Tecniche algebriche per il problema Learning With Errors: algoritmo di Arora-Ge e ottimizzazione con basi di Gröbner

Ludovico Piazza

7 maggio 2022

Sommario

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Indice

1 Il problema: Learning With Errors (LWE)

Learning With Errors (LWE) è un noto problema computazionale introdotto da Regev nel 2005 in [Reg05]. Una delle principali caratteristiche che rende ne interessante lo studio è la sua complessità risolutiva: sotto opportune ipotesi sui parametri, la sua risoluzione può essere ricondotta mediante una riduzione polinomiale quantistica a quella di due famosi problemi sui reticoli (GapSVP_γ e SIVP_γ) che si congettura siano difficili da risolvere anche usando computer quantistici. Ciò porta LWE a candidarsi come fondamento per la costruzione di crittosistemi post-quantistici.

Preliminarmente, diamo un paio di definizioni su due distribuzioni che ci serviranno in seguito.

Definizione 1.1 (**Distribuzione gaussiana discreta**)**.** Dato $\alpha \in \mathbb{R}_{>0}$ chiamiamo distribuzione gaussiana discreta la distribuzione ψ_α su $\mathbb{Z}/(q)$ che:

- prende un valore $r \in \mathbb{R}$ mediante una distribuzione gaussiana con deviazione standard $\sigma = \alpha q$;
- arrotonda r all'intero più vicino, ottenendo $\lfloor r \rceil$;
- proietta $\lfloor r \rceil$ in $\mathbb{Z}/(q)$, ottenendo $\lfloor r \rceil \pmod q$.

Definizione 1.2 (**Distribuzione LWE**)**.** Dato un vettore $\boldsymbol{s} \in \mathbb{Z}/(q)^n$ che chiamiamo **segreto**, definiamo la distribuzione LWE come la distribuzione $\text{A}_{\boldsymbol{s},\chi}$ su $\mathbb{Z}/(q)^n \times \mathbb{Z}/(q)$ ottenuta prendendo $\boldsymbol{a}$ uniformemente da $\mathbb{Z}/(q)^n$, lo scalare e con distribuzione χ da $\mathbb{Z}/(q)$ e dando come risultato $(\boldsymbol{a}, \langle \boldsymbol{s}; \boldsymbol{a} \rangle + e)$.

L'idea che sta alla base della variante del problema che vogliamo studiare è che la distribuzione LWE, definita qui sopra, risulta molto simile ad una distribuzione uniforme, pertanto riuscire ad ottenere informazioni sul suo vettore segreto diventa estremamente difficile.
Qui di seguito la definiamo nel dettaglio:

Definizione 1.3 (**Search-LWE**$_{n,q,\alpha,m}$)**.** Fissato $\alpha \in \mathbb{R}_{>0}$, prendiamo $\mathbf{s}$ uniformemente da $\mathbb{Z}/(q)^n$ ed m coppie indipendenti $(\boldsymbol{a}_i, b_i)$ da $\mathbb{Z}/(q)^n \times \mathbb{Z}/(q)$ mediante la distribuzione $\text{A}_{\mathbf{s},\psi_\alpha}$.
Il problema Search-$\text{LWE}_{n,q,\alpha,m}$ consiste nel ricavare $\mathbf{s}$ avendo a disposizione soltanto le m coppie $(\boldsymbol{a}_i, b_i)$.

Ad ogni problema Search-$\text{LWE}_{n,q,\alpha,m}$ associamo inoltre il valore $\sigma = \alpha q$ (**tasso di rumore**) in quanto, come vedremo tra poco, esso ne caratterizza la complessità computazionale.

2 Un algoritmo algebrico: l'attacco di Arora-Ge

Le soluzioni più immediate che vengono in mente al problema, basate ad esempio su algoritmi di massima verosimiglianza, sono tutte esponenziali. Il primo algoritmo sub-esponenziale è stato trovato da Sanjeev Arora e Rong Ge in [AG11]. La complessità computazionale dell'algoritmo, tuttavia, è sub-esponenziale soltanto a condizione che il *tasso di rumore* sia inferiore $\sqrt{n}$.

3 Ottimizzazione mediante basi di Gröbner

Riferimenti bibliografici

[AG11] Sanjeev Arora e Rong Ge. "New Algorithms for Learning in Presence of Errors". In: *Automata, Languages and Programming*. A cura di M. Henzinger L. Aceto e J. Sgall. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 403–415. DOI: 10.1007/978-3-642-22006-7_34.

[Alb+14] Martin Albrecht et al. *Algebraic algorithms for LWE problems*. Cryptology ePrint Archive, Report 2014/1018. 2014.

[Reg05] Oded Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography." In: *Journal of the ACM* 56.6 (2009), pp. 1–40. DOI: 10.1145/1568318.1568324. Versione preliminare pubblicata in Procedings of STOC'05.

[Sage] W. A. Stein et al. *Sage Mathematics Software (Version 9.3)*. The Sage Development Team. 2021. URL: http://www.sagemath.org.