Elliptic Curves and Their Applications in Cryptography

Tim Shaffer[1]

Youngstown State University

MathFest 2014

[1]Adviser: 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.

Definition

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

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

where the discriminant

$$\Delta = -16(4\alpha^3 + 27\beta^2) \neq 0.$$

▸ Definitions

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

Elliptic Curves

Elliptic Curve Cryptography

Tim Shaffer

Definition

Group Properties

Additive Operation

ECDLP

Cryptography

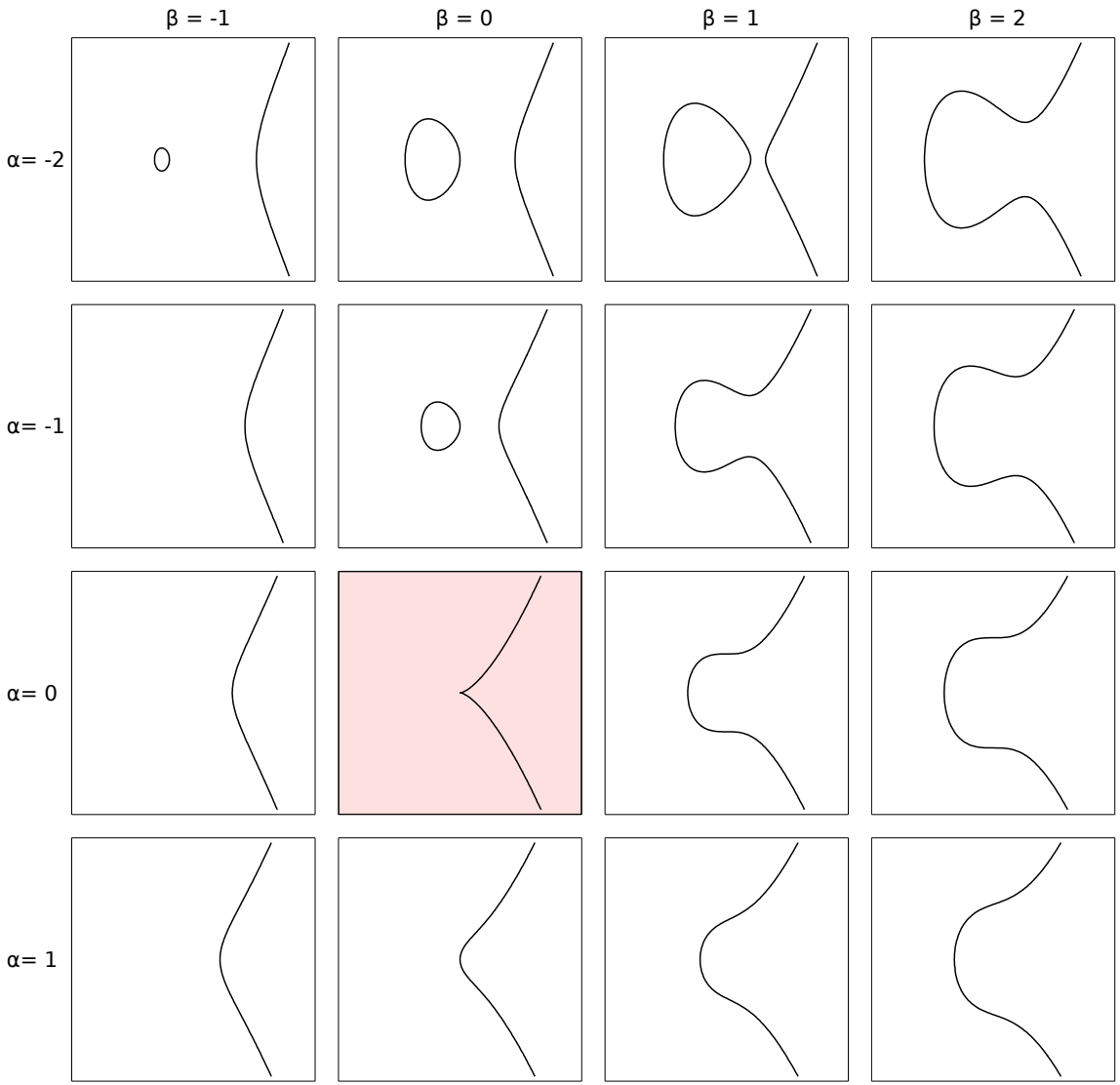
ECDH

Elgamal

ID-based Encryption

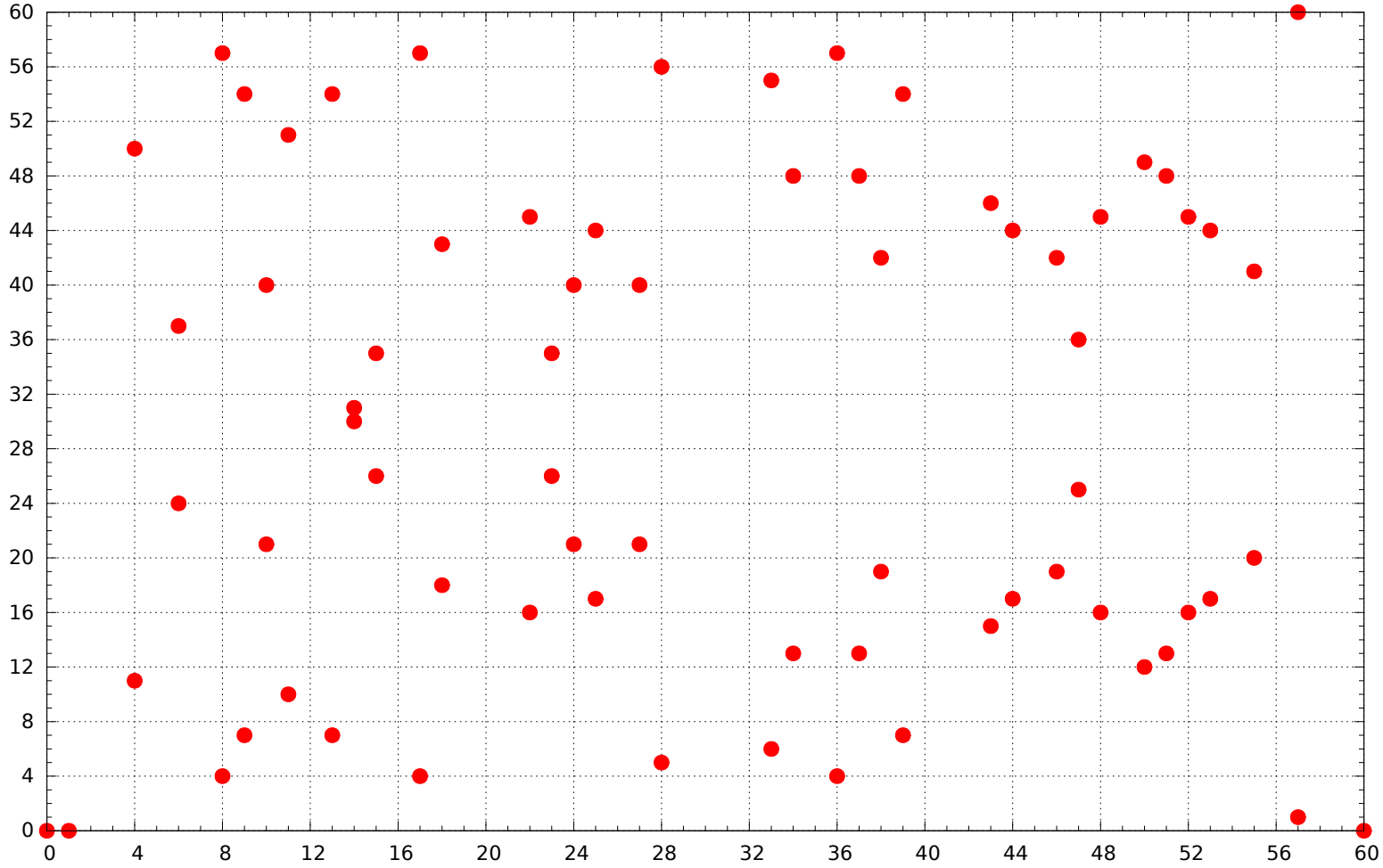
Comparisons

References



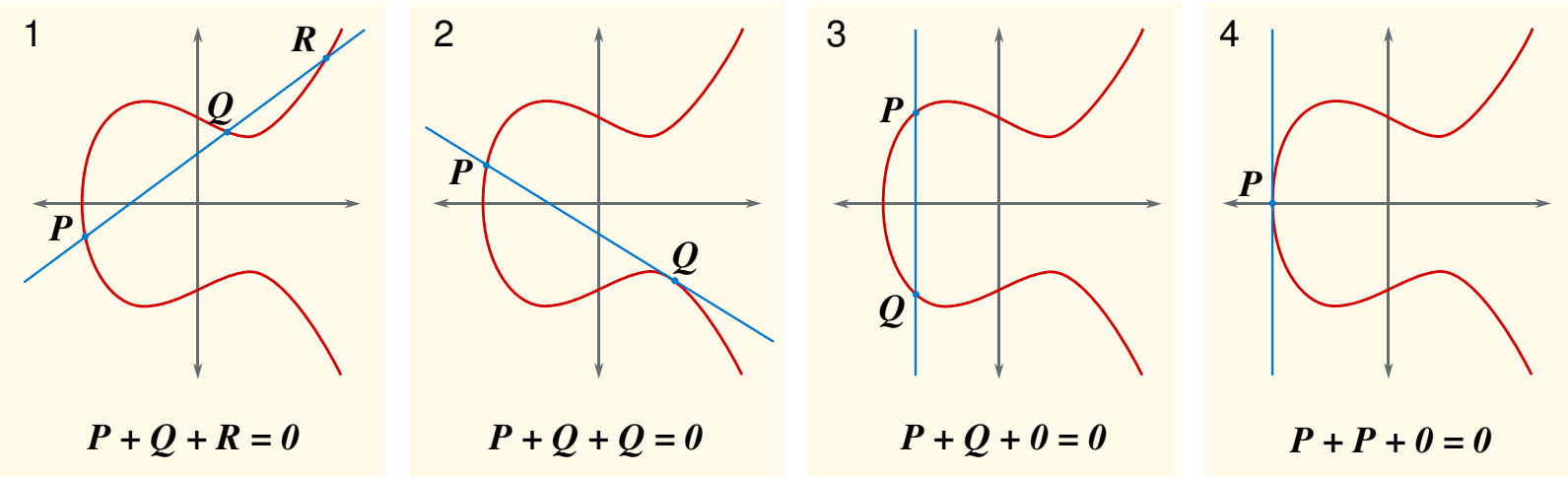
Elliptic Curve $y^2 = x^3 - x$ on $\mathbb{Z}/61\mathbb{Z}$

Elliptic Curve Cryptography
Tim Shaffer
Definition
Group Properties
Additive Operation
ECDLP
Cryptography
ECDH
Elgamal
ID-based Encryption
Comparisons
References



Additive Operation

▸ Point at Infinity



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

$$g = m^2 - a - c$$
$$h = ma - mg - b.$$

▸ Proof

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 $[n]P$.

▸ Implementation

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

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 $\mathcal{E}$.

▸ Pairings

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

Elliptic Curve Cryptography
Tim Shaffer
Definition
Group Properties
Additive Operation
ECDLP
Cryptography
ECDH
Elgamal
ID-based Encryption
Comparisons
References

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
Definition
Group Properties
Additive Operation
ECDLP
Cryptography
ECDH
Elgamal
ID-based Encryption
Comparisons
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

$$C_2 - [b]C_1 = M + [k]B - [b][k]P = M + [kb]P - [bk]P = M.$$

Assume that all parties choose in advance the following parameters.

- $\mathcal{E}$: $y^2 = x^3 - x + 1$
- $\mathbb{F}_{\text{|}}$: $\mathbb{Z}/113\mathbb{Z}$
- P: $(69, 96)$

Let $M = (53, 111)$ be a block of a secret message.

Elgamal Example

Setup

Bob chooses a private key $b = 8$ *and publishes his public key* $B = [b]P = [8](69, 96) = (95, 17)$.

Encryption

Alice chooses a random $k = 11$ *and computes* $C_1 = [k]P = [11](69, 96) = (71, 99)$, $C_2 = M + [k]B = (53, 111) + [11](95, 17) = (96, 23)$ *and sends* (C_1, C_2) *to Bob.*

Decryption

Bob computes $C_2 - [b]C_1 = (96, 23) - [8](71, 99) = (53, 111)$.

Identity-based Encryption

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

Encryption

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

Decryption

Observe that

$$\omega(E, U) = \omega([s]B, [t]P) = \omega(B, P)^{st} = \omega(B, [s]P)^t = \omega(B, S)^t.$$

Bob computes $M = V - \omega(E, U) = V - \omega(B, S)^t$.

Security

NIST Recommended Key Sizes

Symmetric Key Size	RSA and DH Key Size	EC Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Efficiency

Operations per 10 seconds

	Sign	Verify
RSA 1024	51670	819461
RSA 2048	7669	247067
RSA 4096	1072	66025
ECDSA 160	163316	44279
ECDSA 224	144934	64201
ECDSA 521	31128	13824

References I

- Baker, Alan. *A Comprehensive Course in Number Theory*. New York: Cambridge UP, 2012. Print.
- Bernstein, Daniel J. and Tanja Lange. *SafeCurves: choosing safe curves for elliptic-curve cryptography*. http://safecurves.cr.yp.to, accessed 4 August 2014.
- 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.

References II

- Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton: CRC, 1997. Print.
- "The Case for Elliptic Curve Cryptography." *Central Security Service*. NSA, 15 Jan. 2009. Web. 06 Aug. 2014.

Affine Space

Elliptic Curve Cryptography

Tim Shaffer

Definitions

Points in $P^2(\mathbb{F}_q)$

Maps Between Spaces

Addition on $\mathcal{E}$

Pairings

Implementation

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

Schoof's Algorithm

Sample Curve

ECDH Example

Factorization

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 $(a_1, a_2, \ldots, a_n)$ with $a_i \in \mathbb{F}_q$.

Definition

A **point** in $A^n(\mathbb{F}_q)$ is an n-tuple $(a_1, a_2, \ldots, a_n)$ for $a_i \in \mathbb{F}_q$.

Projective Space

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 $[1, a_1, a_2]$ that map to $A^2(\mathbb{F}_q)$
- $q + 1$ **points at infinity** of the form $[0, a_0, a_1]$ with the structure of $P^1(\mathbb{F}_q)$

Algebraic Curves

Elliptic Curve Cryptography

Tim Shaffer

Definitions

Points in $P^2(\mathbb{F}_q)$

Maps Between Spaces

Addition on $\mathcal{E}$

Pairings

Implementation

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

Schoof's Algorithm

Sample Curve

ECDH Example

Factorization

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

Definitions

Points in $P^2(\mathbb{F}_q)$

Maps Between Spaces

Addition on $\mathcal{E}$

Pairings

Implementation

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

Schoof's Algorithm

Sample Curve

ECDH Example

Factorization

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

Definitions

Points in $P^2(\mathbb{F}_q)$

Maps Between Spaces

Addition on $\mathcal{E}$

Pairings

Implementation

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

Schoof's Algorithm

Sample Curve

ECDH Example

Factorization

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

$$y^2z + \alpha_1xyz + \alpha_3yz^2 = x^3 + \alpha_2x^2z + \alpha_4xz^2 + \alpha_6z^3.$$

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

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

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

Number of Points in $P^2(\mathbb{F}_q)$

Elliptic Curve Cryptography
Tim Shaffer
Definitions
Points in $P^2(\mathbb{F}_q)$
Maps Between Spaces
Addition on $\mathcal{E}$
Pairings
Implementation
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Sample Curve
ECDH Example
Factorization

It is clear that the number of points in $A^n(\mathbb{F}_q)$ is q^n.

Proof.

Observe that

$$P^2(\mathbb{F}_q) = \{[1, a, b] | a, b \in \mathbb{F}_q\} \cup \{[0, 1, a] | a \in \mathbb{F}_q\} \cup \{[0, 0, 1]\}$$

It follows that the number of points in $P^2(\mathbb{F}_q)$ is

$$q^2 + q + 1.$$

□

Mappings Between Projective and Affine Spaces

Elliptic Curve Cryptography
Tim Shaffer
Definitions
Points in $P^2(\mathbb{F}_q)$
Maps Between Spaces
Addition on $\mathcal{E}$
Pairings
Implementation
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Sample Curve
ECDH Example
Factorization

Let K be a field and define H as the points at infinity of $P^n(K)$. Mappings λ and ϕ between affine and projective spaces are defined as follows.

$$\lambda : A^n(K) \to P^n(K)$$
$$\lambda(a_1, a_2, \ldots, a_n) = [1, a_1, a_2, \ldots, a_n]$$

$$\phi : P^n(K) - H \to A^n(K)$$
$$\phi([b_0, b_1, \ldots, b_n]) = \left(\frac{b_1}{b_0}, \frac{b_2}{b_0}, \ldots, \frac{b_n}{b_0}\right)$$

Correctness of Additive Operation on $\mathcal{E}$

Let ℓ, the line passing through P and Q, be given by $y = mx - C$ with m as defined for the addition operation and $k = b - ma$. Also let $S = (g', h')$ be the third intersection of $\mathcal{E}$ and ℓ. Substituting the equation for ℓ into that of $\mathcal{E}$,

$$(mx + k)^2 = x^3 + \alpha x + \beta$$

which expands to

$$f(x) = x^3 - m^2x^2 + (\alpha - 2mk)x + \beta - k^2 = 0.$$

Correctness of Additive Operation on $\mathcal{E}$

Since a, c, g' are the x coordinates of p, Q, S, respectively,

$$f(x) = (x - a)(x - c)(x - g')$$

and by expanding and comparing coefficients,

$$g' = M^2 - a - c$$
$$h' = Mg' + N$$

so

$$P + Q = S = (g', -h').$$

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 $g_1 = 1$.

Efficient Computation of $[n]P$

Elliptic Curve Cryptography
Tim Shaffer
Definitions
Points in $P^2(\mathbb{F}_q)$
Maps Between Spaces
Addition on $\mathcal{E}$
Pairings
Implementation
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Sample Curve
ECDH Example
Factorization

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.

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

Elliptic Curve Cryptography
Tim Shaffer
Definitions
Points in $P^2(\mathbb{F}_q)$
Maps Between Spaces
Addition on $\mathcal{E}$
Pairings
Implementation
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Sample Curve
ECDH Example
Factorization

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 $\mathcal{E}$.

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

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.

secp224r1

Elliptic Curve Cryptography
Tim Shaffer
Definitions
Points in $P^2(\mathbb{F}_q)$
Maps Between Spaces
Addition on $\mathcal{E}$
Pairings
Implementation
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Sample Curve
ECDH Example
Factorization

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

over $\mathbb{Z}/p\mathbb{Z}$ with

$$p = 2^224 - 2^96 + 1$$

$$\beta = b4\ 05\ 0a\ 85\ 0c\ 04\ b3\ ab\ f5\ 41\ 32\ 56\ 50$$
$$44\ b0\ b7\ d7\ bf\ d8\ ba\ 27\ 0b\ 39\ 43\ 23\ 55\ ff\ b4$$

and base point

$$(b7\ 0e\ 0c\ bd\ 6b\ b4\ bf\ 7f\ 32\ 13\ 90\ b9\ 4a\ 03$$
$$c1\ d3\ 56\ c2\ 11\ 22\ 34\ 32\ 80\ d6\ 11\ 5c\ 1d\ 21,$$
$$bd\ 37\ 63\ 88\ b5\ f7\ 23\ fb\ 4c\ 22\ df\ e6\ cd\ 43$$
$$75\ a0\ 5a\ 07\ 47\ 64\ 44\ d5\ 81\ 99\ 85\ 00\ 7e\ 34)$$

ECDH Example

Elliptic Curve Cryptography
Tim Shaffer
Definitions
Points in $P^2(\mathbb{F}_q)$
Maps Between Spaces
Addition on $\mathcal{E}$
Pairings
Implementation
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Sample Curve
ECDH Example
Factorization

Setup

- *Alice chooses* $a = 7$ *and sends* $A = [a]P = [7](69, 96) = (62, 96)$ *to Bob.*
- *Bob chooses* $b = 12$ *and sends* $B = [b]P = [12](69, 96) = (60, 87)$ *to Alice.*

Algorithm

- *Alice computes* $[a]B = [7](60, 87) = (67, 2)$.
- *Bob computes* $[b]A = [12](62, 96) = (67, 2)$.

Elliptic Curve Factorization

Elliptic Curve Cryptography
Tim Shaffer
Definitions
Points in $P^2(\mathbb{F}_q)$
Maps Between Spaces
Addition on $\mathcal{E}$
Pairings
Implementation
Order of $\mathcal{E}(\mathbb{F}_q)$
Schoof's Algorithm
Sample Curve
ECDH Example
Factorization

Pollard's $p-1$ algorithm can find prime factors p of a composite integer for which $p-1$ is smooth with respect to some relatively small bound k.

Definition

An integer is called k-**smooth** if all of its prime factors are less than k.

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

Definitions

Points in $P^2(\mathbb{F}_q)$

Maps Between Spaces

Addition on $\mathcal{E}$

Pairings

Implementation

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

Schoof's Algorithm

Sample Curve

ECDH Example

Factorization