Applicazioni di teoria dei numeri alla crittografia

Nadir Murru

Università di Torino, Dipartimento di Matematica G. Peano

La matematica è la regina delle scienze e la teoria dei numeri è la regina della matematica

- Proprietà dei numeri primi
- Test di primalità
- Sequenze pseudocasuali
- Ideazione di sistemi crittografici
- Attacchi a sistemi crittografici

Lo schema RSA

Generazione delle chiavi

- si scelgono due numeri primi (grandi) p, q e si calcola $N = pq$;
- si sceglie un intero e tale che $gcd(e, (p-1)(q-1) = 1$.
  La coppia (N, e) è la *chiave pubblica* o di *criptazione*;
- si calcola $d = e^{-1} \pmod{(p-1)(q-1)}$.
  La tripla (p, q, d) è la *chiave privata* o di *decriptazione*.

Criptazione

Possiamo criptare un messaggio in chiaro $m \in \mathbb{Z}_N$. Il messaggio cifrato è $c = m^e \pmod{N}$.

Decriptazione

Si recupera il messaggio in chiaro calcolando $c^d \pmod{N}$.

Frazioni continue

Le frazioni continue forniscono una raprresentazione per ogni numero reale α_0 per mezzo di una successione di interi:

$$\alpha_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}},$$

dove $a_0, a_1, \ldots$ sono calcolati mediante

$$\begin{cases} a_k = [\alpha_k] \\ \alpha_{k+1} = \dfrac{1}{\alpha_k - a_k} \quad \text{se } \alpha_k \text{ non è intero} \end{cases} \qquad k = 0, 1, 2 \ldots$$

Proposition

Un numero reale α è un'irrazionalità quadratica se e solo se ha un'espansione periodica in frazione continua.

Attacco di Wiener (low private exponent)

Theorem (Wiener, 1990)

Sia $N = pq$, se $q < p < 2q$ e $d < \frac{1}{3}N^{1/4}$, dalla chiave pubblica (N, e) si può ricavare efficientemente la chiave privata d

1. $ed - k\varphi(N) = 1 \Rightarrow |\frac{e}{\varphi(N)} - \frac{k}{d}| = \frac{1}{d\varphi(N)}$
2. $N = pq > q^2 \Rightarrow q < \sqrt{N}$
3. $N - \varphi(N) = p + q - 1 < 3q < 3\sqrt{N}$
4. $|\frac{e}{N} - \frac{k}{d}| < \dfrac{1}{2d^2}$

Il numero razionale $\frac{k}{d}$ è un convergente della frazione continua di $\frac{e}{N}$.

Schemi stile RSA

- RSA può essere attaccato quando l'esponente pubblico o quello privato è piccolo; RSA mostra ulteriori vulnerabilità in scenari diffusi (quando uno stesso messaggio è inviato a differenti destinatari).
- Gli schemi stile RSA sono stati sviluppati per prevenire alcuni di questi attacchi; inoltre hanno solitamente una procedura di decriptazione due volte più veloce.
- Sono basati su isomorfismi tra due gruppi, uno dei quali è un insieme di punti di una curva, solitamente una conica o una cubica.

La conica di Pell

In teoria dei numeri, una delle più famose equazione diofantine è l'equazione di Pell

$$x^2 - Dy^2 = 1,$$

con D intero non quadrato. A partire da essa si può definire la conica di Pell su un generico campo $\mathbb{F}$:

$$\mathcal{H} = \{(x, y) \in \mathbb{F} \times \mathbb{F} : x^2 - Dy^2 = 1\}.$$

Usando il prodotto di Brahmagupta

$$(x, y) \otimes (w, z) = (xw + yzD, yw + xz), \quad \forall (x, y),\ (w, z) \in \mathcal{H},$$

$(\mathcal{H}, \otimes)$ è un gruppo la cui identità è $(1, 0)$ e l'inverso di un elemento (x, y) è $(x, -y)$.

La conica di Pell

La conica di Pell $\mathcal{H}$ può essere parametrizzata mediante la retta

$$y = \frac{1}{m}(x+1)$$

che determina il seguente isomorfismo tra $\mathcal{H}$ e l'insieme dei parametri $P = \mathbb{F} \cup \alpha$:

$$\Phi : m \mapsto \left(\frac{m^2+D}{m^2-D}, \frac{2m}{m^2-D} \right).$$

Il prodotto indotto su P è definito come segue:

$$m \odot n = \frac{mn+D}{m+n}, \quad \forall m, n \in P.$$

Le funzioni di Rédei

Le funzioni di Rédei si definiscono partendo dal seguente sviluppo:

$$(z + \sqrt{d})^n = N_n(d, z) + D_n(d, z)\sqrt{d},$$

per ogni intero $z \neq 0$, d intero non quadrato. Abbiamo

$$N_n(d, z) = \sum_{k=0}^{[n/2]} \binom{n}{2k} d^k z^{n-2k}, \quad D_n(d, z) = \sum_{k=0}^{[n/2]} \binom{n}{2k+1} d^k z^{n-2k-1}.$$

Le funzioni razionali di Rédei sono quindi date da

$$Q_n(d, z) = \frac{N_n(d, z)}{D_n(d, z)}, \quad \forall n \geq 1.$$

Le funzioni di Rédei e la conica di Pell

Proposition

Se $\mathbb{F} = \mathbb{Z}_p$, *allora* P *has order* $p+1$ *e*

$$z^{\odot(p+2)} \equiv z \pmod{p}, \quad \forall z \in P.$$

Proposition

Sia $z^{\odot n} = \underbrace{z \odot \cdots \odot z}_{n}$ *l'n–esima potenza di* z *rispetto al prodotto non standard* $\odot$, *allora*

$$z^{\odot n} = Q_n(d, z)\ .$$

Remark

Le funzioni di Rédei possono essere calcolate in maniera efficiente.

Lo schema sulla conica di Pell

Generazione chiavi:

- p, q primi, $N = pq$, e tali che $\gcd(e, (p+1)(q+1)) = 1$
- $d = e^{-1} \pmod{(p+1)(q+1)}$
- (N, e) chiave pubblica, (p, q, d) chiave privata

Criptazione di due messaggi $M_x, M_y \in \mathbb{Z}_N$:

- $D = \dfrac{M_x^2 - 1}{M_y^2} \pmod{N}$
- $M = \Phi^{-1}(M_x, M_y)$
- $C = M^{\odot e} \pmod{N} = Q_e(D, M) \pmod{N}$

Decriptazione:

- $C^{\odot d} \pmod{N} = M$
- $\Phi(M) = (M_x, M_y)$

Test di primalità

- Test di Fermat e numeri di Carmichael
- Se $p = 2^r s + 1$ è primo, allora

$$a^s \equiv 1 \pmod{p} \quad \text{or} \quad a^{2^k s} \equiv -1 \pmod{p}$$

per ogni $a \in \mathbb{Z}_p^*$ e qualche $0 \leq k < r$. Un numero composto dispari che soddisfi questa condizione è uno *pseudoprimo forte* in base a; non esistono pseudoprimi forti in qualunque base.

- Il test di Baillie–PSW combina tale test con il test di Lucas, una sovrapposizione tra gli pseudoprimi forti e gli pseudoprimi di Lucas non è nota.

Il test di Lucas

Sia $(U_n)_{n\geq 0}$ la successione di Lucas definita da

$$\begin{cases} U_0 = 0, U_1 = 1 \\ U_n = PU_{n-1} - QU_{n-2} \end{cases} .$$

Il test di Lucas è basato sul fatto che quando n è primo con $(n, Q) = 1$, abbiamo

$$U_{n-\left(\frac{P^2-4Q}{n}\right)} \equiv 0 \pmod{n}, \tag{1}$$

dove $\left(\frac{P^2-4Q}{n}\right)$ è il simbolo di Jacobi. Se n è composto ma (1) ancora vale, allora n è chiamato *pseudorpimo di Lucas* con parametri P e Q.

Il test di Pell

Ricordiamo che la conica di Pell $\mathcal{H}$ su un campo finito $\mathbb{Z}_p$ ha ordine $p+1$ se D non è un quadrato, altrimenti ha ordine $p-1$.

Definiamo *pseudoprimi di Pell*, con parametri $D, \tilde{x}, \tilde{y}$, gli interi composti dispari n che soddisfano

$$(\tilde{x}, \tilde{y})^{\otimes n - \left(\frac{D}{n}\right)} \equiv (1, 0) \pmod{n}.$$

GRAZIE PER L'ATTENZIONE!