

Protocollo DH

Cifronò El Gomel

(lunedì) 15 novembre '21
ore 16:00



Cifratura Ibrida

Alice

Bob

m

genera una chiave k (256 bit)

$$\xrightarrow{\quad \left\langle G_{RSA}(k), k_{[pub]} \right\rangle / G_{AES}(m, k) \quad}$$

Decifra il primo
criptogramma con le
sue due chiavi
e trova k

poi decifra il secondo
criptogramma usando
la chiave k

Protocollo DH

Alice e Bob scelgono

- un numero primo p

Molto grande
(migliaia di bit)

- un generatore g per \mathbb{Z}_p^*

P, g

sono pubblici

$$g < p$$

$$g \in \mathbb{Z}_p^*$$

Alice

- sceglie a così
 $1 < a < p-1$

Eve
(conosce i numeri)

g, P

$$A = g^a \pmod{p}$$

- calcola

$$\begin{aligned} k &= B^a \pmod{p} \\ &= g^{b \cdot a} \pmod{p} \end{aligned}$$

Bob

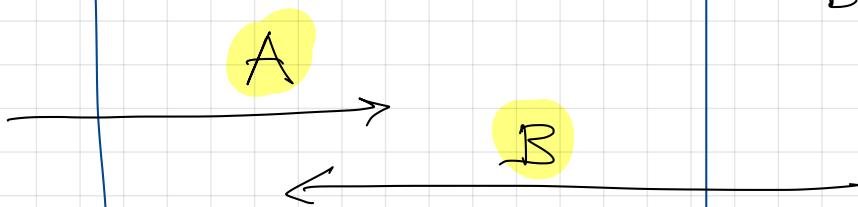
- sceglie b così
 $1 < b < p-1$

$$B = g^b \pmod{p}$$

- calcola

- calcola

$$\begin{aligned} k &= A^b \pmod{p} \\ &= g^{a \cdot b} \pmod{p} \end{aligned}$$



Attacchi

attacchi passivi

: Eve conosce q, p, A, B

per calcolare k deve avere $a, o b$.

$$a = \log_q A$$

$$b = \log_q B$$



~~logaritmo~~ logaritmo discreto.



è vulnerabile agli attacchi altri

"man-in-the-middle"

Attack from the Middle

P, g

Alice

choose

$$1 < e < p-1$$

choose

$$A = g^e \pmod{p}$$

tell

choose

$$1 < x < p-1$$

$$E = g^x \pmod{p}$$

Bob

choose

$$1 < b < p-1$$

$$B = g^b \pmod{p}$$

E

A

B

Alice calc

$$\begin{aligned} k_A &= E^x \pmod{p} \\ &= g^{ex} \pmod{p} \end{aligned}$$

calc

$$\begin{aligned} k_A &= A^x \pmod{p} = g^{ex} \pmod{p} \\ k_B &= B^x \pmod{p} = g^{bx} \pmod{p} \end{aligned}$$

Bob calc

$$\begin{aligned} k_B &= E^b \pmod{p} \\ &= g^{xb} \pmod{p} \end{aligned}$$

Il cifrario di ElGamal

Cifrario di ElGamal (1985)

La sicurezza si basa sulla difficoltà di calcolare i **logaritmi discreti**

Creazione della coppia di chiavi

1. Si sceglie un numero primo p e un generatore g di \mathbb{Z}_p^*
2. Si sceglie a caso un intero $x \in [2, p-2]$
3. Si calcola $y = g^x \text{ mod } p$

Chiave pubblica $k_{\text{pub}} = (p, g, y)$

Chiave privata $k_{\text{priv}} = (x)$

Cifratura e decifrazione

CIFRATURA

- Il messaggio m è codificato come una sequenza binaria, trattata come un numero intero
- $m < p$ (se $m \geq p \rightarrow$ cifratura a blocchi, di $\log_2 p$ bit ciascuno)
- si sceglie a caso un intero $r \in [2, p-2]$
- si calcola la coppia di crittogrammi

$$c = g^r \bmod p \quad d = m \cdot y^r \bmod p$$

DECIFRAZIONE

$$m = d \cdot c^{-x} \bmod p$$

$$\begin{aligned}d \cdot c^{-x} \bmod p &= m \cdot y^r \cdot c^{-x} \bmod p = m \cdot y^r \cdot (g^r)^{-x} \bmod p \\&= m \cdot (g^x)^r \cdot g^{-r x} \bmod p = m \bmod p = m \quad (m < p)\end{aligned}$$

Osservazioni

- La difficoltà di calcolare il logaritmo discreto rende la chiave privata x sicura, anche se y e g sono pubblici
- r è un intero casuale
 - $y^r \text{ mod } p$ è un intero casuale
 - $d = m \cdot y^r \text{ mod } p$ è casuale e non fornisce alcuna informazione su m al crittoanalista
- per “estrarre” r da c occorre risolvere il problema del logaritmo discreto
 - se r è noto si può decifrare: $m = d \cdot y^{-r} \text{ mod } p$
- occorre un nuovo numero casuale r per ogni nuovo messaggio

m_1
 m_2

invia a Bob con lo stesso r

$$\langle c = g^r \bmod p, d_1 = y^r \cdot m_1 \bmod p \rangle$$

$$\langle c = g^r \bmod p, d_2 = y^r \cdot m_2 \bmod p \rangle$$

Eve viene a conoscenza di m_1

P, g , y , c , d_1 , d_2 , m_1

e pu  trovare m_2 in tempo polinomiale.

Come ?

$$d_1 m_1^{-1} = y^r$$

$$m_2 = d_2 (y^r)^{-1}$$

Mod p

$$d_1 = m_1 y^r \text{ mod } p$$

$$d_2 = m_2 y^r \text{ mod } p$$

Crittografia su Curve Ellittiche

Crittografia su curve ellittiche

Sistemi a chiave pubblica di “prima generazione” (RSA, El Gamal, DH)

tempi di cifratura e decifrazione notevolmente maggiori di quelli dei cifrari simmetrici

progressivo aumento della lunghezza della chiave richiesta per garantire un utilizzo sicuro del cifrario

ECC (Elliptic Curve Cryptography), 1985

Sistema alternativo di crittografia a chiave pubblica, in grado di offrire

- prestazioni migliori
- maggiore sicurezza

Idea

sostituire negli algoritmi già esistenti le operazioni basate sull’algebra modulare con operazioni definite sui punti di una curva ellittica.

Victor S. Miller (IBM)

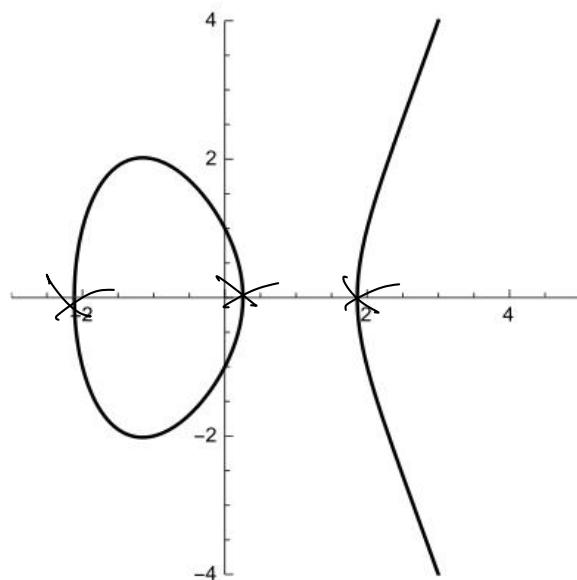
Neil Koblitz (University of Washington)

Curve ellittiche sui numeri reali

Le curve ellittiche sono curve algebriche descritte da equazioni cubiche (simili a quelle utilizzate per il calcolo della lunghezza degli archi delle ellissi)

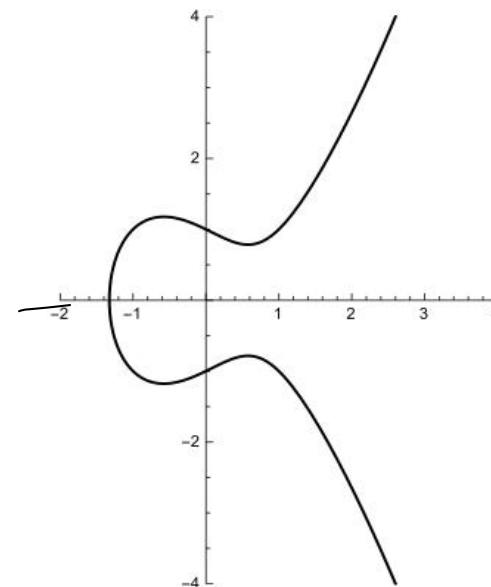
$$E(a, b) = \{ (x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b \}$$

$E(a, b)$ contiene il punto all'infinito O in direzione dell'asse y (la curva ha un asintoto verticale) → Elemento neutro per l'operazione di addizione



(a) Curva $y^2 = x^3 - 4x + 1$

Cubica con tre radici reali



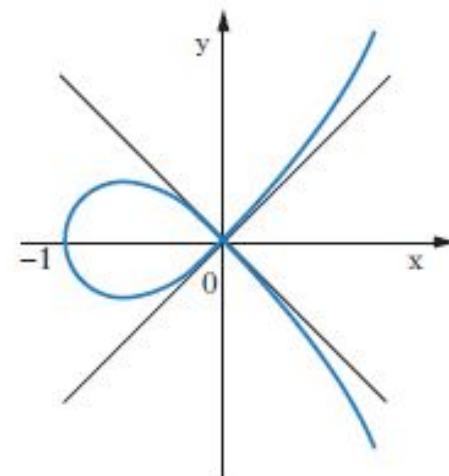
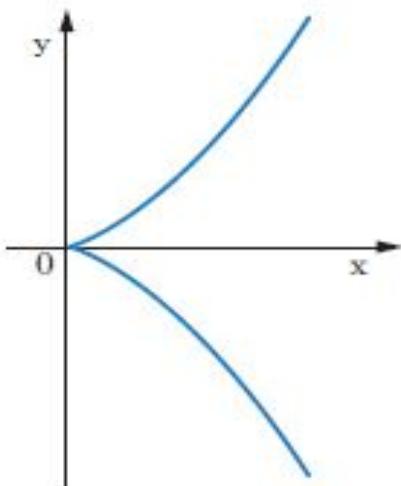
(b) Curva $y^2 = x^3 - x + 1$

Cubica con una radice reale e due complesse coniugate

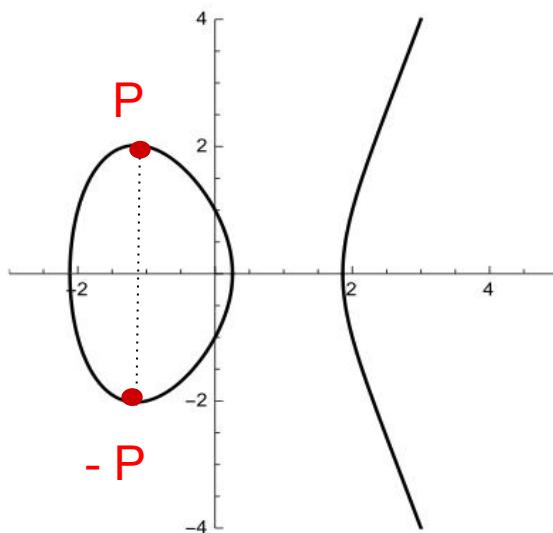
Curve ellittiche sui numeri reali

Per le applicazioni crittografiche si assume $4a^3 + 27b^2 \neq 0$

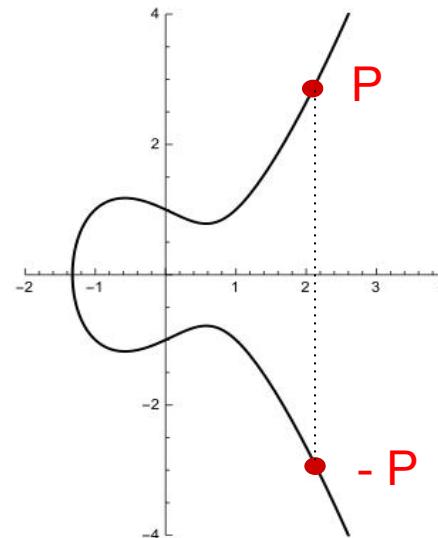
- assicura che il polinomio cubico $x^3 + ax + b$ non abbia radici multiple
- la curva sia priva di punti singolari come “cuspidi” o “nodi” dove non sarebbe definita in modo univoco la tangente.



Curve ellittiche sui numeri reali



(a) Curva $y^2 = x^3 - 4x + 1$



(b) Curva $y^2 = x^3 - x + 1$

Le curve ellittiche presentano una **simmetria orizzontale**

ogni punto **P = (x, y)** sulla curva si riflette rispetto all'asse delle ascisse nel punto **-P = (x, -y)** anch'esso sulla curva

l'immagine speculare rispetto all'asse x del punto all'infinito O è lo stesso O: **-O = O**

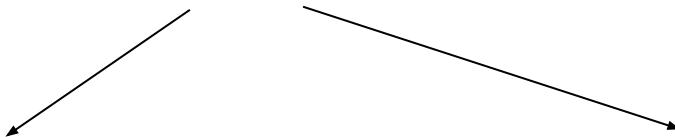
Curve ellittiche: somma di punti

Operazione di addizione su una curva ellittica

Proprietà

ogni retta interseca una curva ellittica in al più tre punti

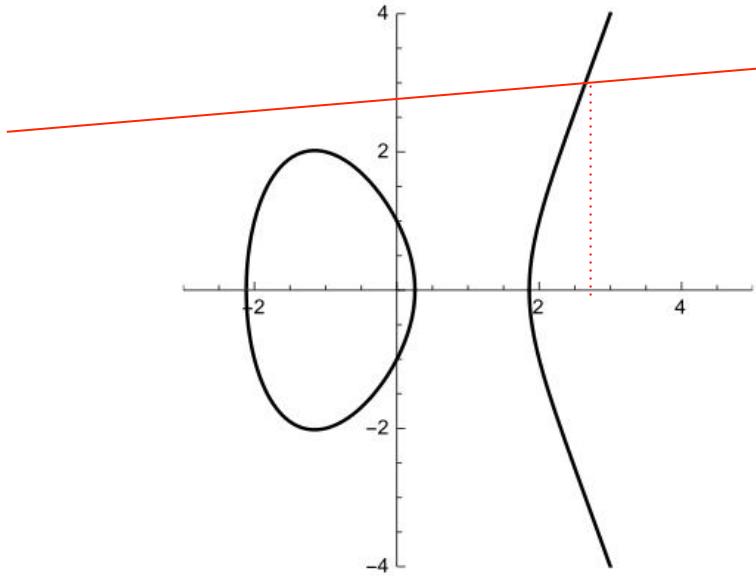
- intersezione tra una curva di terzo grado e una di primo grado (la retta)
- sostituendo nell'equazione della curva $y^2 = x^3 + ax + b$ l'espressione di y della retta si ottiene un'**equazione di terzo grado in x**
- **tre soluzioni**, reali o complesse → ascisse dei punti di intersezione tra la curva ellittica e la retta



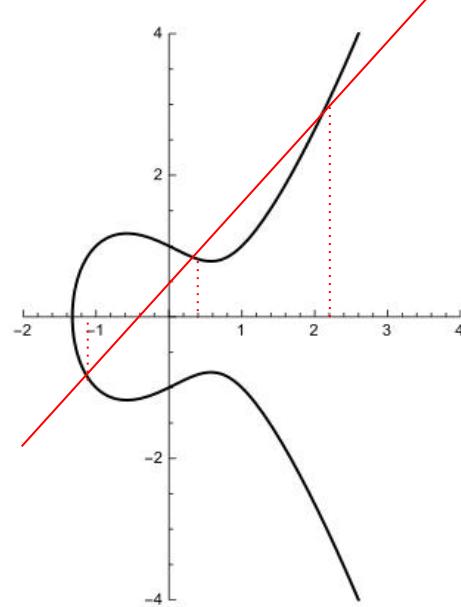
una soluzione reale e due soluzioni complesse e coniugate, quindi un punto (reale) di intersezione

tre soluzioni reali, quindi tre punti di intersezione

Curve ellittiche: somma di punti



(a) Curva $y^2 = x^3 - 4x + 1$



(b) Curva $y^2 = x^3 - x + 1$

una soluzione reale e due soluzioni complesse e coniugate, quindi un punto (reale) di intersezione

tre soluzioni reali, quindi tre punti di intersezione

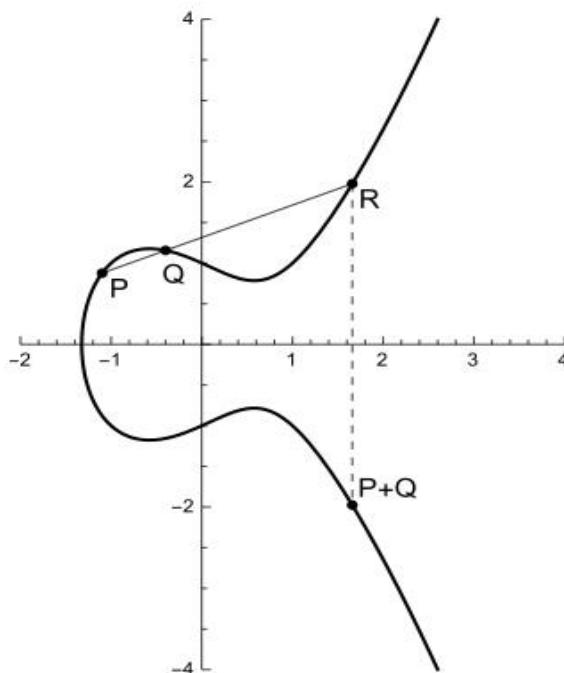
Curve ellittiche: somma di punti

Quindi se una retta interseca la curva $E(a, b)$ in due punti P e Q , coincidenti se la retta è una tangente, allora la retta interseca $E(a, b)$ anche in un terzo punto R

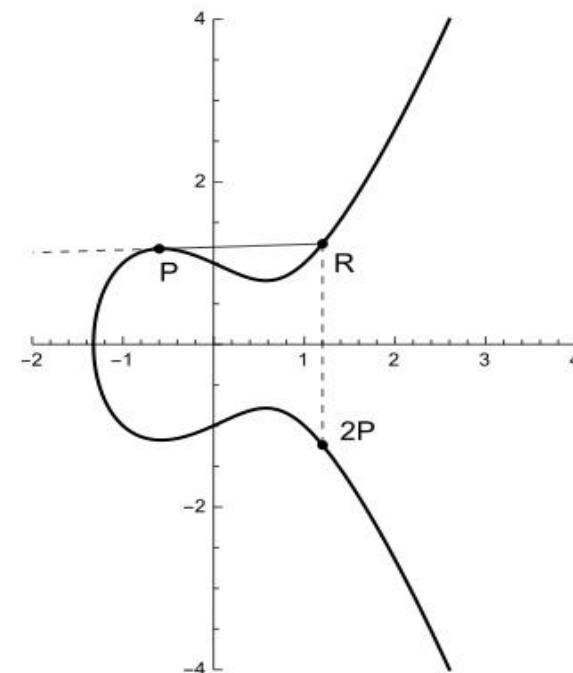
Dati tre punti $P, Q, R \in E(a, b)$, se P, Q e R sono disposti su una retta, si pone

$$P + Q + R = O$$

Da questa definizione, si ricava la regola per sommare due punti P e Q



(a) Somma di due punti P e Q .



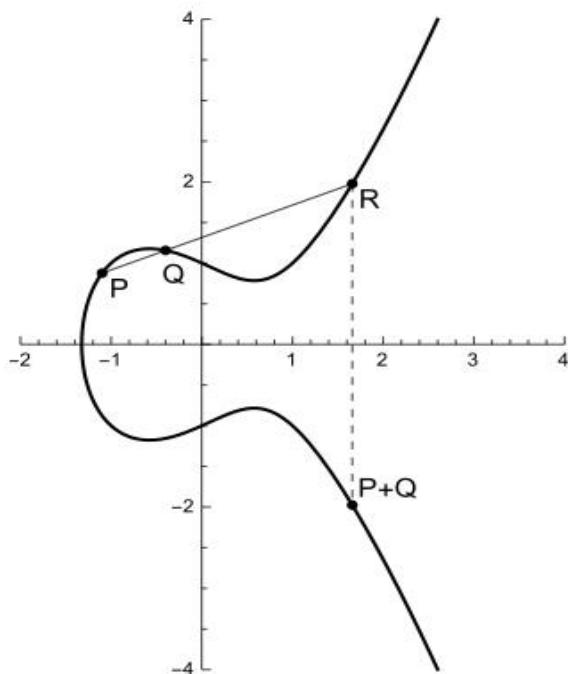
(b) Raddoppio di un punto P

Curve ellittiche: somma di punti

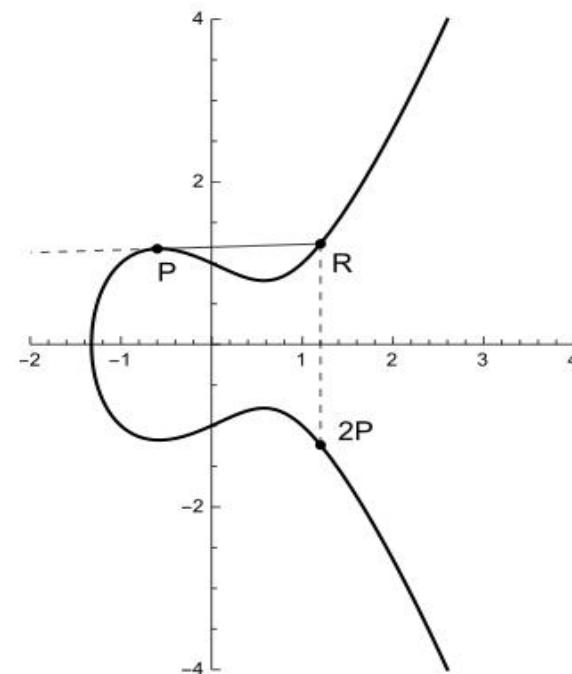
- Si considera la **retta passante per P e Q**, oppure la **tangente in P** se P e Q coincidono
- Si determina il **terzo punto di intersezione R** tra la curva e la retta (o la tangente)
- Si definisce somma di P e Q il punto simmetrico a R rispetto all'asse delle ascisse

$$P + Q = -R$$

La somma è ben definita in quanto anche $-R$ è un punto della curva



(a) Somma di due punti P e Q .



(b) Raddoppio di un punto P