Applied Cryptography and Computer Security
CSE 664 Spring 2020

Lecture 18: Elliptic Curves and Applications

Department of Computer Science and Engineering
University at Buffalo

Lecture Outline

- We previously looked at
  - discrete logarithm problem
  - cryptographic schemes that assume difficulty of discrete logarithm
    - ElGamal encryption
    - Digital signature algorithm
    - Diffie-Hellman key exchange
- What we are going to learn next
  - elliptic curves
  - discrete logarithm over elliptic curves
  - elliptic curves version of cryptographic constructions

Discrete Logarithm

- The discrete logarithm problem
  - we are given a group $(G, \cdot)$ and $g \in G$ of order q
  - given $h \in \langle g \rangle$, find a unique integer $x \in [0, q)$ such that $g^x = h$
- Recall that the discrete logarithm problem is considered hard in
  - the multiplicative group $\mathbb{Z}_p^*$ where p is prime and $p - 1$ has at least one large factor
- It is also hard in
  - the multiplicative group of the field $\mathbb{F}_{p^n}$ where p is prime
  - the group of an elliptic curve over a finite field

Elliptic Curves

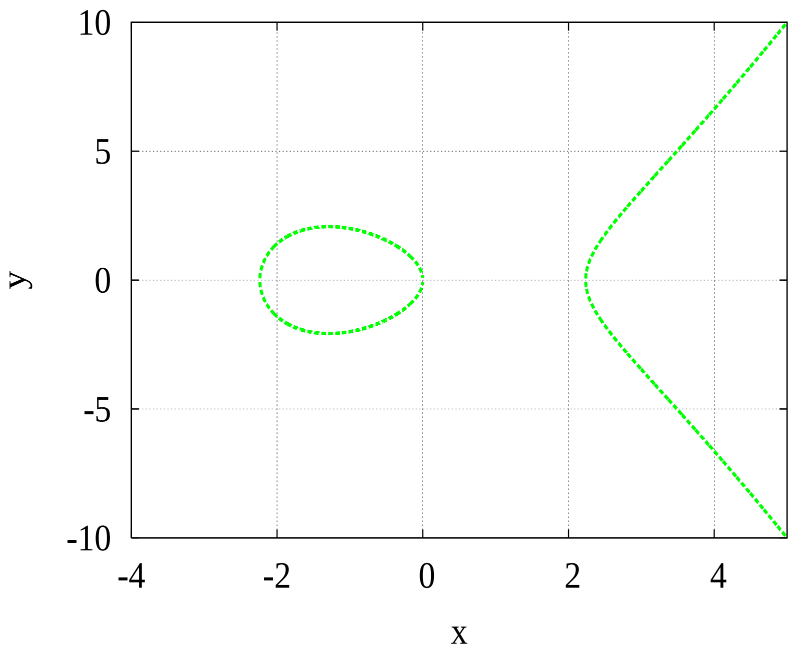
- Elliptic curves are described by a set of solutions to certain equations in two variables x and y
- The curves are solutions to equations of the form $y^2 = x^3 + ax + b$
- They have certain properties that make them useful in cryptography
  - we'll be dealing with elliptic curves modulo a prime p
  - elliptic curve groups can be used in cryptographic algorithms in similar ways multiplicative groups of integers modulo p are used
  - the discrete logarithm problem is harder for elliptic curve groups than for $\mathbb{Z}_p^*$

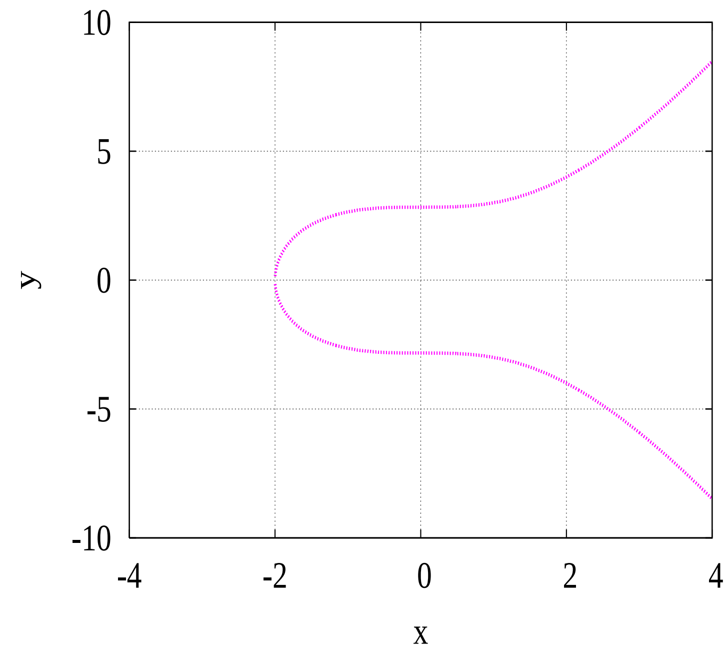
Elliptic Curves

- Definition
  - an elliptic curve is the set E of solutions (x, y) to the equation $y^2 = x^3 + ax + b$
  - here x, y, a, and b are real numbers, rational numbers, or integers modulo $m > 1$
  - the set E also contains a point at infinity ∞
- The point ∞ is not a point on the curve $y^2 = x^3 + ax + b$
  - ∞ is the identity of the elliptic curve group
  - all other points of E are on the curve

Elliptic Curves: Examples

- Curves $y^2 = x^3 - 5x$ (left) and $y^2 = x^3 + 8$ (right)



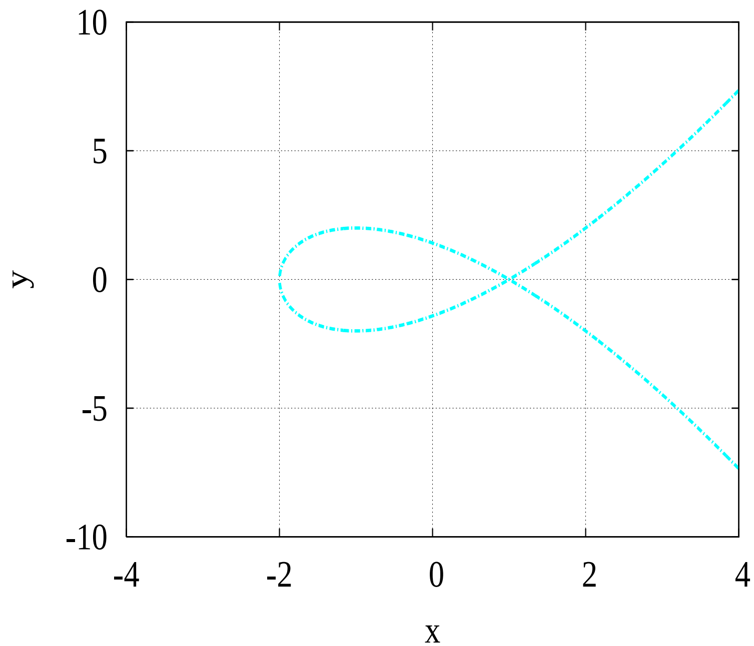


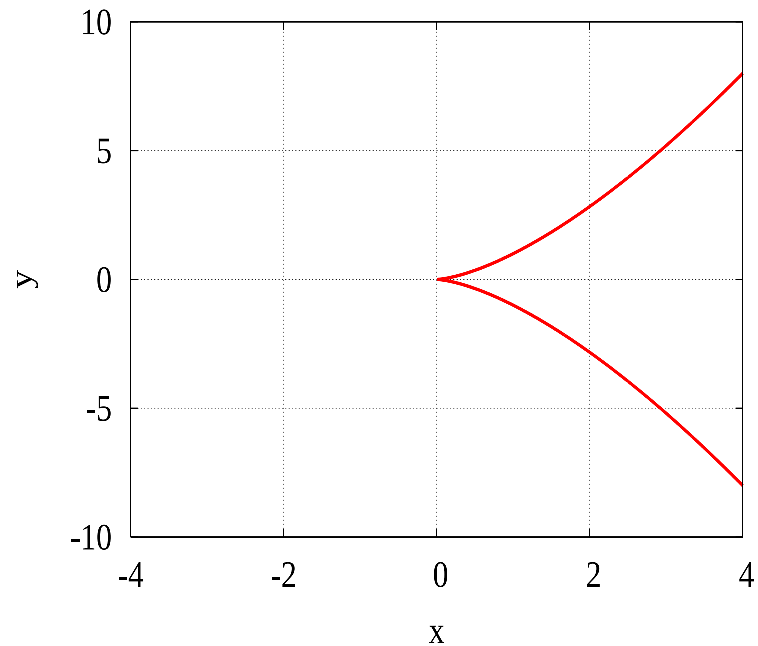
Elliptic Curves

- Number of roots
  - for the cubic equation $y^2 = x^3 + ax + b$, the discriminant is $4a^3 + 27b^2$
  - if $4a^3 + 27b^2 = 0$, then the curve has a repeated root
    - such elliptic curves are called singular
  - if, on the other hand, $4a^3 + 27b^2 \neq 0$, then there are three distinct roots
    - such elliptic curves are called non-singular
  - we are excluding singular elliptic curves

Elliptic Curves: Examples

- Singular curves $y^2 = x^3 - 3x + 2$ (left) and $y^2 = x^3$ (right)





Elliptic Curves

- Operations on elliptic curves
  - we define a binary operation over E that makes it into a commutative group
  - this operation is normally denoted as $+$
  - let P and Q be two points on E such that $P = (x_1, y_1)$ and $Q = (x_2, y_2)$
  - $P + \infty = \infty + P = P$
  - let $P + Q = R$
  - such R is computed depending on the relationship between x_1 and x_2 and y_1 and y_2

Elliptic Curves

- Computing $P + Q = R$
  - there are three cases
  - case 1: $x_1 \neq x_2$
    - draw a line through P and Q and find another point R', where the line intersects the curve
    - reflect R' on the x-axis to obtain R
    - the coordinates (x_3, y_3) are computed as:

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

where λ is the slope computed as $\lambda = (y_2 - y_1)/(x_2 - x_1)$

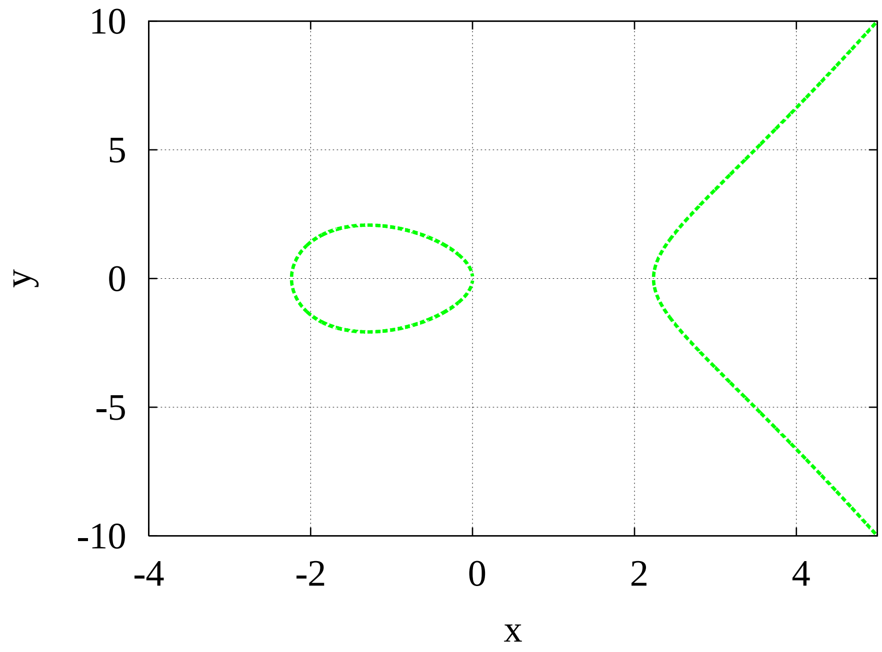
Elliptic Curves

- Computing $P + Q = R$
  - case 2: $x_1 = x_2$ and $y_1 \neq y_2$
    - P is a reflection of Q on the x axis
    - in this case $P + Q = \infty$
    - thus Q is the inverse of P
  - case 3: $x_1 = x_2$ and $y_1 = y_2$
    - i.e., we are computing $P + P$
    - this case is handled similar to case 1
    - instead of drawing a line through P and Q, draw a tangent line to the curve at P
    - x_3 and y_3 are computed using the formulas from case 1

Elliptic Curves

- Computing $P + Q = R$
  - case 3: $x_1 = x_2$ and $y_1 = y_2$ (cont.)
    - the formula for the slope now is $\lambda = (3x_1^2 + a)/(2y_1)$

- Examples



Elliptic Curves

- Elliptic curves modulo a prime p are defined as above except that all operations are replaced by analogous operations in $\mathbb{Z}_p$
  - now the points are the solutions to the congruence $y^2 \equiv x_3 + ax + b \pmod{p}$
  - $a, b \in \mathbb{Z}_p$ are constants such that $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$
  - given points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, as before $P + Q = \infty$ if $x_1 = x_2$ and $y_2 = -y_1$
  - the slope λ is computed as

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & \text{if } P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}, & \text{if } P = Q \end{cases}$$

  - and as before $P + \infty = \infty + P = P$

Elliptic Curves

- Example: points on the elliptic curve $y^2 = x^3 + 3x + 4$ over $\mathbb{Z}_7$

x	$x^3 + 3x + 4 \bmod 7$	y
0	4	2, 5
1	1	1, 6
2	4	2, 5
3	5	none
4	3	none
5	4	2, 5
6	0	0

  – there are 10 points on this elliptic curve (including ∞)

Elliptic Curves

- Example: $y^2 \equiv x^3 + 3x + 4 \pmod 7$ (cont.)
  - to add points $(1, 1)$ and $(2, 5)$
  - to double the point $(2, 2)$

Elliptic Curves

- Discrete logarithms over elliptic curves
  - for $(G, \cdot)$ the discrete logarithm $\mathsf{log}_g h$ was defined as x where $g^x = h$
  - now $+$ is the group binary operation, so the discrete logarithm $\mathsf{log}_P Q$ now is a such that $aP = Q$
- Computing "exponentiation" aP
  - instead of using SQUARE-AND-MULTIPLY algorithm on g and x, we use DOUBLE-AND-ADD algorithm on P and a

Elliptic Curves

- Computing aP
  - note that additive inverses are very easy to compute
  - this is exploited in a generalization DOUBLE-AND-(ADD OR SUBTRACT) algorithm
    - it uses signed binary representation of integer $a = \sum_{i=0}^{\ell-1} a_i 2^i$, where each $a_i \in \{-1, 0, 1\}$
    - given signed binary representation of a, we compute aP by a series of doublings, additions, and subtractions
    - signed representation reduces the number of add/subtract operations

Elliptic Curves

- DOUBLE-AND-(ADD OR SUBTRACT)
  - input: P, $(a_{\ell-1}, \ldots, a_0)$
  - output: aP
  - algorithm steps:

    $Q \leftarrow \infty$
    for $i = \ell - 1$ downto 0 {
        $Q \leftarrow 2Q$
        if $a_i = 1$ then $Q \leftarrow Q + P$
        else if $a_i = -1$ then $Q \leftarrow Q - P$
    }
    return Q

Elliptic Curve Constructions

- Let's look at elliptic curve version of cryptographic schemes
- Elliptic curve Diffie-Hellman key agreement
  - fix an elliptic curve E modulo p and a point P_0 of large order on E
  - Alice chooses a $(0 < a < p)$ and sends aP_0 to Bob
  - Bob chooses b $(0 < b < p)$ and sends bP_0 to Alice
  - Alice computes $k = a(bP_0)$ and Bob computes $k = b(aP_0)$

Elliptic Curve Constructions

- An elliptic curve analogue of ElGamal encryption is then:
  - fix an elliptic curve E modulo p and a point P_0 of large order on E
  - for Alice to generate a key, she chooses secret a_A ($0 < a_A < p$) and publishes $P_A = aP_0$
  - when Bob wants to encrypt message m:
    - he first embeds it into a point P of E
    - he then chooses a random b ($0 < b < p$) and sends to Alice $c = (c_1, c_2) = (bP_0, bP_A + P)$
  - Alice, who knows the secret key a_A, decrypts as follows:

$$P = c_2 - a_A c_1 = bP_A + P - a_A bP_0 = ba_A P_0 + P - ba_A P_0 = P$$

Elliptic Curve Constructions

- An elliptic curve Digital signature algorithm (ECDSA) is then
  - choose one of the recommended elliptic curves and curve parameters
    - government-recommended curves have been questioned in light of past NSA-related events
  - choose a point P_0 of large prime order on the curve and secret key x
  - set the public key to xP_0
  - proceed with signing similar to as before, but using elliptic curve arithmetic
  - see FIPS PUB 186-4 for the details and suggested implementation

Discrete Logarithm Problem

- How hard is the discrete logarithm problem to solve in a group over an elliptic curve E?
  - the powerful index calculus algorithm doesn't work for elliptic curves
  - the best possible algorithm is Pollard rho algorithm with $O(\sqrt{p})$ work
- To be secure until the year of 2030
  - it is suggested to choose $p \approx 2^{224}$ in case of elliptic curves
  - compare this with $p \approx 2^{2048}$ for groups $(\mathbb{Z}_p^*, \cdot)$
  - for that reason, elliptic curves have been gaining popularity, especially on constrained platforms

Summary

- Elliptic curves are solutions to equations of the form $y^2 = x_3 + ax + b$
- Groups over elliptic curves modulo a prime
  - often can be used in similar ways to $(\mathbb{Z}_p^*, \cdot)$
  - require smaller security parameters because the discrete logarithm is harder in such groups