La crittografia a curve iperellittiche

Dott. Stefania Vanzetti

Torino 2011. Crittografia a chiave pubblica: oltre RSA

Università degli Studi di Torino

13 maggio 2011

1.LE CURVE IPERELLITTICHE

Motivazioni al loro utilizzo

Motivazioni al loro utilizzo in crittografia:

- Sono un'alternativa alle curve ellittiche
- Si riesce ad associare una struttura di gruppo abeliano ad ogni curva iperellittica
- Si possono usare i metodi crittografici che si basano sulla difficoltà del logaritmo discreto

però

- L'operazione di gruppo è più complessa
- Non tutte le curve iperellittiche sono adatte, bisogna sceglierle in base al genere, all'ordine del gruppo e al campo su cui sono definite.

Cosa sono?

Definizione (Curva Iperellittica)

Una Curva Iperellittica $\mathbf{C}$ *su un campo* $\mathbb{F}_q$ *di genere* g *è l'insieme dei punti su* $\mathbb{F}_q \times \mathbb{F}_q$ *che soddisfano:*

$$\mathbf{C}: \; y^2 + h(x)y = f(x)$$

dove

1. $h(x) \in \mathbb{F}_q[x]$ *è un polinomio di grado minore o uguale a* g
2. $f(x) \in \mathbb{F}_q[x]$ *è un polinomio di grado* $2g + 1$
3. $\mathbf{C}$ *non presenta punti singolari su* $\overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$.

Nota

Le Curve Ellittiche sono Curve Iperellittiche di genere $g = 1$

2.GRUPPO JACOBIANO DELLA CURVA

Jacobiano di una curva iperellittica

Data $\mathbf{C}$, possiamo definire delle combinazioni finite di punti della curva, che chiameremo *divisori* come:

$$D = \sum m_P P \quad con\ m_P \in \mathbb{Z},\ P \in \mathbf{C}$$

I divisori formano un gruppo abeliano additivo $Div(\mathbf{C})$:

$$\sum m_P P + \sum n_P P = \sum (m_P + n_P) P$$

La somma $\sum m_P$ è il grado di D. L'insieme dei divisori di grado 0 forma un sottogruppo $Div(\mathbf{C})^0$ di $Div(\mathbf{C})$.

Jacobiano di una curva iperellittica

Il *campo delle funzioni* è l'insieme delle frazioni razionali su $\mathbf{C}$

$$\mathbb{F}_q(\mathbf{C}) = Frac\left(\mathbb{F}_q[x,y]/(y^2 + h(x)y - f(x))\right)$$

Theorem

Data una funzione razionale ϕ le si può sempre associare un divisore sulla chiusura proiettiva di C (c'è in più $P_\infty = [0:1:0]$)

I divisori delle funzioni razionali sono tutti di grado 0, sono detti divisori principali $\mathbf{P}$ e formano un sottogruppo di $Div(\mathbf{C})^0$.

Jacobiano di una curva iperellittica

Definizione (Jacobiano di $\mathbf{C}$)

Lo Jacobiano di $\mathbf{C}$ *è il gruppo quoziente*

$$J(\mathbf{C}) = Div(\mathbf{C})^0/\mathbf{P}$$

Quindi $D_1, D_2 \in Div(\mathbf{C})^0$ sono equivalenti se $D_1 - D_2 \in \mathbf{P}$.

Ogni classe d'equivalenza possiede un unico divisore D, detto *divisore ridotto*, di forma

$$D = \sum m_P P - (\sum m_P) P_\infty$$

tale che $\sum m_P \leq g$.

HCC

Lo Jacobiano $J(\mathbf{C})$ è un gruppo abeliano rispetto alla somma sui divisori usato per implementare i crittosistemi HC.

I crittosistemi saranno quelli tradizionali utilizzati sui gruppi finiti, ad esempio:

1. Diffie Hellman (scambio delle chiavi)
2. El Gamal (cifratura)

3.SOMMA NELLO JACOBIANO

Rappresentazione di Mumford dei divisori

Per implementare l'operazione di somma sullo Jacobiano dobbiamo esprimere i divisori in modo differente.

Ad ogni divisore dello Jacobiano si può associare una coppia di polinomi $(a(x), b(x))$ a coefficienti in $\mathbb{F}_q$, dove:

- $deg(b) < deg(a) \leq g$
- a monico
- $a | b^2 + bh - f$

L'ultima condizione permette di capire che l'unico elemento di $J(\mathbf{C})$ rappresentato da tali polinomi è

$$D = MCD(div(a(x)), div(b(x) - y))$$

che si indica come $D = div(a, b)$.

Algoritmo di Cantor

Consta di due parti:

Composizione: Riceve in input due divisori ridotti $D_1 = div(a_1, b_1)$ e $D_2 = div(a_2, b_2)$ e restituisce un divisore $D \sim D_1 + D_2$ di grado $\leq 2g$. I due passi più costosi utilizzano l'algoritmo di Euclide per il calcolo del MCD fra polinomi.

Riduzione: Riceve in input un divisore D e restituisce un divisore ridotto $D' \sim D$, ovvero il rappresentante speciale della classe di D. Ad ogni passo il grado di D diminuisce di 2, al massimo sono necessari $\lceil \frac{g}{2} \rceil$ passi.

NUCOMP

Idea: Fondere i passi di composizione e di riduzione: questo permette di lavorare con dei polinomi di grado minore rispetto a prima e rende meno costosa la riduzione (alla fine del corpo principale dell'algoritmo, se il divisore trovato non è già ridotto, servono al più due ulteriori passi di riduzione).

Risultato: asintoticamente è uguale all'algoritmo di Cantor, ma in pratica svolge un numero di operazioni minore nella maggior parte dei casi.

Moltiplicazione scalare

Nella maggior parte dei protocolli crittografici è necessario calcolare un multiplo del divisore in questione e quindi sommarlo più volte a se stesso.

Algoritmi specifici per questo problema:

1. usando l'algoritmo di Cantor si ottengono divisori di grado molto elevato, esistono algoritmi per velocizzare il passo di riduzione.
2. NUDPL: versione del NUCOMP specifica per il caso in cui i due addendi coincidono.

Quale algoritmo in pratica

La scelta dipende dal genere della curva:

- $g = 2$ e $g = 3$ sono note le formule esplicite. Se $g = 2$ sono necessarie per l'addizione 25 moltiplicazioni e un'inversione e per il doubling 27 moltiplicazioni e un'inversione
- $g < 10$ Cantor
- $g \geq 10$ NUCOMP/NUDPL

4.LOGARITMO DISCRETO NELLO JACOBIANO

Attacchi classici

L'HCDLP è una generalizzazione del ECDLP, ogni attacco conosciuto per le curve ellittiche funziona in alcuni casi per le curve iperellittiche:

- Semplificazione di Pohlig-Hellman: la complessità del HCDLP è pari a quella del DLP nel più grande sottogruppo dello Jacobiano avente ordine primo.
- MOV/Frey-Rück: converte il problema del HCDLP in un problema di DLP sul gruppo moltiplicativo di un campo finito.
- ρ di Pollard: $O(q^{g/2})$ operazioni di gruppo per risolvere l'HCDLP in un sottogruppo di ordine q dello Jacobiano.

Index-Calculus

Sia dato un gruppo $(G, \cdot)$ abeliano finito e sia $G =< a >$ e $|G| = p$, p primo. Si vuole risolvere il problema del DLP in G. L'algoritmo è formato da 3 passi:

1. Si fissa un sottoinsieme $B = \{p_1, ..., p_j\} \subseteq G$.
2. Si trovano $j + t$ relazioni fra gli elementi di B del tipo:

$$\prod_j p_j^{r_{i,j}} = a^{r_i} \ mod p \quad \text{cioè} \quad \prod_j a^{log_a(p_j) r_{i,j}} = a^{r_i} \ mod p$$

che si possono riscrivere come:

$$\sum_j log_a(p_j) r_{i,j} = r_i \ mod p$$

Index-Calculus

3. Calcolare il logaritmo discreto $log_a(p_1), \ldots, log_a(p_j)$ degli elementi di B risolvendo il sistema:

$$\begin{cases} \sum_j log_a(p_j) r_{1,j} \equiv r_1 \ mod p \\ \vdots \\ \sum_j log_a(p_j) r_{j+t,j} \equiv r_{j+t} \ mod p \end{cases}$$

Se $g \in G$ è $B-$smooth, cioè esistono $k, k_i \in \mathbb{N}$ tali che $g^k = p_1^{k_1} \ldots p_j^{k_j}$, si può ricavare il logaritmo discreto di g dalla relazione:

$$k \cdot log_a(g) = k_1 \cdot log_a(p_1) + \cdots + k_j \cdot log_a(p_j)$$

Confronto

L'index calulus è stato adattato al caso delle curve iperellittiche, ma il gruppo è additivo e le relazioni riguardano i divisori.

L'efficienza dipende dalla scelta della base di divisori e dal genere. Confrontiamo l'efficacia dell'index calculus nella versione di Gaudry/Enge con il metodo ρ di Pollard. (q ordine del gruppo)

g	2	3	4	5	6
rho	q	$q^{3/2}$	q^2	$q^{5/2}$	q^3
Gaudry	$q^{4/3}$	$q^{3/2}$	$q^{8/5}$	$q^{5/3}$	$q^{12/7}$

Nota

Se $g = 2$ è più efficiente il metodo di Pollard. Si devono usare curve di $g \leq 2$ oppure fare in modo che lo Jacobiano abbia dimensione tale da rendere l'index calculus intrattabile, ma quindi si avranno anche chiavi più grandi.

Ordine dello Jacobiano

Serve conoscere l'ordine dello Jacobiano sia per implementare i sistemi crittografici, sia per risolvere l'HCDLP coi metodi precedenti.

Consideriamo una curva iperellittica C di genere g definita su $\mathbb{F}_q$, con q potenza di un primo. L'ordine dello Jacobiano su $\mathbb{F}_{q^k}$ giace nell'intervallo di Hasse-Weil:

$$(\sqrt{q}^k - 1)^{2g} \leq \#J(\mathbb{F}_{q^k}) \leq (\sqrt{q}^k + 1)^{2g}$$

Ordine dello Jacobiano

Vediamo come calcolare l'ordine dello Jacobiano utilizzando la funzione $Z_C(t)$.

Sia C definita su $\mathbb{F}_q$, siano M_n il numero di punti $\mathbb{F}_{q^n}$ razionali su C.

La funzione zeta di C è la serie di potenze

$$Z_C(t) = exp(\sum_{r \geq 1} M_r \frac{t^r}{r})$$

Ordine dello Jacobiano

La funzione $Z_C(t)$ può essere riscritta come:

$$Z_C(t) = \frac{P(t)}{(1-t)(1-qt)}$$

dove $P(t)$ è un polinomio di grado $2g$ a coefficienti interi che si fattorizza come:

$$P(t) = \prod_{i=1}^{g}(1-\alpha_i t)(1-\overline{\alpha_i} t).$$

Il numero di punti dello Jacobiano $J(\mathbb{F}_{q^n})$ sarà:

$$\#J(\mathbb{F}_{q^n}) = \prod_{i=1}^{g}|1-\alpha_i^n|^2$$

5.SCELTA DELLA CURVA

Scelta della curva

Alcuni criteri di scelta:

1. Curve definite su campi K di caratteristica 2 (aritmetica efficiente)
2. $\#J_C$ divisibile per un primo r grande (Poligh-Hellman, ρ di Pollard).
3. Se la curva è costruita su $\mathbb{F}_q$, poichè il metodo di Frey-Rück permette di creare un isomorfismo fra J_C e il gruppo moltiplicativo di $\mathbb{F}_{q^k}$, bisogna controllare che r non divida $q^k - 1$ per quei valori di k per i quali in $\mathbb{F}_{q^k}$ il DLP si risolve velocemente.
4. Se $g = 2$ l'index calculus non è più efficiente degli altri metodi e l'ordine dello Jacobiano si calcola più velocemente.

Scelta della curva

Invece di considerare una curva iperellittica generica e calcolare l'ordine del suo Jacobiano per verificare se sia adatta o meno, si può procedere al contrario.

Esistono metodi per scegliere uno Jacobiano "sicuro" e trovare di conseguenza una curva avente Jacobiano di tale ordine.

Nota

Se $g = 2$ questi metodi sono relativamente efficienti, diventano sempre più complessi all'aumentare del genere.

Grazie per l'attenzione!