Algoritmi di Crittografia

Corso di Laurea Magistrale in Informatica

A.A. 2018/2019

Algoritmi di Crittografia

1. Public Key Encryption (2)
   - Realistic RSA implementations
   - Elliptic curve cryptography

Algoritmi di Crittografia

1. Public Key Encryption (2)
   - Realistic RSA implementations
   - Elliptic curve cryptography

Optimal Asymmetric Encryption Padding

- Many pittfalls of the textbook RSA can be avoided using *padding*
- Additional data are “added” to the message and scrambled with hashing
- The following is the (simplified) code that prepares the message (typically, a key K) for RSA encryption

```
def OAEP-prepare(K, n, t, r)
    assert |K| = n-t-r
    R = random nonce # |R| = r bits
    H1 = HASH1(R)    # |H1| = n - r bits
    K1 = K || 10...0 # padded with 1 and t-1
                     # zeros |K1| = n - r
    X = K1 XOR H1    # |X| = n - r
    H2 = HASH2(X)    # |H2| = r bit
    Y = R XOR H2     # |Y| = r bits
    return X || Y
```

Encryption and decryption

- To encrypt a message K (which is typically and significantly shorter than n), first OAEP-prepare K: $M \leftarrow \mathrm{OAEP} - \mathrm{prepare}$
- Then convert M to a number x
- Now apply the RSA function to x to obtain the ciphertext $z = x^e \bmod n$
- To decrypt, first recover $x = z^d \bmod n$ and convert it to a byte string $X||Y$
- To recover the original value K first compute $H2 = \mathrm{HASH2}(X)$ and then $R = Y \oplus H2$
- Once R is known, compute $H1 = \mathrm{HASH1}(R)$ and, finally, recover the padded value of K as $X \oplus H1$

Algoritmi di Crittografia

1. Public Key Encryption (2)
   - Realistic RSA implementations
   - Elliptic curve cryptography

What is an elliptic curve

- Elliptic curves are curves defined by a certain type of cubic equation in two variables
- Elliptic curves over finite fields are interesting since the points on the curve form a group that can be used for cryptographic purposes
- Here we only condider curves of the so-called *Weierstrass form*, i.e., whose equation is:

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

  with a, b belonging to the underlying field (e.g., the real numbers or a finite field $\mathbf{Z}_p$ (p prime)
- Before studying elliptic curves over a finite field, it is instructive to inspect some properties of curves over the reals, where we can get help from geometry

Examples of elliptic curves

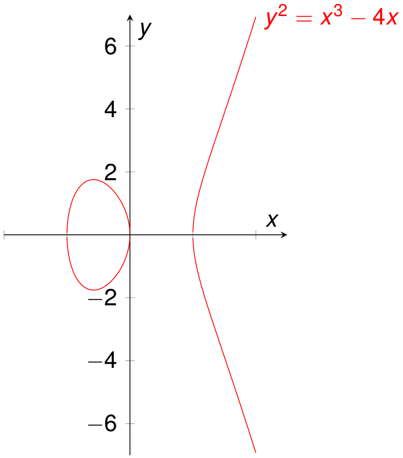
- The next four slides show as many examples of elliptic curves
- The first two are examples of *smooth* curves (i.e., the curve is a continuous map with continuous derivatives)
- We are only interested in smooth elliptic curves
- In general, a curve $E(x, y)$ is smooth if for no points (x_0, y_0) its partial derivatives are both zero
- The curve in the third slide, $E(x, y) = y^2 - x^3$ is non smooth since

$$\frac{\partial E(x,y)}{\partial x}(0,0) = 3x^2|_{0,0} = 0, \qquad \frac{\partial E(x,y)}{\partial y}(0,0) = 2y|_{0,0} = 0$$

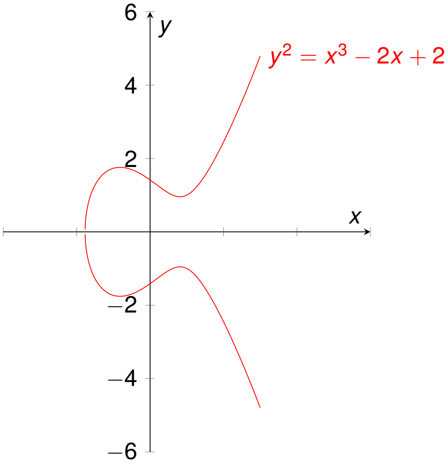
- The curve in the fourth slide, $E(x, y) = y^2 - x^3 + 3x - 2$ is non smooth since

$$\frac{\partial E(x,y)}{\partial x}(1,0) = -3x^2 + 3|_{x=0} = 0, \qquad \frac{\partial E(x,y)}{\partial y}(1,0) = 2y|_{y=0} = 0$$

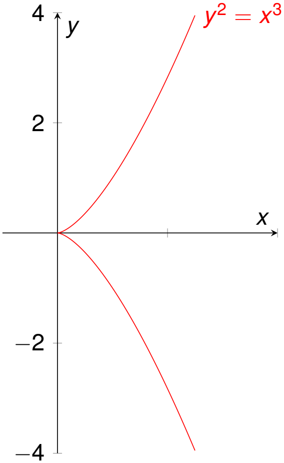
The elliptic curve $y^2 = x^3 - 4x$



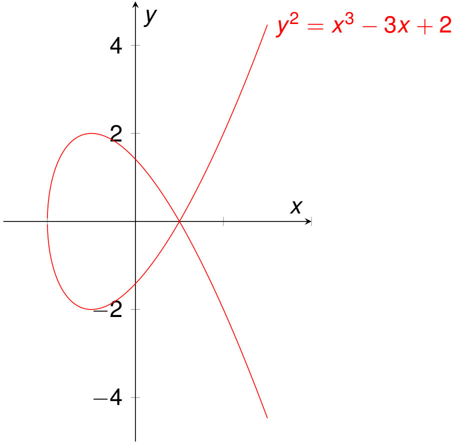
The elliptic curve $y^2 = x^3 - 2x + 2$



The elliptic curve $y^2 = x^3$



The elliptic curve $y^2 = x^3 - 3x + 2$



Smoothness

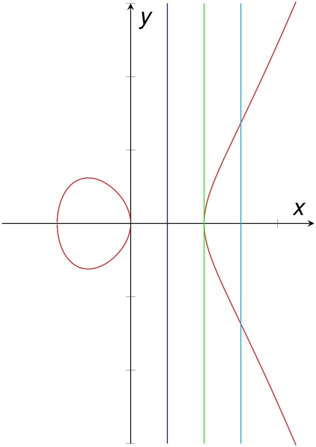
- A curve of the Weierstrass form is smooth if and only if the corresponding polynomial $p(x) = x^3 + ax + b$ has three distinct zeros

  Proof. The partial derivative with respect to y is $2y$, which clearly vanishes at (and only at) $y = 0$. This implies that the curve might be non smooth only at points $(x_o, 0)$; in turn, this requires (beside the condition $\frac{\partial E(x,y)}{\partial x}(x_0, 0) = -3x_0^2 + a = 0$) that $p(x_0) = x_0^3 + ax_0 + b = 0$. In other words x_0 must be a zero of multiplicity at least 2. When this does not happens, i.e., if the polynomial $p(x) = x^3 + ax + b$ has distinct zeros, then the curve is smooth.
- With few algebraic passages, we can easily see that a curve of the Weierstrass form is smooth if and only if the discriminant $4a^3 + 27b^2$ is not zero

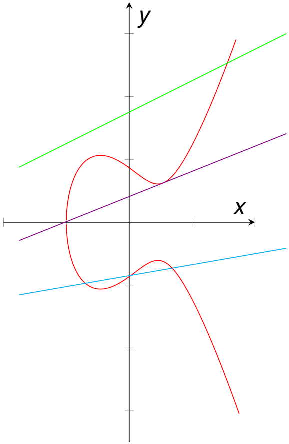
Elliptic curves and straight lines

- Consider a smooth elliptic curve E and let ℓ be a line
- We consider the (possible) intersections of ℓ with E
- First, ℓ may not meet C at all. This may only happen if ℓ is a vertical line (see next slide, line colored in blue)
- A vertical line may otherwise meet the curve in one point (green line) or two points (cyan line)
- A line of equation $ax + by + x = 0$, $a, b \neq 0$, may meet E in one (green line), two violet line), or three points (cyan line). See two slides ahead

Vertical lines



General lines



Elliptic curves and straight lines (cont.d)

- From an algbraic point of view, the coordinates of the intersection points can be determined by solving the system with the curve and the line equations
- The points can thus be obtained essentially by finding the zeros of polynomial of degree two or three
- For vertical lines:

$$\begin{cases} y^2 = x^3 + ax + b \\ x = k \end{cases} \quad \Rightarrow p(y) = y^2 - k^3 - ak - b$$

- For general lines

$$\begin{cases} y^2 = x^3 + ax + b \\ y = mx + q \end{cases} \quad \Rightarrow p(x) = x^3 - m^2x^2 + (a - 2mq)x + b - q^2$$

Elliptic curves and straight lines (cont.d)

- We have pointed out that general lines may have one, two, or three intersections with the curve
- However, if we count multiplicities, in the *extension field* (e.g., the complex number, if the curve is defined over the reals), general lines aways have three intersections
- Vertical lines, however, cannot have three intersections (not even in the extension field) since the polynomial $p(y)$ has degree two
- For our purposes of defining an algebraic structure, this situation is not good, but there is a (simple) solution
- As a matter of notation, if $\mathcal{F}$ is a field, its extension will be denoted by $\overline{\mathcal{F}}$ ($\overline{\mathcal{F}} = \mathcal{F}$ iff $\mathcal{F}$ is closed)
- Points with coordinates in $\mathcal{F}$ are said *rational points*

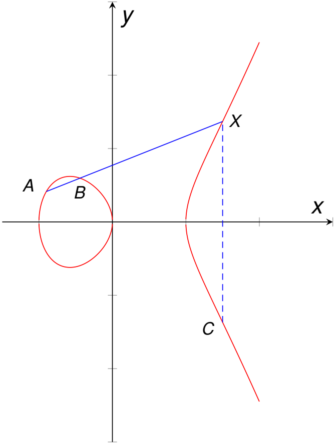
Defining an arithmetic over elliptic curves

- Now, it is an easy fact that, if a cubic polynomial has two rational zeros, then also the third zero is rational
- It follows that, if we take two points (not necessarily distinct) $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on the curve, and consider the line through P and Q, then there is a third intersection point R on the curve, unless $x_1 = x_2$ and $y_1 = y_2$ (i.e., the line is vertical)
- The exception is disturbing, but there is a simple solution
- We introduce a special point O, with the following properties:
  1. O is rational, i.e. it lies on the curve (on every elliptic curve), though it is not a point in the plane
  2. Any vertical line meets the elliptic curve (also) in O
  3. Other lines never intersect the curve at O
- O is often referred to as the *point at infinity*

Definining an arithmetic over elliptic curves

- Thanks to O, we may assert that the following holds for any elliptic curve E over $\mathcal{F}$:
  Any line ℓ intersects E in exactly three points (counting multiplicities) of $\overline{\mathcal{F}}$. Also, if two points are rational, the third is also rational
- We can now define a group structure over the point of an elliptic curve extended with the point at infinity, which will play the role of "neutral element"
- First define the negative of a point $P = (x_p, y_p)$ over a curve E as the point $-P = (x_p, -y_p)$
- Then, if A and B are points on a smooth elliptic curve; we define $C = A + B$ as follows: draw the line r through A and B and let X be the point where r meets again the curve; then $C = -X$ (see next slide)

Addition over an elliptic curve



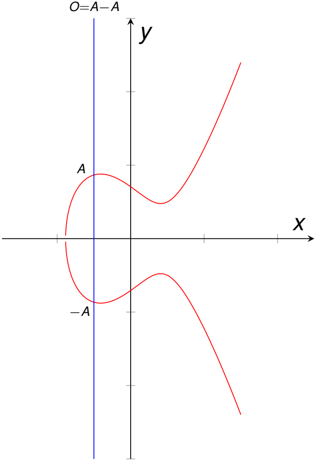
Point addition

- The above procedure also holds if $B = -A$. In that case the line through A and $-A$ meets the curve at O, and clearly the reflection steps does not change things, since $-O = O$ (see next slide)
- This also explain why the negative of a point is defined that way
- One might wonder why point addition is not defined simply as $A + B = X$; i.e., why is the *reflection step* required?
- The fact is that without the reflection step the "addition" would not be associative, and this (as will be soon clear) is crucial
- Associativity allows us to define point-scalar multiplication

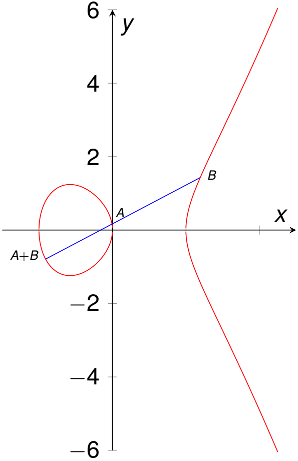
$$kP = \underbrace{P + P + \ldots + P}_{k-\text{times}}$$

  which otherwise would not be well-defined
- The next few slides (graphically) illustrate the issue of associativity

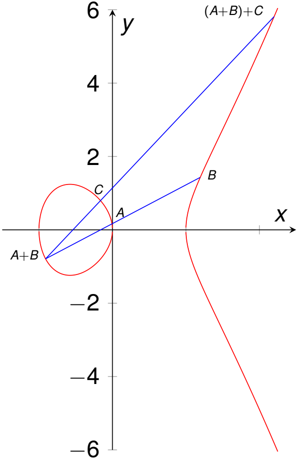
Adding a point and its negative



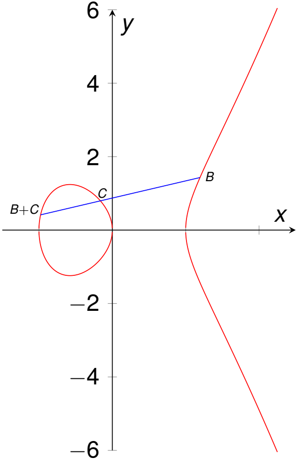
Addition without reflection step: $(A + B) + C$



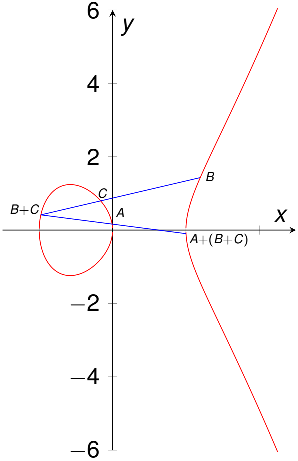
Addition without reflection step: $(A+B)+C$



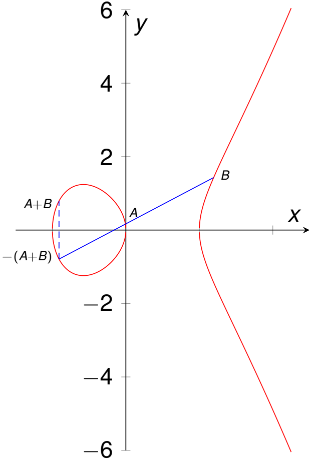
Addition without reflection step: $A + (B + C)$



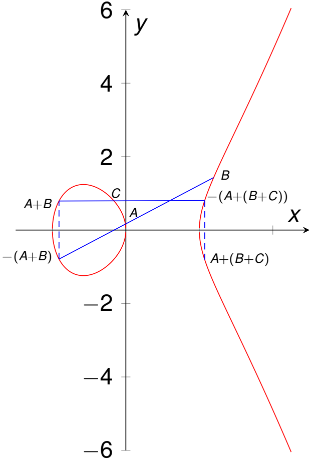
Addition without reflection step: $A + (B + C)$



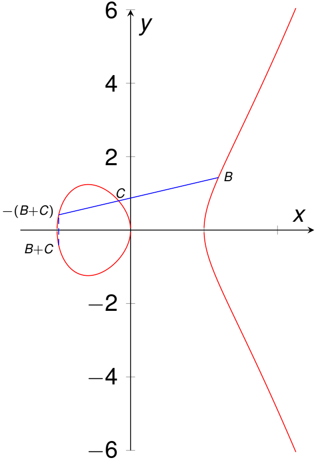
Addition with reflection step: $(A + B) + C$



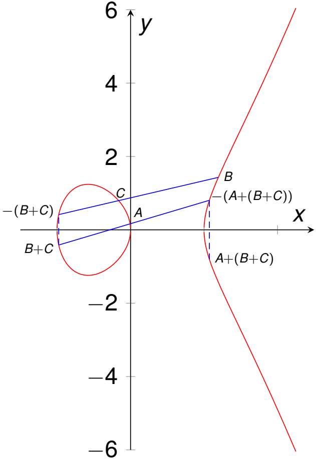
Addition with reflection step: $(A + B) + C$



Addition with reflection step: $A + (B + C)$



Addition with reflection step: $A + (B + C)$



Actually computing $C = A + B$

- We now devise general formulas to compute the coordinates of $C = A + B$
- We start by considering the case $A \neq B$ (and $B \neq -A$)
- Let $y = mx + q$ be the line through A and B
- We already know that the abscissas of A, B, and C are the solutions of the polynomial equation

  $$p(x) = x^3 - m^2x^2 + (a - 2mq)x + b - q^2 = 0$$

  of which we already know two, namely x_A and x_B
- Now, since the coefficient of the x^2 term is the opposite of the sum of all zeros, i.e., $-m^2 = -(x_A + x_B + x_C)$, we simply have

  $$x_C = m^2 - x_A - x_B$$

  and of course

  $$m = \frac{y_B - y_A}{x_B - x_A}$$

Actually computing $C = A + A = 2A$

- If $B = A$ the line passing by A and B is replaced by the tangent at the curve in the point A
- Let $E(x, y) = x^3 - y^2 + ax + b$ be the curve equation; the tangent to the curve at $P = (x_p, y_p)$ is the line of equation

$$\nabla E(x_p, y_p)^T \begin{pmatrix} x - x_p \\ y - y_p \end{pmatrix} = 0$$

that is:

$$\begin{aligned} \nabla E(x_p, y_p)^T \begin{pmatrix} x - x_p \\ y - y_p \end{pmatrix} &= \begin{pmatrix} 3x_p^2 + a \\ -2y_p \end{pmatrix}^T \begin{pmatrix} x - x_p \\ y - y_p \end{pmatrix} \\ &= (3x_p^2 + a)(x - x_p) - 2y_p(y - y_p) \\ &= 0 \end{aligned}$$

Actually computing $C = A + A = 2A$ (cont.d)

- By reordering, we obtain

$$\begin{aligned} y &= y_p + \frac{3x_p^2 + a}{2y_p} - x_p \frac{3x_p^2 + a}{2y_p} \\ &= mx + q \end{aligned}$$

  with

$$m = \frac{3x_p^2 + a}{2y_p} \qquad \text{and} \qquad q = y_p - mx_p$$

- The following slide present the complete algorithm for computing $C = A + B$

Computing $C = A + B$

- If $A = O$ then return B
- If $B = O$ then return A
- Let $A = (x_A, y_A)$ and $B = (x_B, y_B)$
- If $x_A = x_B$ and $y_B = -y_B$ then return O
- If $x_A = x_B$ (and clearly also $y_B = y_B$) then set
$$m = \frac{3x_A^2 + a}{2y_A}$$
  else set
$$m = \frac{y_B - y_A}{x_B - x_A}$$
- Return $C = (x_C, y_C)$, with $x_C = m^2 - x_A - x_B$ and $y_C = -(m(x_C - x_A) + y_A)$