Elliptic Curve Cryptography

Sachin Tripathi

IIT(ISM), Dhanbad

Outline

- Basic pros and cons of ECC vs. RSA/DL schemes.
- What is an elliptic curve?
- Algorithms/Protocols that can be realized with elliptic curves.
- Current security estimations of cryptosystems based on elliptic curves.

Introduction

- Security of RSA and ElGamal depend on their large key space.
- It is estimated that certain conventional systems with a 4096 bits key size can be replaced by 313 bits elliptic curve systems.
- The main attraction of ECC is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.

Contd…

- In DLP, we have observed $\beta=\alpha^x \bmod P$ is computed by repeated multiplication operation.
- In ECC, we basically performed addition over elliptic curve.
- For example: kP=(P+P+…+P k times) where the addition is performed over an elliptic curve.
- need "hard" problem equivalent to discrete log
  - `Q=kP`, where Q,P belong to a prime curve
  - is "easy" to compute Q given k,P
  - but "hard" to find k given Q,P
  - known as the elliptic curve logarithm problem

Elliptic Curves over Real Numbers

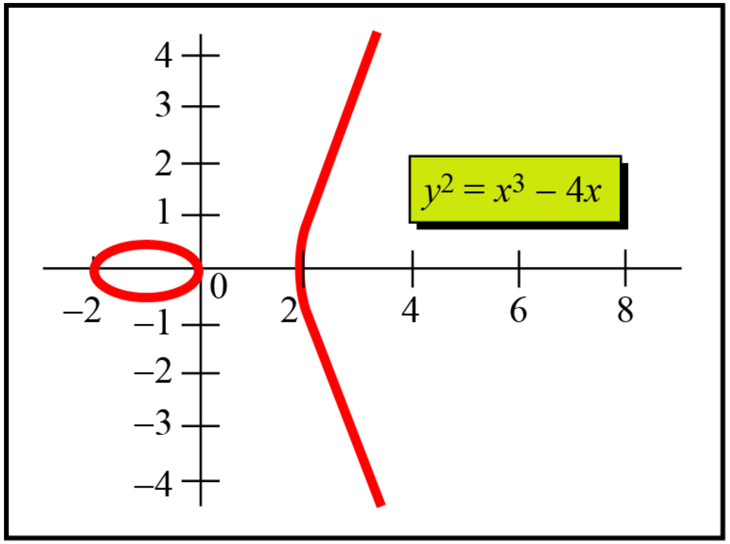
- An elliptic curve E is the graph of an equation
  E: $y^2+axy+by=x^3+cx^2+dx+e$
  where a, b, c, d, and e are all real numbers.
- In cryptography we use special class of elliptic curves of the form
  E: $y^2=x^3+ax+b$
- If we plot such equation then it will be symmetric about x-axis. Since The left-hand side has a degree of 2 while the right-hand side has a degree of 3.
- This means that a horizontal line can intersects the curve in three points if all roots are real.
- However, a vertical line can intersects the curve at most in two points.
- It also represented as E(a,b)

Contd...

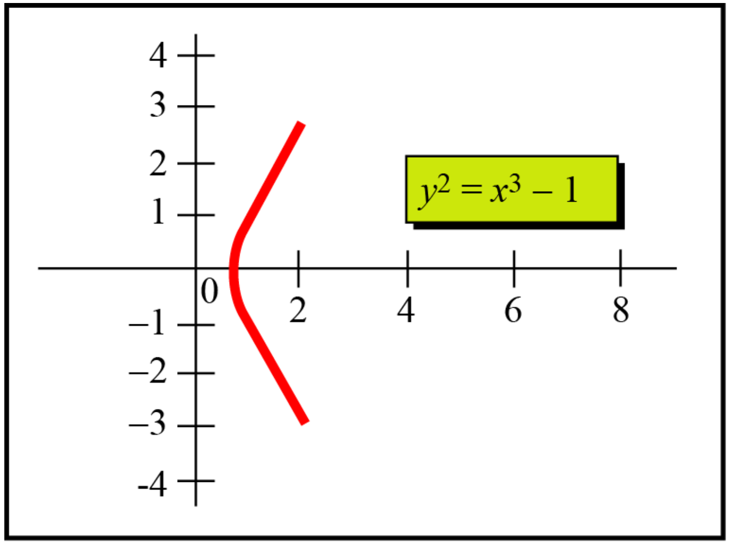
- The graph E has two possible forms, depending on whether the cubic polynomial has one real root or three real roots.
- For E: $y^2=x^3+ax+b$, if $4a^3+27b^2\neq 0$ the equation represents non-singular EC.
- In non-singular EC, the equation $x^3+ax+b=0$ has three distinct roots (real or complex).
- Otherwise, when $4a^3+27b^2=0$ then it is known as singular EC.
- In singular EC, the equation $x^3+ax+b=0$ has no three distinct roots.

Example

- Following Figures show two EC with equations $y^2 = x^3 - 4x$ and $y^2 = x^3 - 1$.
- The first has three real roots ($x = -2$, $x = 0$, and $x = 2$)
- But the second has only one real root ($x = 1$) and two imaginary ones.

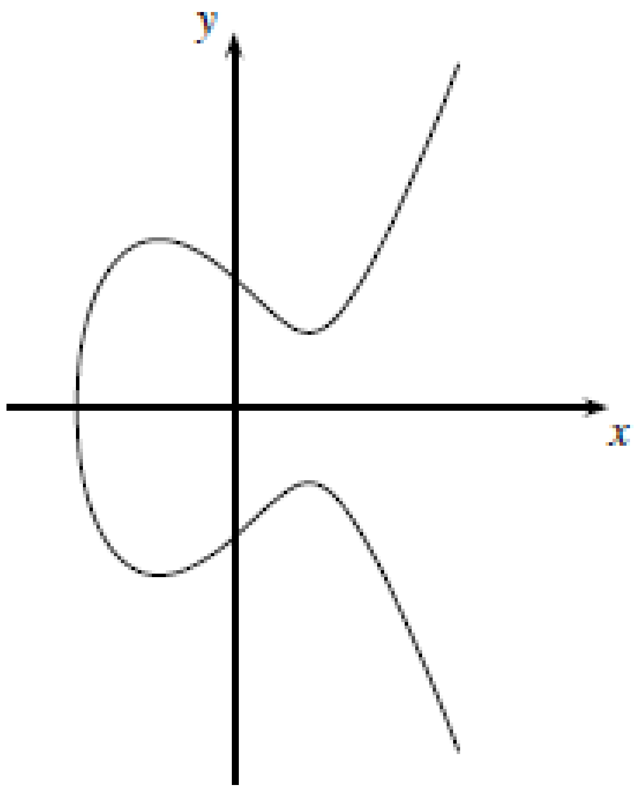


a. Three real roots



b. One real and two imaginary roots

Example

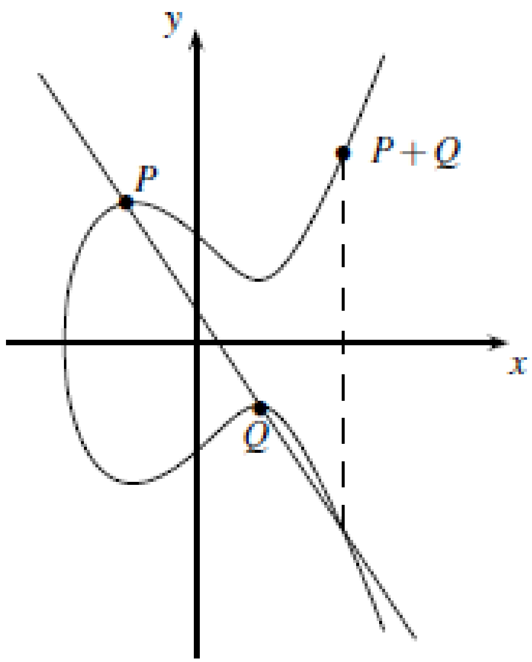


$y^2 = x^3 - 3x + 3$ over $\mathbb{R}$

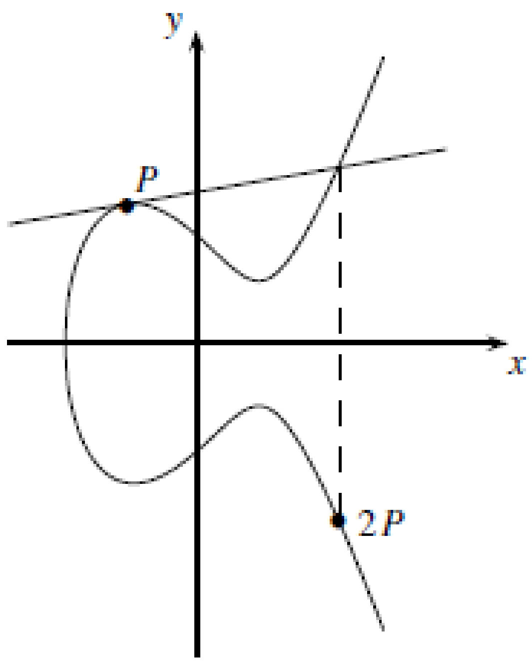
Group Operations on Elliptic Curves

- Given two points and their coordinates, say $P = (x1,y1)$ *and* $Q = (x2,y2)$, *we* have to compute the coordinates of a third point R *such that:* $P+Q = R$.
- **Point Addition: P+Q** (This is the case where we compute R = P+Q and P ≠Q.)
- **Point Doubling: 2P=P+P** (This is the case where we compute P+Q but P=Q.)

Addition

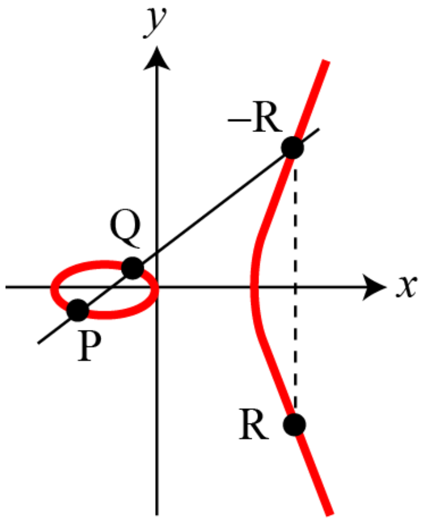


Point addition on an elliptic curve over the real numbers

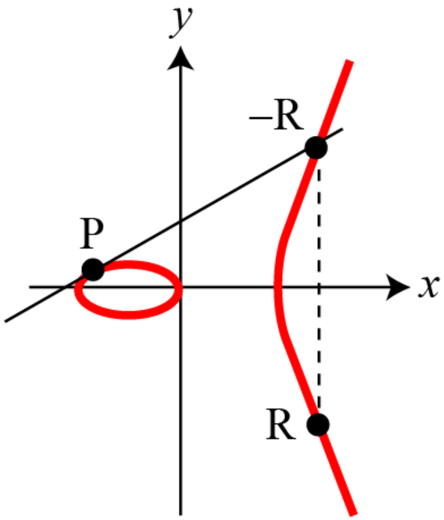


Point doubling on an elliptic curve over the real numbers

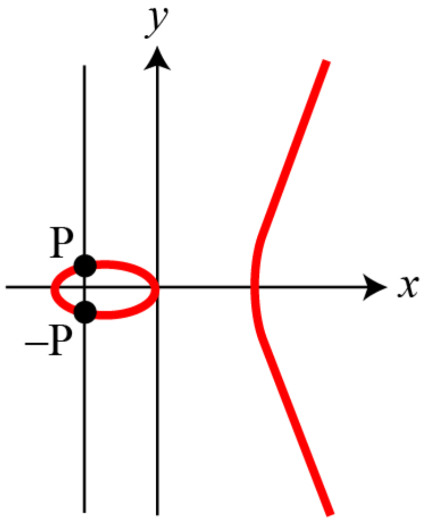
Addition



a. (R = P + Q)



b. (R = P + P)



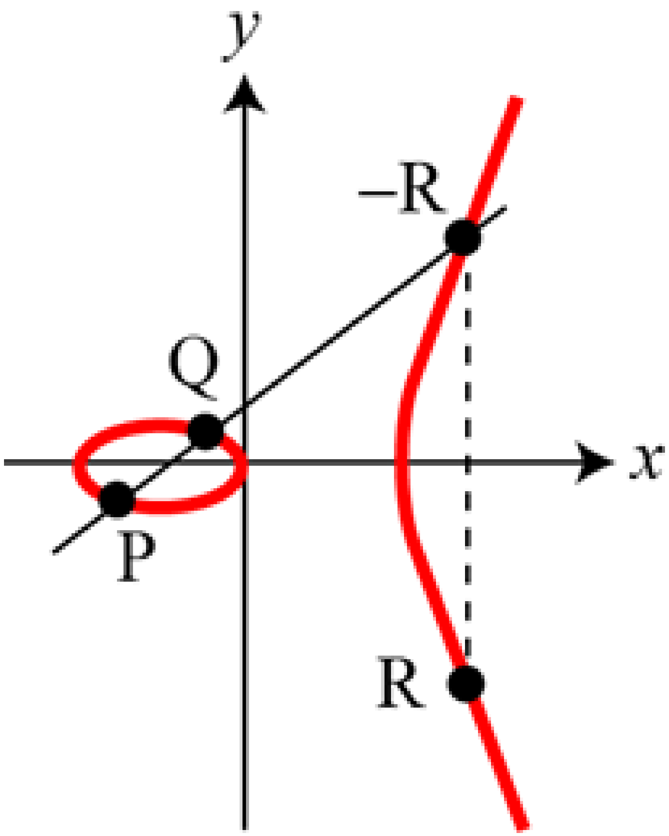
c. (O = P + (– P))

Formula

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

$$\lambda = (y_2 - y_1) / (x_2 - x_1)$$

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1$$



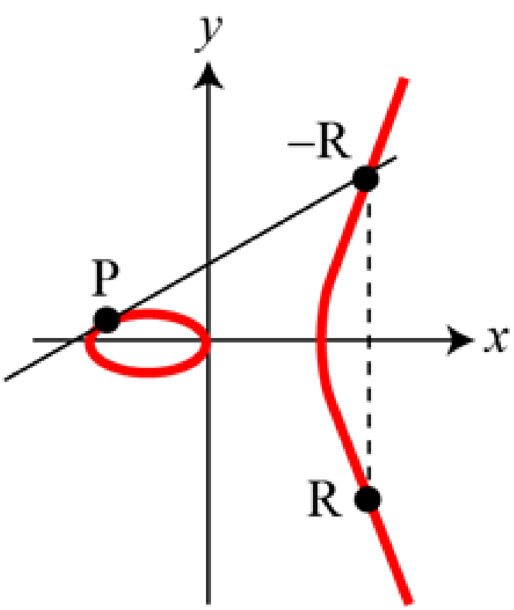
a. (R = P + Q)

Formula

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

$$\lambda = (3x_1^{\ 2} + a)/(2y_1)$$

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda\,(x_1 - x_3) - y_1$$



b. (R = P + P)

Example. Suppose E is defined by $y^2 = x^3 + 73$. Let $P_1 = (2,9)$ and $P_2 = (3,10)$. The line L through P_1 and P_2 is

$$y = x + 7.$$

Substituting into the equation for E yields

$$(x+7)^2 = x^3 + 73,$$

which yields $x^3 - x^2 - 14x + 24 = 0$. Since L intersects E in P_1 and P_2, we already know two roots, namely $x = 2$ and $x = 3$. Moreover, the sum of the three roots is minus the coefficient of x^2 (Exercise 1) and therefore equals 1. If x is the third root, then

$$2 + 3 + x = 1,$$

so the third point of intersection has $x = -4$. Since $y = x + 7$, we have $y = 3$, and $Q = (-4,3)$. Reflect across the x-axis to obtain

$$(2,0) + (3,10) = P_3 = (-4,-3).$$

Contd…

Now suppose we want to add P_3 to itself. The slope of the tangent line to E at P_3 is obtained by implicitly differentiating the equation for E:

$$2y\,dy = 3x^2\,dx, \quad \text{so} \quad \frac{dy}{dx} = \frac{3x^2}{2y} = -8,$$

where we have substituted $(x, y) = (-4, -3)$ from P_3. In this case, the line L is $y = -8(x+4) - 3$. Substituting into the equation for E yields

$$(-8(x+4) - 3)^2 = x^3 + 73,$$

hence $x^3 - (-8)^2x^2 + \cdots = 0$. The sum of the three roots is 64 (= minus the coefficient of x^2). Because the line L is tangent to E, it follows that $x = -4$ is a double root. Therefore,

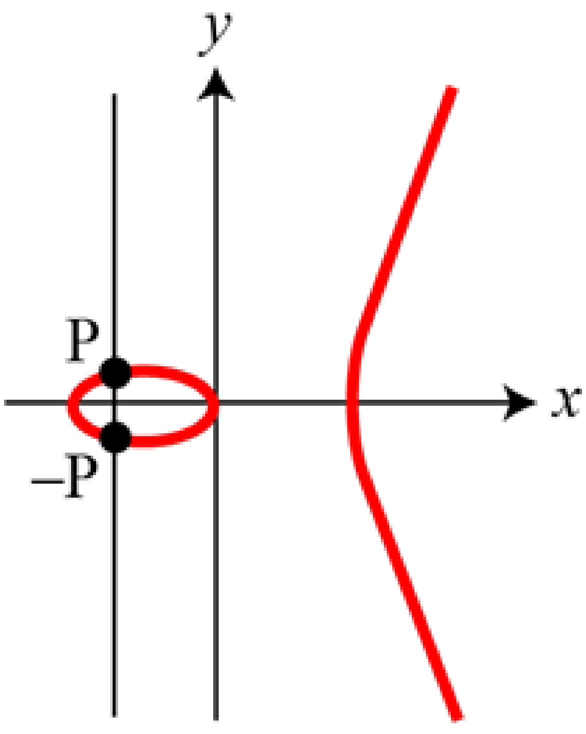
$$(-4) + (-4) + x = 64,$$

so the third root is $x = 72$. The corresponding value of y (use the equation of L) is -611. Changing y to $-y$ yields

$$P_3 + P_3 = (72, 611).$$

Third Case

- If the first point is P=(x1,y1), and the second point is Q=(x1,=y1), then the two points are additive inverse of each other.



c. (O = P + (– P))

Elliptic Curves Mod P

If p is a prime, we can work with elliptic curves mod p using the aforementioned ideas. For example, consider

$$E : y^2 \equiv x^3 + 4x + 4 \pmod 5.$$

The points on E are the pairs (x, y) mod 5 that satisfy the equation, along with the point at infinity. These can be listed as follows. The possibilities for x mod 5 are 0, 1, 2, 3, 4. Substitute each of these into the equation and find the values of y that solve the equation:

$$\begin{array}{lll}
x \equiv 0 \Longrightarrow y^2 \equiv 4 & \Longrightarrow y \equiv 2, 3 & \pmod 5 \\
x \equiv 1 \Longrightarrow y^2 \equiv 9 \equiv 4 & \Longrightarrow y \equiv 2, 3 & \pmod 5 \\
x \equiv 2 \Longrightarrow y^2 \equiv 20 \equiv 0 & \Longrightarrow y \equiv 0 & \pmod 5 \\
x \equiv 3 \Longrightarrow y^2 \equiv 43 \equiv 3 & \Longrightarrow \text{no solutions} & \\
x \equiv 4 \Longrightarrow y^2 \equiv 84 \equiv 4 & \Longrightarrow y \equiv 2, 3 & \pmod 5 \\
x = \infty \Longrightarrow y = \infty. & &
\end{array}$$

The points on E are $(0, 2), (0, 3), (1, 2), (1, 3), (2, 0), (4, 2), (4, 3), (\infty, \infty)$.

Algorithm:

Pseudocode for finding points on an elliptic curve

ellipticCurve_points (p, a, b) // p is the modulus

{

  $x \leftarrow 0$

  while $(x < p)$

  {

    $w \leftarrow (x^3 + ax + b) \bmod p$ // w is y^2

    if (w is a perfect square in $\mathbf{Z}_p$) output $(x, \sqrt{w})$ $(x, -\sqrt{w})$

    $x \leftarrow x + 1$

  {

}

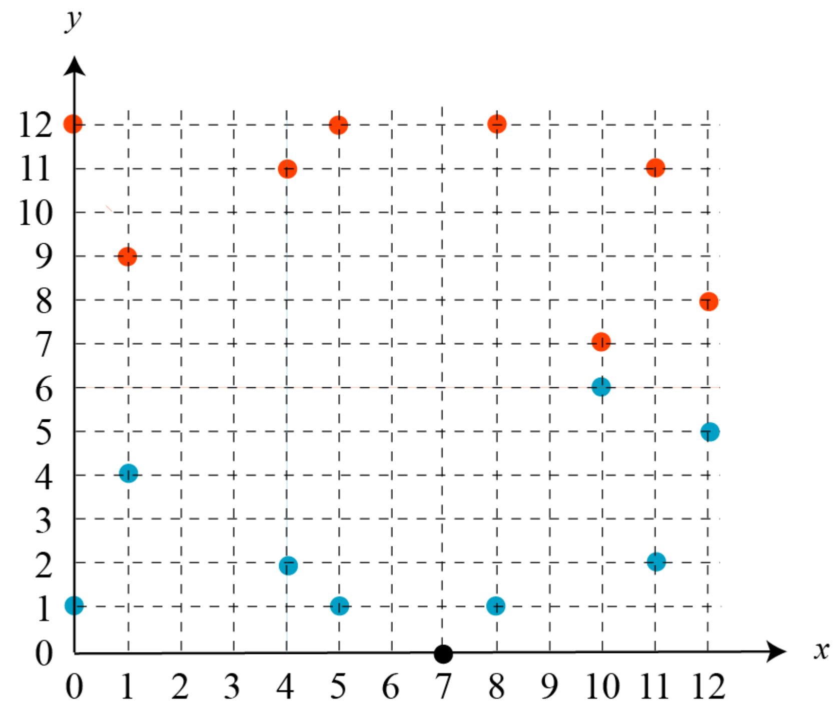
Example

Given Elliptic Curve: $E_{13}(1,1)= y^2 = x^3 + x + 1$ then Points on EC over GF(13) are:

P = –P → (7, 0)

P	–P
(0, 1)	(0, 12)
(1, 4)	(1, 9)
(4, 2)	(4, 11)
(5, 1)	(5, 12)
(7, 0)	(7, 0)
(8, 1)	(8, 12)
(10, 6)	(10, 7)
(11, 2)	(11, 11)
(12, 5)	(12, 18)

Points



Graph

Elliptic Curves over GF(2^m)

Elliptic Curves over GF(2^m)

Recall that a **finite field** GF(2^m) consists of 2^m elements, together with addition and multiplication operations that can be defined over polynomials. For elliptic curves over GF(2^m), we use a cubic equation in which the variables and coefficients all take on values in GF(2^m) for some number m and in which calculations are performed using the rules of arithmetic in GF(2^m).

Table 10.2 Points (other than O) on the Elliptic Curve $E_{2^4}(g^4, 1)$

$(0, 1)$	(g^5, g^3)	(g^9, g^{13})
$(1, g^6)$	(g^5, g^{11})	(g^{10}, g)
$(1, g^{13})$	(g^6, g^8)	(g^{10}, g^8)
(g^3, g^8)	(g^6, g^{14})	$(g^{12}, 0)$
(g^3, g^{13})	(g^9, g^{10})	(g^{12}, g^{12})

It turns out that the form of cubic equation appropriate for cryptographic applications for elliptic curves is somewhat different for $GF(2^m)$ than for Z_p. The form is

$$y^2 + xy = x^3 + ax^2 + b \tag{10.7}$$

where it is understood that the variables x and y and the coefficients a and b are elements of $GF(2^m)$ and that calculations are performed in $GF(2^m)$.

Now consider the set $E_{2^m}(a, b)$ consisting of all pairs of integers (x, y) that satisfy Equation (10.7), together with a point at infinity O.

For example, let us use the finite field $GF(2^4)$ with the irreducible polynomial $f(x) = x^4 + x + 1$. This yields a generator g that satisfies $f(g) = 0$ with a value of $g^4 = g + 1$, or in binary, $g = 0010$. We can develop the powers of g as follows.

$g^0 = 0001$	$g^4 = 0011$	$g^8 = 0101$	$g^{12} = 1111$
$g^1 = 0010$	$g^5 = 0110$	$g^9 = 1010$	$g^{13} = 1101$
$g^2 = 0100$	$g^6 = 1100$	$g^{10} = 0111$	$g^{14} = 1001$
$g^3 = 1000$	$g^7 = 1011$	$g^{11} = 1110$	$g^{15} = 0001$

For example, $g^5 = (g^4)(g) = (g + 1)(g) = g^2 + g = 0110$.

Now consider the elliptic curve $y^2 + xy = x^3 + g^4x^2 + 1$. In this case, $a = g^4$ and $b = g^0 = 1$. One point that satisfies this equation is (g^5, g^3):

$$(g^3)^2 + (g^5)(g^3) = (g^5)^3 + (g^4)(g^5)^2 + 1$$
$$g^6 + g^8 = g^{15} + g^{14} + 1$$
$$1100 + 0101 = 0001 + 1001 + 0001$$
$$1001 = 1001$$

Table 10.2 lists the points (other than O) that are part of $E_{2^4}(g^4, 1)$. Figure 10.6 plots the points of $E_{2^4}(g^4, 1)$.

Inverse point over GF(2^m)

- if $P=(X,Y)$ then $-P= (X, X+Y)$

Point Addition

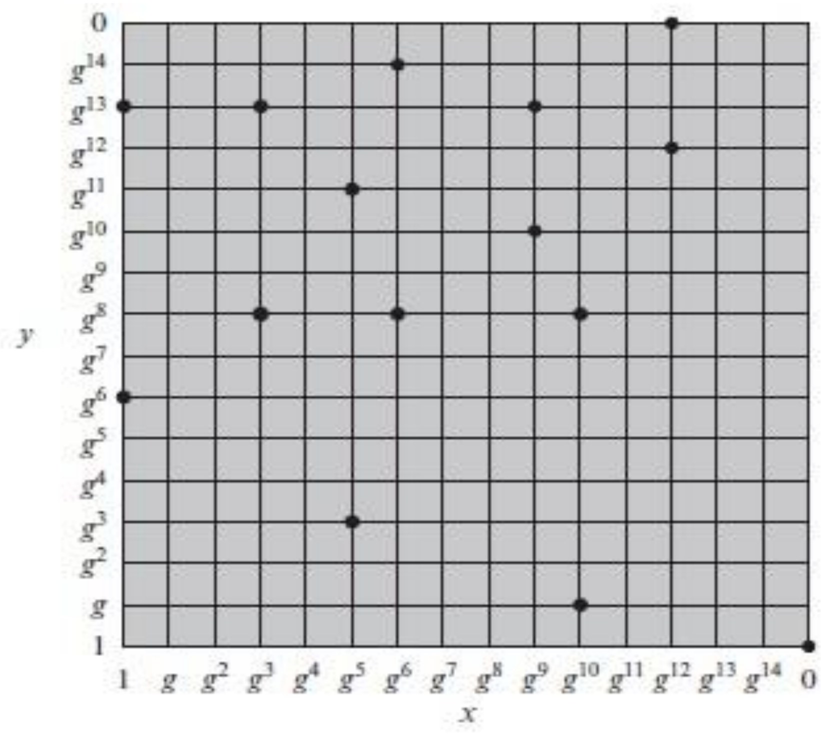
1. $P + O = P$.
2. If $P = (x_P, y_P)$, then $P + (x_P, x_P + y_P) = O$. The point $(x_P, x_P + y_P)$ is the negative of P, which is denoted as $-P$.
3. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ with $P \neq -Q$ and $P \neq Q$, then $R = P + Q = (x_R, y_R)$ is determined by the following rules:

$$x_R = \lambda^2 + \lambda + x_P + x_Q + a$$
$$y_R = \lambda(x_P + x_R) + x_R + y_P$$

where

$$\lambda = \frac{y_Q + y_P}{x_Q + x_P}$$

Elliptic Curve $E_2^4(g^4, 1)$



Point Doubling

If $P = (x_P, y_P)$ then $R = 2P = (x_R, y_R)$ is determined by the following rules:

$$x_R = \lambda^2 + \lambda + a$$

$$y_R = x_P^2 + (\lambda + 1)x_R$$

where

$$\lambda = x_P + \frac{y_P}{x_P}$$

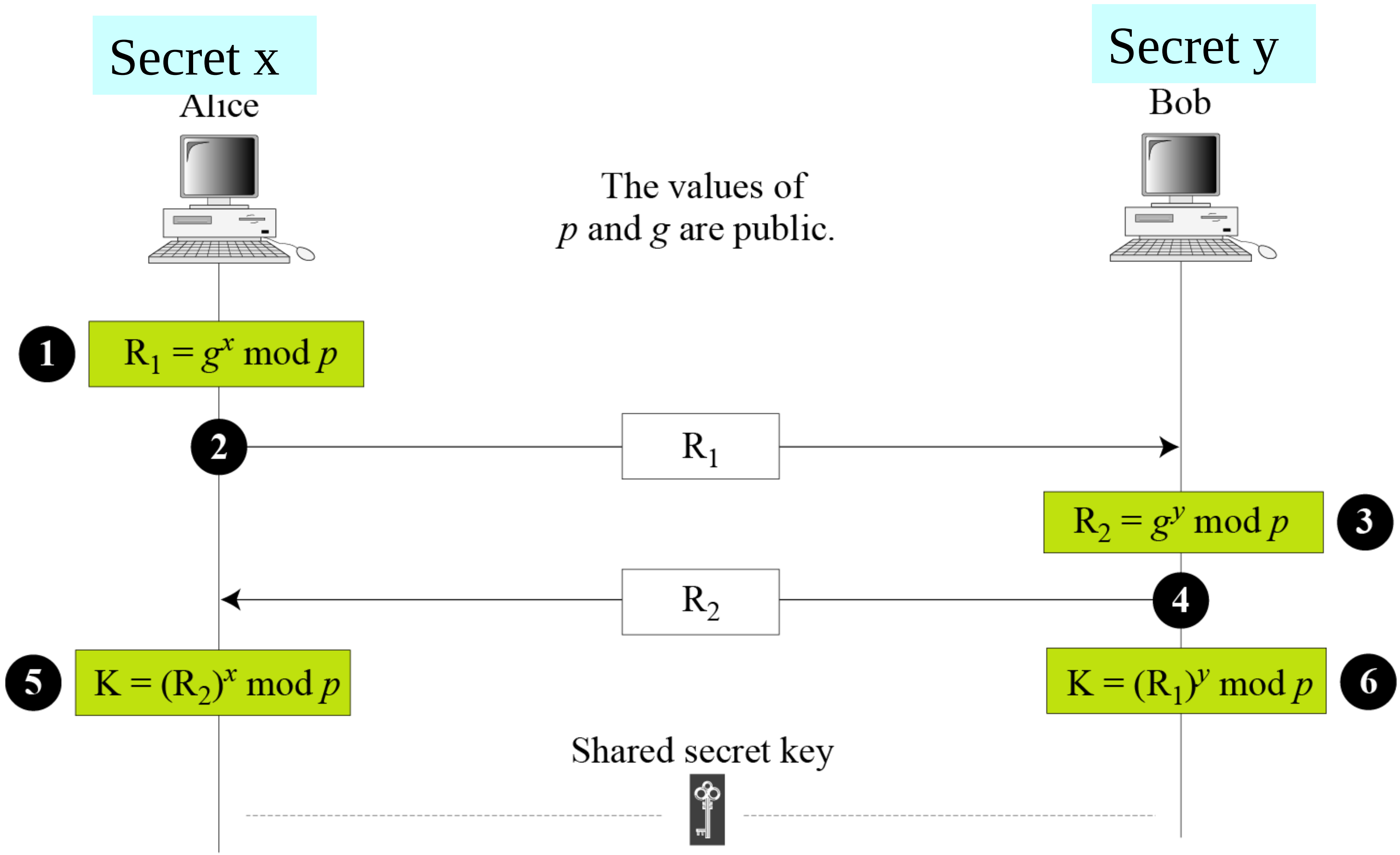
DL on EC

Definition Elliptic Curved Discrete Logarithm Problem (ECDLP)

Given is an elliptic curve E. We consider a primitive element P and another element T. The DL problem is finding the integer d, where $1 \leq d \leq \#E$, such that:

$$\underbrace{P+P+\cdots+P}_{d\ \ times} = d\,P = T.$$

Diffie–Hellman Key Exchange



$$\mathbf{K = g^{xy} \bmod p}$$

Elliptic Curve Diffie Hellman

ECDH Domain Parameters

1. Choose a prime p and the elliptic curve

$$E : y^2 \equiv x^3 + a \cdot x + b \bmod p$$

2. Choose a primitive element $P = (x_P, y_P)$

The prime p, the curve given by its coefficients a, b, and the primitive element P are the domain parameters.

Elliptic Curve Diffie–Hellman Key Exchange (ECDH)

Alice		**Bob**
choose $k_{prA} = a \in \{2, 3, \ldots, \#E - 1\}$		choose $k_{prB} = b \in \{2, 3, \ldots, \#E - 1\}$
compute $k_{pubA} = aP = A = (x_A, y_A)$		compute $k_{pubB} = bP = B = (x_B, y_B)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
compute $aB = T_{AB}$		compute $bA = T_{AB}$

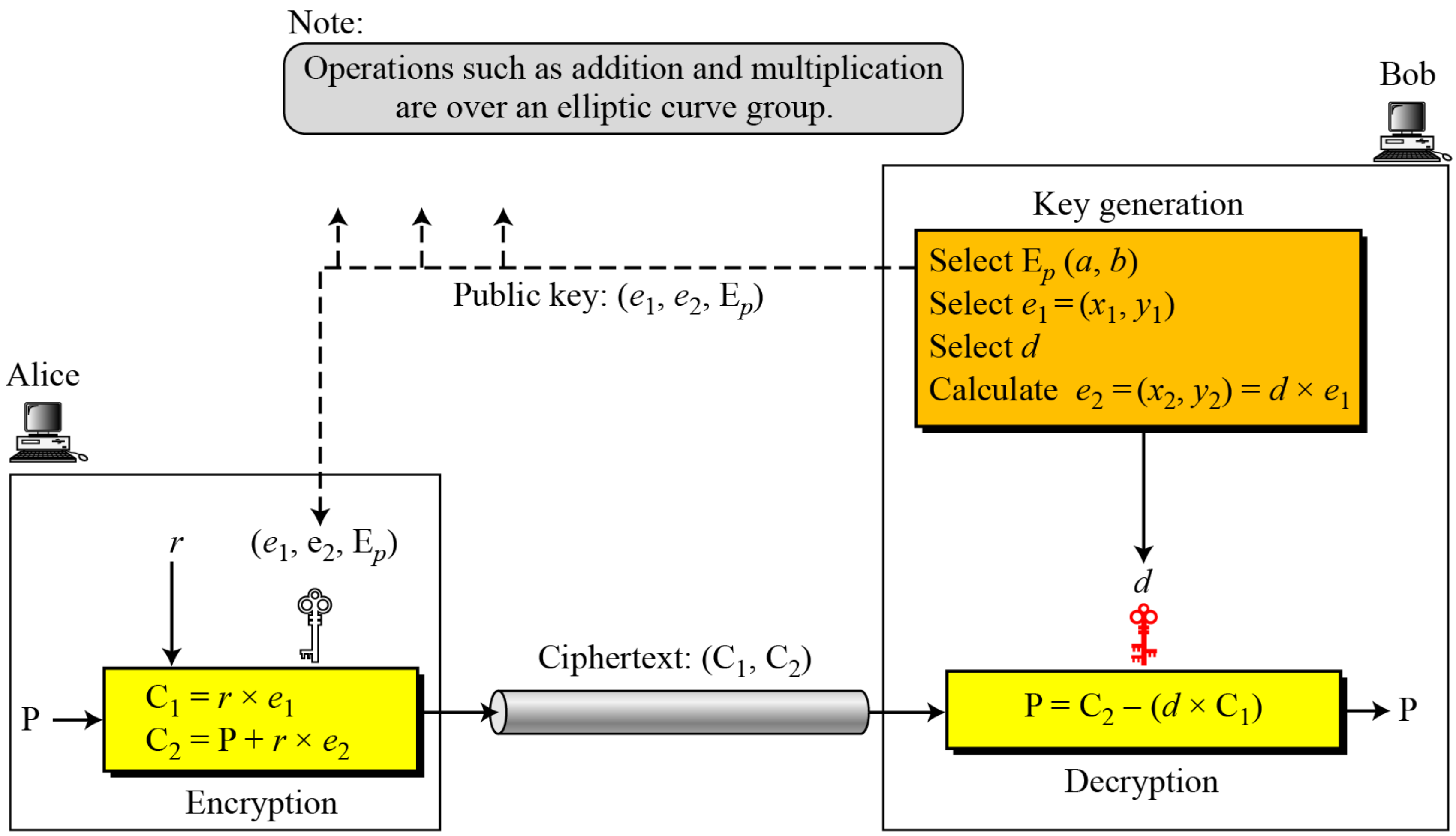
Joint secret between Alice and Bob: $T_{AB} = (x_{AB}, y_{AB})$.

Example

Example We consider the ECDH with the following domain parameters. The elliptic curve is $y^2 \equiv x^3 + 2x + 2 \bmod 17$, which forms a cyclic group of order $\#E = 19$. The base point is $P = (5,1)$. The protocol proceeds as follows:

Alice		Bob
choose $a = k_{pr,A} = 3$		choose $b = k_{pr,B} = 10$
$A = k_{pub,A} = 3P = (10,6)$		$B = k_{pub,B} = 10P = (7,11)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
$T_{AB} = aB = 3(7,11) = (13,10)$		$T_{AB} = bA = 10(10,6) = (13,10)$

ElGamal cryptosystem using EC



Example

Generating Public and Private Keys

$E(a, b) \qquad e_1(x_1, y_1) \qquad d \qquad e_2(x_2, y_2) = d \times e_1(x_1, y_1)$

Encryption

$$\mathbf{C_1 = r \times e_1} \qquad \mathbf{C_2 = P + r \times e_2}$$

Decryption

$\mathbf{P = C_2 - (d \times C_1)}$ The minus sign here means adding with the inverse.

Proof

- The P calculated by Bob is the same as that intended by Alice.

$P = C2 - (d \times C1)$

$= P + r \times e2 - (d \times r \times e1)$

$= P + (r \times d \times e1) - (r \times d \times e1)$

$= P + O$

Security

Security (bits)	ECC-based scheme (size of n in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

ECC based Algorithms/Protocols

- Elliptic curve Diffie–Helman–Meerkle key-exchange
- Elliptic curve Massey–Omura three-pass protocol
- Elliptic curve ElGamal cryptography
- Elliptic curve RSA cryptosystem
- Menezes–Vanstone elliptic curve cryptography
- Elliptic curve digital signature algorithm (ECDSA).