Riassunto

Gabriele Bottani

23 settembre 2024

Nell'era digitale in cui viviamo, la sicurezza delle informazioni è diventata una preoccupazione primaria. La crittografia, l'arte di proteggere le informazioni attraverso la loro codifica, gioca un ruolo fondamentale in questo contesto. Tra le varie branche della crittografia moderna, la crittografia basata sui reticoli emerge come un campo di studio particolarmente promettente e innovativo. I reticoli, strutture matematiche composte da punti regolarmente distribuiti nello spazio n-dimensionale, offrono una base solida per la costruzione di schemi crittografici. La loro importanza risiede in alcuni problemi matematici intrinseci, che risultano essere difficili da risolvere anche per computer quantistici. Questi ultimi infatti rappresentano una minaccia crescente per molti sistemi crittografici tradizionali che, essendo stati pensati per la capacità computazionale odierna, non sono in grado di resistere ai ben più potenti calcolatori quantistici già in sviluppo attualmente. In questo contesto, il sistema crittografico GGH (Goldreich-Goldwasser-Halevi), proposto nel 1997, rappresenta una pietra miliare. GGH sfrutta la complessità computazionale di uno specifico problema sui reticoli, il CVP (Closest Vector Problem) per garantire la sicurezza delle informazioni. Tuttavia, come molti sistemi pionieristici, GGH ha mostrato alcune vulnerabilità nel corso degli anni, stimolando la ricerca di ottimizzazioni e miglioramenti. Una di queste ottimizzazioni è rappresentata da GGH-HNF (GGH - Hermite Normal Form), una variante che mira a rafforzare la sicurezza del sistema originale e cercare di risolverne le principali vulnerabilità. GGH-HNF introduce modifiche significative alla struttura della chiave pubblica, sfruttando la forma normale di Hermite per rendere il sistema più resistente a determinati tipi di attacchi. Sebbene in passato gli schemi crittografici GGH e GGH-HNF fossero stati ritenuti inefficaci per applicazioni pratiche a causa delle loro scarse prestazioni, questo studio esamina come i recenti progressi dell'hardware e del software possano potenzialmente migliorarne le performance, rivalutandone potenzialmente la rilevanza nel contesto tecnologico attuale. Questa tesi si propone quindi di rivisitare i crittosistemi sopracitati con strumenti

moderni, offrendo un'analisi approfondita che comprende sia la spiegazione delle loro proprietà matematiche, che l'esposizione degli algoritmi necessari al loro funzionamento, oltre a una crittoanalisi dettagliata. L'analisi teorica si basa su un pacchetto Python suddiviso in tre moduli: due dedicati specificamente ai crittosistemi esaminati, e un terzo che raccoglie funzioni e metodi comuni, oltre a strumenti utili nell'ambito della crittografia basata sui reticoli. Viene inoltre presentata, oltre alle implementazioni originali, anche una proposta di miglioramento attraverso una versione ibrida, la quale mira a superare alcune delle limitazioni identificate nei sistemi originali. Successivamente ad una disamina approfondita e la discussione dei risultati sperimentali ottenuti, questo studio si pone l'obiettivo di rispondere alla seguente domanda cruciale: GGH e le sue varianti potrebbero essere usate in ambito crittografico pratico? La valutazione finale mirerà quindi a fornire una prospettiva concreta sull'applicabilità di questi sistemi crittografici nel contesto tecnologico attuale, considerando sia i loro punti di forza che le loro potenziali limitazioni.