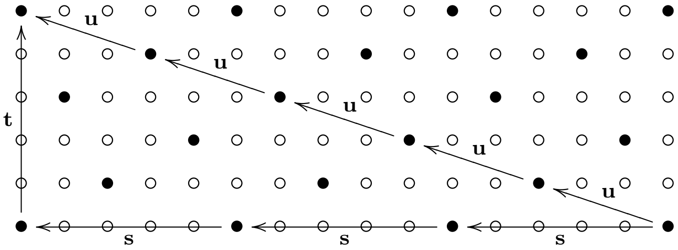
If $n = 1$, $W(r) = 0$, then

$$g(kr, m) = a^{mk} b^{k^2},$$

for all $k \in \mathbb{Z}$.

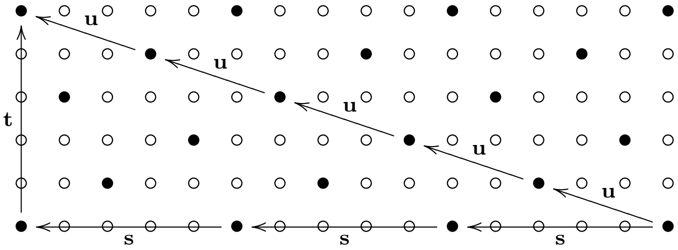
About $\mathbb{F}_q^*$ discrete logarithm equations

Other ways to find them: combine partial periodicity relations.



About $\mathbb{F}_q^*$ discrete logarithm equations

Other ways to find them: combine partial periodicity relations.



giving (where $m = \mathrm{ord}(P)$):

$$\left(\frac{W(m+1,0)W(2,0)}{W(m+2,0)}\right)^k = \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)}\right)^m \left(-\frac{W(1,m)W(2,0)}{W(2,m)W(1,-1)^m}\right).$$

This is similar to Shipsey's equation.

Shipsey's discrete logarithm

From previous slide:

$$\left(\frac{W(m+1,0)W(2,0)}{W(m+2,0)}\right)^k = \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)}\right)^m \left(-\frac{W(1,m)W(2,0)}{W(2,m)W(1,-1)^m}\right).$$

Shipsey's discrete logarithm

From previous slide:

$$\left(\frac{W(m+1,0)W(2,0)}{W(m+2,0)}\right)^k$$
$$= \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)}\right)^m \left(-\frac{W(1,m)W(2,0)}{W(2,m)W(1,-1)^m}\right).$$

Compare to Shipsey's:

$$\frac{W_{E,P,Q}(m+1,m+1)}{W_{E,P,Q}(0,m+1)}\left(\frac{W_{E,P}(k+1)}{W_{E,P}(k)}\right)^{m(m+2)} = W_{E,P}(m+1)^{2k+1}.$$

Shipsey's discrete logarithm

From previous slide:

$$\left(\frac{W(m+1,0)W(2,0)}{W(m+2,0)}\right)^k$$
$$= \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)}\right)^m \left(-\frac{W(1,m)W(2,0)}{W(2,m)W(1,-1)^m}\right).$$

Compare to Shipsey's:

$$\frac{W_{E,P,Q}(m+1,m+1)}{W_{E,P,Q}(0,m+1)} \left(\frac{W_{E,P}(k+1)}{W_{E,P}(k)}\right)^{m(m+2)} = W_{E,P}(m+1)^{2k+1}.$$

Both can be explained as *Tate pairing values*.

Tate pairing

$m \geq 1$
E/K an elliptic curve

Tate pairing

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

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 $m(P) - m(\mathcal{O})$

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 $\operatorname{div}(f_P)$

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:

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

It is bilinear, alternating, and non-degenerate.

Weil and Tate pairing attacks

These are isomorphism attacks:
Elliptic curve E defined over $\mathbb{F}_q$ (prime order, say), $Q = [k]P$.

- Menezes-Okamoto-Vanstone:
  For any auxiliary point T,

  $$e_m(Q,T) = e_m(P,T)^k$$

  and so we transfer the question of finding k to a discrete log in $\mathbb{F}_{q^t}$ for some t which is usually infeasibly large.
- Frey-Rück:

  $$\tau_m(P,Q) = \tau_m(P,P)^k$$

  is an equation in $\mathbb{F}_{q^t}$ where again t is usually infeasibly large.

Pairing from Elliptic Nets

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

Pairing from Elliptic Nets

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

Theorem (S)

Choose $S \in E(K)$ such that $S \notin \{\mathcal{O}, -Q\}$. Let W be an elliptic net with basis $\mathbf{T}$ such that $p \cdot \mathbf{T} = P$, $q \cdot \mathbf{T} = Q$ and $s \cdot \mathbf{T} = S$. Then the quantity

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

is the Tate pairing.

The $\mathbb{F}_q^*$ DLP equation

From older slide:

$$\left(\frac{W(m+1,0)W(2,0)}{W(m+2,0)}\right)^k = \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)}\right)^m \left(-\frac{W(1,m)W(2,0)}{W(2,m)W(1,-1)^m}\right).$$

Becomes...

$$\tau_m(P,-P)^k = \tau_m(Q,-P).$$

Shipsey's $\mathbb{F}_q^*$ DLP equation

$$\frac{W_{E,P,Q}(m+1,m+1)}{W_{E,P,Q}(0,m+1)}\left(\frac{W_{E,P}(k+1)}{W_{E,P}(k)}\right)^{m(m+2)} = W_{E,P}(m+1)^{2k+1}.$$

Becomes...

$$\tau_m(P,Q)\tau_m(Q,P) = \tau_m(P,P)^{2k}.$$

For Further Reading

M. Ward.
Memoir on Elliptic Divisibility Sequences.
American Journal of Mathematics, 70:13–74, 1948.

R. Shipsey.
Elliptic Divisibility Sequences.
Ph. D. Thesis, University of London, 2000.

K. Stange.
Elliptic Nets and Elliptic Curves.
Ph. D. Thesis, Brown University, 2008.

K. Lauter, K. Stange.
The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences.
To appear, SAC 2008.

Slides, Articles and Preprints at http://www.math.brown.edu/~stange/