

CRITOGRAFIA

lezione del 25/11



Protocollo EL GAMAL su curve ellittiche

$E_p(Q, b)$ $m < p$ messaggio

1) $m \rightarrow P_m \in E_p(Q, b)$

Algoritmo di Koblitz.

h intero $(m+1)h < p$

KOBLITZ (m, h, Q, b, p)

for ($i=0$; $i < h$; $i++$) {

$$x = mh + i;$$

$$z = (x^3 + ax + b) \bmod p$$

if (z è un residuo quadrato) {

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

}

$$y \quad \text{return } P_m = (x, y)$$

return "falso"

→ costo polinomiale
perché si lavora modulos
un numero primo

Prob. fallimento \rightarrow per h volte $\geq n$ non è un riuscito
quasiorbitico

$$\approx \left(\frac{1}{2}\right)^h$$

Prob. successo $\rightarrow 1 - \left(\frac{1}{2}\right)^h$

$$P_m = (x, y)$$

$$m = \left\lfloor \frac{x}{h} \right\rfloor = \left\lfloor \frac{mh + i}{h} \right\rfloor = \left\lfloor m + \frac{i}{h} \right\rfloor = m$$

21

Scombi di messaggi

$$E_p(a, b)$$

punto base B di ordine n elevato

$$B \in E_p(a, b)$$

ordine (B) = più piccolo intero n tc.

$$nB = 0$$

Ogni utente costruisce la sua coppia

$$\langle k[\text{pub}], k[\text{priv}] \rangle$$

utente v

$$k[\text{priv}] = n_v < n \quad \text{scelto casuale}$$

$$k[\text{pub}] = n_v B = P_v$$

Alice (mittente)

$m \rightarrow P_m$ (Alg. di Koblitz)

- Sceglie $r < n$ casuale ($n = \text{ordine del punto}$
base B)
- Calcola $V = rB$ (tempo polinomiale, alg. non doppia
ripetuti)

- Calcola $W = P_m + rP_{Bob}$

$\underbrace{\qquad\qquad\qquad}_{\text{messaggio}}$ $\underbrace{r}_{\text{chiave pubblica del destinatario}}$

$$V, W \in E_p(\mathbb{Q}, \mathbb{F})$$

- invia le coppie $\langle V, W \rangle \in \mathbb{F}$

Bob (Deshinskeri)

- receive $\langle V, W \rangle$
- decide colorando

$$W - n_{\text{Bob}} \cdot V = P_m = (x, y)$$

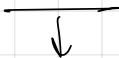
ricava $m = \left\lfloor \frac{x}{h} \right\rfloor$

Dimostrazione Correttezza

$$\begin{aligned} W - n_{\text{Bob}} \cdot V &= P_m + r P_{\text{Bob}} - n_{\text{Bob}} V = \\ &= P_m + r (n_{\text{Bob}} B) - n_{\text{Bob}} (r B) = P_m \end{aligned}$$

Attacchi' penù:

1) trovare $n_{B|B}$ da $P_{B|B} = \frac{n_{B|B}}{B}$



Log. discreto in C.E.

2) Conoscendo r , si può calcolare:

$$W = P_m + r P_{B|B}$$



$$P_m = W - \underbrace{r P_{B|B}}$$

$$V = r B$$

\downarrow log. discreto

Logaritmo discreto algoritmo modulare

index
calculator

$$O\left(2^{\sqrt{b \log b}}\right)$$

b = bit del modulo

modulo p

p minore di b bit

\mathbb{Z}_p (campo)

Logaritmo discreto in CE

pollard - p

$$O\left(2^{\frac{b}{2}}\right)$$

b : bit
dell'ordine
di B

Sicurezza della crittografia su curve ellittiche

È legata alla **difficoltà di calcolare il logaritmo discreto** di un punto, problema per cui non è noto alcun algoritmo efficiente di risoluzione

- Nonostante manchi una dimostrazione formale di intrattabilità, questo problema è considerato **estremamente difficile**
- in particolare **molto più difficile** dei tradizionali problemi della fattorizzazione degli interi e del logaritmo discreto nell'algebra modulare
 - ◆ per questi problemi esiste un **algoritmo subesponenziale (index calculus)** che può essere utilizzato per attaccare sia il protocollo DH che il cifrario RSA
 - ◆ L'algoritmo index calculus frutta una struttura algebrica dei campi finiti che non è presente sulle curve ellittiche
 - ◆ Ad oggi nessuno è stato capace di progettare algoritmi di tipo index calculus per il problema del logaritmo discreto per le curve ellittiche: quindi i protocolli per tali curve sembrano invulnerabili a questo tipo di attacchi
- Il migliore attacco noto (**Pollard p**) richiede in media $O(2^{b/2})$ operazioni per chiavi di b bit ed è dunque **pienamente esponenziale**

Esistono attacchi efficaci contro alcune famiglie di curve, ma queste famiglie sono note e facilmente evitate

Sicurezza

Tabella di equivalenza fra i livelli di sicurezza dei cifrari simmetrici rispetto ai cifrari a chiave pubblica [NIST, National Institute of Standards and Technology]

$O(2^b)$	$O(2^{\sqrt{b \log b}})$	$O(2^{b/2})$
TDEA, AES b (bit della chiave)	RSA e DH b (bit del modulo)	ECC b (bit dell'ordine)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Riporta la dimensione in bit delle chiavi che garantiscono livelli di sicurezza equivalenti nei tre diversi sistemi

due sistemi si considerano di sicurezza equivalente se è richiesto lo stesso costo computazionale per forzarli

È interessante il confronto tra RSA ed ECC

la differenza tra i cifrari asimmetrici RSA/DH ed ECC diventa evidente al crescere del livello di sicurezza richiesto

“Misura universale di sicurezza”

Arjen K. Lenstra, Thorsten Kleinjung e Emmanuel Thom

Universal Security - From Bits and Mips to Pools, Lakes - and Beyond.

Number Theory and Cryptography, 2013

Idea

*misurare la quantità di energia necessaria per forzare un sistema
e confrontarla con la quantità di acqua che quell'energia potrebbe
far bollire*

Forzare un cifrario RSA a 228 bit richiede meno energia di quella
necessaria per far bollire un cucchiaino di acqua

L'energia necessaria per forzare un sistema basato su curve
ellittiche a 228 bit potrebbe far bollire tutta l'acqua sulla Terra