# Elliptic Curve Diffie-Hellman Key Exchange

Nathan Daino

April 21, 2022

# Table of Contents

# What is an elliptic curve?

- Algebraic curve of the Weierstrass form $y^2 = x^3 + \alpha x + \beta$

# What is an elliptic curve?

- Algebraic curve of the Weierstrass form $y^2 = x^3 + \alpha x + \beta$
- ...Or $y^2 = 4x^3 - \sigma x - \omega$

# What is an elliptic curve?

- Algebraic curve of the Weierstrass form $y^2 = x^3 + \alpha x + \beta$
- ...Or $y^2 = 4x^3 - \sigma x - \omega$
- Birationally equivalent

# What is an elliptic curve?

- Algebraic curve of the Weierstrass form $y^2 = x^3 + \alpha x + \beta$
- ...Or $y^2 = 4x^3 - \sigma x - \omega$
- Birationally equivalent
- Projective transformation

# The Projective Plane

- $x^n + yn = 1; x = \frac{a}{c}, y = \frac{b}{d}$

# The Projective Plane

- $x^n + yn = 1; x = \frac{a}{c}, y = \frac{b}{d}$
- $a^n d^n + b^n c^n = c^n d^n; c|d, d|c$

# The Projective Plane

- $x^n + yn = 1; x = \frac{a}{c}, y = \frac{b}{d}$
- $a^n d^n + b^n c^n = c^n d^n; c|d, d|c$
- Equivalent to $x^n + y^n = z^n, x, y \in \mathbb{Z}^+$

# The Projective Plane

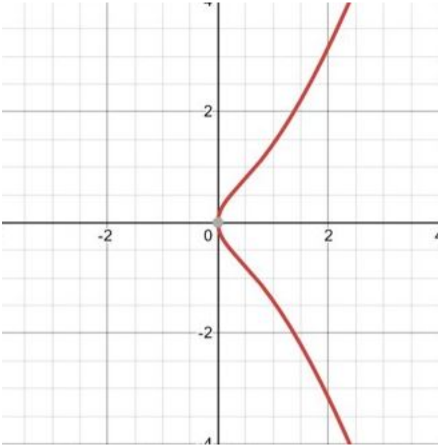
- $x^n + yn = 1; x = \frac{a}{c}, y = \frac{b}{d}$
- $a^n d^n + b^n c^n = c^n d^n; c|d, d|c$
- Equivalent to $x^n + y^n = z^n, x, y \in \mathbb{Z}^+$
- $(tx)^n + (ty)^n = (tz)^n$

# The Projective Plane

- $x^n + yn = 1; x = \frac{a}{c}, y = \frac{b}{d}$
- $a^n d^n + b^n c^n = c^n d^n; c|d, d|c$
- Equivalent to $x^n + y^n = z^n, x, y \in \mathbb{Z}^+$
- $(tx)^n + (ty)^n = (tz)^n$
- Notion of a "point at infinity": $(1, -1, 0) : (1)^1 + (-1)^1 = 0^1$

# What do these curves look like?

$$y^2 = x(x^2 + 1)$$

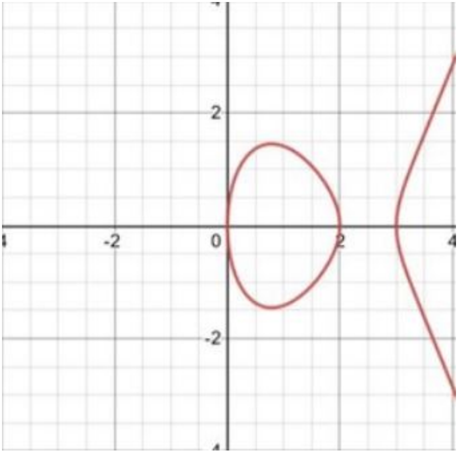



- One real root

# What do these curves look like?

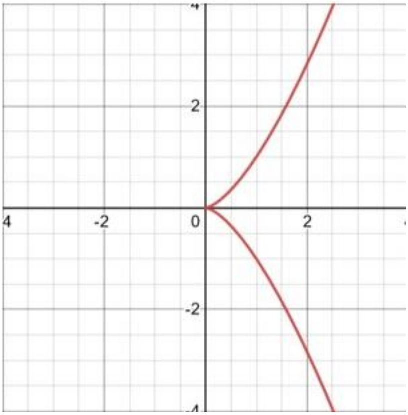
$$y^2 = x(x-2)(x-3)$$

- Three real roots



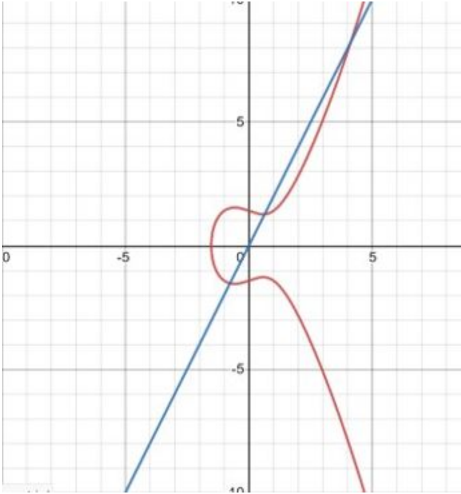
# What do these curves look like?

- Recall: roots must be distinct. Why?



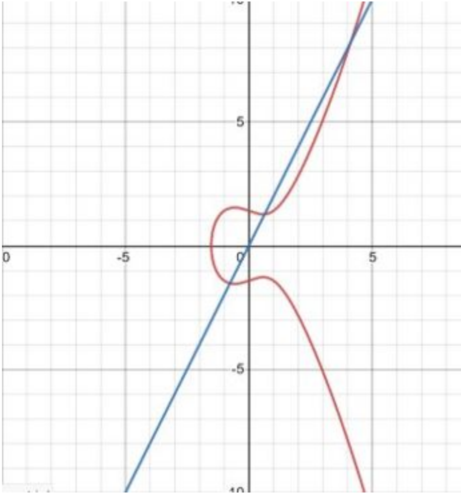
# Point Composition

- Suppose we are given two points on a line.



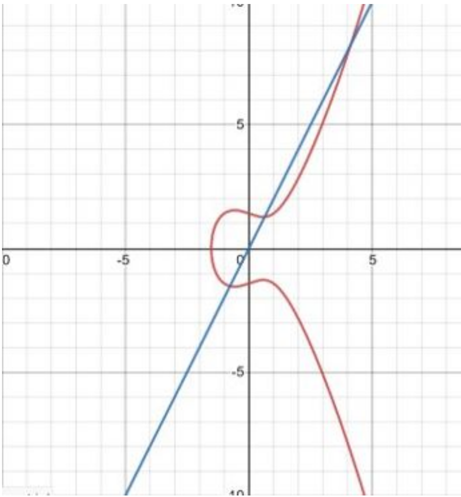
# Point Composition

- Suppose we are given two points on a line.
- We profit from the idea that a line intersects a cubic curve at three points.



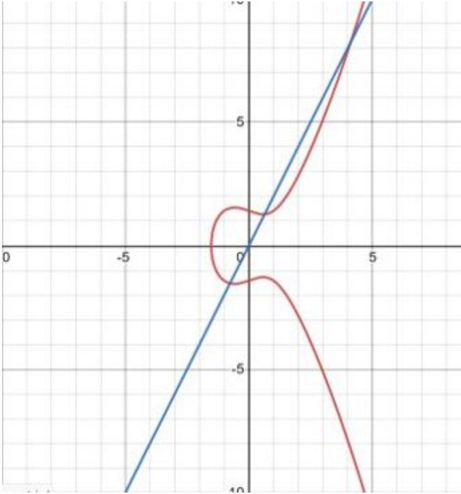
# Point Composition

- Suppose we are given two points on a line.
- We profit from the idea that a line intersects a cubic curve at three points.
- What about two points that construct a vertical line?



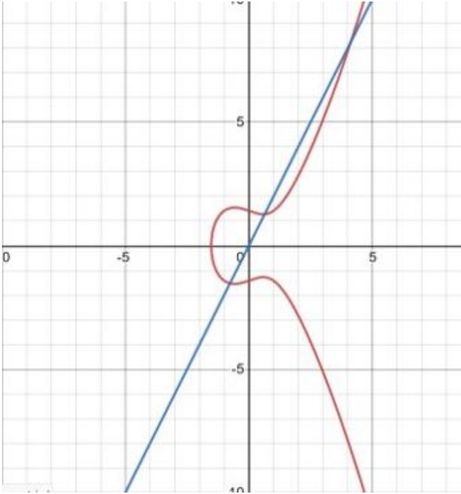
# Point Composition

- Suppose we are given two points on a line.
- We profit from the idea that a line intersects a cubic curve at three points.
- What about two points that construct a vertical line?
- What about two points infinitesimally close?



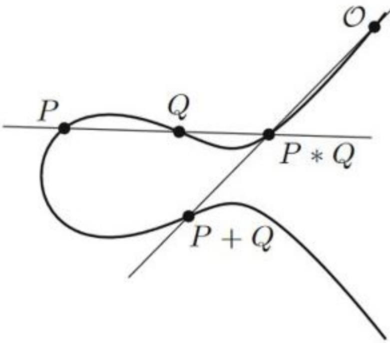
# Point Composition

- Suppose we are given two points on a line.
- We profit from the idea that a line intersects a cubic curve at three points.
- What about two points that construct a vertical line?
- What about two points infinitesimally close?
- If the first two points are rational, the third is rational.



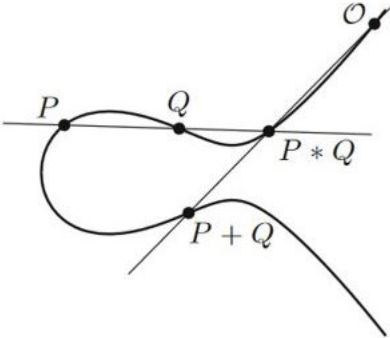
# Geometric Point Addition

- We can craft a new identity element, $O$.



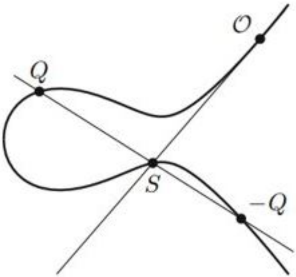
# Geometric Point Addition

- We can craft a new identity element, $O$.
- $P + Q$ becomes a new operation defined by $O * (P * Q)$



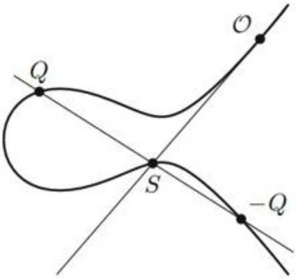
# Geometric Point Addition

- Showing associativity is a bit complex...



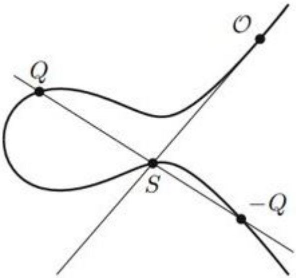
# Geometric Point Addition

- Showing associativity is a bit complex...
- Commutativity



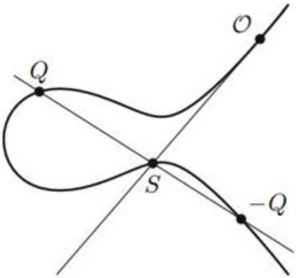
# Geometric Point Addition

- Showing associativity is a bit complex...
- Commutativity
- Identity element: $O$

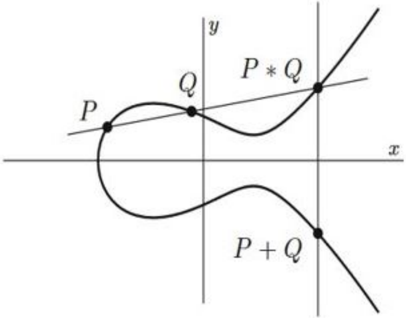


# Geometric Point Addition

- Showing associativity is a bit complex...
- Commutativity
- Identity element: $O$
- Inverse: $Q + -Q = O$



# Moving the Identity Element



# Algebraic Point Addition

- $x_3 = m^2 - a - x_1 - x_2$

# Algebraic Point Addition

- $x_3 = m^2 - a - x_1 - x_2$
- $y_3 = mx_3 + v$

# Finite Fields

- Points can be computed over $F_p$, $p$ prime.

# Finite Fields

- Points can be computed over $F_p$, $p$ prime.
- Consider $y^2 = x^3 + x + 2$ over $F_7$. $x = 1 \in F_7 \implies y^2 = 4$

# Finite Fields

- Points can be computed over $F_p$, $p$ prime.
- Consider $y^2 = x^3 + x + 2$ over $F_7$. $x = 1 \in F_7 \implies y^2 = 4$
- $y = 2, 5$; points on curve in $F_7$ include $(1, 2), (1, 5)$

## Finite Fields

- Points can be computed over $F_p$, $p$ prime.
- Consider $y^2 = x^3 + x + 2$ over $F_7$. $x = 1 \in F_7 \implies y^2 = 4$
- $y = 2, 5$; points on curve in $F_7$ include $(1, 2), (1, 5)$
- How do we add these points? We use our previous algebraic method but compute all quantities mod p.

# Key Exchange Protocol

- Consider 2 parties, A and B, each of which has the same elliptic curve over field $F_p$ and a point on the curve, $p$, in mind.

# Key Exchange Protocol

- Consider 2 parties, A and B, each of which has the same elliptic curve over field $F_p$ and a point on the curve, $p$, in mind.
- A has a secret number $n_1$ to which $P$ is raised to generate $Q_1$. $Q_1$ is sent to B.

# Key Exchange Protocol

- Consider 2 parties, A and B, each of which has the same elliptic curve over field $F_p$ and a point on the curve, $p$, in mind.
- A has a secret number $n_1$ to which $P$ is raised to generate $Q_1$. $Q_1$ is sent to B.
- Similarly, B has a secret number $n_2$ to which $P$ is raised to generate $Q_2$. $Q_2$ is sent to A.

# Key Exchange Protocol

- Consider 2 parties, A and B, each of which has the same elliptic curve over field $F_p$ and a point on the curve, $p$, in mind.
- A has a secret number $n_1$ to which $P$ is raised to generate $Q_1$. $Q_1$ is sent to B.
- Similarly, B has a secret number $n_2$ to which $P$ is raised to generate $Q_2$. $Q_2$ is sent to A.
- A and B take each other's $Q$ value and raise it to their own secret exponent.

# Key Exchange Protocol

- Consider 2 parties, A and B, each of which has the same elliptic curve over field $F_p$ and a point on the curve, $p$, in mind.
- A has a secret number $n_1$ to which $P$ is raised to generate $Q_1$. $Q_1$ is sent to B.
- Similarly, B has a secret number $n_2$ to which $P$ is raised to generate $Q_2$. $Q_2$ is sent to A.
- A and B take each other's $Q$ value and raise it to their own secret exponent.
- A then has $(Q_2)^{n_1} = (P^{n_2})^{n_1} = (P^{n_1})^{n_2} = (Q_1)^{n_2}$, the latter of which B has. Both parties arrive at the same decryption key, while an eavesdropper does not.

# Classical Discrete Logarithm Problem

- Consider a multiplicative cyclic group $G_p$, with elements $b_j$. Because any $b_j$ can be expressed as the power, $k$, of a generator, $g$, i.e., $b_j = g^k$, we may define $\log_g(b_j) = k (\mathrm{mod} p)$

# Classical Discrete Logarithm Problem

- Consider a multiplicative cyclic group $G_p$, with elements $b_j$. Because any $b_j$ can be expressed as the power, $k$, of a generator, $g$, i.e., $b_j = g^k$, we may define $\log_g(b_j) = k(\mathrm{mod} p)$
- If we have a generator of the group and an arbitrary element, can we compute k?

# Elliptic Curve Discrete Logarithm Problem

- Given two points $Q, P$ of $E(F_P)$, we wish to find $n$ such that $Q = P + P + ... + P = nP$

# Elliptic Curve Discrete Logarithm Problem

- Given two points $Q, P$ of $E(F_P)$, we wish to find $n$ such that $Q = P + P + ... + P = nP$
- In other words, we wish to find $\log_P Q = n$, the number of times $P$ operates on itself.

# Elliptic Curve Discrete Logarithm Problem

- Given two points $Q, P$ of $E(F_P)$, we wish to find $n$ such that $Q = P + P + ... + P = nP$
- In other words, we wish to find $\log_P Q = n$, the number of times $P$ operates on itself.
- Problems may arise where no $n$ exists such that $nP = Q$, or where multiple values $n$ exist that satisfy the equation.

# How difficult is this to compute?

- Naive way: Increment by $P$ each time (i.e., find $P$, then $2P$, ..., $tP$ and so on until n is found.

# How difficult is this to compute?

- Naive way: Increment by $P$ each time (i.e., find $P$, then $2P$, ..., $tP$ and so on until n is found.
- Clever way: Operate two lists, one beginning the same as above, one taking the form $Q - k1P$, $Q - k2P$, etc. If one value from each list matches, then $Q = (t + k1)P$ and n is found.

# How difficult is this to compute?

- Naive way: Increment by $P$ each time (i.e., find $P$, then $2P$, ..., $tP$ and so on until n is found.
- Clever way: Operate two lists, one beginning the same as above, one taking the form $Q - k1P$, $Q - k2P$, etc. If one value from each list matches, then $Q = (t + k1)P$ and n is found.
- Fastest methods take $\sqrt{P}$ calculations in $E(F_p)$. $F_p$ should be large!

# References

- Hoffstein, Pipher, Silverman; An Introduction To Mathematical Cryptography

# References


- Hoffstein, Pipher, Silverman; An Introduction To Mathematical Cryptography
- Silverman Tate; Rational Points on Elliptic Curves

# References


- Hoffstein, Pipher, Silverman; An Introduction To Mathematical Cryptography
- Silverman Tate; Rational Points on Elliptic Curves
- "Discrete Logarithm Problem"; https://www.doc.ic.ac.uk/ mrh/330tutor/ch06s02.html

# References


- Hoffstein, Pipher, Silverman; An Introduction To Mathematical Cryptography
- Silverman Tate; Rational Points on Elliptic Curves
- "Discrete Logarithm Problem"; https://www.doc.ic.ac.uk/ mrh/330tutor/ch06s02.html
- Numerous in-slide image and text citations coming soon

# References

Gratitude is in order for:

- Directed reading program administrators

# References

Gratitude is in order for:

- Directed reading program administrators
- Mr. Paul Teszler (advisor)

# References

Gratitude is in order for:

- Directed reading program administrators
- Mr. Paul Teszler (advisor)
- Audience

Questions?