La crittografia a curve elittiche e applicazioni

Dott. Emanuele Bellini

Torino 2011. Crittografia a chiave pubblica: oltre RSA

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

13 Maggio 2011

Index

1. LE CURVE ELLITTICHE

. . . Cosa sono?

Siano $\mathbb{K}$ un campo e $f : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ una funzione della forma

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

dove

- $a_1, \ldots, a_6,\ x, y \in \mathbb{K}$
- f è non singolare

Definition

Una *curva ellittica* $\mathbf{E}$ su un campo $\mathbb{K}$, che denoteremo con $\mathbf{E}/\mathbb{K}$, o semplicemente con $\mathbf{E}$, è l'insieme dei punti $(x, y) \in \mathbb{K}^2$ che soddisfano l'equazione $f(x, y) = 0$, più un punto $\mathcal{O}$ che chiameremo "punto all'infinito".

Se $\mathbb{K}$ è finito, allora $\mathbf{E}$ ha un numero finito di punti $|\mathbf{E}|$.

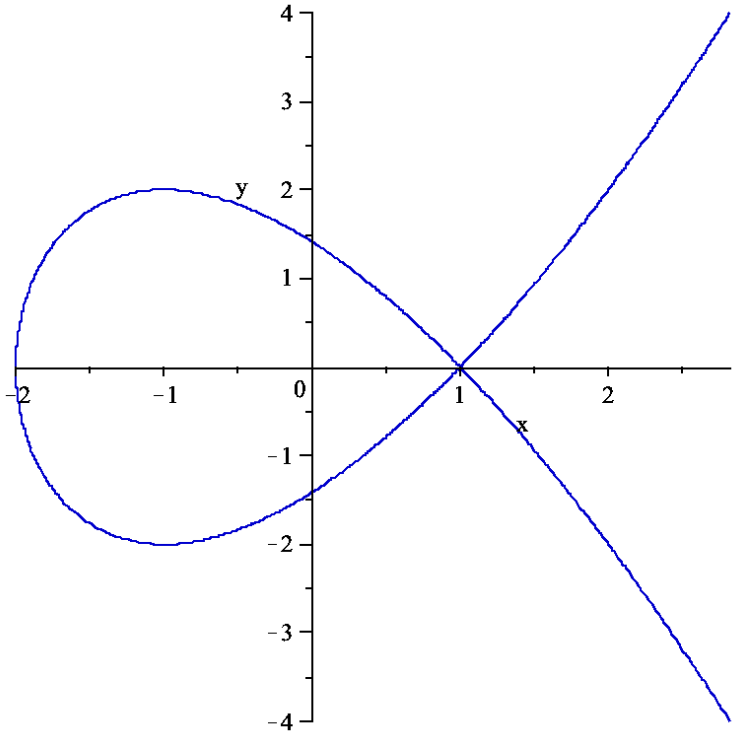
$\Longrightarrow$ Dato un campo $\mathbb{K}\ldots$

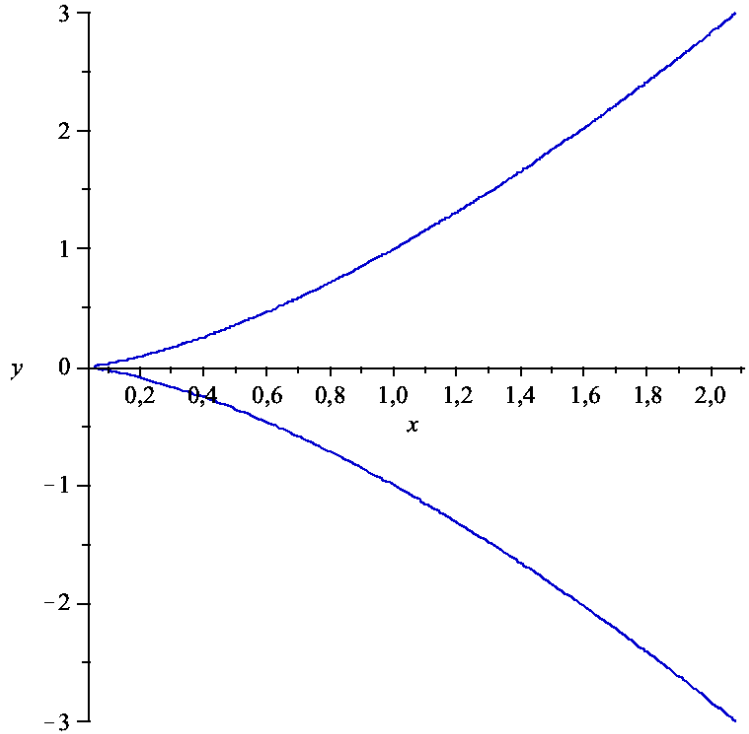
Curva Ellittica E:

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

Curve singolari

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





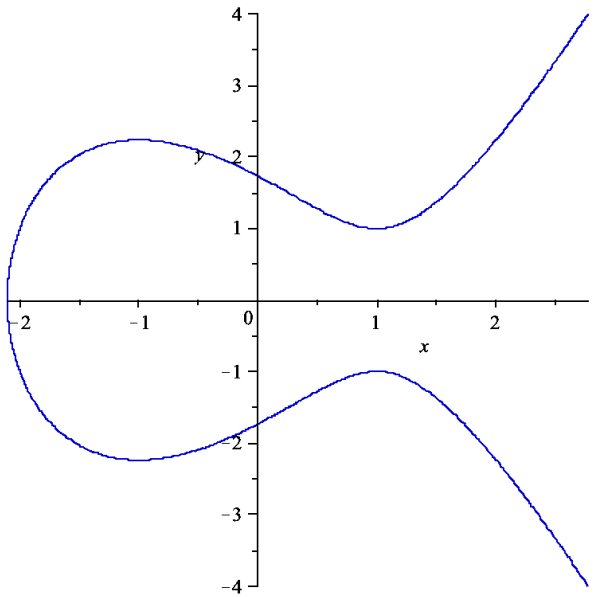
Un punto $P = (x, y)$, con $x, y \in \overline{\mathbb{K}}$ si dice **punto singolare** se

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

CURVA NON SINGOLARE

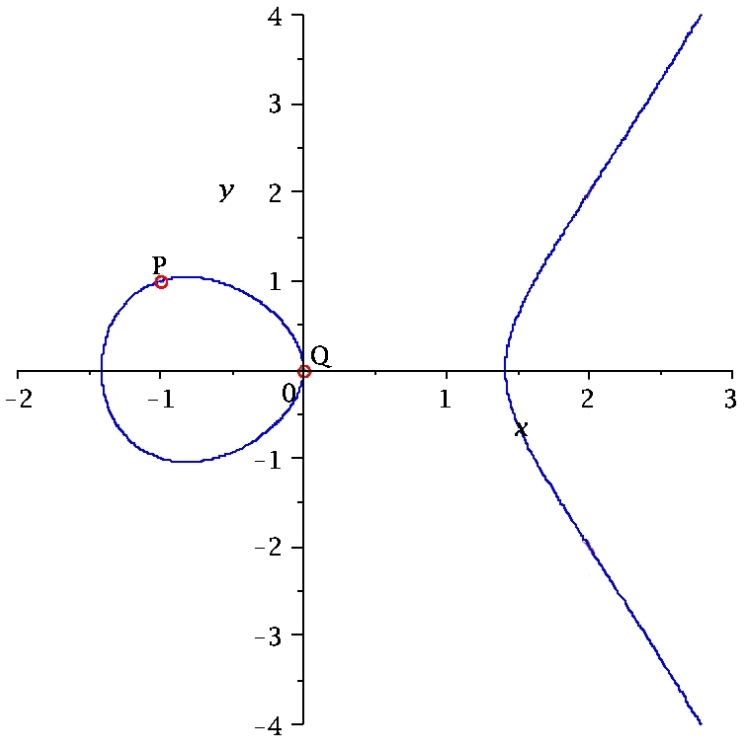
=

curva senza punti singolari



Legge di gruppo

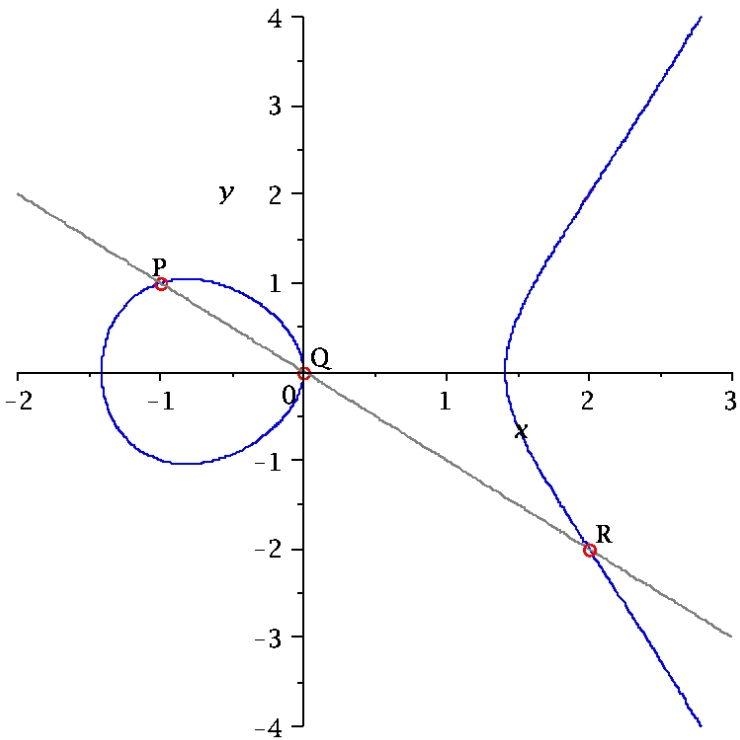
SOMMA ($P \oplus Q$)



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

Legge di gruppo

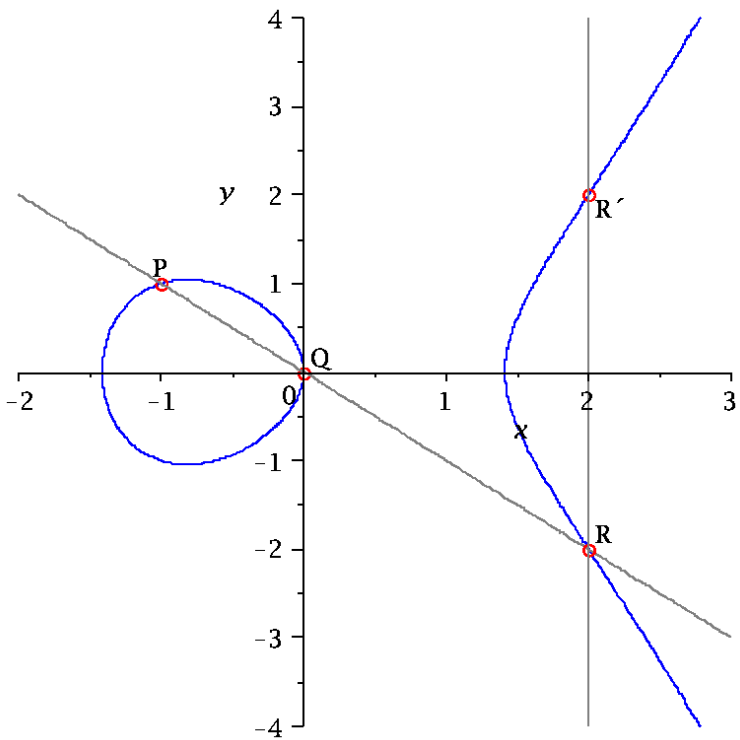
SOMMA ($P \oplus Q$)



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

Legge di gruppo

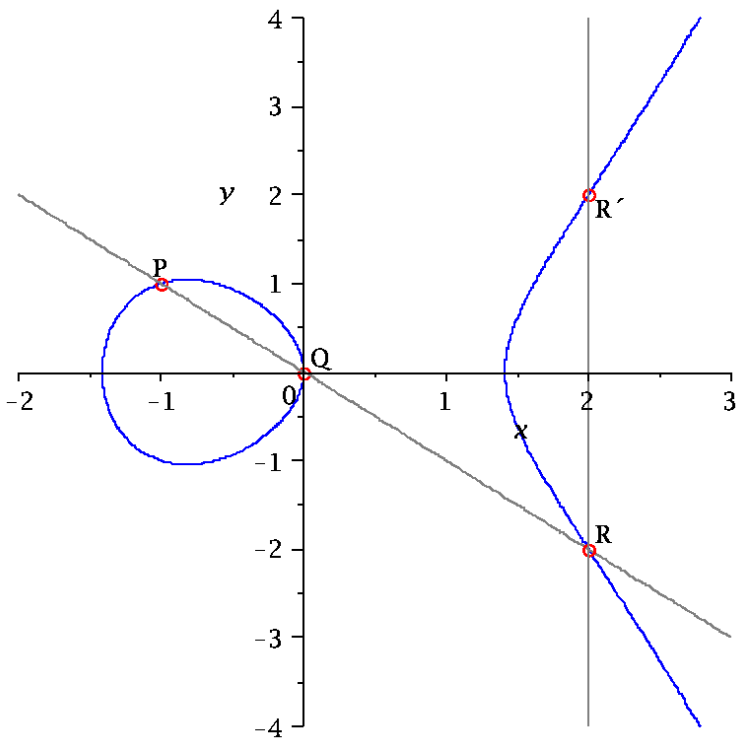
SOMMA ($P \oplus Q$)



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



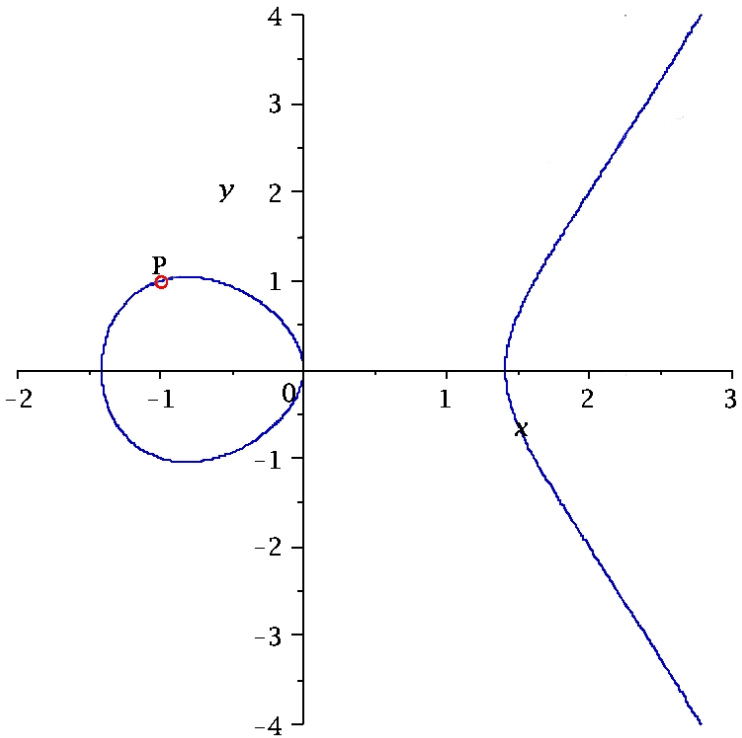
- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $P, Q \in \mathbf{E}$;
- L retta che congiunge P con Q;
- R terzo punto di intersezione di **E** con L;
- L' retta passante per R ed il punto all' infinito $\mathcal{O}$;
- R' terzo punto di intersezione tra **E** ed L';

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

Legge di gruppo

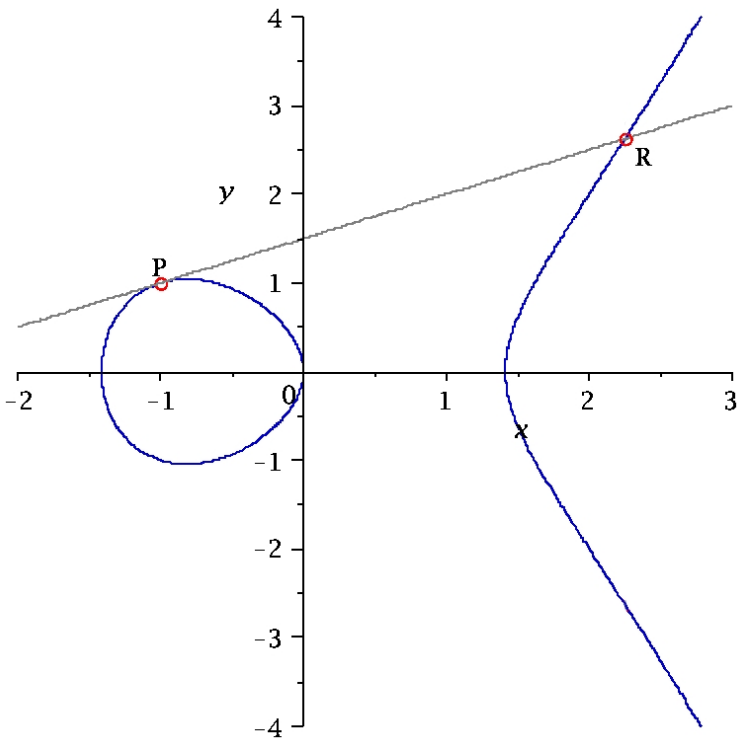
RADDOPPIO ($2P$)

Se $P = Q \ldots$



Legge di gruppo

RADDOPPIO ($2P$)



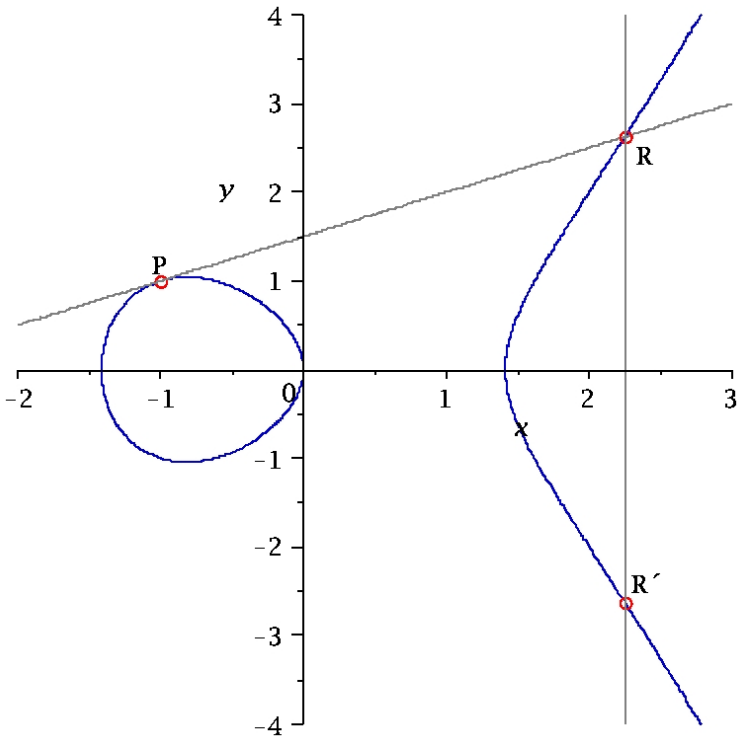
Se $P = Q \ldots$

$\Downarrow$

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

Legge di gruppo

RADDOPPIO ($2P$)



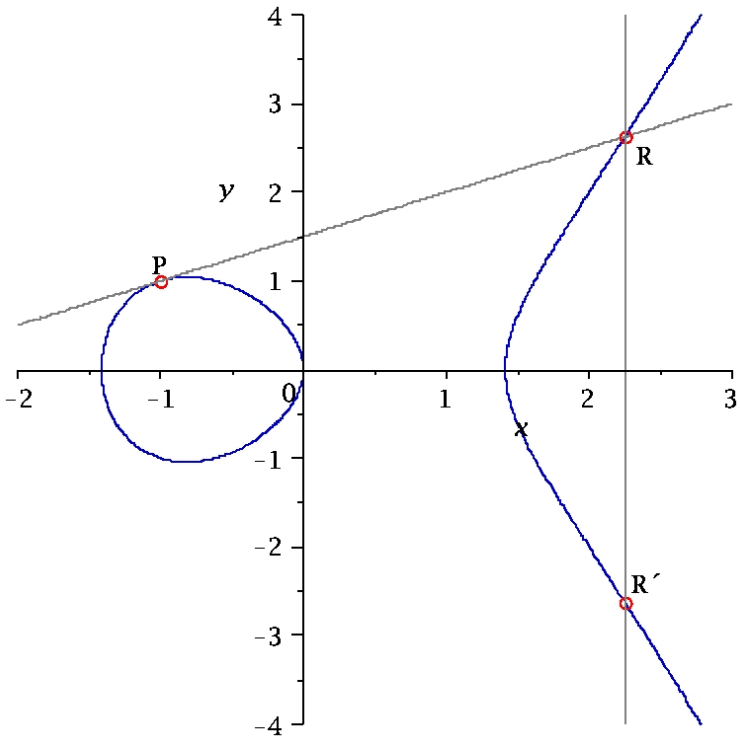
Se $P = Q \ldots$

$\Downarrow$

- 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 ($2P$)



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 $2P$.

Legge di gruppo

Teorema

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

$\Longrightarrow$ I sottogruppi ciclici di **E** sono usati per i sistemi ECC (Elliptic Curve Cryptography)

Moltiplicazione scalare

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

$$\begin{aligned} h \quad &: \quad \mathbf{E} \to \mathbf{E} \\ &\quad P \to hP = \underbrace{P \oplus P \oplus \ldots \oplus P}_{h} \end{aligned}$$

- $h = 0$: $0P = \mathcal{O}$
- $-P = -(x, y) = (x, -y)$
- $h < 0$: $hP = (-h)(-P)$

Ordine di un punto/Ordine della curva

- L' *ordine* N di $P \in \mathbf{E}$
  è il più piccolo intero positivo, se esiste, t.c. $NP = \mathcal{O}$

  Se tale N non esiste $\implies$ P ha *ordine infinito*

- L' *ordine* $|\mathbf{E}|$ della curva $\mathbf{E}$ (su $\mathbb{F}_q$)
  è il numero di punti razionali su $\mathbb{F}_q$ che appartengono ad $\mathbf{E}$.

$$q + 1 - 2\sqrt{q} \leq |\mathbf{E}| \leq q + 1 + 2\sqrt{q}$$

Due categorie di curve

E curva ellittica su $\mathbb{F}_q$, $char(\mathbb{F}_q) = p$

1. se $|\mathbf{E}| \equiv 1 \mod p$

   $\Longrightarrow$ **CURVA SUPERSINGOLARE**

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

2. LA CRITTOGRAFIA A CURVE ELLITTICHE (ECC)

Scopi della Crittografia a Chiave Pubblica

I cifrari a chiave pubblica servono per:

SCOPO	CIFRARIO UTILIZZATO
Scambio della chiave	ECDH, ECMQV
Scambio di un messaggio	ECIES
Firma di un messaggio	ECDSA

La sicurezza dei cifrari su curve ellittiche si basa sulla difficoltà di risolvere il problema del Logaritmo Discreto sul gruppo formato dai punti di una curva ellittica (ECDLP).

Il problema del logaritmo discreto su curva ellittica (ECDLP)

Dati...

- $\mathbf{E} = \mathbf{E}/\mathbb{F}_q$
- $P \in \mathbf{E}$ di ordine N
- $Q = hP$ per qualche h

trovare l'intero $h \in \{0, \ldots, N-1\}$ t.c. $Q = hP$

$$\Longrightarrow \quad h = \log_P Q$$

(LOGARITMO DISCRETO DI Q IN BASE P)

Scambio della chiave: Diffie-Hellman su curva ellittica (ECDH)

- Solo Alice conosce a
- Solo Bob conosce b

Informazioni pubbliche:

Tutti conoscono **E**, P, il suo ordine N, aP e bP (chiavi pubbliche)

$\Longrightarrow$ Chiave segreta comune: $abP = a(bP) = b(aP)$

Scambio della chiave: Menezes-Qu-Vanstone (ECMQV)

L' *Elliptic Curve Menezes-Qu-Vanston* è un protocollo di autenticazione basato sullo schema di Diffie-Hellman.

Scambio di un messaggio: Integrated Encryption Scheme (ECIES)

L' *Elliptic Curve Integrated Encryption Scheme* è uno schema di crittazione con autenticazione, basato sul problema di Diffie-Hellman.
Offre solo sicurezza semantica (avversario passivo).
Richiede l'utilizzo di KDF (Key Derivation Function), di un MAC (Message Autentication Code) e di un sistema di crittazione simmetrica.

Firma di un messaggio: algoritmo di firma digitale (ECDSA)

La firma digitale consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico.

ECDSA (*Elliptic Curve Digital Signature Algorithm*) è un algoritmo basato su Diffie-Hellman.
Richiede l'utilizzo di una funzione di Hash.
E' corretto nel senso che chi verifica accetta solo messaggi firmati correttamente.

3. ATTACCHI

Possibili attacchi

Attacchi possibili all'ECDLP

Attacchi generici:

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

Attacchi specifici:

- MOV
- curve anomale

Parametro di complessità

Per confrontare gli attacchi tra loro utilizziamo un parametro di complessità, indicato in blu

$$n = log_2 N$$

La cui sicurezza reale sarà invece indicata in verde, sempre con la lettera n.
2^n è il numero di operazioni elementari per rompere un cifrario con chiave di lunghezza n, quindi avremo sempre che $n \geq n$.

Il metodo ρ di Pollard

Siano $P, Q \in \mathbf{E}$ con P di ordine N e tali che $h \cdot P = Q$.

Idea:

- trovare 4 interi n_1, n_2, n_3, n_4 tali che $n_1 P + n_2 Q = n_3 P + n_4 Q$
  In questo modo $h = (n_1 - n_3)/(n_4 - n_2) \bmod N$.
- I quattro interi vanno cercati tramite un cammino pseudorandom in $< P >$, che termina in $\mathcal{O}(\sqrt{N})$ con probabilità del 50% (*"Paradosso dei Compleanni"*).

CONTROMISURA:

Scegliere N in modo che $\sqrt{N}$ sia un numero intrattabile di calcoli.

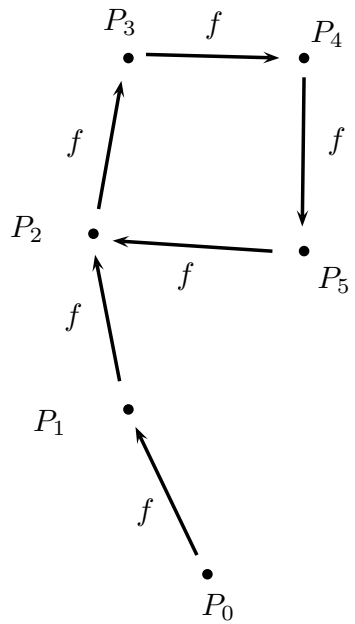
COSTO:

$$\sqrt{N} = 2^{\frac{1}{2}\log N} = 2^{n/2} = 2^{n} \Rightarrow n = n/2$$

Il metodo ρ di Pollard

Sia $\mathbf{E}$ una curva ellittica, e siano A e B tali che $hA = B$. Tramite una funzione pseudorandom $f : \mathbf{E} \to \mathbf{E}$ e due funzioni $g, j : \mathbf{E} \times \mathbb{Z} \to \mathbb{Z}$, è possibile effettuare un cammino pseudorandom in $< P >$:

1. $a_0 = 0,\ b_0 = 0,\ P_0 = 0$
2. $P_i = f(P_{i-1})$,
   $a_i = g(P_{i-1}, a_{i-1}),\ b_i = j(P_{i-1}, b_{i-1})$
3. $P_{2i} = f(f(P_{i-1}))$,
   $a_{2i} = g(f(P_{2i-2}), g(P_{2i-2}, a_{2i-2}))$,
   $b_{2i} = j(f(P_{2i-2}), j(P_{2i-2}, b_{2i-2}))$
4. se $P_i = P_{2i}$ allora abbiamo vinto
   (se $b_i - b_{2i}$ è invertibile mod N)
   $h = (a_{2i} - a_i)(b_i - b_{2i})^{-1} \bmod N$
5. se $P_i \neq P_{2i}$ allora $i = i + 1$



Il metodo Baby step-Giant step

- P, Q come prima.

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

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

CONTROMISURA:

Scegliere N in modo che $\sqrt{N}$ sia un numero intrattabile di calcoli e di occupazione di memoria.

COSTO:

$\mathcal{O}(\sqrt{N})$ operazioni elementari e $O(\sqrt{N})$ celle di memoria.
Anche qua $n = n/2 = \frac{1}{2} \log N$.

Il metodo Silver-Pohlig-Hellman

- P, Q come prima.
- $N = \prod_{i=1}^{t} {q_i}^{e_i}$ con q_i primi e e_i interi positivi $(\forall i = 1, \ldots, t)$

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

CONTROMISURA:

Selezionare N primo o con un divisore primo molto grande

Il metodo Menezes, Okamoto, Vanstone (MOV)

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

Idea: trovare un isomorfismo tra **E** e il gruppo moltiplicativo di un campo $\mathbb{F}_{q^m}$ estensione di $\mathbb{F}_q$, nel quale il DLP si risolve con un metodo subesponenziale chiamato Function Field Sieve.

CONTROMISURA:

Verificare che N non divida $q^s - 1$ per valori piccoli di s

$\Longrightarrow$ Esclusione delle curve supersingolari

COSTO:

Costo subesponenziale in m.

Curve Anomale

1. Una curva ellittica **E** è attaccabile se c'è un isomorfismo *efficientemente calcolabile* (e.c.) tra **E** e una somma diretta $\oplus\mathbb{Z}_{n_i}$ con n_i "piccoli".
2. Una curva ellittica **E** è attaccabile con attacchi di tipo index-calculus se c'è un isomorfismo e.c. tra **E** e lo Jacobiano di una curva iperellittica di genere maggiore di 2.
3. Una curva ellittica **E** è attaccabile in tempi polinomiali se c'è un isomorfismo e.c. tra la curva e $(\mathbb{F}_q, +)$.

4. SCELTA DELLA CURVA

Scegliere la curva, sicurezza

Come possiamo scegliere i parametri di una curva ellitica **E** per difenderci dagli attacchi generici e specifici?

Attacco	**Precauzione**
Pohlig-Hellman + Pollard ρ + Baby step Giant step	N deve avere un fattore r tale che $\sqrt{r}$ risulti essere un numero intrattabile di operazioni
Isomorfismo a $(\mathbb{F}_q, +)$	il fattore più grande di N deve essere diverso da q
MOV	$q^s \not\equiv 1 \mod r$ per s piccolo
Isomorfismo allo Jacobiano	m primo o se m è composto bisogna scegliere una curva opportuna

Scegliere la curva, efficienza

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

Scegliere la curva: Procedura Classica

1. Scelta del livello di sicurezza n (dove n è la dimensione in bit della cardinalità del gruppo generato dal punto base), tenendo conto che la sicurezza reale sarà però data da $n = n/2$.
2. Scelta del campo (caratteristica e cardinalità)
3. Scelta dei coefficienti della curva
4. Calcolo dell'ordine della curva (algoritmi di tipo Schoof)
5. Controllo sulla resistenza agli attacchi
6. Scelta del punto base P (avente ordine primo grande)

Scegliere la curva, Procedura della Moltiplicazione Complessa

Questo metodo permette di generare curve con ordine prefissato. E' veloce per curve con un "piccolo" numero della classe, per le quali però si pensa possano essere scoperti nuovi attacchi specifici.

1. Scelta del livello di sicurezza n
2. Scelta del campo
3. Scelta dell'ordine del punto base
4. Generazione dei coefficienti e di un punto base P

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.

5. Accenno ad applicazioni di ECC

Vantaggi dell'ECC : { **EFFICIENZA** / **SICUREZZA**

- 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 $\rightsquigarrow$ 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 adempiere alle prestazioni richieste per l'uso commerciale

Obiettivo:

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

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