I codici post-quantum basati sui reticoli

Nadir Murru
Giordano Santilli

9 Maggio 2019

I reticoli

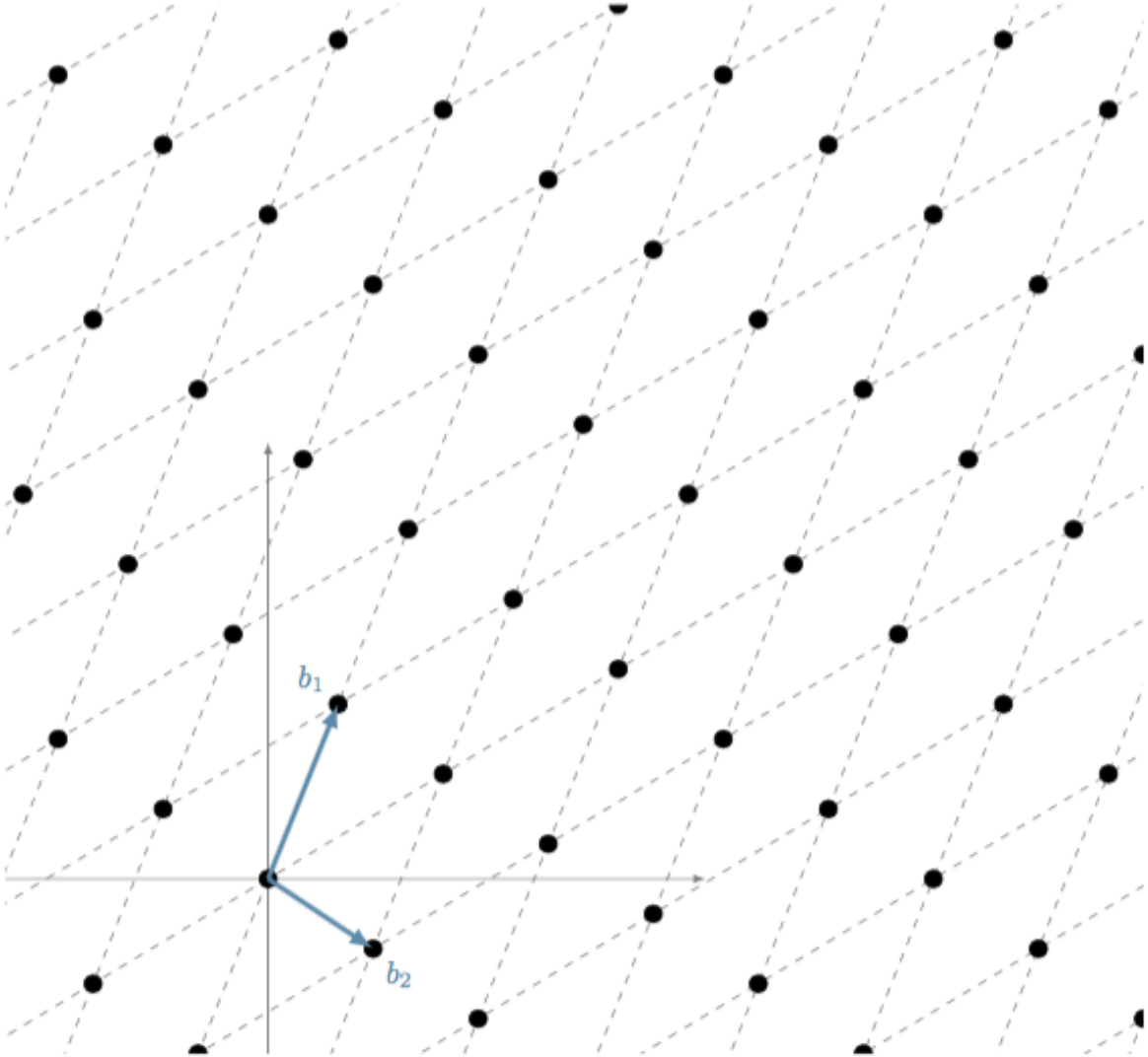
Definizione

Sia $B = \{b_0, \ldots, b_{m-1}\}$ *un insieme di vettori linearmente indipendenti di* $\mathbb{R}^n$, *con* $n \geq m$. *Il* ***reticolo*** *generato da* B *è l'insieme delle combinazioni lineari a coefficienti interi dei vettori* b_i*:*

$$\mathcal{L} = \{l_0 b_0 + \ldots + l_{m-1} b_{m-1} | l_0, \ldots, l_{m-1} \in \mathbb{Z}\}.$$

L'insieme B *è detto* ***base*** *del reticolo,* m *è il* ***rango*** *del reticolo ed* n *la sua* ***dimensione****. Se* $m = n$ *si parla di* ***reticolo di rango massimo****.*

I reticoli



Reticoli Ideali

E' possibile associare ogni elemento di un reticolo ad un polinomio, utilizzando la mappa

$$\mathbb{Z}^n \to \mathbb{Z}[x]_{<n}, \quad (a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}.$$

Un **reticolo ideale** è un reticolo $\mathcal{L} \subseteq \mathbb{Z}^n$ tale che $\mathcal{L}$ è isomorfo ad un ideale $I \subseteq \mathbb{Z}[x]/(f(x))$, con $f \in \mathbb{Z}[x]$ polinomio monico ed irriducibile.

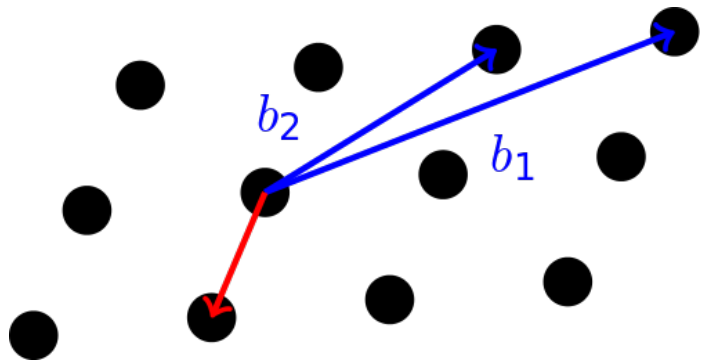
SVP

Sia $\mathcal{L} \subseteq \mathbb{Z}^n$ un reticolo.

Shortest Vector Problem (SVP)

Trovare il vettore $v \in \mathcal{L}$ tale che

$$\|v\| = \min_{x \in \mathcal{L} \setminus 0} \|x\|.$$



SVP

Sia $\mathcal{L} \subseteq \mathbb{Z}^n$ un reticolo.

SVP Approssimato (SVP-γ)

Sia $\gamma \geq 1$ un fattore di approssimazione. Trovare il vettore $v \in \mathcal{L}$ tale che

$$\|v\| \leq \gamma \min_{x \in \mathcal{L} \setminus 0} \|x\|$$

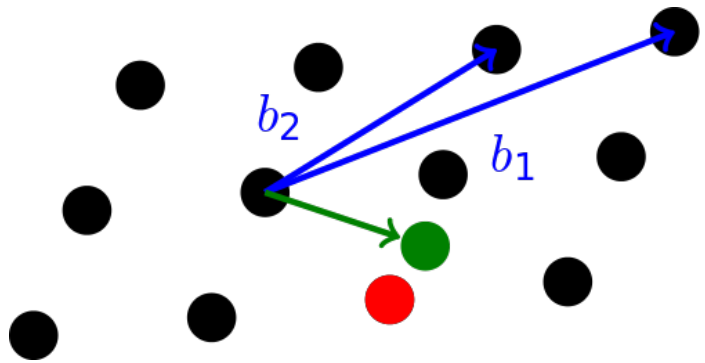
CVP

Sia $\mathcal{L} \subseteq \mathbb{Z}^n$ un reticolo e sia $w \in \mathbb{R}^n$.

Closest Vector Problem (CVP)

Trovare il vettore $v \in \mathcal{L}$ tale che

$$\|v - w\| = \min_{x \in \mathcal{L} \setminus 0} \|x - w\|.$$



Distribuzioni R-LWE

Siano $n \in \mathbb{N}^+$ e $R = \mathbb{Z}[X]/(X^n + 1)$. Inoltre definiamo q un primo e $R_q = R/qR$. Sia $s \in R_q$ un elemento fissato chiamato *segreto*. La **Distribuzione R-LWE** $A_{s,\chi}$ è definita come

$$A_{s,\chi} = \{(a, b)\} \subseteq R_q \times R_q,$$

tale che:

- $a \in R_q$ è ottenuto casualmente da una distribuzione uniforme.
- $b \in R_q$ è definito come

$$b = (s \cdot a + e) \bmod q,$$

dove $e \in R$ è un valore estratto casualmente da una Distribuzione Gaussiana Discretizzata.

RLWE

Ring Learning With Errors (RLWE) - Search RLWE

Il problema Search-RLWE$_{q,\chi,m}$ consiste nel trovare un $s \in R_q$ fissato, date m coppie (a, b).

Ring Learning With Errors (RLWE) - Decision RLWE

Il problema Decision-RLWE$_{q,\chi,m}$ consiste nello stabilire, date m coppie (a, b), se esse provengono da una distribuzione RLWE con uno stesso $s \in R_q$ fissato o se sono delle estrazioni casuali da una distribuzione uniforme in $R_q \times R_q$.

Gli algoritmi post-quantum sui reticoli

- CRYSTALS-KYBER
- CRYSTALS-DILITHIUM
- FrodoKEM
- LAC
- **NewHope**
- **NTRU**
- NTRU Prime
- Round 5
- SABER
- Three Bears
- FALCON
- qTESLA

NTRU

Si considerano tre numeri interi p, q, N, $\gcd(p, q) = 1$, quattro insiemi di polinomi $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_\phi$, $\mathcal{L}_m$ di grado $N - 1$. Tutte le operazioni tra polinomi si effettuano nell'anello $R = \mathbb{Z}[X]/(X^N - 1)$.

Generazione delle chiavi

Chiave privata

- $f \in \mathcal{L}_f$, con inversi F_p e F_q modulo p e q, rispettivamente
- $g \in \mathcal{L}_g$

Chiave pubblica

- $h \equiv F_q \cdot g \pmod{q}$

NTRU

Criptazione

Sia m scelto dall'insieme dei messaggi in chiaro $\mathcal{L}_m$ e $\phi \in \mathcal{L}_\phi$ polinomio random, il messaggio criptato è

$$c \equiv p\phi \cdot h + m \pmod{q}$$

Decriptazione

Si calcola $a \equiv f \cdot c \pmod{q}$, usando i rappresentanti di $\mathbb{Z}_q$ in $(-q/2, q/2)$; dal messaggio criptato c si ricava il messaggio in chiaro m calcolando

$$F_p \cdot a \pmod{p}$$

Si noti che

$$a \equiv f \cdot p\phi \cdot F_q \cdot g + f \cdot m \pmod{q} = p\phi \cdot g + f \cdot m \pmod{q}$$

dove i coefficienti di $p\phi \cdot g + f \cdot m$ sono *quasi sempre* in $(-q/2, q/2)$, ovvero a coincide proprio con tale polinomio in R. Quindi riducendo a modulo p e moltiplicandolo per l'inverso di f modulo p si ricava m.

Osservazione

Per evitare *fallimenti* in fase di decriptazione occorre che

$$|f \cdot m| \leq q/4, \quad |p\phi \cdot g| \leq q/4$$

Attacchi basati sui reticoli

Dalle informazioni pubbliche è possibile costruire un reticolo di rango $2N$ dove la chiave privata 'concatenata' $(\alpha f, g)$ è il vettore di norma minima

$$\left(\begin{array}{cccc|cccc} \alpha & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & \alpha & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right)$$

dove α è un parametro da determinare in maniera opportuna

NewHope

Si fissa $n = 512$ o $n = 1024$ ed inoltre $q = 12289$. Le variabili vengono viste come polinomi in $R_q = \mathbb{Z}_q[X]/(X^n + 1)$.

Generazione delle chiavi

- $publicseed = \text{Random}(\{0, \ldots, 255\}^{32})$,
  $noiseseed = \text{Random}(\{0, \ldots, 255\}^{32})$.
- $a =$ Polinomio in R_q generato da *publicseed*,
- $e =$ Polinomio random in R_q generato da *noiseseed*.

Chiave privata

- $s =$ Polinomio random in R_q generato da *noiseseed*.
- s è la **chiave privata**.

Chiave pubblica

- $b = a \cdot s + e$.
- $(b, publicseed)$ è la **chiave pubblica**.

NewHope

Cifratura

- μ è il **messaggio** e $(b, publicseed)$ è la **chiave pubblica**.
- $s', e', e'' =$ Polinomi random in R_q generato da *noiseseed* tramite una distribuzione binomiale.
- $u = a \cdot s' + e'$.
- $v = b \cdot s' + e'' + \mu$.
- v viene inviato come messaggio cifrato insieme ad u.

Decifratura

- Il messaggio si ritrova da $v - u \cdot s$.

NewHope

Il messaggio che si ottiene è simile, ma non uguale al messaggio inviato.
Scegliendo i termini di errore e, e', e'' abbastanza piccoli, si minimizza la probabilità di ricevere un messaggio diverso da quello di partenza.
La sicurezza si basa sul RLWE riformulato per la distribuzione binomiale.

GRAZIE
PER L'ATTENZIONE!