Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves

Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings

Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption

References

Elliptic Curves and Their Applications in Cryptography

Tim Shaffer[1]

Youngstown State University

MathFest 2014

[1] Advisor: Dr. Jacek Fabrykowski

Fermat's Last Theorem

Pierre de Fermat:

> *It is impossible to write a cube as the sum of two cubes, a fourth power as the sum of two fourth powers, and, in general, any power beyond the second as the sum of two similar powers. For this I have discovered a truly wonderful proof but the margin is too small to contain it.*

1995–Andrew Wiles published the first successful proof.

Elliptic Curve Factorization

Elliptic Curve Cryptography

Tim Shaffer

Definitions
- Affine Space
- Projective Space
- Algebraic Curves
- Singular Points
- Elliptic Curves

Group Properties
- Additive Operation
- ECDLP
- Order of $\mathcal{E}(\mathbb{F}_q)$
- Schoof's Algorithm
- Pairings

Cryptography
- ECDH
- Elgamal
- Tripartite Key Exchange
- ID-based Encryption

References

Pollard's $p-1$ algorithm can find prime factors p of a composite integer for which $p-1$ is smooth.

Elliptic curve factorization is a generalization of Pollard's $p-1$ algorithm using random elliptic curve groups over $\mathbb{Z}/p\mathbb{Z}$.

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves
Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings
Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption
References

Definition

An elliptic curve is a projective algebraic curve with affine coordinates given by

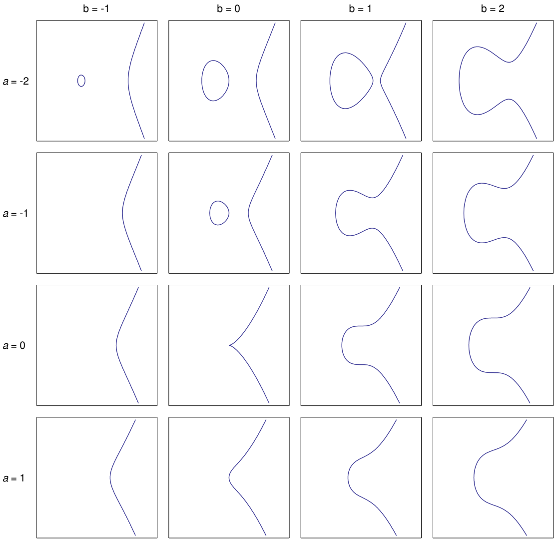
$$y^2 = x^3 + \alpha x + \beta$$

where

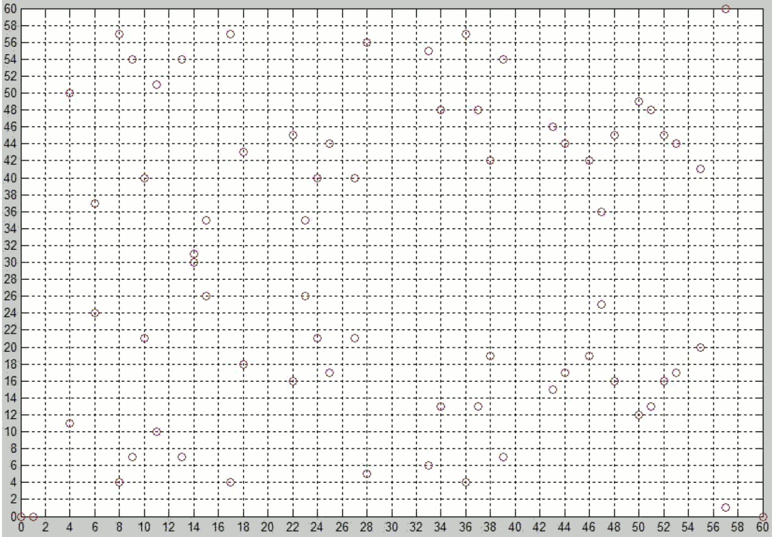
$$4\alpha^3 + 27\beta^2 \neq 0.$$

Elliptic curves over finite fields (usually $\mathbb{Z}/p\mathbb{Z}$) are of particular interest in cryptography.

Elliptic Curves



Elliptic Curve on $\mathbb{Z}/61\mathbb{Z}$



Elliptic Curve Cryptography

Tim Shaffer

Definitions
- Affine Space
- Projective Space
- Algebraic Curves
- Singular Points
- Elliptic Curves

Group Properties
- Additive Operation
- ECDLP
- Order of $\mathcal{E}(\mathbb{F}_q)$
- Schoof's Algorithm
- Pairings

Cryptography
- ECDH
- Elgamal
- Tripartite Key Exchange
- ID-based Encryption

References

Affine Space

Definition

Given a finite field with q elements, $\mathbb{F}_q$, affine n-space over $\mathbb{F}_q$, denoted $A^n(\mathbb{F}_q)$, is the set of n-tuples $(a_0, a_1, \ldots, a_{n-1})$ with $a_i \in \mathbb{F}_q$.

Definition

A **point** in $A^n(\mathbb{F}_q)$ is an n-tuple $(a_0, a_1, \ldots, a_{n-1})$ for $a_i \in \mathbb{F}_q$.

Projective Space

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves
Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings
Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption
References

Definition

Projective n-space over $\mathbb{F}_q$, denoted $P^n(\mathbb{F}_q)$, is the set of equivalence classes of nonzero elements of $A^{n+1}(\mathbb{F}_q)$ under the equivalence relation

$$(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n)$$

iff there exists a $0 \neq \lambda \in \mathbb{F}_q$ such that

$$a_i = \lambda b_i$$

for all $i = 0, 1, \ldots, n$.

Projective Space

Definition

A **point** in $P^n(\mathbb{F}_q)$, denoted $[a_0, a_1, \ldots, a_n]$, is the equivalence class containing $(a_0, a_1, \ldots, a_n)$.

While $A^2(\mathbb{F}_q)$ has q^2 points, $P^2(\mathbb{F}_q)$ has $q^2 + q + 1$ points.

The points in $P^2(\mathbb{F}_q)$ can be broken into 2 subsets:

- q^2 **finite points** of the form $[a_0, a_1, 1]$ that map to $A^2(\mathbb{F}_q)$
- $q + 1$ **points at infinity** of the form $[a_0, a_1, 0]$ with the structure of $P^1(\mathbb{F}_q)$

Algebraic Curves

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves
Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings
Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption
References

Definition

An affine algebraic curve over $\mathbb{F}_q$ is defined by $f(x, y) = 0$ for an irreducible polynomial $f(x, y) \in \mathbb{F}_q[x, y]$.

Definition

A projective algebraic curve over $\mathbb{F}_q$ is defined by $f(x, y, z) = 0$ for an irreducible homogeneous polynomial $f(x, y, z) \in \mathbb{F}_q[x, y, z]$.

Singular Points

Elliptic Curve Cryptography

Tim Shaffer

Definitions
- Affine Space
- Projective Space
- Algebraic Curves
- Singular Points
- Elliptic Curves

Group Properties
- Additive Operation
- ECDLP
- Order of $\mathcal{E}(\mathbb{F}_q)$
- Schoof's Algorithm
- Pairings

Cryptography
- ECDH
- Elgamal
- Tripartite Key Exchange
- ID-based Encryption

References

Definition

A point P on an affine curve $f(x, y) = 0$ is called **singular** if

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) = (0, 0)$$

Definition

An algebraic curve is called **nonsingular** or **smooth** if it contains no singular points.

Elliptic Curves

Elliptic Curve Cryptography

Tim Shaffer

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves

Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings

Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption

References

The **projective Weierstrass equation** of an elliptic curve is given by

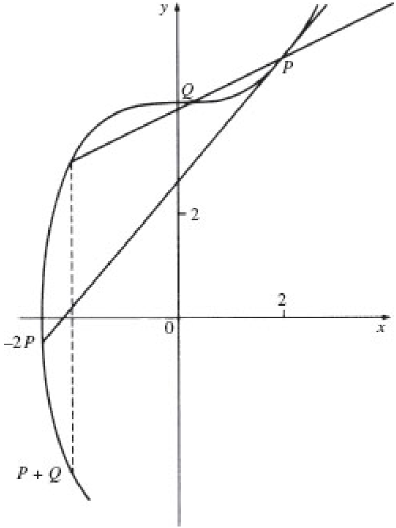
$$y^2z + \alpha_1 xyz + \alpha_3 yz^2 = x^3 + \alpha_2 x^2 z + \alpha_4 xz^2 + \alpha_6 z^3.$$

The affine **Weierstrass normal form** of an elliptic curve is

$$y^2 - x^3 - \alpha x - \beta = 0$$

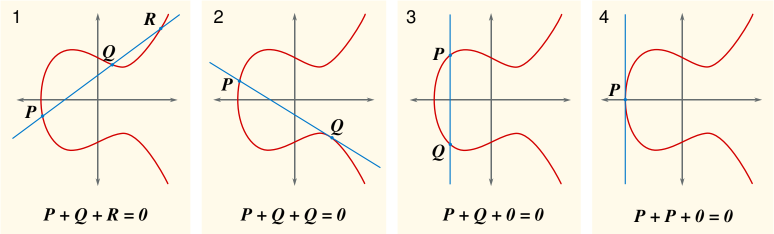
with discriminant $\Delta = -16(4\alpha^3 + 27\beta^2)$.

Additive Operation



Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves
Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings
Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption
References

Additive Operation



Additive Operation

Theorem

For an elliptic curve $\mathcal{E}(\mathbb{F}_q)$ and $a, b, c, d \in \mathbb{F}_q$, let $P = (a, b)$ and $Q = (c, d)$ be two points on $\mathcal{E}$ such that $Q \neq -P = (a, -b)$. Define

$$M = \begin{cases} \dfrac{d-b}{c-a} & \text{if } a \neq c \\ \dfrac{3a^2+\alpha}{2b} & \text{if } a = c. \end{cases}$$

Then the point $P + Q$ is given by $R = (g, h)$ where

$$\begin{aligned} g &= M^2 - a - c \\ h &= Ma - Mg - b. \end{aligned}$$

Elliptic Curve Discrete Logarithm Problem

Given $P = (a, b)$ on $\mathcal{E}$, it is possible to efficiently compute $\overbrace{P + \cdots + P}^{n \text{ times}}$, denoted $[n]P$.

However, given P and $[n]P$, it can be *very* difficult to compute the value of n.

Efficient Computation of $[n]P$

Algorithm

1. *Write n in its binary form, i.e. $n = n_0 + 2n_1 + 2^2 n_2 + \cdots + 2^t n_t$, with $n_i \in \{0, 1\}$ and $n_t = 1$.*
2. *Let $P_0 = P$.*
3. *For $i = 1, \ldots, t$, compute $P_i = [2^i]P = [2]P_{i-1}$ recursively.*
4. *Then, $[m]P = \sum_{i=0}^{t} [n_i] P_i$.*

While naïve application of the group operator requires n additions, this algorithm can be carried out in $2t \leq 2 \log n$ additions.

Elliptic Curve Cryptography

Tim Shaffer

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves

Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings

Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption

References

Order of $\mathcal{E}(\mathbb{F}_q)$

A curve with a small number of points would be vulnerable to cryptanalysis.

If an elliptic curve on $\mathbb{F}_p$ has exactly p points, the ECDLP can be transformed into addition in $\mathbb{Z}_p$.

Definition (Hasse-Weil Bound)

Let N be the number of points in $\mathbb{F}_q$ on an elliptic curve $\mathcal{E}$.

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves

Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings

Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption

References

Schoof's Algorithm

The number of points on an elliptic curve can be calculated efficiently using a deterministic polynomial time algorithm.

Schoof's Algorithm works by computing $q + 1 - N \pmod{p}$ for a large number of primes whose product is greater than $4\sqrt{q}$, then calculating $q + 1 - N$ by the Chinese Remainder Theorem.

With improvements by Atkin and Elkies, Schoof's Algorithm runs in $O(\log^4 q)$ time.

Pairings on Elliptic Curves

Definition

Given abelian groups G_1, G_2, G_3, a pairing $\omega : G_1 \times G_2 \to G_3$ maps every pair of elements in $G_1 \times G_2$ to some element in G_3.

A *cryptographically useful* pairing is also

- bilinear: if $g_1, g_1' \in G_1$ and $g_2, g_2' \in G_2$ then $\omega(g_1 g_1', g_2) = \omega(g_1, g_2)\omega(g_1', g_2)$ and $\omega(g_1, g_2 g_2') = \omega(g_1, g_2)\omega(g_1, g_2')$.
- nondegenerate: if $\omega(g_1, g_2) = 1$ for all $g_2 \in G_2$ then it follows that $g_1 = 1$.

Assume that all parties agree in advance on a choice of elliptic curve $\mathcal{E}$ on finite field $\mathbb{F}_p$, $P \in \mathcal{E}(\mathbb{F}_p)$, and paring ω on $\mathcal{E}$.

The chosen parameters are assumed to be public knowledge and to possess the properties appropriate for security.

Let $M \in \mathcal{E}(\mathbb{F}_p)$ be a message (encoded as a point on $\mathcal{E}(\mathbb{F}_p)$) that Alice would like to send to Bob.

Elliptic Curve Diffie-Hellman Exchange

Setup

- *Alice chooses a random secret $a \in \mathbb{Z}$ and sends $A = [a]P$ to Bob over an insecure channel.*
- *In the same way, Bob chooses a random secret $b \in \mathbb{Z}$ and sends $B = [b]P$ to Alice.*

Algorithm

- *Alice computes $Q = [a]B = [ab]P$.*
- *Bob computes $Q = [b]A = [ba]P$.*

Elgamal Encryption

Elliptic Curve Cryptography

Tim Shaffer

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves

Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings

Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption

References

Setup

Bob chooses a private key $b \in \mathbb{Z}$ and computes his public key $B = [b]P$. Bob is free to publish B.

Encryption

Alice chooses a random $k \in \mathbb{Z}$ and computes $C_1 = [k]P$, $C_2 = M + [k]B$ and sends (C_1, C_2) to Bob.

Decryption

Bob computes $M = C_2 - [a]C_1$.

Tripartite Key Exchange

Elliptic Curve Cryptography

Tim Shaffer

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves

Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings

Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption

References

Setup

Alice, Bob, and Carl each choose a random secret $a, b, c \in \mathbb{Z}$, respectively. They compute and share $A = [a]P$, $B = [b]P$, and $C = [c]P$ over insecure channels.

Algorithm

Each computes the shared secret as follows using his/her respective secret:

- *Alice:* $\omega(B, C)^a$
- *Bob:* $\omega(A, C)^b$
- *Carl:* $\omega(A, B)^c$

Identity-based Encryption

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves
Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings
Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption
References

Let Trent act as the trusted authority.

Setup

1. *Trent chooses a master secret $s \in \mathbb{Z}$ and publishes $S = [s]P$.*
2. *Bob encodes his identity (e.g. username, email, etc.) as $b \in \mathbb{Z}$. Anyone can compute Bob's public key $B = [b]P$.*
3. *Bob requests his private key $E = [s]B = [sb]P$ from Trent.*

Identity-based Encryption

Elliptic Curve Cryptography

Tim Shaffer

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves

Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings

Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption

References

Encryption

Alice chooses a random secret $t \in \mathbb{Z}$ *and sends* $(U, V) = ([t]P, M + \omega(B, S)^t)$ *to Bob.*

Decryption

Bob computes $M = V - \omega(E, U)$*.*

References

Elliptic Curve Cryptography

Tim Shaffer

Definitions
Affine Space
Projective Space
Algebraic Curves
Singular Points
Elliptic Curves

Group Properties
Additive Operation
ECDLP
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Pairings

Cryptography
ECDH
Elgamal
Tripartite Key Exchange
ID-based Encryption

References

- Baker, Alan. *A Comprehensive Course in Number Theory*. New York: Cambridge UP, 2012. Print.
- Boutet, Emmanuel. Example Elliptic Curves. Digital image. *Wikimedia Commons*. Wikimedia Foundation, 25 Oct. 2007. Web. 16 July 2014. (CC BY-SA 3.0)
- Ireland, Kenneth F., and Michael I. Rosen. *A Classical Introduction to Modern Number Theory*. Vol. 84. New York: Springer-Verlag, 1990. Print. Graduate Texts in Mathematics.
- Ling, San, Huaxiong Wang, and Chaoping Xing. *Algebraic Curves in Cryptography*. Boca Raton: CRC, 2013. Print.
- Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton: CRC, 1997. Print.

Definitions
- Affine Space
- Projective Space
- Algebraic Curves
- Singular Points
- Elliptic Curves

Group Properties
- Additive Operation
- ECDLP
- Order of $\mathcal{E}(\mathbb{F}_q)$
- Schoof's Algorithm
- Pairings

Cryptography
- ECDH
- Elgamal
- Tripartite Key Exchange
- ID-based Encryption

References