Elliptic curve cryptography

Outline

- Elliptic curves.
  - Over the reals.
    - Elliptic curve addition.
      - Geometric and algebraic.
  - Over finite fields, GF(p).

Elliptic curves

- We have seen some problems, DLP, CDHP, DDHP which are considered hard.
- Some of these problems are over Abelian fields or groups.
- We have looked at fields GF(p) where the elements of the field are simply integers, and the operations are modular.
- But these are not the only domains we can use.
- Miller and Koblitz, independently, suggested the use of elliptic curves for constructing public-key cryptosystems.

- We can take an Elliptic curve over a field, GF(p), or GF(p^m).
  - We are effectively restricting solutions to an equation to elements of a particular field.
- The problems like DLP are not necessarily hard in those fields, so we need to be a little careful.

Relative key sizes: For similar security

Symmetric (key size)	ECC-based (group order)	RSA/DSA (modulus size)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

- We will see later why this is the case.

Elliptic curves over the reals

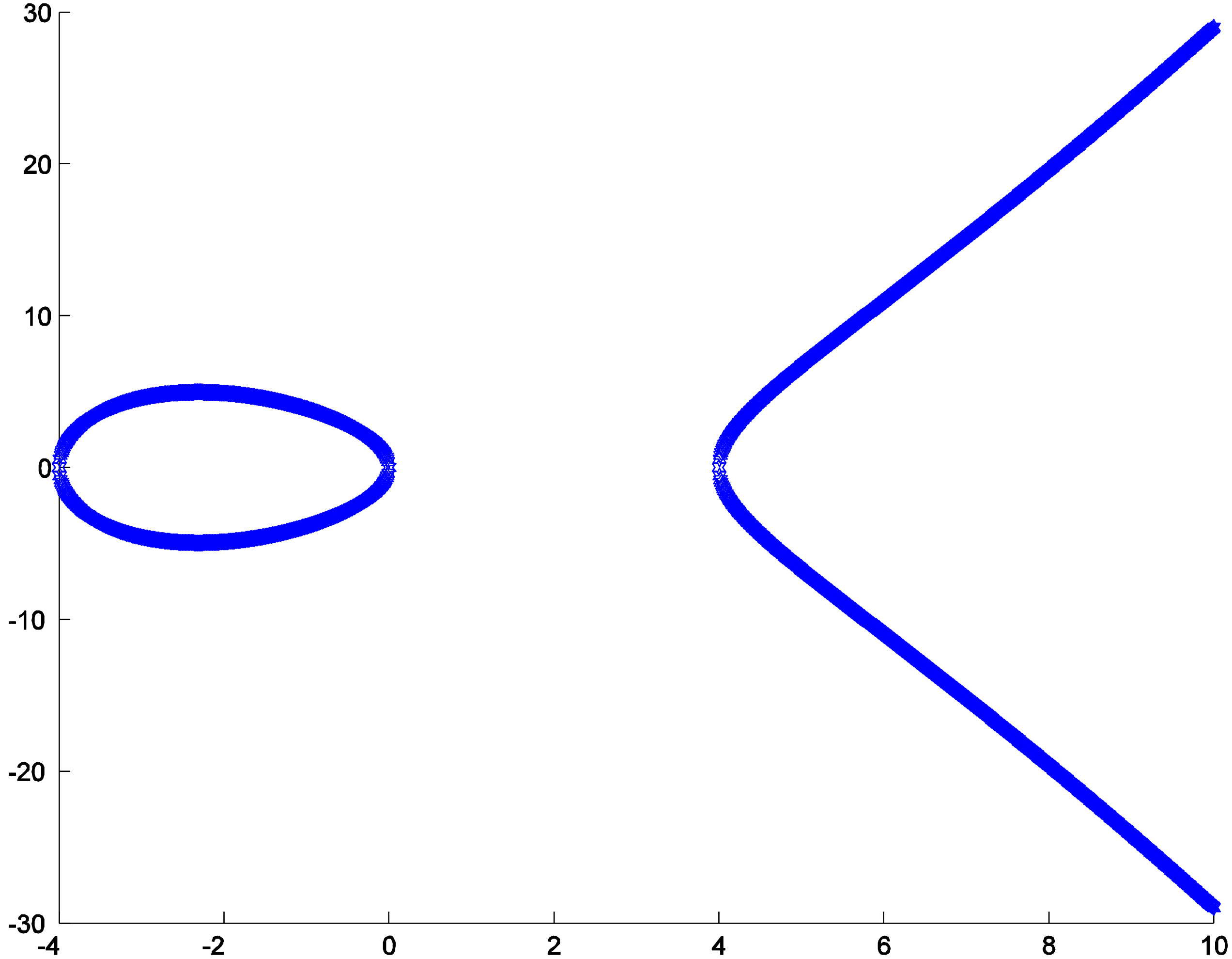
- Constant $a,b \in \Re$ (reals) satisfying the discriminant $\Delta = -4a^3 - 27b^2 \neq 0$.
- A *non-singular elliptic curve* is the set E of solutions $(x,y) \in \Re \times \Re$ to the equation

$$y^2 = x^3 + ax + b$$

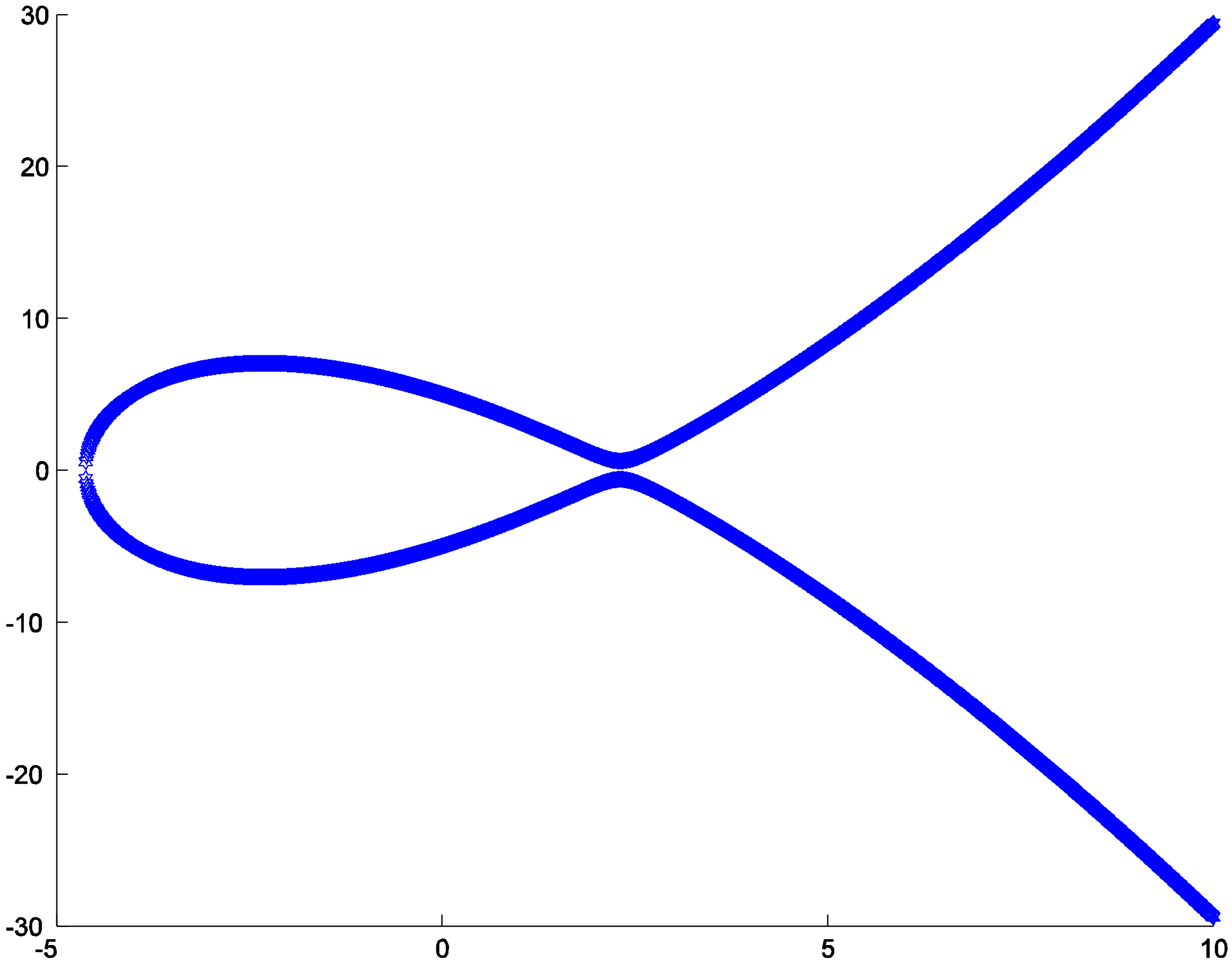
along with a point O, referred to as the *point at infinity*.

This is the form we are interested in.

$y^2=x^3-16x$



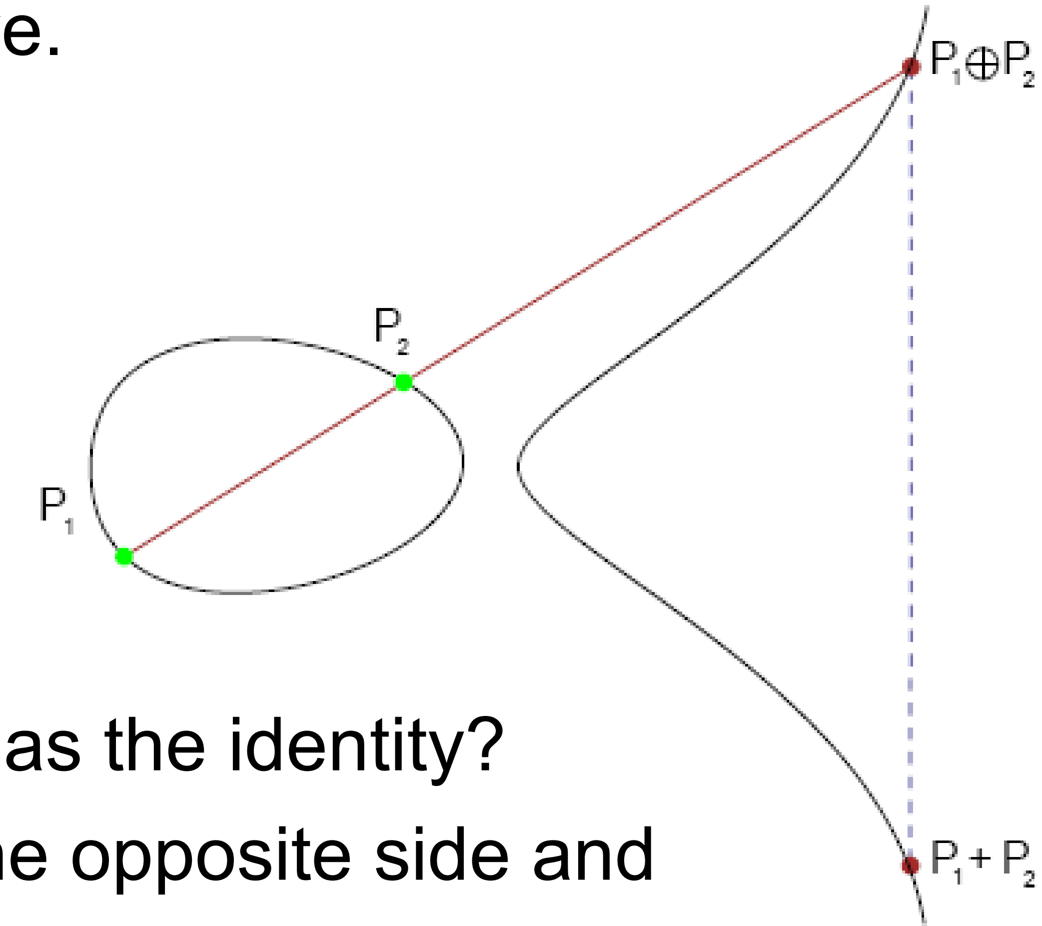
$y^2=x^3-16x+25$



Elliptic curve “addition”

- To get to an Abelian group we need a commutative binary operation.
  - This addition can be defined geometrically, making use of intersections and mirror images.
  - The addition can, alternately, be represented algebraically.
- The point at infinity acts as the identity.

- Let P_1 and P_2 be elements of E.
- We can calculate P_1+P_2 geometrically by drawing a line through P_1 and P_2 and recording the point on interception of the curve.



- The reflection across the x axis and onto the elliptic curve E is the solution P_1+P_2.

- How does infinity act as the identity?
- "A vertical line" hits the opposite side and reflects back.

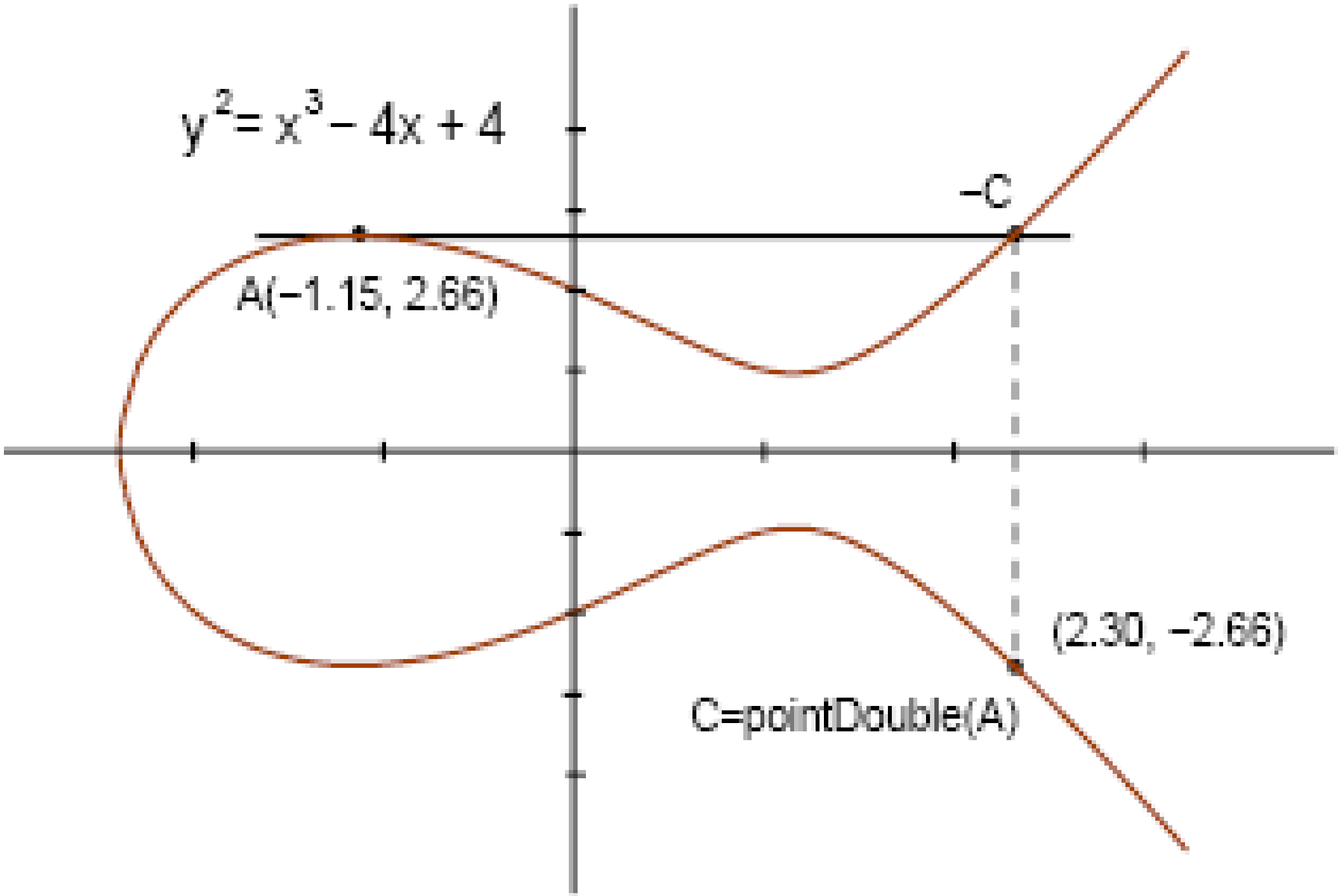
What about algebraically?

- Consider the P_1 is at (x_1,y_1) and that P_2 is at (x_2,y_2).
- Then $P_1+P_2=P_3$ at (x_3,y_3) where

  $x_3=s^2-x_1-x_2$ and $y_3= -y_1+s(x_1-x_3)$ with

  $s=(y_1-y_2)/(x_1-x_2)$ being the slope.

- In the case of $x_1=x_2$ we have either
- … $y_1=-y_2$, so the points are inverses and we get a vertical line which intercepts the point set at infinity (i.e. at the identity…)
- Or … we have $y_1=y_2$, so we are "point doubling" or adding the point to itself.
  - In this case we take the tangent at the curve at the point to be the line through it (corresponding to $s=(3x_1^2+a)/(2y_1)$.



From Chang et.al.

Elliptic curves over GF(p)

- The reals are an infinite field.
- In cryptography the finite fields are more frequently used.
- We can consider elliptic curves where the operations are all carried out with the elements being elements of some field, and operations being “modular”.
- E is the set of solutions (x,y) to $y^2=x^3+ax+b$ (mod p), where $4a^3+27b^2\neq 0$ (mod p), along with the point at infinity.

Stinson page 252

$y^2=x^3+x+6$ over GF(11)

x	$x^3+x+6 \bmod 11$	QR?	y
0	6		
1	8		
2	5		
3	3		
4	8		
5	4		
6	8		
7	4		
8	9		
9	7		
10	4		

Stinson page 252

$y^2=x^3+x+6$ over GF(11)

x	x^3+x+6 mod 11	QR?	y
0	6	No	
1	8	No	
2	5	Yes	4,7
3	3	Yes	5,6
4	8	No	
5	4	Yes	2,9
6	8	No	
7	4	Yes	2,9
8	9	Yes	3,8
9	7	No	
10	4	yes	2,9

The set is the point at infinity and (2,4),(2,7),(3,5),(3,6) (5,2),(5,9),(7,2),(7,9), (8,3), (8,8),(10,2),(10,9).

13 elements. Since the order is prime, every element other than the point at infinity is a generator.

The elliptic curve specifies how elements are added.

Example: Given $E: y^2 = x^3+2x+2 \bmod 17$ and point $P=(5,1)$

Goal: Compute $2P = P+P = (5,1)+(5,1)= (x_3,y_3)$

- **Example**: Given $E: y^2 = x^3+2x+2 \bmod 17$ and point $P=(5,1)$
  Goal: Compute $2P = P+P = (5,1)+(5,1) = (x_3,y_3)$

$$s = \frac{3x_1^2 + a}{2y_1} = (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) = 2^{-1} \cdot 9 \equiv 9 \cdot 9 \equiv 13 \bmod 17$$

$$x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \bmod 17$$
$$y_3 = s(x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \bmod 17$$

Finally $\boldsymbol{2P = (5,1) + (5,1) = (6,3)}$

椭圆曲线上的点构加上无穷远点成一个循环子群

$2P = (5,1)+(5,1) = (6,3)$

$3P = 2P+P = (10,6)$

$4P = (3,1)$

$5P = (9,16)$

$6P = (16,13)$

$7P = (0,6)$

$8P = (13,7)$

$9P = (7,6)$

$10P = (7,11)$

$11P = (13,10)$

$12P = (0,11)$

$13P = (16,4)$

$14P = (9,1)$

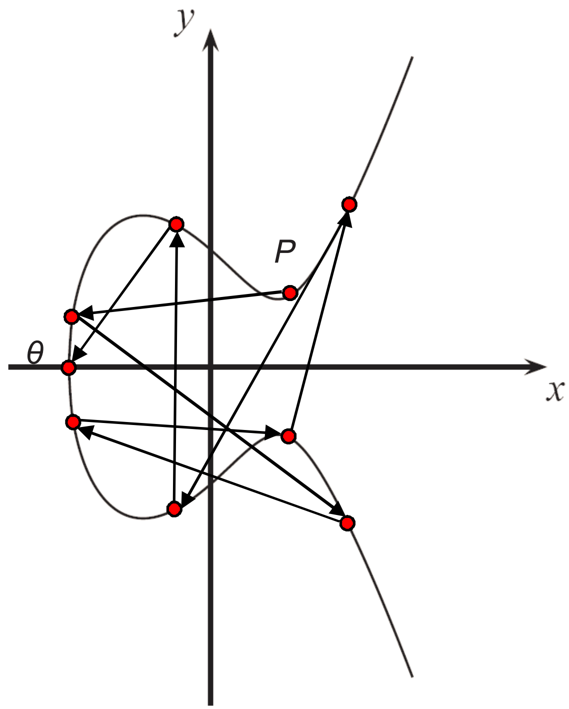
$15P = (3,16)$

$16P = (10,11)$

$17P = (6,14)$

$18P = (5,16)$

$19P = \theta$



这个椭圆曲线的位数为19，因为其包含19个点

ECC based crypto version

Outline

- The ECDLP Problem:
  - Getting a group.
  - Order.
- Diffie-Hellman Key Exchange.
- Elliptic Curve Diffie-Hellman Key Exchange
- Elliptic Curve El-Gamal.

The ECDLP Problem

- The most common hard problem that underlies the use of public key elliptic curve cryptosystems is the **E**lliptic **C**urve **D**iscrete **L**ogarithm **P**roblem.
- Let E be the set of points of our elliptic curve defined over the field GF(p).
  – The collection of points and the operation of addition, as defined earlier, form a group which we could denote E(GF(p)).
  – In this group the common operation is “scalar multiplication”.

- Notice that we have a group not a field.
- Scalar multiplication is not an additional binary operation, rather is an extension of the addition rule.
- We write scalar multiplication, of a point P, by an integer k as kP, and define it as P+P+…+P with k copies of P in the sum.

- We can now define the **E**lliptic **C**urve **D**iscrete **L**ogarithm **P**roblem:
  - Given two points in E, P_1 and P_2, find k: $P_1=kP_2$.

Order … group and element …

- We denote by #E the number of points on the curve, that is, the number of elements in our group E(GF(p)).
  - #E(GF(p^m)) = $p^m+1 - t$

    t is called the trace of Frobenius at p^m and satisfies (Hasse's theorem):

$$-2\sqrt{p^m} \leq t \leq 2\sqrt{p^m}$$

- Each element (point) P also has an order, the smallest element x: xP = $\mathcal{O}$ (the identity or point at infinity).
- If the group order is prime, the group is cyclic, all elements, except the point at infinity, are generators and all have an order equal to the group order.
  - We want such an Abelian group.
  - We don't always get one directly!

Diffie-Hellman Key Exchange

- The first public key system.
- Security is based on the difficulty of computing discrete logarithm.
  - Actually security it is based on the computational Diffie-Hellman problem.
- System Setup
  - A finite field Z_p, where *p* is prime.
  - A primitive element $g \in Z_p$.
  - *p* and *g* are public.

Diffie-Hellman Key Exchange

- The Protocol
  - Alice selects a secret X_A, for $X_A \in Z_p$, and computes her public key $Y_A = g^{X_A}$ mod p.
  - Bob selects a secret X_B, for $X_B \in Z_p$, and computes his public key $Y_B = g^{X_B}$ mod p.
  - Alice sends Y_A to Bob.
  - Bob sends Y_B to Alice.
  - Alice computes the shared secret key $K = Y_B^{X_A}$ mod p.
  - Bob computes the shared secret key $K = Y_A^{X_B}$ mod p.

EC Diffie-Hellman key exchange

- We can carry out a similar exchange using an Abelian group over an Elliptic curve.
- The two users agree upon a curve over a field, E(GF(q)), of known order n, and on a generator P, a base point.
- Each user selects a secret key $k_{si}<n$, and calculates their public key $K_{pi}=k_{si}P$.

- So, with Alice and Bob, we have temporary pairs (k_{sA},K_{pA}) and (k_{sB},K_{pB}).
- Alice gets the public key of Bob and calculates $K=k_{sA}K_{pB}$.
- Bob gets the public key of Alice and calculates $K=k_{sB}K_{pA}$.

- Both have the secret key K.

EC El-Gamal

- The parameters are, as in Diffie-Hellman Key Exchange over an Elliptic Curve, E(GF(p)), GF(p), P and n.
- Alice wants to encrypt a message for Bob.
- Alice knows the public component of Bob's key pair (k_{sB},K_{pB}).
- Alice chooses a random $r < n$, and determines $U=rP$.
- She also calculates $(x_q,y_q)=Q=rK_{pB}$.

- Finally Alice calculates $c = M \text{ XOR } x_q$.
- The encrypted message is $<U,c>$.
- To decrypt, Bob calculates

  $$(x_q,y_q) = Q = k_{sB}U$$

  then

  $$M=c \text{ XOR } x_q.$$

- This works since $Q = rK_{pB}= rk_{sB}P = k_{sB}(rP) = k_{sB}U$.

Bilinear Pairing

Outline

- Motivating the use of bilinear pairings.
- Bilinear pairing
- Security problems

Motivating the use of bilinear pairings

- Specifically, consider that we have two cyclic groups G_1 and G_2.

- Furthermore assume that there exists an isomorphism $\varphi : G_1 \rightarrow G_2$, and that this isomorphism can be carried out efficiently.

- Then, the difficulty of a problem, say the discrete log problem, in G_1, cannot be significantly greater than the difficulty of the problem in G_2.

For example…

- Consider that in G_1 we have the DLP:

  Given P_1 and Q_1 determine k where $P_1=kQ_1$.
- We can calculate $P_2 = \varphi(P_1)$.
- Now it follows from the definition of an isomorphism that $P_2=\varphi(kQ_1)=k\varphi(Q_1)$.
- Thus we have the DLP in G_2:

  Given P_2 and Q_2 determine k where $P_2=kQ_2$.

Bilinear pairings

- Let G_1,G_2 be additive groups of prime order p
- Let G_3 be multiplicative group of prime order p
- There is a mapping (the bilinear pairing)

$$e:G_1 \times G_2 \rightarrow G_3.$$

- The mapping is required to have several properties:
  - Bilinearity:
    - $e(P+Q,R)=e(P,R).e(Q,R)$
    - $e(P,R+S)=e(P,R).e(P,S)$

    This implies $e(aP,bR)=e(P,R)^{ab}=e(bP,aR)=e(R,P)^{ab}$.
  - Non-degeneracy: $\exists(P,R)\in G_1 \times G_2 : e(P,R)\neq 1$
  - Efficiency: $e(P,R)$ can be efficiently calculated.

Bilinear pairings

- Weil Pairing
- Tate Pairing

Security for pairing over EC

- Security depends on the hardness of one of a number of computational or decisional problems.
  - We have already seen the Elliptic Curve Discrete Log Problem (ECDLP).
  - We will now briefly look at the Bilinear Diffie-Hellman problem (BDHP).

BDHP

- **The Bilinear Diffie-Hellman Problem**:

For P a generator, given the collection $\langle P, aP, bP, cP \rangle$, for $a,b,c \in_R Z_r$, compute $e(P,P)^{abc}$.

- And, in the standard relationship manner, the corresponding BDH assumption is that there is no efficient algorithm to solve the BDHP with non-negligible probability.

CDH and DDH

- There are also the CDH and DDH problems.
  - For elliptic curves these are expressed for additive groups.
- Computational Diffie-Hellman problem
  - Given P in G, xP, and yP, compute xyP
- Decisional Diffie-Hellman problem
  - Given P in G, xP, yP, and Q = zP, decide whether z = xy.

DDH in pairing

- DDH problem in pairing is easy

  Given P in G, xP, yP, and Q = zP, decide whether z = xy

  $e(xP,yP) = e(P,P)^{xy}$

  $e(P,zP) = e(P,P)^{z}$