# Introduzione alla crittografia basata su curve ellittiche

Lezione tenuta dal
Prof. P. D'Arco

Presentazione di:

Francesco Apicella
Raffaele De Feo
Ermanno Travaglino

## LE CURVE ELLITTICHE

Una curva ellittica è una curva definita da un'equazione in due incognite del tipo:

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

Le curve ellittiche svolgono un ruolo importante nella teoria dei numeri. Per esempio furono utilizzate da Andrew Wiles per la risoluzione dell'ultimo teorema di Fermat.



Prof. Andrew Wiles

**Applicazioni in Crittografia**



Neal Koblitz

Le curve ellittiche definite su campi finiti hanno molteplici applicazioni in crittografia. Il loro utilizzo venne proposto indipendentemente da Neal Koblitz e Victor S. Miller nel 1985.

2

# LE CURVE ELLITTICHE

**Obiettivo**

Il nostro obiettivo è comprendere l'utilizzo delle curve ellittiche attraverso la realizzazione di un crittosistema a chiave pubblica simile al crittosistema di El-Gamal.



El-Gamal



**Passi**

- ✓ Crittosistema di El-Gamal
- ✓ Introduzione e definizione di una curva ellittica sui numeri reali
- ✓ Definizione di una curva ellittica su un campo finito
- ✓ ECIES

3

# CRITTOSISTEMA DI EL-GAMAL

**Set-up**

- Sia p un primo di grossa taglia
- Sia $Z^*_p$ il gruppo moltiplicativo di $Z_p$
- Sia $\alpha$ un generatore di $Z^*_p$, i.e.



$$< \alpha > = \{\alpha^0, \alpha^1, \ldots \ldots, \alpha^{p-2}\} = \{1,2,\ldots,p,\ldots,p-1\} = Z^*_p$$

Si scelga uniformemente a caso a $\epsilon_R \{1, \ldots \ldots, p-2\}$ e sia $\beta = \alpha^a$

A questo punto abbiamo a disposizione la chiave privata e la chiave pubblica

**Chiave pubblica** $(p, \alpha, \beta)$



**Chiave privata (a)**

4

# CRITTOSISTEMA DI EL-GAMAL

**Cifratura:** Sia $x \in Z^*_p$ il messaggio da cifrare.

Si scelga $k \in_R \{1,\ldots \ldots,p-2\}$

$y_1 = \alpha^k \bmod p$

$y_2 = x\,\beta^k \bmod p$

$e_{pub}(x) = (y_1,y_2)$



**Decifratura:** Sia $(y_1,y_2)$ il messaggio da decifrare.

$d_{priv}(y_1,y_2) = y_2\,(y_1^a)^{-1} \bmod p$

**Correttezza:**

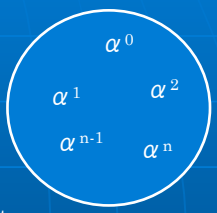
$$x\,\beta^k\,[(\alpha^k)^a]^{-1} \bmod p = x\,\beta^k\,[(\alpha^a)^k]^{-1} \bmod p = x\,\beta^k\,(\beta^k)^{-1} \bmod p = x$$

messaggio decifrato

5

# CRITTOSISTEMA DI EL-GAMAL

Per poter implementare il crittosistema di El-Gamal, abbiamo bisogno di:




$G = <\alpha>$

**Operazioni effettuate**

**Cifratura**

$\beta = \alpha^a = \alpha\ \alpha\ \ldots\ \alpha$
effettuate "a" moltiplicazioni

$y_1 = \alpha\ \alpha\ \ldots\ \alpha$
effettuate "k" moltiplicazioni

$x\,\beta^k = x\ \beta\ \beta\ \ldots\ \beta$
effettuate "k+1" moltiplicazioni



**Decifratura**

$y_2\,(y_1\ y_1\ \ldots\ y_1)^{-1}$

"a+1" moltiplicazioni più il calcolo dell'inverso moltiplicativo

6

# CRITTOSISTEMA DI EL-GAMAL

**In conclusione serve un gruppo** (G, ◦)**:**

- ✓ G chiuso rispetto all'operazione ◦
- ✓ L'operazione ◦ associativa
- ✓ Esistenza di un elemento neutro rispetto a ◦
- ✓ Esistenza dell'inverso per ogni elemento appartenente a G



- La sicurezza del crittosistema di El-Gamal si basa sulla presunta difficoltà di risolvere il DLP (problema del logaritmo discreto).
- Se riuscissimo a risolvere efficientemente il DLP, El-Gamal non sarebbe sicuro.

7

# DISCRETE LOGARITHM PROBLEM

**Cerchiamo di capirne di più**

Sia p un numero primo *di grossa taglia* e sia g un generatore *g* di $Z^*_p$. Per ogni y in $Z^*_p$, risulta

$$y = g^x \pmod p$$

**Problema:** dati *g*, *y* e *p* determinare l'intero *x*.

Affinché DLP in $Z^*_p$ sia computazionalmente difficile (allo stato attuale delle conoscenze) è necessario che il primo p sia almeno 1024 bit

Efficienza del crittosistema

- lunghezza del messaggio cifrato: 2048 bit
- Esponenziazione modulare (operazione pesante)



8

# CRITTOSISTEMA DI EL-GAMAL EFFICIENZA

Possiamo migliorare l'efficienza del crittosistema di El-Gamal mantenendo lo stesso grado di sicurezza con:

- Cifrature "più corte"
- Computazioni più efficienti

trovando "ambienti" in cui i migliori algoritmi per risolvere il DLP che si conoscono impongano vincoli meno restrittivi



9

# COSA SERVE PER L'EFFICIENZA

- Il DLP deve risultare difficile (espresso in termini dell'operazione del gruppo G)
- Gli elementi di G devono essere rappresentabili con "meno bit"
- Le operazioni sugli elementi devono essere più efficienti

Esistono gruppi in cui il DLP è facile: si consideri il gruppo $(Z_p, +_{\text{mod } p})$

- ✓ $Z_p$ è chiuso rispetto all'operazione +
- ✓ + è associativa
- ✓ esiste l'elemento neutro
- ✓ esiste l'inverso additivo

$y = g + g + \ldots + g$ (x volte) quindi $y = gx \bmod p$

Problema FACILE

Infatti basta calcolare $g^{-1}$ (alg. di Euclide esteso) e risulta:

$g^{-1}y \bmod p = g^{-1}gx \bmod p = x$

10

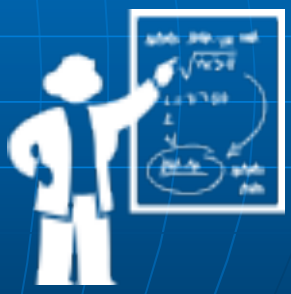
# CRITTOSISTEMA DI EL-GAMAL
# LA RICERCA DEL GRUPPO

Possiamo trovare un gruppo $(G,\circ)$ che va bene e raggiunge gli obiettivi di efficienza desiderati.

Per trovare questo gruppo abbiamo bisogno di alcuni concetti e strumenti matematici.

Infatti (G,+) è un insieme di **punti di una curva ellittica** definita su un **campo finito**, e munito di **un'operazione di somma sui punti** della curva opportunamente definita.

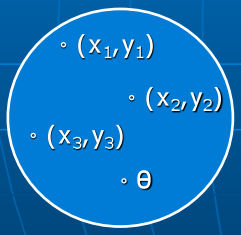
Cominciamo con l'introdurre le curve ellittiche sul campo reale.

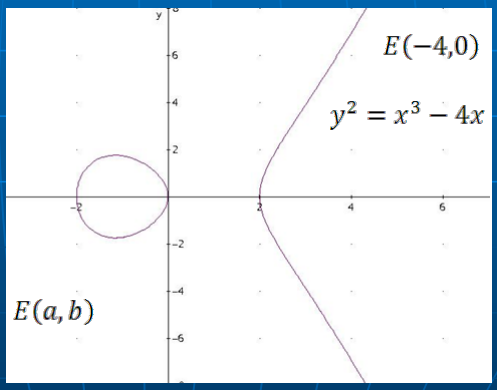


11

# CURVE ELLITTICHE SUI REALI

- **Definizione:** Siano $a,b \in \mathbb{R}$ t.c. $4a^3 + 27b^2 \neq 0$.
  Una curva ellittica non singolare è l'insieme E di soluzioni $(x,y) \in \mathbb{R}\times\mathbb{R}$ dell'equazione $y^2 = x^3 + ax + b$, più un punto speciale $\theta$ (detto punto all'infinito).




12

# CURVE ELLITTICHE SUI REALI

Proviamo a definire l'operazione di somma tra punti della curva.
Sia P ≡ $(x_1,y_1)$ e Q ≡ $(x_2,y_2)$.

Consideriamo tre casi:

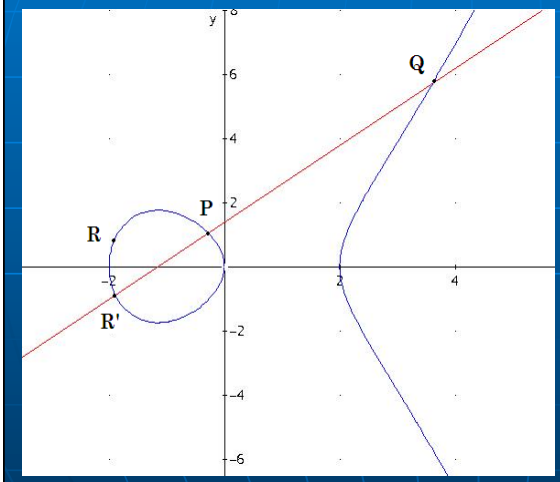
1. $x_1 \neq x_2$
2. $x_1 = x_2$ e $y_1 = -y_2$
3. $x_1 = x_2$ e $y_1 = y_2$



13

# CASO 1

Sia L la retta che passa attraverso P e Q




La retta L interseca la curva E in P e Q e in un ulteriore punto R'. Riflettendo R' rispetto all'asse delle ascisse si ottiene un punto R.
Definiamo P+Q=R

14

# CASO 1

Cerchiamo di capire come possiamo calcolare le coordinate del punto R

L'equazione della retta L è data da $y = \lambda x + \nu$

dove il coeff. angolare $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ e $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$

Per trovare i punti $L \cap E$ sostituiamo l'equazione di L nell'equazione di E ottenendo:

$(\lambda x + \nu)^2 = x^3 + ax + b \rightarrow \lambda^2 x^2 + \nu^2 + 2\lambda x \nu = x^3 + ax + b \rightarrow$
$x^3 - \lambda^2 x^2 + x(a - 2\lambda\nu) + b - \nu^2 = 0$

L'equazione risultante è un'equazione cubica sui reali avente due radici reali, e quindi anche la terza sarà reale. La somma delle tre radici deve essere uguale a $\lambda^2$, cioè l'opposto del coefficiente del termine quadratico

$x_1 + x_2 + x_3 = \lambda^2 \Leftrightarrow x_3 = \lambda^2 - x_1 - x_2$

15

# CASO 1

… la somma delle tre radici deve essere uguale a $\lambda^2$, cioè l'opposto del coefficiente del termine quadratico …

Esempio

$P(x) = (x - 2)(x-3)(x-4)$

$= (x^2 - 3x - 2x + 6)(x - 4)$

$= (x^3 - 4x^2 - 3x^2 - 12x - 2x^2 - 8x + 6x - 24)$

$= x^3 - (2+3+4)\,x^2 + (6+8+12)x - 24$

**opposto somma radici**

somma prodotti a due a due

opposto somma prodotti radici a tre a tre

# CASO 1

Quindi $x_3$ è l'ascissa del punto R'. Indichiamo con $-y_3$ l'ordinata. Un modo facile per calcolare $y_3$ è usare il coefficiente angolare $\lambda$ della retta L. Infatti è determinato da ogni coppia di punti della retta L. Cioè,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \Leftrightarrow y_3 = \lambda (x_1 - x_3) - y_1$$

Trovato $y_3$ abbiamo trovato il punto R.
Quindi, nel caso 1, abbiamo derivato una formula per calcolare $P + Q = (x_3, y_3)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda (x_1 - x_3) - y_1$$




17

# CASI 2 e 3

**Caso 2** $x_1 = x_2$ e $y_1 = -y_2$

Definiamo $(x,y) + (x,-y) = \theta$ per tutti i punti $(x,y) \in E$
Il punto $\theta$ è l'elemento unitario (identità), cioè $P + \theta = \theta + P = P$, per ogni $P \in E$. Inoltre, per ogni punto $(x,y) \in E$, il punto $(x,-y)$ funge da inverso.

**Caso 3** $x_1 = x_2$ e $y_1 = y_2$

In questo caso stiamo sommando P a se stesso. Supponiamo $y_1 \neq 0$ altrimenti vale il caso precedente. E' possibile dimostrare che valgono le stesse regole di calcolo del caso 1. Varia soltanto il calcolo di $\lambda$ che risulta uguale a:

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

**In conclusione** abbiamo costruito un gruppo E munito di un'operazione (+) tale che:

- ✓ E è chiuso rispetto a +
- ✓ L'operazione di somma (+) è commutativa
- ✓ $\theta$ è l'elemento neutro
- ✓Ogni punto di E ha un inverso
- ✓ L'operazione di somma (+) è associativa (complicato da mostrare)

18

# CURVE ELLITTICHE SU CAMPI FINITI

**Cos'è un campo finito:**

Un campo finito F consiste di un numero finito di elementi su cui sono definite due operazioni che godono di alcune proprietà (prop. di un campo).

L'ordine di un campo finito è il numero di elementi del campo.



Molti sistemi crittografici basati su curve ellittiche restringono l'ordine del campo o ad un primo dispari oppure a una potenza di *2*.

GF(p)

GF($2^n$)

19

# CURVE ELLITTICHE SU CAMPI FINITI

Invece del campo reale R, consideriamo il campo finito ($Z_p$, +, ◦) con p primo

**Definizione:**

Sia p > 3 primo

La curva ellittica $y^2 = x^3 + ax + b$ su $Z_p$ è l'insieme delle soluzioni $(x,y) \in Z_p \times Z_p$ alla congruenza:

$$y^2 = x^3 + ax + b \bmod p$$

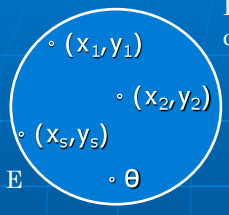
dove $a,b \in Z_p$ sono costanti tali che $4a^3 + 27\,b^2 \neq 0 \pmod p$

con un punto speciale $\theta$, detto punto all'infinito



20

# L'OPERAZIONE DI SOMMA




L'operazione di somma $+_E$ tra punti di E si definisce come segue:

Siano $P = (x_1,y_1)$ e $Q = (x_2,y_2)$ punti di E

Se $x_2 = x_1$ e $y_2 = -y_1$ allora $P +_E Q = \theta$

Altrimenti dove:

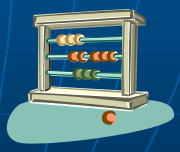
$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda (x_1 - x_3) - y_1$$

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

Risulta $\forall P \in E$

$$P +_E Q = Q +_E P$$



21

# CALCOLO DEI PUNTI

**Nota:** Non esiste come nel caso reale un'interpretazione geometrica per l'operazione di somma ma $(E, +_E)$ costituisce un gruppo abeliano

Esempio: Il nostro campo $Z_{11} = \{0,1,2,\ldots,10\}$

La nostra curva $E = y^2 = x^3 + x + 6 \bmod 11$

**Calcoliamo i punti di E**

Possiamo calcolare, per ogni $x \in Z_{11}$, il valore $z = x^3 + x + 6 \bmod 11$

Possiamo poi applicare il criterio di Eulero per vedere se z è un residuo quadratico ( i.e. $\exists w: w^2 = z \bmod p$ )

**Criterio di Eulero:** sia p un primo dispari allora a è un residuo quadratico se e solo se $a^{(p-1)/2} \equiv 1 \bmod p$

22

# CURVE ELLITTICHE SU CAMPI FINITI CALCOLO DEI PUNTI

Inoltre se p ≡ 3 mod 4 è possibile calcolare le radici di z mod p applicando la formula:

$$\pm z^{\frac{p+1}{4}} \bmod p$$

nel nostro caso significa $\pm z^{\frac{11+1}{4}} \bmod 11 \rightarrow \pm z^3 \bmod 11$

| x | $x^3+x+6$ mod 11 | Test di Eulero | y |
|---|---|---|---|
| 0 | 6 | NO | |
| 1 | 8 | NO | |
| 2 | 5 | SI | 4,7 |
| 3 | 3 | SI | 5,6 |
| 4 | 8 | NO | |
| 5 | 4 | SI | 2,9 |
| 6 | 8 | NO | |
| 7 | 4 | SI | 2,9 |
| 8 | 9 | SI | 3,8 |
| 9 | 7 | NO | |
| 10 | 4 | SI | 2,9 |

punti della curva ellittica

$y^2 = x^3 + x + 6 \bmod 11$

la curva ha in totale **13** punti compreso il punto all'infinito

23

# CALCOLO DELLE POTENZE

**Teorema:** se l'ordine di un gruppo è primo, il gruppo è ciclico e ogni elemento (escluso $\theta$) di G è un generatore.

Sia $\alpha = (2,7)$ il generatore. Allora possiamo calcolare le "potenze" di $\alpha$ (poiché l'operazione sugli elementi di E è $+_E$ le potenze sono multipli di $\alpha$)

Per calcolare $2\alpha = \alpha + \alpha = (2,7) +_E (2,7)$ dobbiamo prima calcolare $\lambda$

$\lambda = (3 \times 2^2 + 1)(2 \times 7)^{-1} \bmod 11$
$= 2 \times 3^{-1} \bmod 11$
$= 2 \times 4 \bmod 11$
$= 8$



Calcoliamo $(x_3,y_3)$

$x_3 = 8^2 - 2 - 2 \bmod 11 = 5$

$y_3 = 8(2-5) - 7 \bmod 11 = 2$

quindi $2\alpha = (5,2)$

24

# CALCOLO DELLE POTENZE

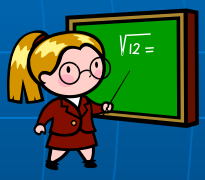
Calcoliamo la potenza successiva $3\alpha = \alpha + \alpha + \alpha = 2\alpha + \alpha = (5,2) +_E (2,7)$

$\lambda = (7 - 2)(2 - 5)^{-1} \bmod 11 = 5 \circ 7 \bmod 11 = 2$

Calcoliamo $(x_3,y_3)$

$x_3 = 2^2 - 5 - 2 \bmod 11 = 8$

$y_3 = 2(5 - 8) - 2 \bmod 11 = 3$



quindi: $3\alpha = (8,3)$

Proseguendo si ottiene la sequenza completa di punti di E

| | | |
|---|---|---|
| $\alpha = (2,7)$ | $2\alpha = (5,2)$ | $3\alpha = (8,3)$ |
| $4\alpha = (10,2)$ | $5\alpha = (3,6)$ | $6\alpha = (7,9)$ |
| $7\alpha = (7,2)$ | $8\alpha = (3,5)$ | $9\alpha = (10,9)$ |
| $10\alpha = (8,8)$ | $11\alpha = (5,9)$ | $12\alpha = (2,4)$ |

25

# REALIZZAZIONE DI UN CRITTOSISTEMA EL-GAMAL-LIKE

Supponiamo di scegliere come generatore $\alpha = (2,7)$, e che la chiave privata di "Bob" sia 7. Allora con El-Gamal:



Quindi $\beta = 7\alpha \rightarrow (7,2)$

Chiave privata

7



Chiave pubblica

( E , $\alpha$ , $\beta$ , 13 )

Numero di punti in E

La cifratura risulta:

$$e_k = (x,k) = (k(2,7), x +_E k(7,2))$$

($y_1 \in E$ under $\alpha$; $y_2 \in E$ under $\beta$)

dove $x \in E$ e $0 \le k \le 12$

La decifratura risulta:

$$d_k(y_1,y_2) = y_2 - 7y_1 = y_2 +_E 7\,(-y_1)$$

26

# ESEMPIO

Supponiamo che "Alice" voglia cifrare il messaggio x = (10,9)

se sceglie k=3 allora

$y_1 = 3(2,7) = (8,3)$

$y_2 = (10,9) +_E 3(7,2) \rightarrow (10,9) +_E (3,5) = (10,2)$



Quindi il cifrato risulta ((8,3),(10,2))



Ora se "Bob" riceve il cifrato, decifra come segue

$x = (10,2) - 7(8,3) = (10,2) - (3,5) = (10,2) +_E (3,6) = (10,9)$

messaggio

La decifratura è CORRETTA!

27

# OSSERVAZIONI

**Problema:** vogliamo che il DLP sia difficile

**Teorema di Hasse:** sia E una curva ellittica definita su $Z_p$ (p > 3 e primo). Il numero di punti di E, indicato con #E, risulta:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$$




Quindi possiamo dire che su E ci saranno circa p punti. Il numero preciso può essere calcolato tramite un algoritmo efficiente (algoritmo di Schoof)

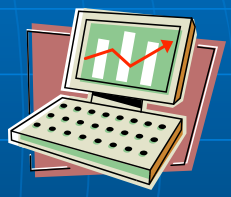
**Nota:** non è detto che E sia ciclico. Se #E è primo o è un prodotto di primi distinti, allora è ciclico

28

# OSSERVAZIONI

In generale esistono risultati di teoria dei numeri che permettono di capire se una curva E possiede un sottogruppo ciclico H in cui il DLP è difficile e può quindi essere usato per implementare il crittosistema di El-Gamal

La versione del cifrario di El-Gamal implementato su E ha due problemi:





- ✓ Il messaggio deve essere un punto di E
- ✓ Il cifrato è costituito da 4 valori di $Z_p$

Possiamo fare meglio?

29

# POINT COMPRESS –POINT DECOMPRESS

Dato x ci sono due valori di y tali che $y^2 = x^3 + ax + b \bmod p$.
Questi due valori sono uno il negato dell'altro. Poiché p è primo:

- ✓ uno sarà pari e l'altro dispari
- ✓ è possibile definire un punto P = (x,y) specificando il valore di x e usare un bit per indicare la parità.

Formalmente possiamo definire un'operazione di compressione e decompressione di un punto

**Point Compress:**

$E \setminus \{\theta\} \rightarrow Z_p \times Z_2$

Point-Compress (P) = (x,y mod 2)

dove P=(x,y) ϵ E



30

# POINT COMPRESS – POINT DECOMPRESS

L'operazione inversa, Point-Decompress, ricostruisce il punto P(x,y)

**Algoritmo:**



Point_decompress(x,i)

$z \leftarrow x^3 + ax + b \bmod p$

se z non è un residuo quadratico

return "fallito"

altrimenti

$y \leftarrow \sqrt{z} \bmod p$

se $y \equiv i \pmod 2$ return (x, y)

altrimenti return (x, p – y)

31

# SIMPLIFIED ECIES (ELLIPTIC CURVE INTEGRATED ENCRYPTION SCHEME)

Sia E una curva ellittica definita su $Z_p$ (p > 3 primo) t.c. E contiene un sottogruppo H = < P > di ordine primo n, in cui DLP è intrattabile. Sia Q = mP.

Chiave privata

$m \in Z^*_n$



Chiave pubblica

( E , P , Q , n )

**Cifratura**

Sia $x \in Z^*_p$ il messaggio da cifrare

scegliamo a caso $k \in Z^*_n$

calcoliamo $kQ = (x_0,y_0)$ con $x_0 \neq 0$

calcoliamo $e_k(x,k) = (\text{POINT_COMPRESS}(kP) , x\, x_0 \bmod p)$

**Decifratura**

Sia $y = (y_1,y_2)$ il messaggio da decifrare con $y_1 \in Z_p \times Z_2$ , $y_2 \in Z^*_p$

definiamo $d_k(y) = y_2(x_0)^{-1} \bmod p$

dove $(x_0,y_0) = m \circ \text{POINT_DECOMPRESS}(y_1)$

32

# ESEMPIO

Sia P = (2,7) e sia m=7 la chiave privata di "Bob"

"Bob" calcola Q = 7P = 7(2,7) = (7,2)

La chiave pubblica è ( E , (2,7) , (7,2) ,13 )



**"Alice" vuole cifrare x = 9**

Sceglie k=6. Calcola kQ = 6(7,2) = (8,3)

calcola kP = 6(2,7) = (7,9)

calcola POINT_COMPRESS (7,9) = (7,1)

calcola $y_2 = 8 \times 9 \bmod 11 = 6$

$e_k(9,6) = ((7,1),6)$



**"Bob" decifra y come segue:**

calcola POINT_DECOMPRESS(7,1) = (7,9)

calcola $(x_0,y_0) = 7(7,9) = (8,3)$

$d_k = ((7,1),6) = 6 \times 8^{-1} \bmod 11 = 9$

33

# EFFICIENZA DEI CRITTOSISTEMI BASATI SU CURVE ELLITTICHE

| Sym | ECC | RSA |
|---|---|---|
| 56 | 112 | 512 |
| 80 | 160 | 1024 |
| 112 | 224 | 2048 |
| 128 | 256 | 3072 |
| 192 | 384 | 7680 |
| 256 | 512 | 15360 |

Questa tabella mostra la dimensione delle chiavi dei crittosistemi a parità di sforzo computazionale richiesto dall'analisi crittografica



34

## SCAMBIO DI CHIAVI DIFFIE-HELLMAN

Sia E una curva ellittica e P un punto di E di ordine n







**"Alice"** **"Bob"**

Sceglie un intero $n_A < n$
calcola $P_A = n_A P$
invia $P_A$ a "Bob"

$P_A$ →

Sceglie un intero $n_B < n$
calcola $P_B = n_B P$
invia $P_B$ ad "Alice"

← $P_B$

Calcola

$k_{AB}\, n_A P_B = n_A (n_B P) = n_A n_B P$

Calcola

$k_{AB} = n_B P_A = n_B (n_A P) = n_A n_B P$

La chiave di cifratura/decifratura può essere calcolata applicando una funzione di derivazione al punto $k_{AB}$ sia da "Alice" che da "Bob"

35

## SQUARE AND MULTIPLY

L'operazione principale nella ECC è kP, i.e. calcolare multipli di un punto P. Si può fare questa operazione in modo efficiente

**Esponenziazione modulare**

$x^c$

$c = c_{l-1}\, c_{l-2} \ldots c_0$

$x^c \bmod n$

**SQUARE AND MULTIPLY (x,c,n)**

$z \leftarrow 1$

**for** $i \leftarrow l - 1$ **downto** 0 **do**

$z \leftarrow z^2 \bmod n$

**if** $c_i = 1$ **then** $z \leftarrow (zx) \bmod n$

**return** z




36

# SQUARE AND MULTIPLY

**Nota:** su una curva ellittica l'inverso additivo di un punto è facile da calcolare e.g. P = (x,y) → (x,-y)

Sia c un intero. Una rappresentazione binaria con segno di c è un'equazione della forma:

$$\sum_{i=0}^{l-1} c_i \circ 2^i \qquad \text{dove } c_i \in \{1,0,-1\} \textit{ per ogni } i$$

**Esempio**

$11 = 8 + 2 + 1 = 16 - 4 - 1$

quindi $(c_4,c_3,c_2,c_1,c_0)$

→ (0,1,0,1,1)

→ (1,0,-1,0, -1)



Sono entrambe rappresentazioni binarie, con segno, di 11

37

# DOUBLE AND (ADD OR SUBSTRACT)

Sia P un punto di ordine n di una curva ellittica

Data la rappresentazione binaria con segno $(c_{l-1}, \ldots, c_0)$ di un intero $0 \leq c \leq n-1$ è possibile calcolare il multiplo cP attraverso una serie di raddoppi (2P), addizioni e sottrazioni, usando il seguente algoritmo:

DOUBLE AND (ADD OR SUBSTRACT) $(P,(c_{l-1}, \ldots, c_0),n)$

$Q \leftarrow 0$

for $i \leftarrow l-1$ downto 0 do

**$Q \leftarrow 2Q$**

**if $c_i = 1$ then $Q \leftarrow Q + P$**

**else if $c_i = -1$ then $Q \leftarrow Q - P$**

**return Q**



38

# RAPPRESENTAZIONE NAF (NON ADJACENT FORM)

Una rappresentazione binaria con segno $(c_{l-1}, \ldots, c_0)$ di un intero c è detta in forma non adiacente ( NAF ) se non ci sono due $c_i$ consecutivi diversi da zero

**Trasformazione**

E' semplice trasformare la rappresentazione binaria di un intero c (positivo) in rappresentazione NAF.

L'idea alla base della trasformazione è di sostituire le sottostringhe di forma (0,1,1, … , 1) nella rappresentazione binaria tramite la sottostringa (1,0, … ,0,-1).

Tale sostituzione non cambia il valore di c poiché vale l'identità

$$2^i + 2^{i-1} + \ldots + 2^j = 2^{i+1} - 2^j$$

dove $i > j$

Questo processo viene ripetuto fin quando è necessario, partendo dai bit meno significativi e procedendo verso sinistra

39

# RAPPRESENTAZIONE NAF (NON ADJACENT FORM)

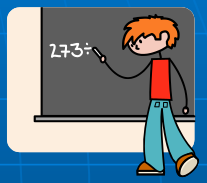
**Esempio**

1111 0011 0111

1111 0 011 1 00 –1

11110 100 –1 00 –1

1000 –10100 – 100 –1 → NAF




Quindi ogni intero non negativo ha una rappresentazione NAF.
Si può dimostrare che tale rappresentazione è UNICA

In genere una rappresentazione NAF contiene **più zeri** rispetto alla rappresentazione standard in binario di un intero positivo.

Infatti può essere dimostrato che un intero di l bit, in media, contiene:

- ✓ $\frac{l}{2}$ bit = 0 nella rappresentazione binaria tradizionale
- ✓ $\frac{2}{3}$ $l$ bit = 0 nella rappresentazione NAF

40

# OSSERVAZIONI



DOUBLE AND ADD ($P, c_{l-1}, \ldots, c_0, n$) binaria tradizionale

$l$ raddoppi

$l / 2$ addizioni



DOUBLE AND (ADD OR SUBSTRACT)

$l$ raddoppi

$l / 3$ add. o sub.

Assumendo che un'operazione di raddoppio richieda circa lo stesso tempo di una add o substract il rapporto tra i tempi medi di soluzione tra i due algoritmi è

$$\frac{l+\frac{l}{2}}{l+\frac{l}{3}} \rightarrow \frac{\frac{3}{2}l}{\frac{4}{3}l} \rightarrow \frac{3}{2}l \cdot \frac{3}{4}l \rightarrow \frac{9}{8} \rightarrow 1.125$$

41

C'è, quindi, un guadagno dell' 11% circa

# Riferimenti


- Doug Stinson, "Cryptography: Theory and practice", CRC Press 2006
- Willian Stallings, "Crittografia e sicurezza delle reti", Prentice Hall 2007.
- Un link utile http://www.certicom.com/index.php/10-introduction
- A. H.Koblitz and N. Koblitz and A. Menezes, Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift, http://eprint.iacr.org/2008/390.pdf