La crittografia a curve elittiche e applicazioni

Prof. Massimiliano Sala

MINICORSI 2011. Crittografia a chiave pubblica: oltre RSA

Università degli Studi di Trento, Lab di Matematica Industriale e Crittografia

24 marzo 2011

1. LE CURVE ELLITTICHE

... Cosa sono?

Equazione di Weierstrass:

$$F(x, y, z) = y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3 = 0$$

dove

- $\mathbb{K}$ campo
- $a_1, \ldots, a_6,\ x, y, z \in \mathbb{K}$

Curva Ellittica $\mathbf{E}/\mathbb{K}$ = Insieme delle soluzioni nel piano proiettivo $\mathbb{P}^2(\mathbb{K})$ di una equazione di Weierstrass

Prendiamo $\mathbf{E}/\mathbb{K} = \mathbf{E}$.
Se $\mathbb{K}$ è finito, allora $\mathbf{E}$ ha un numero finito di punti, che indichiamo con N.

- CASO 1: $z \neq 0$

$$\text{sostituzione } (x, y, z) \mapsto (\tfrac{x}{z}, \tfrac{y}{z}, 1)$$

$$\Longrightarrow \quad f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

- CASO 2: $z = 0$

$$x^3 = 0$$

$\Longrightarrow$ Soluzioni: tutti i punti dell'insieme $(0, y, 0)$ al variare di y, con $y \neq 0$

$\Longrightarrow$ Unica soluzione: punto all'infinito $(\mathcal{O} = (0 : 1 : 0))$

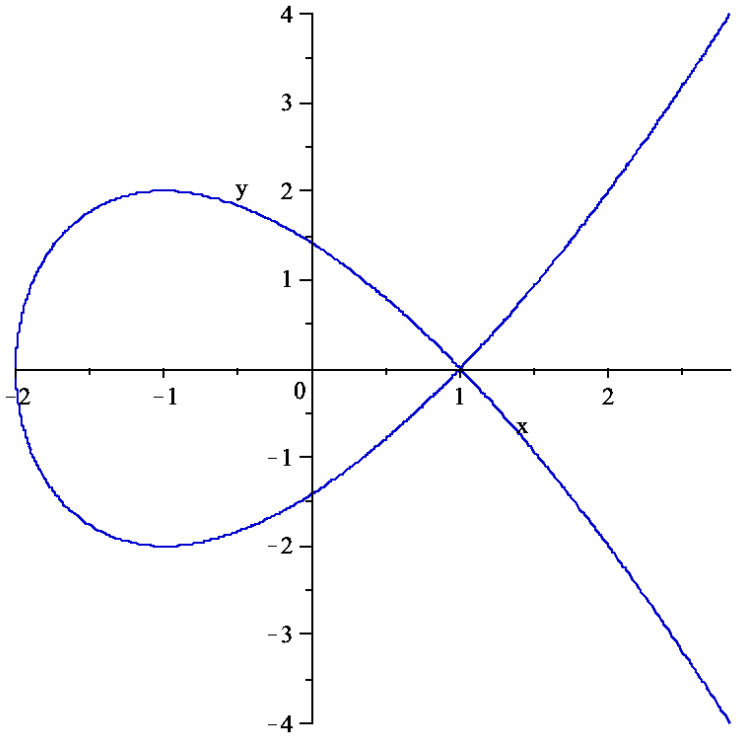
$\Longrightarrow$ Dato un campo $\mathbb{K}\ldots$

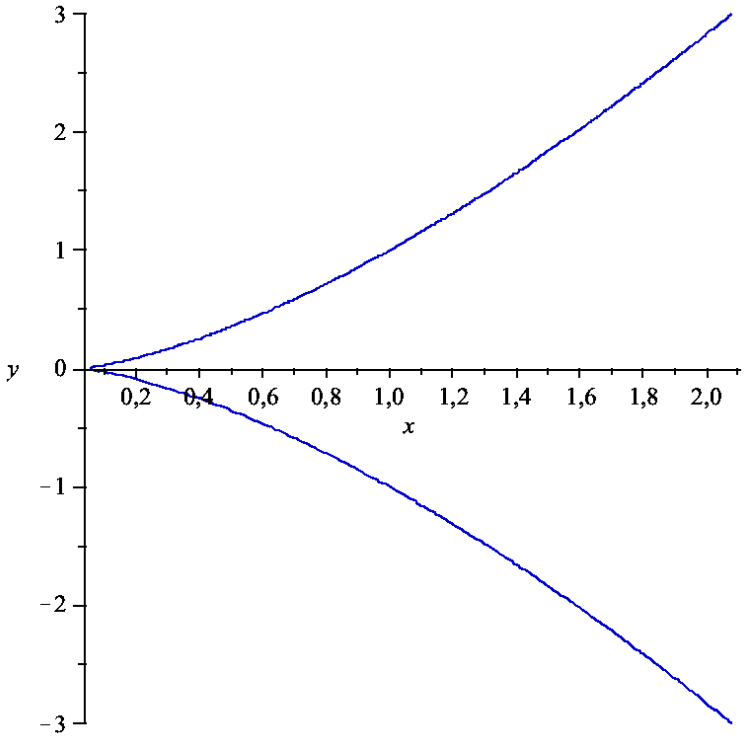
Curva Ellittica E:

$$\text{insieme delle soluzioni di } f(x,y)=0$$
$$+$$
$$\text{punto all'infinito } \mathcal{O}$$

Curve singolari

Evitare curve in cui la tangente a qualche punto non è ben definita





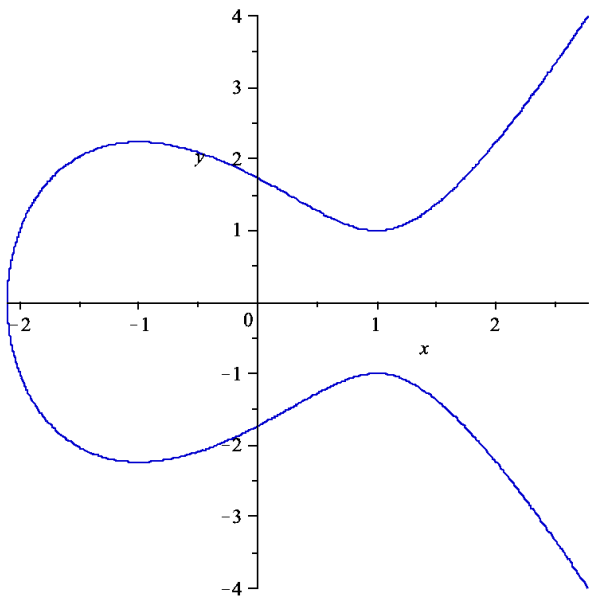
Un punto $P = (x, y, z)$ si dice **punto singolare** se

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0.$$

CURVA NON SINGOLARE

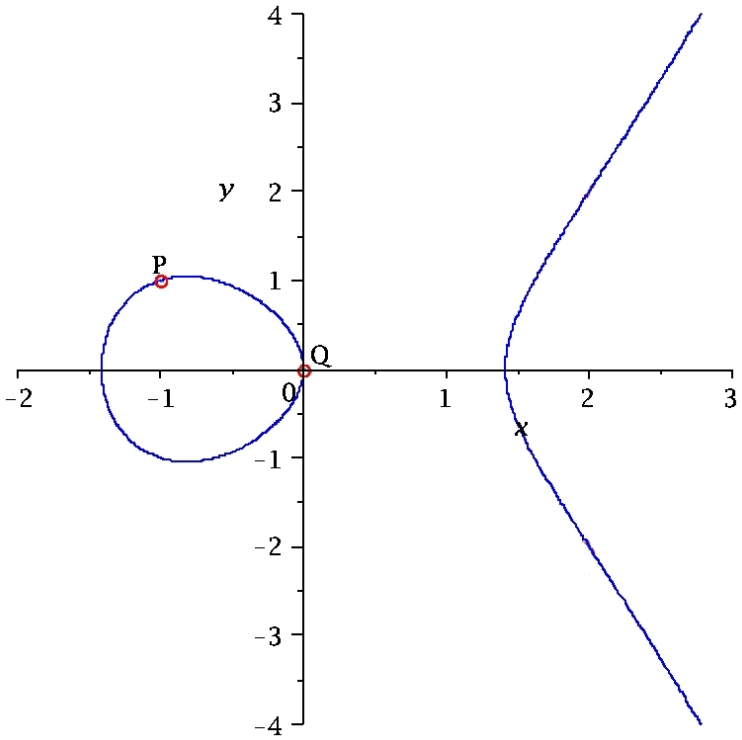
=

curva senza punti singolari



Legge di gruppo

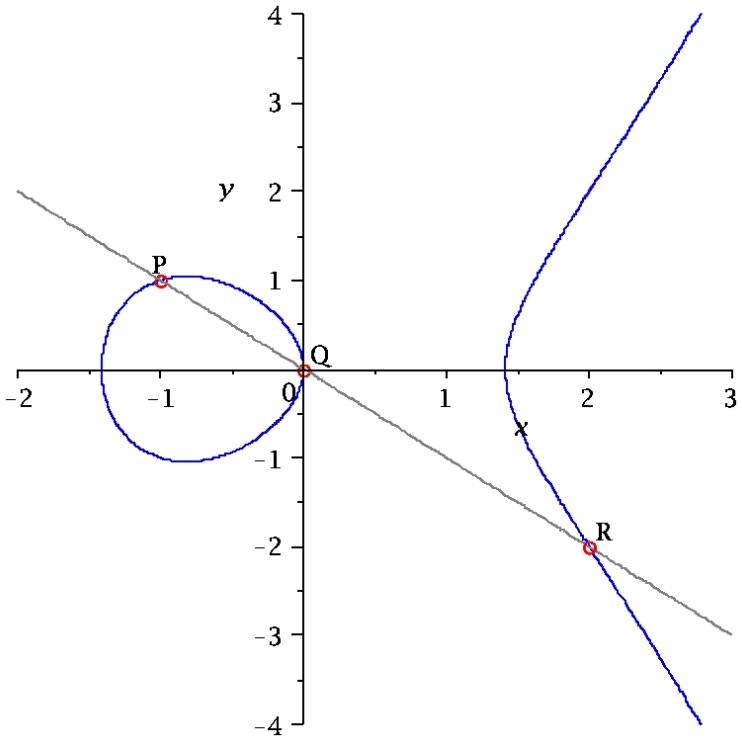
SOMMA ($P \oplus Q$)



- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $P, Q \in$ **E**;

Legge di gruppo

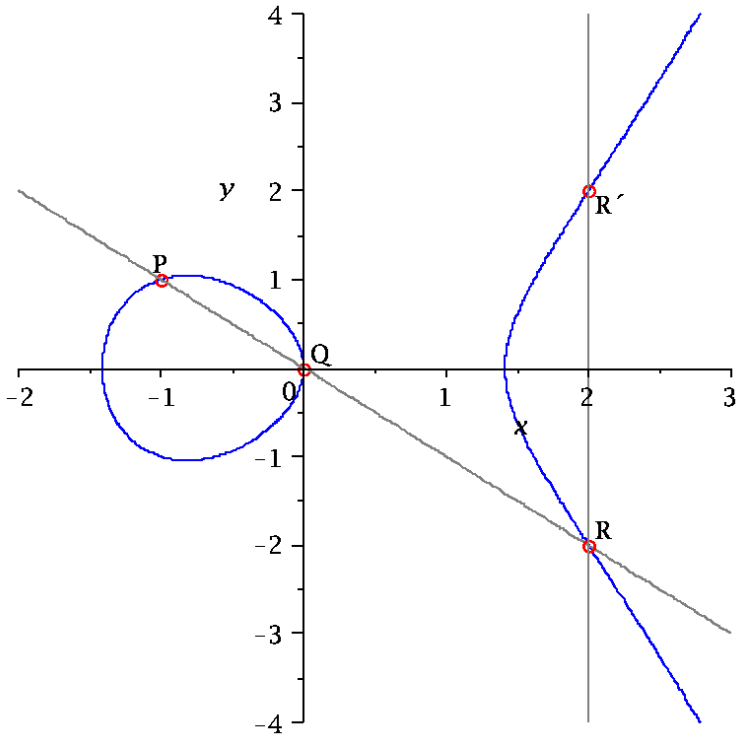
SOMMA ($P \oplus Q$)



- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $P, Q \in$ **E**;
- L retta che congiunge P con Q;
- R terzo punto di intersezione di **E** con L;

Legge di gruppo

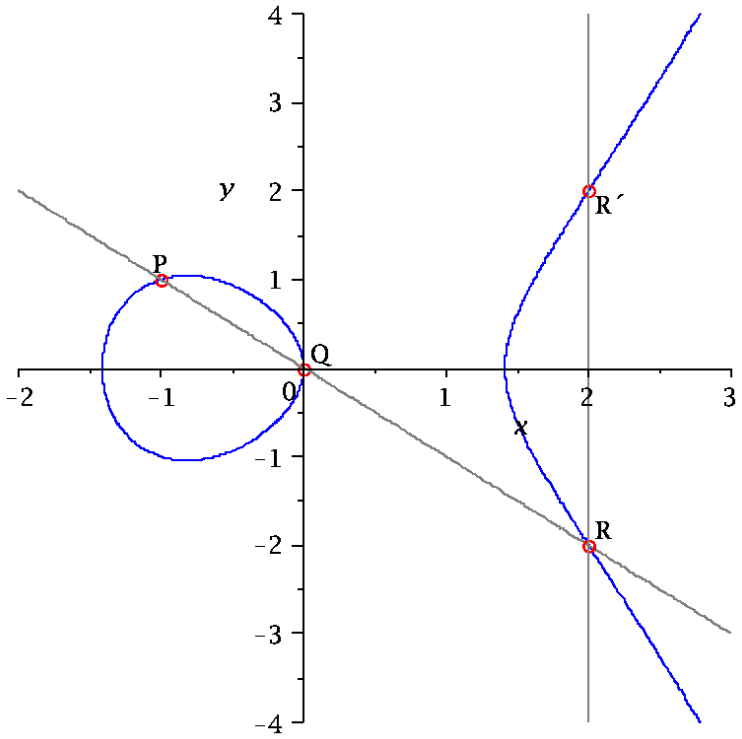
SOMMA ($P \oplus Q$)



- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $P, Q \in$ **E**;
- L retta che congiunge P con Q;
- R terzo punto di intersezione di **E** con L;
- L' retta passante per R ed il punto all' infinito $\mathcal{O}$;
- R' terzo punto di intersezione tra **E** ed L';

Legge di gruppo

SOMMA ($P \oplus Q$)



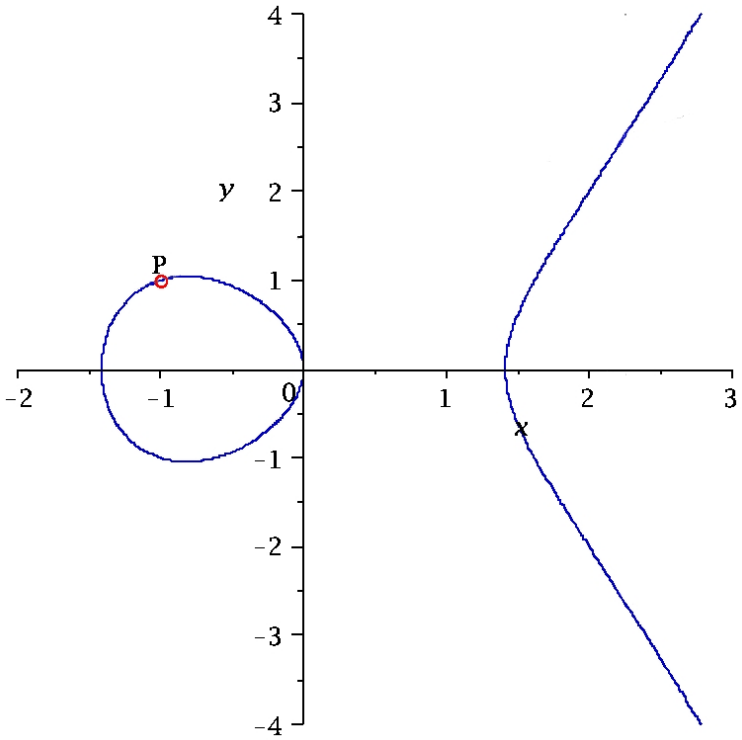
- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $P, Q \in$ **E**;
- L retta che congiunge P con Q;
- R terzo punto di intersezione di **E** con L;
- L' retta passante per R ed il punto all' infinito $\mathcal{O}$;
- R' terzo punto di intersezione tra **E** ed L';

$\Longrightarrow$ R' è la **somma** $P \oplus Q$.

Legge di gruppo

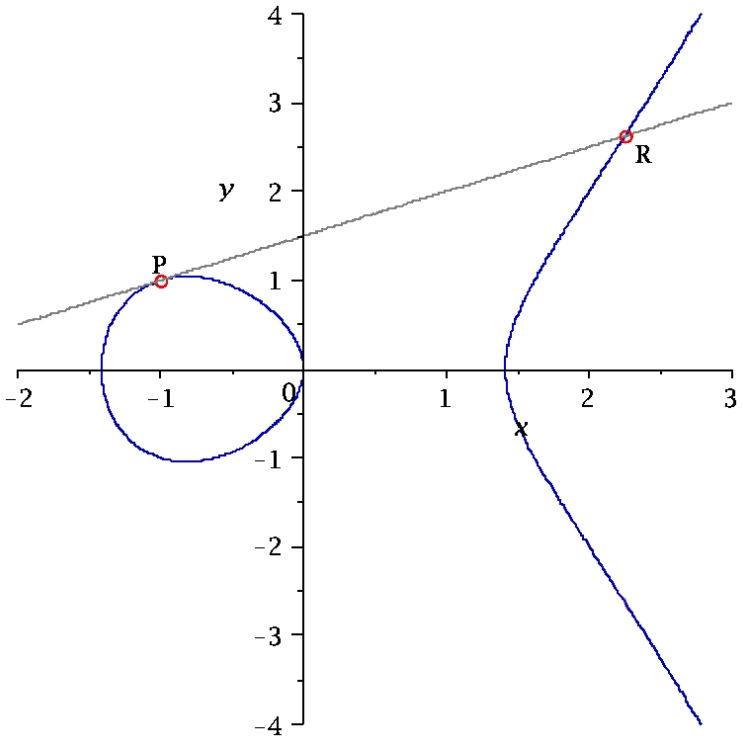
RADDOPPIO ($[2]P$)

Se $P = Q \ldots$



Legge di gruppo

RADDOPPIO ($[2]P$)



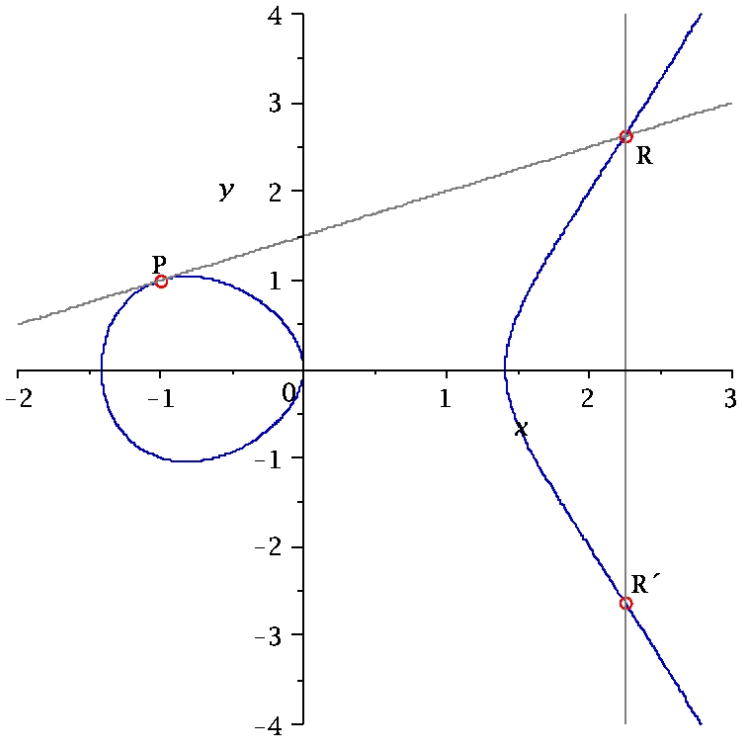
Se $P = Q \ldots$

$\Downarrow$

- L = tangente alla curva in P
- R punto di intersezione di $\mathbf{E}$ con L;

Legge di gruppo

RADDOPPIO ($[2]P$)



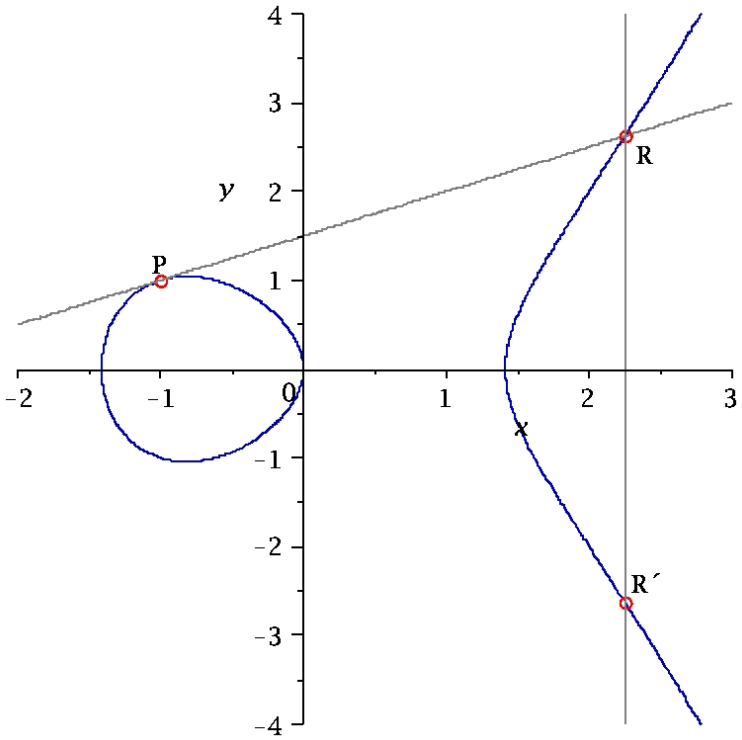
Se $P = Q \ldots$

$\Downarrow$

- L = tangente alla curva in P
- R punto di intersezione di **E** con L;
- L' retta passante per R e il punto all' infinito $\mathcal{O}$;
- R' terzo punto di intersezione tra **E** ed L'

Legge di gruppo

RADDOPPIO ($[2]P$)



Se $P = Q\ldots$

$\Downarrow$

- L = tangente alla curva in P
- R punto di intersezione di **E** con L;
- L' retta passante per R e il punto all' infinito $\mathcal{O}$;
- R' terzo punto di intersezione tra **E** ed L'

$\Longrightarrow$ R' è il raddoppio $[2]P$.

Legge di gruppo

Teorema

Una curva ellittica **E** *non singolare è un gruppo abeliano rispetto all'operazione* $\oplus$*, con elemento neutro* $\mathcal{O}$*.*

$\Longrightarrow$ Gruppo usato per i sistemi ECC (Elliptical Curve Cryptography)

Moltiplicazione scalare

- $k \in \mathbb{N}$:

$$\begin{aligned} [k] \quad : \quad & \mathbf{E} \to \mathbf{E} \\ & P \to [k]P = \underbrace{P \oplus P \oplus \ldots \oplus P}_{k} \end{aligned}$$

- $k = 0$: $[0]P = \mathcal{O}$
- $k < 0$: $[k]P = [-k](-P)$

Ordine di un punto/Ordine della curva

- Ordine di $P \in \mathbf{E}$
  il più piccolo $m \in \mathbb{Z}$, $m > 0$, se esiste, t.c. $[m]P = \mathcal{O}$

  Se tale m non esiste $\Longrightarrow$ P ha *ordine infinito*

- Ordine della curva $\mathbf{E}/\mathbb{F}_p$
  numero di punti razionali su $\mathbb{F}_p$che appartengono ad $\mathbf{E}$

Due categorie di curve

Punto di **n**-torsione
$= P \in \mathbf{E}$ t.c. $[n]P = \mathcal{O}$ (con $n \in \mathbb{Z}$, $n > 0$)

$\Longrightarrow$ Kernel di **[n]**: $E[n] = \{P \in \mathbf{E}/\overline{\mathbb{K}} \mid [n]P = \mathcal{O}\}$

E curva ellittica, $\mathrm{char}(\mathbb{K}) = p$

1. se $N \equiv 1 \mod p$

   $\Longrightarrow$ **CURVA SUPERSINGOLARE**

2. altrimenti $\Longrightarrow$ **CURVA ORDINARIA**

2. LA CRITTOGRAFIA A CURVE ELLITTICHE (ECC)

Due tipi di Cifrari a Chiave Pubblica

Ricordiamo che ci sono cifrari a chiave pubblica che servono per:

- per scambiare un messaggio
- per scambiare o negoziare una chiave segreta, da usare poi in altri crittosistemi

Il problema del logaritmo discreto su curva ellittica (ECDLP)

Dati...

- $\mathbf{E} = \mathbf{E}/\mathbb{F}_q$
- $P \in \mathbf{E}$ di ordine n
- $Q = [k]P$ per qualche k

trovare l'intero $k \in \{0, \ldots, n-1\}$ t.c. $Q = [k]P$

$$\Longrightarrow \quad k = \log_P Q$$

(**LOGARITMO DISCRETO DI Q IN BASE P**)

Diffie-Hellman su curva ellittica

$$\underline{\text{Informazioni pubbliche}} : \begin{cases} \mathbf{E} \\ P \in \mathbf{E}\ (\textit{base}),\ \text{di ordine } n \end{cases}$$

$\xrightarrow{[a]P}$

$\xrightarrow{[b]P}$

$$\Longrightarrow \quad \underline{\text{Chiave segreta}}:\ [ab]P = [a]([b]P) = [b]([a]P)$$

Massey-Omura su curva ellittica

Sia M il messaggio che Alice vuole trasmettere a Bob.

$$\underline{\text{Informazioni pubbliche}} : \begin{cases} \mathbf{E} \\ N \end{cases}$$

$\ldots e \in \{1, \ldots, N\}$, primo con N, d t.c. $d \equiv e^{-1} (mod\ N)) \ldots$

1.  $\xrightarrow{[e_a]M}$ 

2.  $[e_b]([e_a]M) = [e_b e_a]M$ $\xrightarrow{}$ 

3.  $[d_a]([e_b e_a]M) = [e_b]M$ $\xrightarrow{}$ 

4.  $[d_b]([e_b]M) = M$

3. ATTACCHI e SICUREZZA

Attacchi possibili all'ECDLP

Curva generica:

- Silver-Pohlig-Hellman
- Baby step-Giant step
- Pollard

Curva speciale:

- MOV
- curve anomale

Il metodo Silver-Pohlig-Hellman

- A, B punti di una curva ellittica $\mathbf{E}$ t.c. $[k]A = B$
- $N := |\mathbf{E}| = \prod_{i=1}^{t} {q_i}^{e_i}$ con q_i primi e e_i interi positivi $(\forall i = 1, \ldots, t)$

Idea: trovare $k(mod\, {q_i}^{e_i})$ e utilizzare il Teorema Cinese dei Resti per ottenere $k(mod\, N)$.

CONTROMISURA:

Selezionare N primo o con un divisore primo molto grande

COSTO:

Il tempo richiesto dall'algoritmo è $\sqrt{q_i}$. Dove q_i è il più grande fattore di N.

Il metodo Baby step-Giant step

- A, B punti di una curva ellittica $\mathbf{E}$ t.c. $[k]A = B$

$$\textbf{Idea}: \; k = \lceil \sqrt{N} \rceil c + d \quad \text{con} \quad 0 \leq c, d < \lceil \sqrt{N} \rceil.$$

$\Longrightarrow$ provare i valori di k passando in rassegna i valori di c e d

CONTROMISURA:

Già con valori non troppo elevati di N, richiede troppa memoria

$$N \geq 2^{120} \quad \Longrightarrow \quad \text{Impraticabile}$$

COSTO:

Il tempo richiesto dall'algoritmo è $\sqrt{N}$. Però richiede una occupazione di memoria di $O(\sqrt{N})$.

Il metodo ρ di Pollard

- A, B punti di una curva ellittica $\mathbf{E}$ t.c. $[k]A = B$

Idea: *"Paradosso del Compleanno"*

(scegliendo a caso degli elementi da un gruppo G di ordine N, è sufficiente selezionarne $\mathcal{O}(\sqrt{N})$ per assicurarsi una probabilità del 50% di avere *collisione*)

CONTROMISURA:

Selezionare $N \geq 2^{160}$

COSTO:

La complessità di questo algoritmo è : $\sqrt{N} = N^{\frac{1}{2}} = 2^{\frac{1}{2}\log N}$.

Scegliere la curva, 1

Come possiamo scegliere i parametri di una curva generica ellitica **E** per difendersi dagli attacchi generici?

Attacco	**Precauzione**
Pohlig - Hellman Pollard ρ Baby step Giant step	*(i)* N grande *(ii)* N deve avere un fattore r tale che $\sqrt{r}$ risulti essere un numero intrattabile di operazioni *(iii)* P deve avere ordine r
calcolo DLP	no curve supersingolari

Il metodo Menezes, Okamoto, Vanstone (MOV)

- P, Q punti di una curva ellittica $\mathbf{E}/\mathbb{F}_q$ t.c. $Q = [k]P$
- n ordine di P (t.c. $MCD(n, q) = 1$)

Idea: ridurre il problema del logaritmo discreto sulle curve ellittiche ad un problema di logaritmo discreto nel gruppo moltiplicativo di un campo più grande

CONTROMISURA:

Verificare che n non divida $q^k - 1$ per tutti i valori $1 \leq k \leq 100$
$\Longrightarrow$ Esclusione delle curve supersingolari

COSTO:

Sia $E[n] \subseteq \mathbf{F}_{q^m}$, allora il costo di quest'algoritmo è subesponenziale in m, dove $m \geq \log n$.

Curve Anomale

Una curva ellittica **E** è facilmente attaccabile:

1. se la curva è isomorfa a $(\mathbb{F}_q, +)$
2. in generale se c'è un isomorfismo tra **E** e una somma diretta di $\mathbb{Z}_p$
3. se c'è un isomorfismo tra **E** e lo Jacobiano di una curva iperellittica in cui è facile il calcolo del DLP

Scegliere la curva, 2

Come possiamo scegliere i parametri di una curva ellitica **E** per difendersi dagli attacchi speciali?

Attacco	**Precauzione**
Isomorfismo a $(\mathbb{F}_q, +)$	il fattore più grande di N deve essere diverso da q
MOV	$q^k \not\equiv 1 \mod r$ per $0 < k < 100$
Isomorfismo allo Jacobiano	m primo o se m è composto bisogna scegliere un'opportuna curva

Scegliere la curva, 3

Possiamo scegliere i parametri i modo tale da migliorare l'efficienza.

Situazione	**Migliorare l'efficienza**
Campi primi $\mathbb{F}_p$	p primo, lunghezza in bit = multiplo della lunghezza word. p primo di Mersenne o *simile*
Campi binari $\mathbb{F}_{2^m}$	m primo o m composto con opportuna curva
OptimalExtensionField $\mathbb{F}_{p^m}$	Sconsigliati
Coefficienti	$a = -3$ o Curve con Endomorfismi Efficientemente Calcolabili

Molto importante è scegliere con cura la curva **E** e il punto P in modo da bilanciare sicurezza ed efficienza.

Nelle implementazioni questo talvolta manca.

4. Accenno ad applicazioni di ECC

$$\underline{\text{Vantaggi dell'ECC}} : \begin{cases} \textbf{EFFICIENZA} \\ \textbf{SICUREZZA} \end{cases}$$

- Incremento dell'uso dell'ECC in diversi prodotti
- Incorporazione dell'ECDSA in svariati standard di sicurezza di governi e grandi istituzioni di ricerca

APPLICAZIONI COMMERCIALI

- crittografia CERTICOM per reti di sensori e sicurezza Voip
- comunicazioni Wireless con ECC (Texas Instruments)
- Standard industriali: IEEE, IETF, VPNC, ASC X9
- ...

Cosa sono le smart cards?

Piccoli dispositivi della forma e della grandezza di una carta di credito, ma molto flessibili. . .

Usi più frequenti:

- carte di credito
- tickets elettronici
- carte d'identità

smart = sveglio, intelligente $\rightsquigarrow$ microchip integrato

Sicurezza e gestione delle chiavi...

Generatore di chiavi interno $\Longrightarrow$ Eseguire crittazione e decrittazione, senza "far uscire" la chiave segreta

...chiave generata, usata e distrutta senza alcuna possibilità di essere letta dall'esterno

$\Longrightarrow$ **strumento di firma digitale**

Prototipo di smart card basato su ECC

I. Z. Berta e *Z. Á. Mann*, 2002:
implementazione di un prototipo ECC basato sulla tecnologia Java Card e in grado di funzionare sulle smart cards...

prodotto software $\Longrightarrow$ potrebbe non adempire alle prestazioni richieste per l'uso commerciale

Obiettivo:

dimostrare che un algoritmo complesso come l'ECC può essere implementato sulle "deboli" smart cards

Architettura delle Smart Cards

La struttura del microchip integrato è simile a quella di un computer, essendo composta da:

- CPU
- ROM, EEPROM (memoria nonvolatile)
- Circuito di Sicurezza
- Periferiche I/O

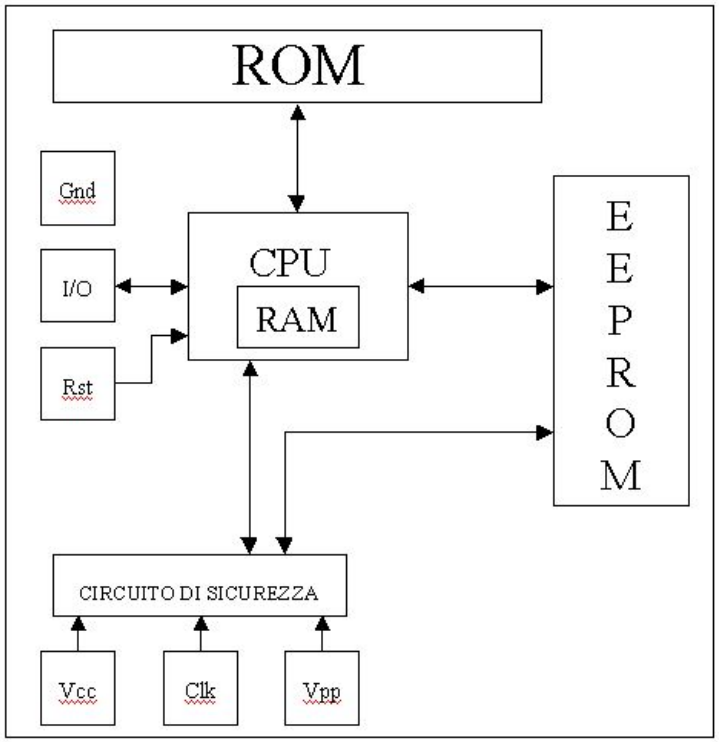


Figura 4 : Struttura Hardware

Altre applicazioni...

- **Internet**

  commercio elettronico: uso di smart cards ed ECC per transazioni sicure con carte di credito via web

- **PDA** (*Personal Digital Assistant*)

  potenza computazionale più elevata rispetto agli altri dispositivi mobili
  $+$ larghezza di banda limitata

- **PC**

  proteggere dati e crittare messaggi e-mail o istantanei con l'uso dell'ECC