Elliptic Curve Cryptography

Matthew England

Department of Mathematics, MACS
Heriot Watt University
Edinburgh

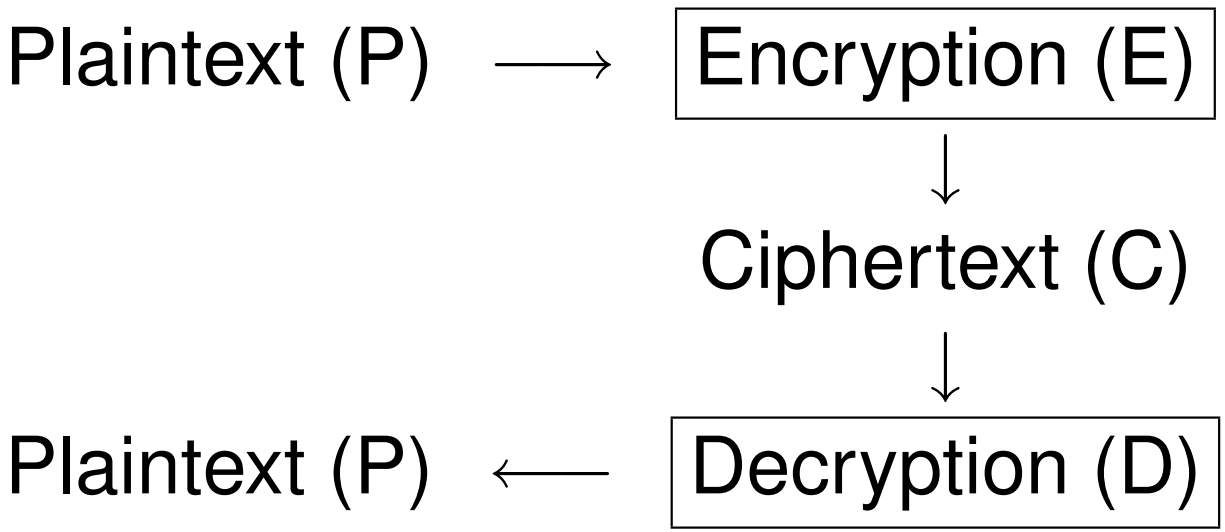
MACS Seminar
22nd February 2008

Outline

Outline

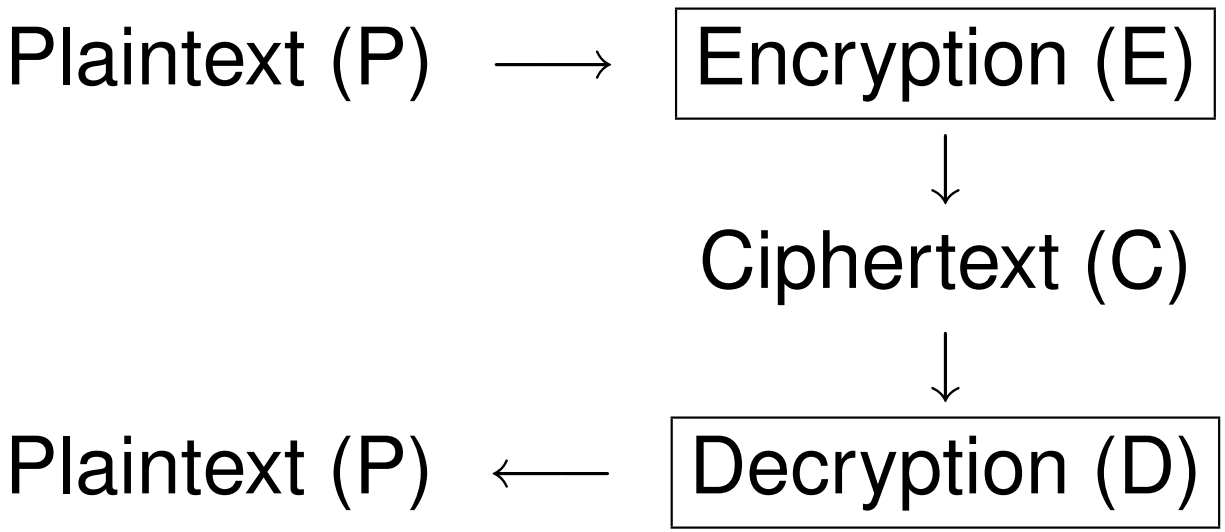
Cryptosystems

Cryptosystems are constructed to securely send messages.



Cryptosystems

Cryptosystems are constructed to securely send messages.



- P and C are often just bit streams (0s and 1s).

What is cryptography?

Definition

CRYPTOGRAPHY is the science of keeping messages secure.

Definition

CRYPTANALYSIS are the techniques for breaking ciphertext.

What is cryptography?

Definition

CRYPTOGRAPHY is the science of keeping messages secure.

+

Definition

CRYPTANALYSIS are the techniques for breaking ciphertext.

= CRYPTOLOGY

This is all more important now that ever!

Development of cryptography

- Use Key based systems rather than Restricted algorithms

Development of cryptography

- Use Key based systems rather than Restricted algorithms
- Aim for Computational Security — cryptosystem cannot be broken with available resources.

Development of cryptography

- Use Key based systems rather than Restricted algorithms
- Aim for Computational Security — cryptosystem cannot be broken with available resources.

Two main types of cryptosystems:

Symmetric Key Systems

- Decryption key $=$ Encryption key
- Users need to agree on this key **before** communicating securely.

Symmetric key systems

These are usually based on *Substitutions* and *Permutations*.

Symmetric key systems

These are usually based on *Substitutions* and *Permutations*.

Example: The Caesar Cipher

In this simple cipher each letter is moved 3 places to the right

$$\text{eg} \quad \text{CRYPTOGRAPHY} \longrightarrow \text{FUBSWRJUDSKB}$$

This cipher could be broken with a minimal amount of effort!

- However, there are much more sophisticated systems regularly used in the real world (eg DES, AES).

Two main types of cryptosystem

Symmetric Key Systems

- Decryption key $=$ Encryption key
- Users need to agree on this key **before** communicating securely.

OR

Public Key Systems

- Decryption key $\neq$ Encryption key
- Encryption Key $=$ Public
  Decryption Key $=$ Private

A Public Key Encryption system

Private:  **Public**: 

A Public Key Encryption system

Private:  **Public**: 

A Public Key Encryption system

Alice ⟶ Plaintext

↓

Encryption  Bob's Public Key

↓

Ciphertext

↓

Decryption  Bob's Private Key

↓

Bob ⟵ Plaintext

Private:  **Public**: 

Public key systems

In the above diagram:

- No keys exchanged!
- Bob is the only person who could read this message.

Public key systems

In the above diagram:

- No keys exchanged!
- Bob is the only person who could read this message.

These systems are usually based on mathematical functions!

$\Longrightarrow$ **one way functions**

Public key systems

In the above diagram:

- No keys exchanged!
- Bob is the only person who could read this message.

These systems are usually based on mathematical functions!
$\Longrightarrow$ **Trapdoor one way functions**

Public key systems

In the above diagram:

- No keys exchanged!
- Bob is the only person who could read this message.

These systems are usually based on mathematical functions!
$\Longrightarrow$ **Trapdoor one way functions**

- First suggested by Diffie and Hellman (1976)
- First put into practise by RSA (1978)
- Other notable schemes include El Gamal (1984)

A Public Key System can be used for authentication as well as encryption...

A Public Key Authentication system

Private:  **Public**: 

A Public Key Authentication system

Private:  **Public:** 

A Public Key Authentication system

Private:  **Public**: 

Alice ⟶ Plaintext

↓

Encryption ←  Alice's Private Key

↓

Ciphertext

↓

Decryption ←  Alice's Public Key

↓

Bob ⟵ Plaintext

A Public Key Authentication system

Private:  **Public**: 

Alice ⟶ Plaintext

↓

Encryption  Alice's Private Key

↓

Ciphertext

↓

Decryption  Alice's Public Key

↓

Bob ⟵ Plaintext

- Only Alice could have possibly sent the message!

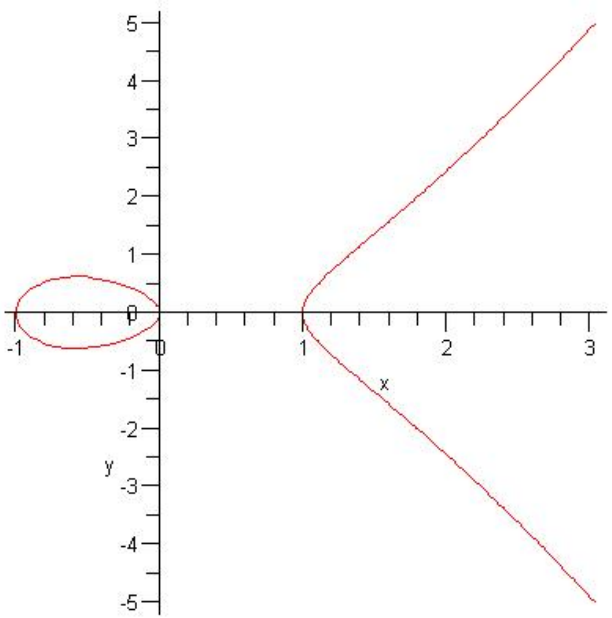
Outline

What is an elliptic curve?

Definition

An elliptic curve is a (non-singular) algebraic curve defined by an equation of the form

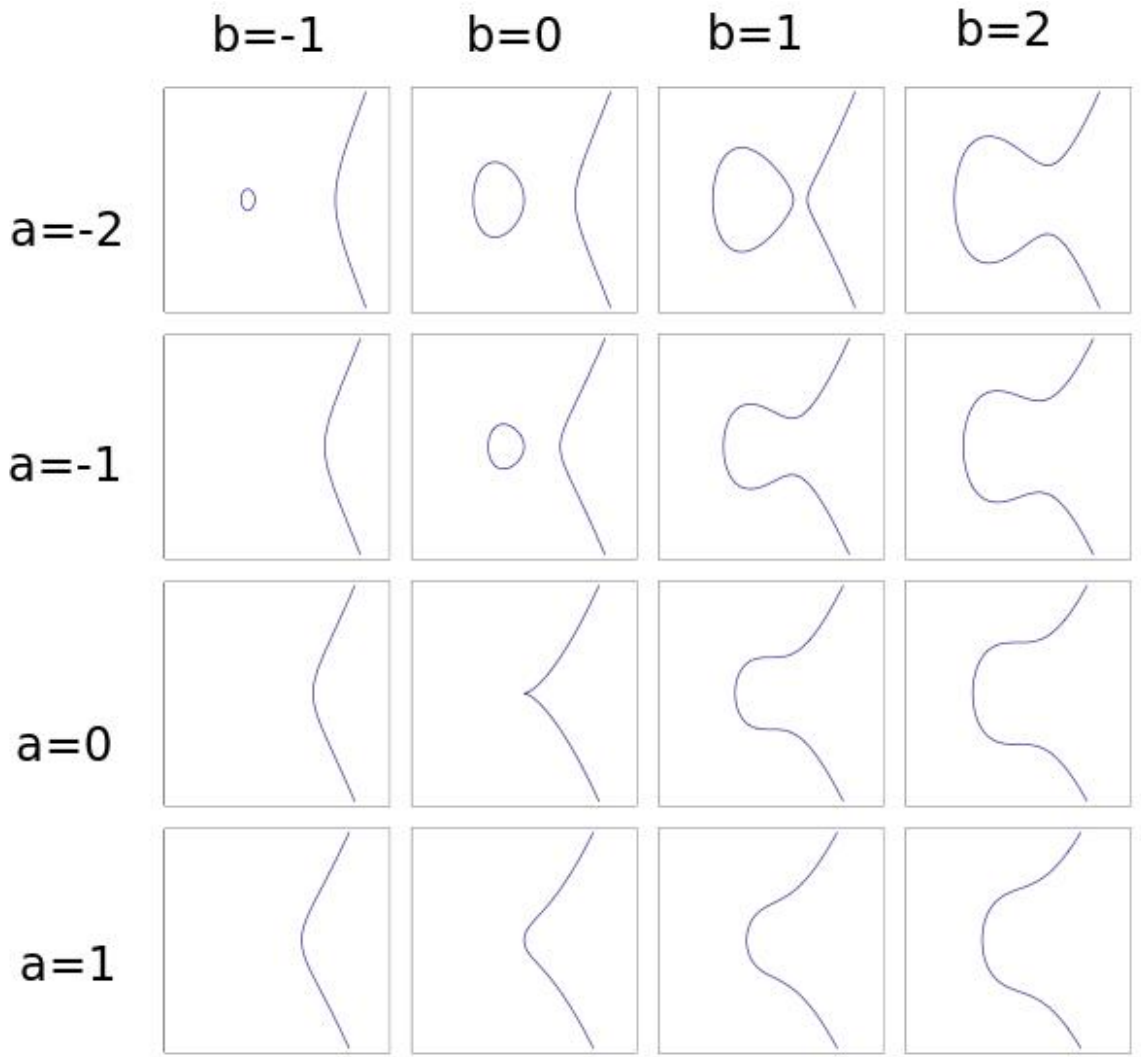
$$Y^2 = X^3 + aX + b$$



For example, when
$a = -1$ and $b = 0$ we have:

$$Y = X^3 - X$$

More examples of elliptic curves



Defining an addition operation

We define an addition operation for points on an elliptic curve:

Defining an addition operation

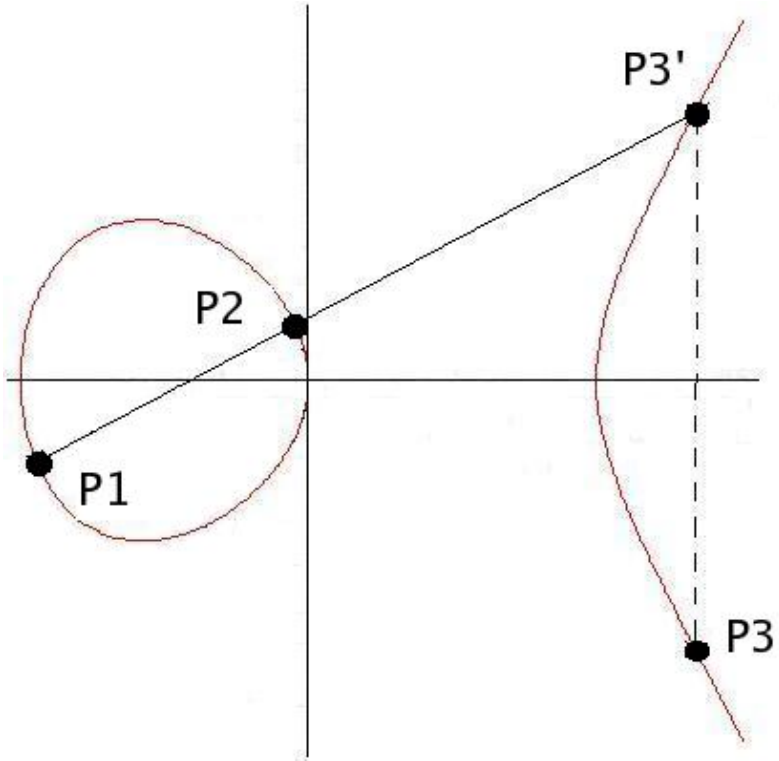
We define an addition operation for points on an elliptic curve:

Given two points $P1$ and $P2$:

1. Find the straight line connecting them.
2. Calculate the third point of intersection $P3'$.
3. Reflect to find $P3$.

Define the addition law as

$$P1 + P2 = P3$$



▸ Infinity

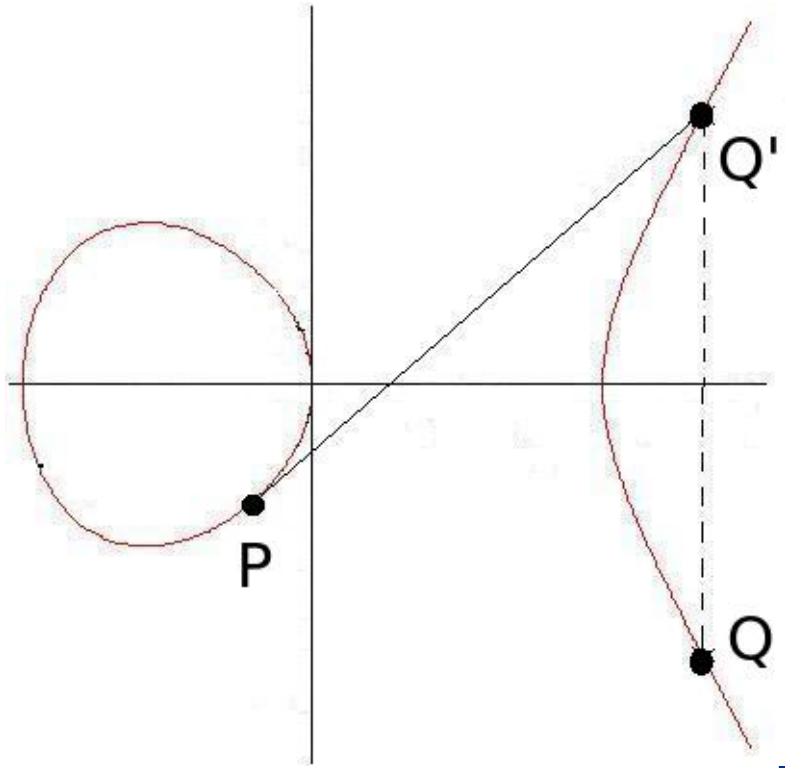
Sorting out the exceptions

Q) How do we add a point, P, to itself?

Sorting out the exceptions

Q) How do we add a point, P, to itself?

A) Instead of drawing the line connecting the two points, draw the tangent line to the curve at the point.
Then, as before, find the third point of intersection, Q' and reflect to find the point Q. Define $P + P = Q$.



▸ Infinity

Sorting out the exceptions

Q) Is there always a third point of intersection?

Sorting out the exceptions

Q) Is there always a third point of intersection?

A) Yes, unless the line we draw is vertical. This will occur when $P1$ and $P2$ have the same x-coordinate, or if we are adding a point to itself and it has y-coordinate zero.

P1+P2 P+P

Sorting out the exceptions

Q) Is there always a third point of intersection?

A) Yes, unless the line we draw is vertical. This will occur when $P1$ and $P2$ have the same x-coordinate, or if we are adding a point to itself and it has y-coordinate zero.

- In these cases we define the sum as the *special* point, ∞.

P1+P2 P+P

Sorting out the exceptions

Q) Is there always a third point of intersection?

A) Yes, unless the line we draw is vertical. This will occur when $P1$ and $P2$ have the same x-coordinate, or if we are adding a point to itself and it has y-coordinate zero.

- In these cases we define the sum as the *special* point, ∞.
- For all points on the curve, $P + \infty = P$. Identity Element

P1+P2 P+P

Sorting out the exceptions

Q) Is there always a third point of intersection?

A) Yes, unless the line we draw is vertical. This will occur when $P1$ and $P2$ have the same x-coordinate, or if we are adding a point to itself and it has y-coordinate zero.

- In these cases we define the sum as the *special* point, ∞.
- For all points on the curve, $P + \infty = P$. ▸ Identity Element
- Think of ∞ as sitting at both the top (and bottom) of the y-axis — then these rules coincide with the process above.

▸ P1+P2 ▸ P+P

Sorting out the exceptions

Q) Is there always a third point of intersection?

A) Yes, unless the line we draw is vertical. This will occur when $P1$ and $P2$ have the same x-coordinate, or if we are adding a point to itself and it has y-coordinate zero.

- In these cases we define the sum as the *special* point, ∞.
- For all points on the curve, $P + \infty = P$. ▸ Identity Element
- Think of ∞ as sitting at both the top (and bottom) of the y-axis — then these rules coincide with the process above.
- The point ∞ lies upon the elliptic curve.

For more information study projective geometry!

▸ P1+P2 ▸ P+P

Points on an elliptic curve form a group!

Consider an operation $*$ and a set of objects, G. These form a group $(G, *)$ if the four axioms below are satisfied.

Points on an elliptic curve form a group!

Consider an operation $*$ and a set of objects, G. These form a group $(G, *)$ if the four axioms below are satisfied. We will show that that the set of points upon an elliptic curve (including ∞) form a group with the addition operation defined above!

Points on an elliptic curve form a group!

Consider an operation $*$ and a set of objects, G. These form a group $(G, *)$ if the four axioms below are satisfied. We will show that that the set of points upon an elliptic curve (including ∞) form a group with the addition operation defined above!

- **Closure**: For all a, b in $G \Longrightarrow a * b$ is also in G.

Points on an elliptic curve form a group!

Consider an operation $*$ and a set of objects, G. These form a group $(G, *)$ if the four axioms below are satisfied. We will show that that the set of points upon an elliptic curve (including ∞) form a group with the addition operation defined above!

- **Closure**: For all a, b in $G \Longrightarrow a * b$ is also in G.
  Sum of two points on the curve, gives a point on the curve.

Points on an elliptic curve form a group!

Consider an operation $*$ and a set of objects, G. These form a group $(G, *)$ if the four axioms below are satisfied. We will show that that the set of points upon an elliptic curve (including ∞) form a group with the addition operation defined above!

- **Closure**: For all a, b in $G \Longrightarrow a * b$ is also in G.
  Sum of two points on the curve, gives a point on the curve.
- **Identity**: There is an element e in G such that for all a in G

$$e * a = a * e = a$$

Points on an elliptic curve form a group!

Consider an operation $*$ and a set of objects, G. These form a group $(G, *)$ if the four axioms below are satisfied. We will show that that the set of points upon an elliptic curve (including ∞) form a group with the addition operation defined above!

- **Closure**: For all a, b in $G \Longrightarrow a * b$ is also in G.
  Sum of two points on the curve, gives a point on the curve.
- **Identity**: There is an element e in G such that for all a in G

$$e * a = a * e = a$$

The point ∞ satisfies the identity property. ▸ infinity

Points on an elliptic curve form a (mathematical) group!

- **Inverse**: For each a in G, there exists an element b in G such that, $a * b = b * a = e$, where e is an identity element.

Points on an elliptic curve form a (mathematical) group!

- **Inverse**: For each a in G, there exists an element b in G such that, $a * b = b * a = e$, where e is an identity element. The inverse is the other point with the same x-coordinate. (If there isn't one then the point is a self inverse.)

Points on an elliptic curve form a (mathematical) group!

- **Inverse**: For each a in G, there exists an element b in G such that, $a * b = b * a = e$, where e is an identity element. The inverse is the other point with the same x-coordinate. (If there isn't one then the point is a self inverse.)
- **Associativity**: For all a, b, c in G

$$(a * b) * c = a * (b * c).$$

Points on an elliptic curve form a (mathematical) group!

- **Inverse**: For each a in G, there exists an element b in G such that, $a * b = b * a = e$, where e is an identity element. The inverse is the other point with the same x-coordinate. (If there isn't one then the point is a self inverse.)
- **Associativity**: For all a, b, c in G

$$(a * b) * c = a * (b * c).$$

True, but a lot of work to prove!

Points on an elliptic curve form a (mathematical) group!

- **Inverse**: For each a in G, there exists an element b in G such that, $a * b = b * a = e$, where e is an identity element. The inverse is the other point with the same x-coordinate. (If there isn't one then the point is a self inverse.)
- **Associativity**: For all a, b, c in G

$$(a * b) * c = a * (b * c).$$

True, but a lot of work to prove!

An abelian group satisfies the additional property:

- **Commutative**: For all a, b in $G \implies a * b = b * a$.

Points on an elliptic curve form a (mathematical) group!

- **Inverse**: For each a in G, there exists an element b in G such that, $a * b = b * a = e$, where e is an identity element.
  The inverse is the other point with the same x-coordinate.
  (If there isn't one then the point is a self inverse.)
- **Associativity**: For all a, b, c in G

$$(a * b) * c = a * (b * c).$$

  True, but a lot of work to prove!

An abelian group satisfies the additional property:

- **Commutative**: For all a, b in $G \implies a * b = b * a$.
  Clear from the definition of the addition operation.

Outline

Why can elliptic curves be used in cryptography?

Work with an elliptic curve defined over a finite field.

Definition

Let k be a positive integer, and P a point on an elliptic curve. Then multiplying P by k is defined as

$$kP = P + P + P + ... + P \qquad (k \text{ times})$$

Let Q is the point given by $Q = kP$:

Why can elliptic curves be used in cryptography?

Work with an elliptic curve defined over a finite field.

Definition

Let k be a positive integer, and P a point on an elliptic curve. Then multiplying P by k is defined as

$$kP = P + P + P + ... + P \qquad (k \text{ times})$$

Let Q is the point given by $Q = kP$:

- Finding Q given k, P — Easy! (Use successive doubling)

Why can elliptic curves be used in cryptography?

Work with an elliptic curve defined over a finite field.

Definition

Let k be a positive integer, and P a point on an elliptic curve. Then multiplying P by k is defined as

$$kP = P + P + P + ... + P \qquad (k \text{ times})$$

Let Q is the point given by $Q = kP$:

- Finding Q given k, P — Easy! (Use successive doubling)
- Finding k given Q, P — Difficult

Why can elliptic curves be used in cryptography?

Work with an elliptic curve defined over a finite field.

Definition

Let k be a positive integer, and P a point on an elliptic curve. Then multiplying P by k is defined as

$$kP = P + P + P + ... + P \qquad (k \text{ times})$$

Let Q is the point given by $Q = kP$:

- Finding Q given k, P — Easy! (Use successive doubling)
- Finding k given Q, P — Difficult , often infeasible!

$\Longrightarrow$ one-way function, ideal for Public Key Cryptography!

Real World

The Diffie-Hellman Key Exchange for elliptic curves

Alice and Bob agree on an elliptic curve, E, and a point upon it, P (chosen carefully!). The choice (E,P) is public.

The Diffie-Hellman Key Exchange for elliptic curves

Alice and Bob agree on an elliptic curve, E, and a point upon it, P (chosen carefully!). The choice (E,P) is public.

1. Alice chooses a secret integer a, computes $P_a = aP$ and sends P_a to Bob.
2. Bob chooses a secret integer b, computes $P_b = bP$ and sends P_b to Alice.

The Diffie-Hellman Key Exchange for elliptic curves

Alice and Bob agree on an elliptic curve, E, and a point upon it, P (chosen carefully!). The choice (E,P) is public.

1. Alice chooses a secret integer a, computes $P_a = aP$ and sends P_a to Bob.
2. Bob chooses a secret integer b, computes $P_b = bP$ and sends P_b to Alice.
3. Alice computes $aP_b = abP$. Bob computes $bPa = abP$.
4. They agree of a way to extract a key from abP.

The Diffie-Hellman Key Exchange for elliptic curves

Alice and Bob agree on an elliptic curve, E, and a point upon it, P (chosen carefully!). The choice (E,P) is public.

1. Alice chooses a secret integer a, computes $P_a = aP$ and sends P_a to Bob.
2. Bob chooses a secret integer b, computes $P_b = bP$ and sends P_b to Alice.
3. Alice computes $aP_b = abP$. Bob computes $bPa = abP$.
4. They agree of a way to extract a key from abP.

A spy would know E, P, P_a and P_b. Finding abP from this information is infeasible!

Real World

The El Gamal cryptosystem for elliptic curves

Bob sets up the cryptosystem by choosing an elliptic curve, E, a point, P and a secret integer s. He computes $B = sP$ and makes, E, P and B public, (keeping s private).

The El Gamal cryptosystem for elliptic curves

Bob sets up the cryptosystem by choosing an elliptic curve, E, a point, P and a secret integer s. He computes $B = sP$ and makes, E, P and B public, (keeping s private). Then:

1. Alice encodes her message as a point M.

The El Gamal cryptosystem for elliptic curves

Bob sets up the cryptosystem by choosing an elliptic curve, E, a point, P and a secret integer s. He computes $B = sP$ and makes, E, P and B public, (keeping s private). Then:

1. Alice encodes her message as a point M.
2. Alice chooses a secret integer r, and computes

$$M_1 = rP, \qquad \text{and} \quad M_2 = M + rB$$

3. Alice sends M_1, M_2 to Bob.

The El Gamal cryptosystem for elliptic curves

Bob sets up the cryptosystem by choosing an elliptic curve, E, a point, P and a secret integer s. He computes $B = sP$ and makes, E, P and B public, (keeping s private). Then:

1. Alice encodes her message as a point M.
2. Alice chooses a secret integer r, and computes

$$M_1 = rP, \qquad \text{and} \quad M_2 = M + rB$$

3. Alice sends M_1, M_2 to Bob.

Bob can then find M by calculating

$$M_2 - sM_1 = \qquad\qquad = M$$

The El Gamal cryptosystem for elliptic curves

Bob sets up the cryptosystem by choosing an elliptic curve, E, a point, P and a secret integer s. He computes $B = sP$ and makes, E, P and B public, (keeping s private). Then:

1. Alice encodes her message as a point M.
2. Alice chooses a secret integer r, and computes

$$M_1 = rP, \qquad \text{and} \quad M_2 = M + rB$$

3. Alice sends M_1, M_2 to Bob.

Bob can then find M by calculating

$$M_2 - sM_1 = (M + rB) - s(rP) = (M + rsP) - s(rP) = M$$

The El Gamal cryptosystem for elliptic curves

Bob sets up the cryptosystem by choosing an elliptic curve, E, a point, P and a secret integer s. He computes $B = sP$ and makes, E, P and B public, (keeping s private). Then:

1. Alice encodes her message as a point M.
2. Alice chooses a secret integer r, and computes

$$M_1 = rP, \qquad \text{and} \quad M_2 = M + rB$$

3. Alice sends M_1, M_2 to Bob.

Bob can then find M by calculating

$$M_2 - sM_1 = (M + rB) - s(rP) = (M + rsP) - s(rP) = M$$

A spy would know M_1 and M_2 but not s. The spy may know (E, P, B), but finding s from this is infeasible!

Public Key Cryptography in real life

Is any of this used in the real world?

Public Key Cryptography in real life

Is any of this used in the real world?

- Public Key schemes take more time and memory than symmetric schemes (to give the same level of security).

Public Key Cryptography in real life

Is any of this used in the real world?

- Public Key schemes take more time and memory than symmetric schemes (to give the same level of security).
- In practise, public key schemes are usually used for the *key exchange* and *authentication*. The actual message is then encoded with an efficient symmetric system.

Public Key Cryptography in real life

Is any of this used in the real world?

- Public Key schemes take more time and memory than symmetric schemes (to give the same level of security).
- In practise, public key schemes are usually used for the *key exchange* and *authentication*. The actual message is then encoded with an efficient symmetric system.
- RSA has so far dominated the use of Public Key cryptography...

Public Key Cryptography in real life

Is any of this used in the real world?

- Public Key schemes take more time and memory than symmetric schemes (to give the same level of security).
- In practise, public key schemes are usually used for the *key exchange* and *authentication*. The actual message is then encoded with an efficient symmetric system.
- RSA has so far dominated the use of Public Key cryptography...
- Elliptic curve systems give a similar level of security to RSA while using a much smaller bit size!

Further Reading

Simon Singh.
The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.
Fourth Estate, 1999.

Steven Levy.
Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age.
Chapman and Hall/CRC, 2003.

Lawrence C. Washington.
Elliptic Curves: Number Theory and Cryptography.
Chapman and Hall/CRC, 2003.