Università degli Studi di Milano
Facoltà di Scienze e Tecnologie
Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

CRITTOGRAFIA POST-QUANTISTICA BASATA SUI RETICOLI: IMPLEMENTAZIONE E CRITTOANALISI DI GGH

Relatore: Prof. Stelvio CIMATO

Tesi di:
Gabriele BOTTANI
Matricola: 01701A

Anno Accademico 2023-2024

Indice

1 Introduzione **1**

2 Proprietà e problemi sui reticoli **2**
2.1 Reticoli 2
2.1.1 Nozioni base 2
2.1.2 Dominio Fondamentale 4
2.2 Problemi sui reticoli 6
2.3 Riduzione di un reticolo 7
2.3.1 Rapporto di Hadamard 7
2.3.2 Ortogonalizzazione Gram-Schmidt 7
2.3.3 Algoritmo di Lenstra-Lenstra-Lovász 8
2.3.4 Varianti di LLL 10
2.4 Algoritmi per la risoluzione del CVP 11
2.4.1 Algoritmi di Babai 11
2.4.2 Tecnica di incorporamento 14

3 Crittosistema a chiave pubblica GGH **17**
3.1 Struttura e funzionamento di GGH 17
3.1.1 Generazione delle chiavi 18
3.1.2 Esempio pratico 20
3.2 Crittoanalisi di GGH 22
3.2.1 Crittoanalisi originale 22
3.2.2 Attacco di Nguyen 24
3.2.3 Attacco basato su informazioni parziali 28

4 Migliorare GGH usando la Forma Normale di Hermite **30**
4.1 Struttura e funzionamento di GGH-HNF 30
4.1.1 Esempio pratico 32
4.2 Limiti pratici di GGH-HNF 33

Capitolo 1

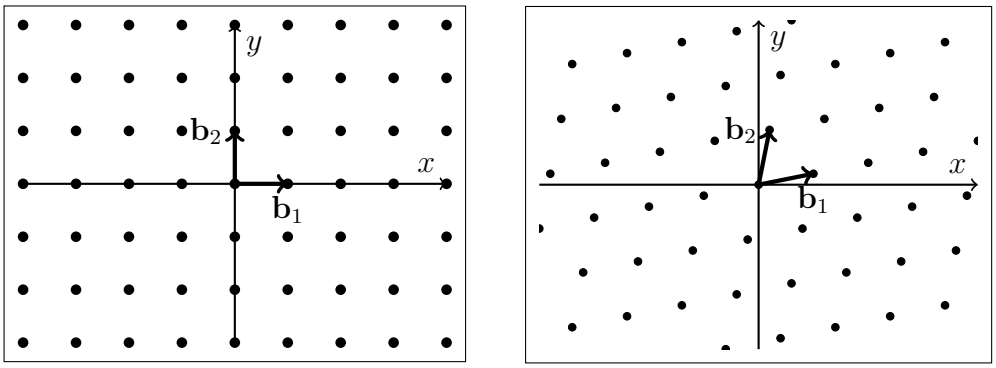
Introduzione

Capitolo 2

Proprietà e problemi sui reticoli

2.1 Reticoli

2.1.1 Nozioni base



(a) $\mathcal{L} = \mathbb{Z}^n$ (b) $\mathcal{L} = \mathbf{B}\mathbb{Z}^n$ dove $\mathbf{B} \in \mathbb{R}^{m \times n}$

Figura 1: Due esempi di strutture reticolari

Un reticolo è un insieme di punti in uno spazio di dimensione n che forma una struttura periodica. Ogni punto del reticolo può essere generato come combinazione lineare di n vettori, chiamati base, che sono linearmente indipendenti tra loro. La struttura e le proprietà di un reticolo dipendono dai vettori di base che, partendo dall'origine, definiscono il suo pattern di disposizione indicando le direzioni e le distanze tra i punti del reticolo.
Una proprietà fondamentale su cui si basa la definizione di reticolo è la proprietà dei coefficienti integrali: la base di un reticolo ha sempre coefficienti integrali, il che significa che tutti i vettori nella base sono combinazioni lineari intere l'uno dell'altro.

I reticoli possono essere formati in diversi modi, il più comune è il reticolo quadrato (Figura 1a) nel quale la base è allineata con gli assi cartesiani. Le altre varianti sono ottenibili applicando delle trasformazioni lineari alla base del reticolo quadrato (Figura 1b).
I reticoli sono normalmente definiti in uno spazio bidimensionale o tridimensionale, ma il concetto può essere esteso a spazi di dimensioni superiori. La rappresentazione dei vettori in questa tesi è quella per riga, al contrario della scelta presa dagli autori di [5] che utilizzarono una notazione per colonna nel loro crittosistema a chiave pubblica Goldreich Goldwasser Halevi (GGH), oggetto di questa tesi. Quindi per esempio, una matrice $\mathbf{B} \in \mathbb{R}^{m \times n}$ sarà divisa in vettori $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$.
Una base può essere rappresentata da una matrice $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n] \in \mathbb{R}^{n \times n}$ avente, come precedentemente anticipato, i vettori base come righe. Utilizzando la matrice come notazione, il reticolo generato da una matrice $\mathbf{B} \in \mathbb{R}^{n \times n}$ può essere definito come $\mathcal{L}(\mathbf{B}) = \{\mathbf{xB} : \mathbf{x} \in \mathbb{Z}^n\}$, dove $\mathbf{xB}$ è una comune moltiplicazione matriciale.
Si definisca ora l'i-esimo minimo $\lambda_i(\mathcal{L})$ come il raggio della sfera più piccola, centrata nell'origine, che contiene i vettori linearmente indipendenti del reticolo. Si chiami "gap" il rapporto tra il secondo e il primo minimo, $\frac{\lambda_1(\mathcal{L})}{\lambda_2(\mathcal{L})}$. Questo valore misura la differenza relativa tra i due vettori più corti linearmente indipendenti del reticolo, fornendo un'indicazione importante sulla sua struttura. Più formalmente, dati n vettori linearmente indipendenti $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$, il reticolo generato da essi è un set di vettori

$$\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \sum_{i=1}^{n} \mathbf{b}_i \cdot \mathbb{Z} = \{\mathbf{xB} : \mathbf{x} \in \mathbb{Z}^n\}.$$

Lo stesso reticolo può essere generato da più basi composte ciascuna da vettori diversi

$$\mathcal{L} = \sum_{i=1}^{n} \mathbf{c}_i \cdot \mathbb{Z}.$$

Il determinante di un reticolo è il valore assoluto del determinante della matrice base $\det(\mathcal{L}(\mathbf{B})) = |\det(\mathbf{B})|$. Di conseguenza, per ogni matrice unimodulare (ovvero avente determinante +1 o -1) $\mathbf{U} \in \mathbf{Z}^{n \times n}$, $\mathbf{UB}$ è una base di $\mathcal{L}(\mathbf{B})$. Per verificare se due basi $\mathbf{R}$ e $\mathbf{B}$ generano lo stesso reticolo, è possibile utilizzare la matrice pseudo-inversa e trovare un $\mathbf{U}$ tale per cui $\mathbf{UR} = \mathbf{B}$.
Computando $\mathbf{R}^+$, ovvero la matrice pseudo-inversa di $\mathbf{R}$, si ha che:

$$\mathbf{U} = \mathbf{B}\ \mathbf{R}^+.$$

$\mathbf{R}^+$ è particolarmente facile da ottenere in questo caso in quanto i vettori riga di $\mathbf{R}$

sono linearmente indipendenti per definizione. Di conseguenza la matrice pseudo-inversa assume la seguente forma:

$$\mathbf{R}^{+} = (\mathbf{R}^{*}(\mathbf{R}\ \mathbf{R}^{*})^{-1})$$

con $\mathbf{R}^{*}$ che è la matrice trasposta coniugata di $\mathbf{R}$. Dato che $\mathbf{R}$ è una matrice composta da soli interi, la matrice trasposta coniugata è uguale alla matrice trasposta normale. Si ottiene quindi che:

$$\mathbf{U} = \mathbf{B}(\mathbf{R}^{T}(\mathbf{R}\ \mathbf{R}^{T})^{-1})$$

Esempio 2.1.1. (Verificare che due basi generino lo stesso reticolo)
Siano $\mathbf{R}$ e $\mathbf{B}$ due basi generanti entrambi il reticolo $\mathcal{L}$ con

$$\mathbf{R} = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} \quad \text{e} \quad \mathbf{B} = \begin{bmatrix} 5 & 4 \\ -6 & -6 \end{bmatrix}$$

allora deve esistere una matrice unimodulare $\mathbf{U}$ tale che $\mathbf{UR} = \mathbf{B}$. Per trovare $\mathbf{U}$ è possibile calcolare:

$$\mathbf{U} = \mathbf{B}(\mathbf{R}^{T}(\mathbf{R}\ \mathbf{R}^{T})^{-1}) = \begin{bmatrix} 2 & 1 \\ -3 & -1 \end{bmatrix}.$$

Ora è sufficiente controllare che

$$\mathbf{UR} = \mathbf{B} \quad \text{ovvero} \quad \begin{bmatrix} 2 & 1 \\ -3 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 4 \\ -6 & -6 \end{bmatrix}$$

inoltre dato che $\det(\mathbf{U}) = 1$, si può affermare che $\mathbf{R}$ e $\mathbf{B}$ sono entrambe basi di $\mathcal{L}$.

2.1.2 Dominio Fondamentale

Il dominio fondamentale è un concetto molto importante nei reticoli, grazie al quale è possibile capire la struttura matematica che li compone. Data una base abritraria $\mathbf{B}$ e un reticolo $\mathcal{L}$ è possibile immaginare il dominio fondamentale come un parallelepipedo che ha come vertici: i vettori base $\mathbf{b}$ generanti il reticolo, il punto di origine e come quarto punto la somma dei vettori base all'origine.
Di tale parallelepipedo è possibile calcolarne il volume $\mathcal{F}(\mathbf{B})$, il quale è strettamente legato al determinante del reticolo. E' possibile osservare in Figura 2 un reticolo con due sue basi: nonostante i domini fondamentali abbiano forme diverse, l'area coperta dal loro volume è la medesima. Come dimostrato in [10, Sezione 7.4], proprio come per il determinante, il dominio fondamentale è un'invariante che è indipendente dalla scelta delle basi per il reticolo. Inoltre ne deriva la proprietà:

$$\mathcal{F}(\mathbf{B}) = \det(\mathcal{L})$$

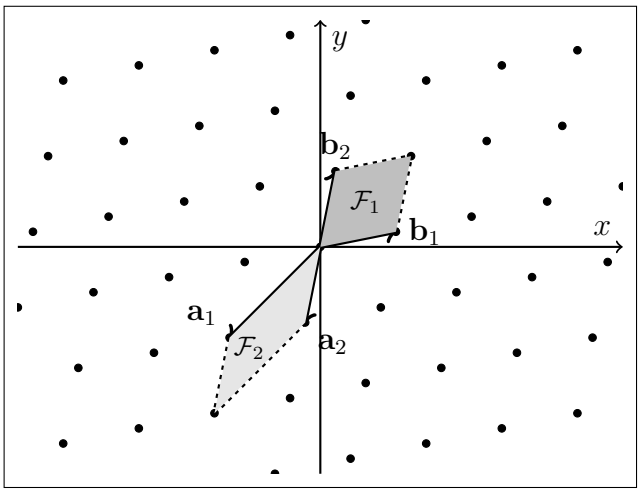


Figura 2: Un reticolo con due suoi domini fondamentali

e ricollegandoci a quanto detto nella sezione 2.1.1: $\mathcal{F}(\mathbf{B}) = \det(\mathcal{L}) = |\det(\mathbf{B})|$.
Una seconda proprietà fondamentale, sempre dimostrata in [10] è che tramite il dominio fondamentale è possibile ricostruire l'intero reticolo (Figura 3). In altre parole, ogni vettore $\mathbf{t} \in \mathbb{R}^n$ con $\mathcal{L} \subset \mathbb{R}^n$ può essere ottenuto sommando ripetutamente a un vettore $\mathbf{f} \in \mathcal{F}$ un altro vettore $\mathbf{v} \in \mathcal{L}$. Più formalmente:

$$\mathcal{F} + \mathbf{v} = \{\mathbf{f} + \mathbf{v} \mid \mathbf{f} \in \mathcal{F}, \mathbf{v} \in \mathcal{L}\}$$

comprende esattamente tutti i vettori nel reticolo $\mathcal{L}$.

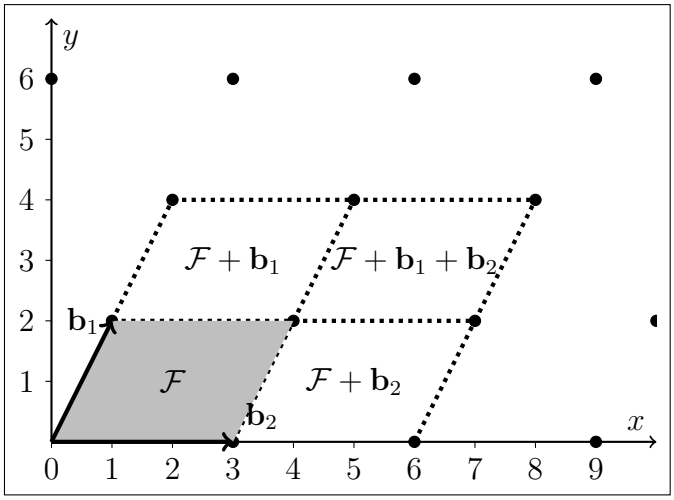


Figura 3: Il dominio fondamentale comprende esattamente tutti i vettori di $\mathcal{L}$

2.2 Problemi sui reticoli

L'utilizzo della crittografia basata su reticoli si basa sull'assunto che, soprattutto nei casi di spazi multidimensionali, la complessità computazionale derivante da determinati problemi su di essi, sia un limite invalicabile. I problemi reticolari più conosciuti e usati in ambito crittografico sono i seguenti:

- Problema del Vettore più Corto (SVP): Data una base di un reticolo $\mathbf{B}$, trovare il vettore non nullo di lunghezza minima in $\mathcal{L}(\mathbf{B})$.
- Problema del Vettore più Vicino (CVP): Data una base di un reticolo $\mathbf{B}$ e un vettore target $\mathbf{t}$ (non necessariamente nel reticolo), trovare il vettore $\mathbf{w} \in \mathcal{L}(\mathbf{B})$ più vicino a $\mathbf{t}$ minimizzando $\|\mathbf{t} - \mathbf{w}\|_2$.
- Problema dei Vettori Lineramente Indipendenti più Corti (SIVP): Data una base di un reticolo $\mathbf{B} \in \mathbb{Z}^{n \times n}$, trovare n vettori linearmente indipendenti $\mathbf{S} = [\mathbf{s}_1, \ldots, \mathbf{s}_n]$ (dove $\mathbf{s}_i \in \mathcal{L}(\mathbf{B})$) per tutte le i) minimizzando la quantità $||\mathbf{S}|| = \max_i ||\mathbf{s}_i||$. SIVP è una variante di SVP, ma a differenza di quest'ultimo, SIVP mira a identificare un insieme di vettori indipendenti che siano i più corti possibile, in altre parole la ricerca di una base ortogonale o ortonormale che generi il reticolo e che minimizzi la lunghezza dei suoi vettori.

La complessità per risolvere CVP è stata provata essere NP-difficile[8], stessa cosa vale per SVP, ma sotto alcune circostanze specifiche[9]. Per questi motivi vengono comparati come problemi dalla stessa difficoltà anche se, in pratica, risolvere CVP è considerato essere un po' più difficile di SVP nella stessa dimensione. Ognuno di questi due problemi ha un relativo sotto-problema che nient'altro è che una variante approssimativa: il Problema del Vettore più Vicino Approssimato (apprCVP) e Problema del Vettore più Corto Approssimato (apprSVP). Questi sotto-problemi sono riferibili alla necessità di trovare un vettore non nullo la cui lunghezza sia maggiore di un fattore dato $\Psi(n)$, rispetto ad un vettore non nullo corretto che risulti essere più corto o più vicino, a seconda del problema.
In particolare GGH si basa sulla risoluzione del CVP basandosi su una delle proprietà fondamentali dei reticoli: la possibilità di usare più basi per lo stesso reticolo. Utilizzando due basi $\mathbf{A}$ e $\mathbf{B}$, definite rispettivamente come "buona" e "cattiva", ma che generano lo stesso reticolo, diventa più agevole risolvere determinati problemi sui reticoli utilizzando la base $\mathbf{A}$ piuttosto che con $\mathbf{B}$. Per questi motivi il CVP sarà il fulcro dei problemi discussi in questa tesi assieme al SVP, il quale verrà trattato prevalentemente per quanto riguarda la crittoanalisi di GGH.

2.3 Riduzione di un reticolo

2.3.1 Rapporto di Hadamard

Si supponga di avere a disposizione due basi **A** e **B** che godono della proprietà di generare lo stesso reticolo. Seppur condividendo tale caratteristica, **A** e **B** sono in realtà molto diverse nella loro struttura; in particolare **A** è composta da vettori corti e quasi ortogonali fra loro mentre **B** è composta da vettori lunghi e quasi paralleli fra loro.
La qualità di una base risiede in queste differenze dei vettori costituenti le basi, chiamiamo quindi base "buona" **A** e base "cattiva" **B**. E' necessario però definire una metrica per valutare quanto una base sia buona o meno; a tal proposito Hadamard[10] introdusse una formula quantitativa per misurare la qualità di una base reticolare, il cosiddetto rapporto di Hadamard.

Data una base $\mathbf{B} = [\mathbf{b_1}, \mathbf{b_2}. \ldots, \mathbf{b}_n]$ e un reticolo $\mathcal{L}$ di dimensione n generato da **B**, il rapporto di Hadamard della base **B** è definito dal valore:

$$\mathcal{H}(\mathbf{B}) = \left(\frac{\det(\mathcal{L})}{\|\mathbf{b}_1\|_2 \cdot \|\mathbf{b}_2\|_2, \cdots \|\mathbf{b}_n\|_2} \right)^{\frac{1}{n}}$$

Il rapporto di Hadamard si configura nell'intervallo $(0, 1]$, dove più vicino all'1 si è e più la base è buona, viceversa più vicino allo 0 si è e più la base è cattiva. Questa formula verrà utilizzata come unica misura per verificare la qualità degli esempi di basi che verranno presentate più avanti in questa tesi.

2.3.2 Ortogonalizzazione Gram-Schmidt

Ora che è possibile giudicare una base dato il suo rapporto di Hadamard, utilizziamo la base **B** definita nella precedente sezione, la quale ipotizziamo abbia un $\mathcal{H}(\mathbf{B})$ prossimo allo zero. Se volessimo utilizzare questa base per risolvere uno dei problemi dei reticoli, molto probabilmente non riusciremmo mai a raggiungere una soluzione che sia valida o quantomeno che sia vicina alla soluzione ottima. A questo proposito sono stati ideati degli algoritmi in grado di ortogonalizzare una base cattiva per convertirla in una buona e mantenere le proprietà del reticolo iniziale, si ottiene quindi una base $\mathbf{B}'$ tale che: $\mathcal{H}(\mathbf{B}^*) \approxeq 1$ e che $\det(\mathbf{B}) = \det(\mathbf{B}^*)$. Nell'ambito della riduzione di reticoli è importante notare come il gap di un reticolo giochi un ruolo chiave: è noto che più il gap è grande e più la riduzione è semplice.

Prima di discutere questo tipo di algoritmi è necessario affrontare brevemente l'algoritmo di Gram-Schmidt, il quale, esegue un tipo di ortogonalizzazione che viene applicata su spazi vettoriali e che è anche chiamata Ortogonalizzazione Gram-Schmidt (GSO). Questo algoritmo non è adottabile direttamente sulle basi reticolari in quanto esso andrebbe a violare la proprietà dei coefficienti integrali, di fondamentale importanza nella definizione di reticolo. Nonostante ciò, questo algoritmo gode di una proprietà chiave che viene utilizzata in algoritmi di riduzione dei reticoli. Come dimostrato in [10, Teorema 7.13]:
siano $\text{span}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ e $\text{span}(\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*)$ gli spazi vettoriali generati rispettivamente dalle righe di $\mathbf{B}$ e $\mathbf{B}^*$, allora se $\mathbf{B}^*$ è il risultato di GSO applicato a $\mathbf{B}$:

$$\text{span}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \text{span}(\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*).$$

Quindi facendo uso del GSO come subroutine di un algoritmo per la trasformazione delle matrici di spazi vettoriali, si ottiene una importante riduzione del costo computazionale e nel contempo, si semplifica l'implementazione di algoritmi per la riduzione di reticoli.

Algoritmo 1: Algoritmo di Gram-Schmidt

Input: Una matrice $\mathbf{B}$ tale che rango($\mathbf{B}$) = righe($\mathbf{B}$)
Output: Una matrice $\mathbf{B}^*$ ortogonale
$\mathbf{b}_1^* = \mathbf{b}_1$
for $i = 2$ **to** n **do**
  for $j = 1$ **to** $i - 1$ **do**
    $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$
  end
  $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*$
end
return $\mathbf{B}^*$

Dove rango() indica il rango e righe() il numero delle righe.

2.3.3 Algoritmo di Lenstra-Lenstra-Lovász

L'algoritmo di Lenstra-Lenstra-Lovász (LLL)[11, 10] è noto come uno dei più famosi algoritmi per la riduzione dei reticoli. In teoria, opera con un tempo polinomiale $O(n^6(\log \mathcal{E})^3)$, dove n è la dimensione di un reticolo $\mathcal{L}$ dato ed $\mathcal{E}$ rappresenta la massima lunghezza euclidea dei vettori nella base fornita. Il risultato di LLL è una base

ridotta, il cui vettore più breve può essere considerato una soluzione approssimata dell'apprSVP con un fattore di $2^{(n-1)/2}$ rispetto alla lunghezza del vettore corretto più corto. Nonostante questo fattore sia esponenziale, l'algoritmo si dimostra sorprendentemente efficiente nella pratica e ciò lo rende un tassello fondamentale negli algoritmi di risoluzione del CVP e del SVP.
Una base $\mathbf{B}^*$ per essere considerata LLL-ridotta deve soddisfare due condizioni:

- Condizione di grandezza: $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle} \leq \eta$ per ogni $1 \leq j < i \leq n$.
- Condizione di Lovász: $\langle \mathbf{b}_i^*, \mathbf{b}_i^* \rangle \geq (\delta - \mu_{i,i-1}^2) \langle \mathbf{b}_i^*, \mathbf{b}_i^* \rangle$ per ogni $1 < i \leq n$.

I valori δ e η sono standardizzati rispettivamente a $\frac{3}{4}$ e $\frac{1}{2}$.

Algoritmo 2: Algoritmo di LLL, con $\delta = \frac{3}{4}, \eta = \frac{1}{2}$

Input: Una matrice $\mathbf{B}$ che sia base di un reticolo
Output: Una matrice $\mathbf{B}^*$ LLL-ridotta
$k = 1$
$\mathbf{b}_1^* = \mathbf{b}_1$
while $k <= n$ **do**
  for $j = k - 1$ **to** 0 **do**
    if $|\mu_{k,j}| > \eta$ **then** `// Condizione di grandezza`
      $\mathbf{b}_k = \mathbf{b}_k - \lfloor \mu_{k,j} \rceil \mathbf{b}_j$
      GramSchmidt($\mathbf{B}$)
    end
  end
  if $\langle \mathbf{b}_k^*, \mathbf{b}_k^* \rangle \geq (\delta - \mu_{k,k-1}^2) \langle \mathbf{b}_{k-1}^*, \mathbf{b}_{k-1}^* \rangle$ **then** `// Condizione di Lovász`
    $k = k + 1$
  end
  else
    Scambia $\mathbf{b}_{k-1}$ e $\mathbf{b}_k$
    GramSchmidt($\mathbf{B}$)
    $k = \max(k - 1, 1)$
  end
end

Esempio 2.3.1. (Riduzione di una base con LLL) Sia $\mathcal{L}$ un reticolo generato dalla matrice:

$$\mathbf{B} = \begin{bmatrix} 87634 & 88432 & 94345 \\ 32323 & 27883 & 40323 \\ -21221 & -11234 & -32123 \end{bmatrix}$$

$$\text{con } \mathcal{H}(\mathbf{B}) = 0.14318 \text{ e } \det(\mathbf{B}) = -1079906335101.$$

Si applichi ora una riduzione LLL alla matrice $\mathbf{B}$:

$$\mathbf{B}^* = \begin{bmatrix} -784 & 632 & 2701 \\ -14823 & 9207 & -7717 \\ -13454 & -14753 & -97 \end{bmatrix}$$

Ricalcolando $\mathcal{H}(\mathbf{B}^*)$ è possibile osservare che:

$$\mathcal{H}(\mathbf{B}^*) = 0.99442 \text{ e } \det(\mathbf{B}^*) = 1079906335101.$$

E' stato ottenuto un incremento notevole del rapporto di Hadamard grazie alla riduzione LLL senza interferire con le proprietà della base $\mathbf{B}$. Infatti $|\det(\mathbf{B})| = |\det(\mathbf{B}^*)|$ e, usando la formula descritta nella Sezione 2.1, è possibile trovare una matrice di interi

$$\mathbf{U} = \begin{bmatrix} -1 & 4 & 2 \\ -6 & 25 & 14 \\ -3 & 11 & 5 \end{bmatrix} \quad \text{con } \det(\mathbf{U}) = -1$$

tale per cui $\mathbf{UB} = \mathbf{B}^*$.

2.3.4 Varianti di LLL

LLL è un eccellente algoritmo in grado di restituire in un tempo polinomiale una matrice quasi ortogonale partendo da una con vettori quasi paralleli, o che comunque è ritenibile di bassa qualità. Esistono però varianti che ne velocizzano i calcoli, così come altri algoritmi capaci di restituire una base di qualità ancora superiore rispetto a quella ottenuta con la riduzione LLL. Di seguito vengono presentate brevemente tre versioni dell'algoritmo.

La prima versione discussa è quella in virgola mobile (FPLLL)[12], la quale utilizza aritmetica in virgola mobile a precisione arbitraria per accelerare i calcoli razionali dell'algoritmo originale. Questa versione ha come vantaggio un aumento delle performance: in comparazione con LLL il tempo di computazione nel caso peggiore è $O(n^3(\log \mathcal{E})^2)$. E' importante notare che l'utilizzo di aritmetica a virgola mobile per velocizzare i calcoli è una tenica comune e utilizzabile per tutti gli algoritmi di riduzione dei reticoli spiegati in questa sezione.

La seconda versione è stata presentata da Schnorr-Euchner [13] ed il suo nome originale è "deep insertions" ovvero inserzioni profonde. In LLL (Algoritmo 2), è presente un passaggio in cui avviene uno scambio tra il vettore $\mathbf{b}_{k-1}$ e $\mathbf{b}_k$, il quale di solito permette qualche riduzione di grandezza ulteriore del nuovo $\mathbf{b}_k$. Nella variante deep insertions, viene invece inserito $\mathbf{b}_k$ tra $\mathbf{b}_{i-1}$ e $\mathbf{b}_i$ con i che viene scelta in modo

da apportare una maggiore riduzione di grandezza. L'algoritmo risultante, nel caso peggiore, potrebbe non terminare in un tempo polinomiale, ma in pratica, quando eseguito sulla maggioranza dei reticoli, termina rapidamente e può fornire in output una base ridotta significativamente migliore di quella di LLL standard.
L'ultima variante discussa è basata sull'algoritmo di riduzione Korkin–Zolotarev (KZ)[2, Sezione 18.5]. Le caratteristiche di una base KZ-ridotta sono generalmente migliori rispetto a quelle di LLL, ma richiedono una complessità maggiore e un tempo di computazione non polinomiale; per le proprietà complete si veda il riferimento. Più nel dettaglio, il problema principale, è che non esiste un algoritmo in grado di computare una base KZ in tempo polinomiale. L'algoritmo più veloce conosciuto richiede un tempo di computazione esponenziale rispetto alla dimensione. Per compensare a tale problema KZ apporta un grande vantaggio in rispetto all'accuratezza della riduzione, infatti, il primo vettore di una base KZ-ridotta è sempre una soluzione al SVP. Dato che la complessità di KZ cresce con n, è logico pensare che a basse dimensioni sia comunque sufficientemente veloce. Un'idea è quindi quella di computare una riduzione di proiezioni a dimensioni più basse del reticolo originale. L'algoritmo in questa configurazione prende il nome di Korkine-Zolotarev a blocco (BKZ), il quale, se combinato con LLL, diventa una variante di quest'ultimo chiamata LLL-BKZ. Questa variante è in grado di bilanciare costo computazionale e qualità di riduzione ottenendo così l'algoritmo più efficiente per SVP in grandi dimensioni, dimostrando anche una qualità di riduzione significativamente migliore di quella di LLL standard.

Per reticoli di dimensioni ancora maggiori, dove anche BKZ potrebbe risultare computazionalmente oneroso, è stata sviluppata una versione ulteriormente ottimizzata chiamata BKZ "pruned" o potata [14]. Questa variante mantiene l'efficacia di BKZ nel bilanciare costo computazionale e qualità della riduzione, ma introduce una tecnica di potatura nell'enumerazione dei vettori. Tale tecnica è spesso usata in informatica al fine di ottimizzare algoritmi riducendo lo spazio di ricerca, permettendo così di ottenere soluzioni approssimate (e solitamente corrette) in tempi significativamente minori rispetto all'esplorazione completa.

2.4 Algoritmi per la risoluzione del CVP

2.4.1 Algoritmi di Babai

Nel 1986 Babai[4] propose due algoritmi per la risoluzione di apprCVP, i cosiddetti: "Metodo del Piano più Vicino" e "Tecnica di Arrotondamento". Ai fini di questa tesi, entrambi verranno trattati, sebbene il primo sarà discusso in modo più conciso poiché, come verrà spiegato nei prossimi capitoli, non è stato utilizzato nelle implementazioni proposte.

Il metodo del piano più vicino è il primo algoritmo presentato da Babai, esso si basa sull'impiegare l'ortogonalizzazione di Gram-Schmidt per semplificare il problema. L'algoritmo inizia quindi ortogonalizzando la base del reticolo fornita in input attraverso Gram-Schmidt. Successivamente, procede in maniera iterativa a partire dalla dimensione più alta: il vettore input viene proiettato sul vettore base ortogonale corrispondente e questa proiezione viene approssimata al multiplo intero più vicino del vettore della base originale. Tale approssimazione viene sottratta dal vettore input, generando un nuovo vettore residuo. Questo processo viene ripetuto per le dimensioni inferiori, una alla volta, fino a coprire tutte le dimensioni. Al termine, l'algoritmo fornisce come risultato una soluzione all'apprCVP. Grazie alla sua complessità polinomiale, l'algoritmo riesce a bilanciare efficacemente l'accuratezza dell'approssimazione con il tempo di esecuzione. Per ulteriori dettagli e informazioni sull'algoritmo si veda [2].
Il secondo algoritmo è la tecnica di arrotondamento che, come da nome, si basa principalmente sull'arrotondare dei valori frazionari all'intero più vicino. Seppur la sua implementazione risulti semplice e banale, in realtà la sua dimostrazione teorica è tutt'altro che immediata. A differenza del precedente, non utilizza l'ortogonalizzazione di Gram-Schmidt, ma mantiene comunque una complessità polinomiale. Di seguito viene fornita una spiegazione del suo funzionamento.
Come discusso nella sezione 2.1.2, dati un reticolo $\mathcal{L}$ di dimensione n e una sua base $\mathbf{B}$, per ogni vettore $\mathbf{t} \in \mathbb{R}^n$, con $\mathbf{t} \notin \mathcal{L}$, un'unica decomposizione $\mathbf{t} = \mathbf{f} + \mathbf{v}$ può essere sempre trovata in modo tale che $\mathbf{v} \in \mathcal{L}$ e $\mathbf{f}$ si collochi nel dominio fondamentale $\mathcal{F}$ di $\mathbf{B}$. Questa proprietà fornisce l'idea dietro alla risoluzione dell'apprCVP usata da questo algoritmo: identificare il dominio fondamentale (traslato) rispettivamente a $\mathbf{v} \in \mathcal{L}$, nel quale il vettore target $\mathbf{t}$ si trova. Sia $\mathcal{L}$ un reticolo con dimensione n generato da una base (buona) $\mathbf{B}$ e sia $\mathbf{t}$ un vettore tale che $\mathbf{t} \in \mathbb{R}^n$ e $\mathbf{t} \notin \mathcal{L}$. Dato che $\mathbf{B}$ è una matrice di rango massimo, è possibile calcolare:

$$\mathbf{x} = \mathbf{t}\mathbf{B}^{-1}$$

Da qui si applica la tecnica di arrotondamento, la quale è semplicemente:

$$\mathbf{w} = \sum_{i=1}^{n} \lfloor \mathbf{x}_i \rceil \mathbf{b}_i$$

con $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ e $\lfloor \mathbf{x} \rceil$ che significa prendere l'intero più vicino al numero reale $\mathbf{x}$. Questo algoritmo mira ad identificare il dominio fondamentale (traslato) che il vettore $\mathbf{t}$ localizza e la sua correttezza è strettamente legata alla forma geometrica del dominio fondamentale, è necessaria quindi una base di alta qualità al fine di avere risultati validi.

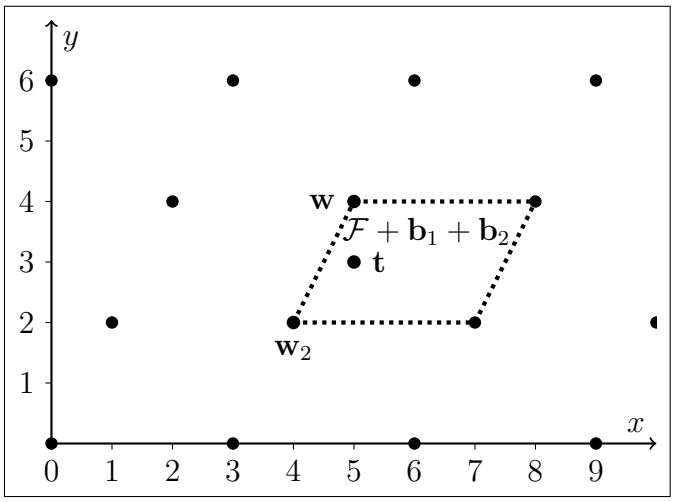


Figura 4: Risoluzione del CVP usando la tecnica di arrotondamento di Babai: $\mathbf{w}$ è il vertice del dominio fondamentale traslato localizzato da $\mathbf{t}$, quindi è soluzione per apprCVP.

Esempio 2.4.1. (Risoluzione del CVP usando la tecnica di arrotondamento di Babai)

Siano $\mathbf{R}$ e $\mathbf{B}$ le stesse basi definite nell'Esempio 2.1.1 e sia $\mathbf{t} \in \mathbb{R}^n, \mathbf{t} \notin \mathcal{L}$ con

$$\mathbf{t} = \begin{bmatrix} 5 & 3 \end{bmatrix}.$$

Si inizi con l'applicare l'algoritmo, dal primo passo si ottiene:

$$\mathbf{R}^{-1} = \begin{bmatrix} 0 & 0.33 \\ 0.5 & -0.16 \end{bmatrix} \quad \text{e} \quad \mathbf{x} = \mathbf{t}\mathbf{R}^{-1} = \begin{bmatrix} 1.5 & 1.16 \end{bmatrix}$$

si applichi ora la tecnica di arrotondamento a $\mathbf{x}$:

$$\lfloor \mathbf{x} \rceil = \begin{bmatrix} 2 & 1 \end{bmatrix}$$

si proceda infine con l'ottenere il risultato finale:

$$\mathbf{w} = \mathbf{x}\mathbf{R} = \begin{bmatrix} 5 & 4 \end{bmatrix}$$

che, come mostrato in Figura 4, è il vettore più vicino a $\mathbf{t}$ con $\|\mathbf{t} - \mathbf{w}\|_2 = 1$. Se si dovesse valutare la qualità della base, si otterrebbe che $\mathcal{H}(\mathbf{R}) = 0.94574$ e, grazie a tali proprietà ortogonali di $\mathbf{R}$, il dominio fondamentale derivante assume una forma geometrica tale per cui l'algoritmo è in grado di raggiungere facilmente la soluzione. Si riesegua ora l'algoritmo su $\mathbf{B}$. Calcolando $\mathcal{H}(\mathbf{B}) = 0.33231$ si scopre che $\mathbf{B}$ offre

una qualità molto più bassa rispetto a $\mathbf{R}$. Procedendo si ottiene che:

$$\mathbf{x}_2 = \mathbf{t}\mathbf{B}^{-1} = \begin{bmatrix} 1.5 & 1.16 \end{bmatrix} \quad \text{e quindi} \quad \lfloor \mathbf{x}_2 \rceil = \begin{bmatrix} 2 & 1 \end{bmatrix}.$$

Computando l'ultimo passaggio, il vettore risultante è:

$$\mathbf{w}_2 = \mathbf{x}_2\mathbf{B} = \begin{bmatrix} 4 & 2 \end{bmatrix}$$

il quale non è soluzione corretta all'apprCVP in quanto $\|\mathbf{t} - \mathbf{w}_2\|_2 = 1.41 > \|\mathbf{t} - \mathbf{w}\|_2$.

La principale differenza tra i due algoritmi di Babai è che il metodo del piano più vicino risulta essere più preciso in quanto i valori frazionari vengono arrotondati in maniera adattiva piuttosto che tutti insieme in un'unica volta. Inoltre l'utilizzo dell'aritmetica in virgola mobile, introdotta nella sezione 2.3.4, consente di ottenere tempi di esecuzione ulteriormente più rapidi.

2.4.2 Tecnica di incorporamento

Babai, oltre alla presentazione dei due algoritmi precedentemente trattati, ha dimostrato anche quanto una base ridotta migliori l'approssimazione della soluzione ad apprCVP. In particolare, con una base LLL-ridotta, questo porta ad un fattore di approssimazione esponenziale per entrambi i suoi algoritmi. Nella pratica però, il metodo migliore per risolvere apprCVP, è la cosiddetta tecnica di incorporamento[2], tecnica euristica che si basa sul ridurre il CVP a un SVP.
Sia $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ la base di un reticolo $\mathcal{L}$ di dimensione n e sia $\mathbf{t} \in \mathbb{R}^n, \mathbf{t} \notin \mathcal{L}$. La tecnica di incorporamento impone la costruzione di un reticolo di dimensione $n+1$ con la seguente struttura:

$$\mathbf{M} = \begin{bmatrix} \cdots & \mathbf{b}_1 & \cdots & 0 \\ \cdots & \vdots & \cdots & 0 \\ \cdots & \mathbf{b}_n & \cdots & 0 \\ \cdots & \mathbf{t}_1 & \cdots & 1 \end{bmatrix}$$

Il nuovo reticolo $\mathcal{L}(\mathbf{M})$ è strutturato in modo tale da avere lo stesso determinante di $\mathcal{L}(\mathbf{B})$ e quasi la stessa dimensione, ci si può quindi aspettare che il vettore più corto di $\mathcal{L}(\mathbf{M})$ abbia quasi la stessa lunghezza di quello di $\mathcal{L}(\mathbf{B})$. Si assuma che $\mathbf{w} \in \mathcal{L}$ minimizzi la distanza per $\mathbf{t}$ e sia $\mathbf{u} = \mathbf{t} - \mathbf{w}$, allora il vettore

$$\mathbf{v} = \begin{bmatrix} \mathbf{u} & 1 \end{bmatrix}$$

appartiene a $\mathcal{L}(\mathbf{M})$ e, se dovesse anche essere il suo vettore più corto, si potrebbe risolvere l'apprCVP di $\mathcal{L}(\mathbf{B})$ determinando l'apprSVP di $\mathcal{L}(\mathbf{M})$. Per ottenere $\mathbf{v}$ è

sufficiente ridurre $\mathbf{M}$ mediante algoritmi come LLL (o meglio BKZ) per poi ottenere $\mathbf{w}$ calcolando $\mathbf{t} - \mathbf{u}$. È importante notare che il gap del reticolo di $\mathcal{L}(\mathbf{M})$ è approssimativamente il rapporto tra la lunghezza del vettore più corto di $\mathcal{L}(\mathbf{B})$ e la lunghezza di $\mathbf{u}$. Aumentare la lunghezza del vettore più corto di $\mathcal{L}(\mathbf{B})$ rende il gap del reticolo di $\mathcal{L}(\mathbf{M})$ più ampio, facilitando così la riduzione. Quando si discute del gap del reticolo in relazione a un'istanza del CVP, è importante chiarire che ci si riferisce in realtà al gap del reticolo dell'istanza SVP corrispondente. Questa istanza SVP viene creata attraverso una tecnica di embedding che trasforma l'istanza CVP originale in un'istanza SVP equivalente. Pertanto, il concetto di gap del reticolo, originariamente definito per SVP, viene esteso indirettamente alle istanze CVP attraverso questa trasformazione. Un problema nella pratica sta nella scelta di $\mathbf{t}$: teoricamente $\mathbf{t}$ può appartenere all'insieme $\mathbb{R}$, ma questo creerebbe problemi nella costruzione della nuova base $\mathbf{M}$ la quale non soddisferebbe più la proprietà dei coefficienti integrali che sta alla base della definizione di reticolo. Tale problema viene discusso e affrontato nell'attacco di Nguyen contro GGH presentato nella sezione 3.2.2. Nel concreto si tenta di mantenere $\mathbf{t} \in \mathbb{Z}^n$ in modo da evitare problemi di questa natura.

Esempio 2.4.2. (Risoluzione del CVP usando la tecnica di incorporamento) Siano $\mathbf{R}$, $\mathbf{B}$ e $\mathbf{t}$ le stesse basi definite nell'Esempio 2.4.1. Seguendo quanto descritto nella tecnica di incorporamento, si costruisca la matrice

$$\mathbf{M} = \begin{bmatrix} \mathbf{r}_{0,0} & \mathbf{r}_{1,0} & 0 \\ \mathbf{r}_{0,1} & \mathbf{r}_{1,1} & 0 \\ \mathbf{t}_{0,0} & \mathbf{t}_{1,0} & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 \\ 3 & 0 & 0 \\ 5 & 3 & 1 \end{bmatrix}$$

e la si riduca usando un algoritmo di riduzione, in questo caso LLL:

$$\mathbf{M}^* = \begin{bmatrix} 0 & -1 & 1 \\ 1 & 1 & 1 \\ 2 & -1 & -1 \end{bmatrix}.$$

Infine è necessario che si estraggano i primi n valori dal vettore riga più corto di $\mathbf{M}^*$ e sottrarli poi a $\mathbf{t}$. In questo caso il vettore più corto risulta essere il primo, quindi $\mathbf{u} = [0 \ -1]$. Completando questo passaggio si deduce che:

$$\mathbf{w} = \mathbf{t} - \mathbf{u} = \begin{bmatrix} 5 & 3 \end{bmatrix} - \begin{bmatrix} 0 & -1 \end{bmatrix} = \begin{bmatrix} 5 & 4 \end{bmatrix}$$

la quale è soluzione all' apprCVP con $\|\mathbf{t} - \mathbf{w}\|_2 = 1$. Utilizzando la base cattiva $\mathbf{B}$,

invece, si otterrebbe:

$$\mathbf{M}_2 = \begin{bmatrix} 5 & 4 & 0 \\ -6 & -6 & 0 \\ 5 & 3 & 1 \end{bmatrix} \quad \text{con} \quad \mathbf{M}_2^* = \begin{bmatrix} 0 & -1 & 1 \\ -1 & -1 & -1 \\ 2 & -1 & -1 \end{bmatrix}.$$

Ed effettuando l'ultimo passaggio:

$$\mathbf{w}_2 = \mathbf{t} - \mathbf{u}_2 = \begin{bmatrix} 5 & 3 \end{bmatrix} - \begin{bmatrix} 0 & -1 \end{bmatrix} = \begin{bmatrix} 5 & 4 \end{bmatrix}$$

che è la stessa soluzione ottenuta con la base $\mathbf{R}$.

Grazie a questo esempio si può comprendere meglio l'efficacia nella pratica di questa tecnica: in comparazione con l'algoritmo di arrotondamento di Babai, nonostante la bassa qualità della seconda base, si è riusciti comunque a trovare una soluzione corretta.

Capitolo 3

Crittosistema a chiave pubblica GGH

3.1 Struttura e funzionamento di GGH

Nel 1996, Oded Goldreich, Shafi Goldwasser e Shai Halevi[5] hanno introdotto un nuovo sistema crittografico a chiave pubblica basato sulla difficoltà di risolvere CVP in reticoli di dimensioni elevate.
L'idea dietro GGH è la seguente: si supponga di avere un messaggio $\mathbf{m}$ codificato in un vettore appartenente ad un reticolo $\mathcal{L}$, un vettore target $\mathbf{t} \notin \mathcal{L}$ vicino ad $\mathbf{m}$ e due basi $\mathbf{R}$ e $\mathbf{B}$ entrambe generanti $\mathcal{L}$ e rappresentanti rispettivamente base privata e base pubblica. Siano $\mathbf{R}$ una base buona e $\mathbf{B}$ una base cattiva, allora, tramite l'utilizzo di uno degli algoritmi di risoluzione del CVP (Sezione 2.4), sarà possibile ritrovare il vettore più vicino a $\mathbf{t}$ (che risulterà essere $\mathbf{m}$) usando la base privata, ma non usando la base pubblica.
Più formalmente, GGH è definito da una funzione trapdoor (ovvero una funzione matematica che è facile da calcolare in una direzione, ma molto difficile da invertire senza dei dati segreti), la quale è composta da 4 funzioni probabilistiche di complessità polinomiale:

- Generate: Dato in input un intero positivo n vengono generate due basi $\mathbf{R}$ e $\mathbf{B}$ di rango massimo in $\mathbb{Z}^n$ e un numero positivo reale σ. Le basi $\mathbf{R}$ e $\mathbf{B}$ sono rappresentate da matrici $n \times n$ e sono rispettivamente denominate base privata e base pubblica. Sia $\mathbf{R}$ che $\mathbf{B}$ generano lo stesso reticolo $\mathcal{L}$ e, insieme a σ, danno origine a chiave privata e chiave pubblica. Per maggiori dettagli riguardo la generazione delle chiavi si veda la prossima sezione.

- Sample: Dati in input $\mathbf{B}, \sigma$ vengono originati i vettori $\mathbf{m}, \mathbf{e} \in \mathbb{R}^n$.
  Il vettore $\mathbf{m}$ viene scelto casualmente da un cubo in $\mathbb{Z}^n$ che sia sufficientemente

grande. Gli autori suggeriscono di scegliere in maniera casuale ogni valore di $\mathbf{m}$ uniformemente dall'intervallo $[-n^2, -n^2+1, \ldots, +n^2]$, sottolineando però che la scelta di n^2 è arbitraria e che non hanno prove di come essa possa influenzare la sicurezza del crittosistema stesso. Un intervallo sufficientemente grande che viene normalmente utilizzato è $[-128, 127]$.
Il vettore $\mathbf{e}$ invece, viene scelto casualmente in $\mathbb{R}^n$ in modo tale la media dei valori sia zero e la varianza sia σ^2. Il metodo più semplice per generare tale vettore è quello di scegliere ogni valore di $\mathbf{e}$ come $\pm\sigma$ con probabilità $\frac{1}{2}$. Questo vettore ha l'importante funzione di essere un errore che viene aggiunto al calcolo del testo cifrato per complicarne la decifratura.

- Evaluate: Dati in input $\mathbf{B}, \sigma, \mathbf{m}, \mathbf{e}$ si calcola $\mathbf{c} = \mathbf{mB} + \mathbf{e}$. Con questo calcolo si ottiene il messaggio cifrato che è rappresentato da $\mathbf{c}$.

- Invert: Dati in input $\mathbf{R}, \mathbf{c}$ si utilizza la tecnica di arrotondamento di Babai per invertire la funzione trapdoor e ricavare il messaggio originale.

3.1.1 Generazione delle chiavi

La generazione delle chiavi è un elemento cruciale in tutti i crittosistemi asimmetrici. In GGH, per costruire le chiavi, è indispensabile ottenere prima due basi: una pubblica e una privata. La sicurezza di questo crittosistema si basa sul fatto che la base pubblica non sia di qualità sufficientemente alta, in modo tale da impedire l'applicazione efficace di un algoritmo di risoluzione del CVP al testo cifrato, evitando così di recuperare il messaggio originale. È dunque fondamentale il modo in cui vengono generate la base privata e, soprattutto, la base pubblica, per garantire le caratteristiche necessarie a mantenere la sicurezza del crittosistema. In questa sezione verrà quindi analizzata la struttura della funzione Generate, la quale si occupa di quanto introdotto precedentemente.
Questa funzione prende come unico parametro in input la dimensione n dalla quale dipende la grandezza delle basi generate. In linea con quanto detto nella Sezione 2.2, più n cresce e più i problemi sui reticoli si fanno complessi, rendendo quindi più sicuro il crittosistema. A discapito di ciò però, man mano che la complessità aumenta, il tempo di esecuzione delle funzioni e lo spazio in bits delle basi diventano più onerosi. Gli autori di [5, Sezione 3.3.1] a tal proposito ipotizzarono che, presi in considerazione gli algoritmi di riduzione disponibili al tempo, un n tra 150 e 200 fosse sufficiente, anche se ciò si rivelerà essere sbagliato. Dopo aver scelto un n adeguato, si procede con il generare la base privata $\mathbf{R}$ e, successivamente, decidere la distribuzione con la quale essa verrà originata. Due sono le proposte avanzate:

1. Generare una base $\mathbf{R}$ casuale: ogni elemento viene scelto in maniera casuale uniformemente nell'intervallo $[-l, \ldots, l]$ per qualche valore l. In [5] è stato provato

che la scelta di l non influenza particolarmente la qualità della base generata, per cui è stato scelto un l tra ± 4 al fine di semplificare alcune operazioni di calcolo.

2. Generare una base $\mathbf{R}$ rettangolare: si inizia con il moltiplicare la matrice identità $\mathbf{I}$ per qualche numero k ottenendo così $k\mathbf{I}$. Si genera poi una matrice $\mathbf{R}'$ casuale (punto 1.) per poi computare $\mathbf{R} = \mathbf{R}' + k\mathbf{I}$.

Come preannunciato, una volta generata la base privata $\mathbf{R}$, è necessario derivare la base pubblica rappresentata da un'altra base $\mathbf{B}$, tale che $\mathbf{R}$ e $\mathbf{B}$ generino lo stesso reticolo $\mathcal{L}$. Dato che ogni base di $\mathcal{L}(\mathbf{R})$ è ottenuta con $\mathbf{B} = \mathbf{UR}$ per qualche matrice unimodulare $\mathbf{U}$, allora ottenere $\mathbf{B}$ equivale ad ottenere una matrice unimodulare casuale. Anche in questo caso, due sono i metodi proposti per generare tali matrici:

1. Il primo metodo consiste nell'applicare una sequenza di operazioni elementari sulle colonne della matrice identità, mantenendo però gli uni sulla diagonale principale. Ad ogni step viene aggiunta alla i-esima colonna una combinazione lineare intera casuale delle altre colonne. I coefficienti della combinazione lineare sono scelti casualmente in $\{-1, 0, 1\}$ con un bias verso zero (probabilità $\frac{5}{7}$), in modo che i numeri non crescano troppo velocemente. Viene suggerito dagli autori stessi di eseguire l'algoritmo almeno due volte.

2. Il secondo metodo si basa sul generare delle matrici triangolari superiori ($\mathbf{S}$) e inferiori ($\mathbf{L}$) con ± 1 sulla diagonale principale. I restanti elementi della matrice che non sono zeri vengono scelti casualmente tra $\{-1, 0, 1\}$. In particolare sarà necessario moltiplicare $\mathbf{R}$ per almeno 4 paia di $\mathbf{SL}$ al fine di ottenere un $\mathbf{B}$ sufficientemente sicuro.

E' stato provato dagli stessi autori che entrambi i metodi offrono lo stesso livello di sicurezza, anche se il secondo, in comparazione, genera matrici con numeri più grandi andando quindi a complicare i calcoli successivi.
Dopo aver generato due $\mathbf{R}$ e $\mathbf{B}$ con le qualità necessarie, non rimane altro che determinare σ. Questo valore è molto importante perchè esso aggiunge una complessità maggiore per quanto riguarda l'inversione della funzione trapdoor, diventando così un fattore di bilanciamento. Richiamando quanto definito nelle Sezioni 2.2 e 2.4.1, la tecnica di arrotondamento di Babai è una proposta per la risoluzione dell'apprCVP, il quale, ritorna un vettore più vicino che non sempre risulta essere la soluzione più corretta. Dato che GGH si basa su questo algoritmo per decifrare un messaggio, è possibile definire questo crittosistema come probabilistico: in certe situazioni neanche la base privata può essere usata per ritrovare il messaggio originale $\mathbf{m}$ e, viceversa, in altre situazioni, la base pubblica potrebbe essere usata per decifrare il messaggio. Per evitare questi casi è stato ideato il parametro σ, il quale, viene utilizzato per

generare il vettore di errore $\mathbf{e}$ che, una volta aggiunto a $\mathbf{c}$, complicherà ulteriormente l'inversione. L'idea è che la qualità di $\mathbf{B}$ sia sufficientemente bassa da non poter correggere l'errore, ma allo stesso tempo, permettere a $\mathbf{R}$ di essere in grado di farlo. È cruciale che σ non sia né troppo grande, altrimenti $\mathbf{R}$ non riuscirebbe a recuperare il messaggio, né troppo piccolo, per evitare che $\mathbf{B}$ possa riuscirci.
In [5, Sezione 3.2] vengono proposte due metriche, ciascuna basata rispettivamente sulla norma L_1 e L_∞, per definire un limite a σ in maniera che non possa causare errori di inversione usando la base privata. La prima metrica è la più solida, poiché limita σ a un valore massimo che garantisce sempre il successo dell'inversione. La seconda, invece, restringe σ a un livello in cui la probabilità di errori d'inversione è molto bassa. In entrambi i casi, con dimensioni elevate, il valore massimo di σ si aggira intorno a 3, risultando in un valore standard che bilancia sicurezza e affidabilità.
Ora che tutti i parametri sono stati determinati è possibile costruire le due chiavi:

- La chiave pubblica è definita semplicemente dalla coppia $(\mathbf{B}, \sigma)$
- La chiave privata, invece, non è definita semplicemente da $\mathbf{R}$ in quanto, seppure logicamente corretto, non è il metodo più efficiente. Verrà quindi utilizzata la coppia $(\mathbf{R}, \mathbf{R}^{-1})$ in modo da velocizzare la decifratura.

La decifratura avviene tramite la tecnica di arrotondamento di Babai spiegata in sezione 2.4.1:

$$\mathbf{m} = \lfloor \mathbf{c}\mathbf{R}^{-1} \rceil \mathbf{R}\mathbf{B}^{-1}$$

dove, per semplicità:

$$\mathbf{m} = \mathbf{w}\mathbf{B}^{-1} \quad \text{con} \quad \mathbf{w} = \lfloor \mathbf{c}\mathbf{R}^{-1} \rceil \mathbf{R}.$$

3.1.2 Esempio pratico

Prima di affrontare le varie tipologie di attacchi a GGH, viene mostrato un semplice esempio (a dimensione 3) di come due entità, rispettivamente Alice e Bob, possano utilizzare questo crittosistema per scambiare messaggi.

Esempio 3.1.1. (Esempio di funzionamento di GGH) Sia $\mathbf{R}$ la base privata di Alice definita come:

$$\mathbf{R} = \begin{bmatrix} 12 & -4 & -1 \\ 1 & 8 & -1 \\ -4 & 1 & 14 \end{bmatrix} \quad \text{con } \mathcal{H}(\mathbf{R}) = 0.96762$$

Alice procede col generare la sua base pubblica $\mathbf{B}$ moltiplicando $\mathbf{R}$ con una matrice unimodulare casuale $\mathbf{U}$:

$$\mathbf{U} = \begin{bmatrix} 12 & -3 & -1 \\ -3 & 1 & 1 \\ -14 & 3 & 0 \end{bmatrix} \quad \text{quindi } \mathbf{B} = \mathbf{U}\mathbf{R} = \begin{bmatrix} 145 & -73 & -23 \\ -39 & 21 & 16 \\ -165 & 80 & 11 \end{bmatrix}.$$

E' possibile osservare come $\mathbf{B}$ abbia un rapporto di Hadamard molto basso, più precisamente $\mathcal{H}(\mathbf{B}) = 0.07403$. Infine, utilizzando $\sigma = 3$, Alice compone le sue due chiavi:

$$\mathbf{K}_{private} = (\mathbf{R}, \mathbf{R}^{-1}) \text{ e } \mathbf{K}_{public} = (\mathbf{B}, \sigma).$$

Bob decide di mandare un messaggio $\mathbf{m} = [-48\ 29 - 76]$ con vettore di errore $\mathbf{e} = [3\ 3\ 3]$. Utilizza quindi la chiave pubblica di Alice e ottiene il corrispondente testo cifrato:

$$\mathbf{c} = \begin{bmatrix} -48 & 29 & -76 \end{bmatrix} \begin{bmatrix} 145 & -73 & -23 \\ -39 & 21 & 16 \\ -165 & 80 & 11 \end{bmatrix} . + \begin{bmatrix} 3 & 3 & 3 \end{bmatrix} = \begin{bmatrix} 4452 & -1964 & 735 \end{bmatrix}.$$

Alice, una volta ricevuto il messaggio cifrato, è in grado di decifrarlo in maniera efficiente usando la sua chiave privata. Infatti, avendo a disposizione

$$\mathbf{R}^{-1} = \begin{bmatrix} \frac{113}{1363} & \frac{55}{1363} & \frac{12}{1363} \\ -\frac{10}{1363} & \frac{164}{1363} & \frac{11}{1363} \\ \frac{33}{1363} & \frac{4}{1363} & \frac{100}{1363} \end{bmatrix} \text{ e } \mathbf{B}^{-1} = \begin{bmatrix} -\frac{1049}{1363} & -\frac{1037}{1363} & -\frac{685}{1363} \\ -\frac{2211}{1363} & -\frac{2200}{1363} & -\frac{1423}{1363} \\ \frac{345}{1363} & \frac{445}{1363} & \frac{198}{1363} \end{bmatrix}$$

Alice, ottiene il messaggio originale calcolando:

$$\mathbf{x} = \lfloor \mathbf{c}\mathbf{R}^{-1} \rceil = \begin{bmatrix} 401 & -55 & 77 \end{bmatrix} \text{ e } \mathbf{m} = \mathbf{x}\mathbf{R}\mathbf{B}^{-1} = \begin{bmatrix} -48 & 29 & -76 \end{bmatrix}.$$

Si supponga ora che ci sia una terza persona, chiamata Eve, in ascolto nel canale di comunicazione tra Alice e Bob. Eve riesce ad ottenere la chiave pubblica di Alice e il messaggio cifrato inviato da Bob. Decide quindi di provare a decifrarlo usando la base pubblica invece della privata. Dato che non è in possesso della chiave privata di Alice, Eve tenterà la decifrazione usando solo la base pubblica $\mathbf{B}$.
Dato che $\mathbf{B}\mathbf{B}^{-1} = 1$, la tecnica di arrotondamento di Babai si semplifica alla seguente formula:

$$\mathbf{m}' = \lfloor \mathbf{c}\mathbf{B}^{-1} \rceil = \begin{bmatrix} -54 & 23 & -80 \end{bmatrix}$$

Il vettore $\mathbf{m}'$ ottenuto presenta evidenti similitudini con il messaggio originale $\mathbf{m}$, differenziandosi solo per alcune cifre. Sebbene in questo caso l'errore possa apparire quasi trascurabile è importante precisare che l'esempio è stato presentato in una dimensione molto bassa. Infatti la grandezza dell'errore è direttamente proporzionale all'aumentare della dimensione delle chiavi usate. Di conseguenza, il solo uso della base pubblica, non è sufficiente ad ottenere il messaggio originale.

3.2 Crittoanalisi di GGH

In questa sezione saranno esaminate le vulnerabilità di GGH e gli attacchi derivanti da esse. I principali attacchi a cui GGH è soggetto includono:

- Computazione di una chiave privata: eseguendo una riduzione della base pubblica $\mathbf{B}$ si tenta di ottenere una chiave privata $\mathbf{B}'$ di qualità pari o simile a quella originale.
- Risoluzione diretta del CVP: tentare di risolvere il CVP del testo cifrato $\mathbf{c}$ rispetto al reticolo definito dalla base pubblica $\mathbf{B}$.
- Attacco di Nguyen: sfruttando la particolare struttura del vettore di errore $\mathbf{e}$ adottata dagli autori del crittosistema, è possibile ricondursi ad un'istanza del CVP molto più semplice di quella proposta da GGH.
- Attacco basato su informazioni parziali: conoscendo sufficienti elementi del messaggio originale è possibile costruire un'istanza del CVP ancora più semplice di quella ottenuta tramite l'attacco di Nguyen.

3.2.1 Crittoanalisi originale

L'attacco più ovvio e semplice tra quelli proposti è la computazione di una chiave privata per invertire la funzione trapdoor. Uno studio dettagliato e combinato con esperimenti pratici ha portato però gli autori a considerarlo inefficace per una dimensione maggiore di 100. Un miglioramento dell'attacco appena descritto consiste nell'utilizzo di uno degli algoritmi per approssimare il CVP presentati nella Sezione 2.4.1, si rientra quindi nell'attacco basato su risoluzione diretta del CVP. Gli autori, basandosi su quanto descritto finora, hanno ipotizzato che, se l'algoritmo di riduzione utilizzato è LLL, il loro schema risulti sicuro per dimensioni superiori a 150 indipendentemente dal tipo di algoritmo scelto per risolvere il CVP. Tuttavia, poiché esistono algoritmi di riduzione migliori (Sezione 2.3.4), la loro conclusione è che la funzione trapdoor di GGH dovrebbe essere sicura per dimensioni comprese tra 250 e 300.
Di seguito viene presentato un esempio in dimensione 3 dell'attacco basato su risoluzione diretta del CVP. Per eseguire tale attacco sono stati utilizzati l'algoritmo LLL e la tecnica di incorporamento. Nonostante BKZ sia l'opzione più efficace, la bassa dimensionalità del problema rende i risultati ottenuti con LLL molto simili se non uguali. Pertanto, per semplicità, è stato scelto l'algoritmo LLL.

Esempio 3.2.1. (Esempio di risoluzione diretta del CVP tramite incorporamento) Siano $(\mathbf{B}, \sigma)$ e $\mathbf{c}$ rispettivamente chiave pubblica e testo cifrato utilizzati tra Alice e Bob nell'esempio 3.1.2. Supponiamo che Eve abbia intercettato il testo cifrato

e la chiave pubblica, e stia cercando di attaccare il crittosistema GGH risolvendo direttamente il CVP.
Decide di procedere tramite tecnica di incorporamento costruendo quindi la seguente matrice:

$$\mathbf{M} = \begin{bmatrix} 145 & -73 & -23 & 0 \\ -39 & 21 & 16 & 0 \\ -165 & 80 & 11 & 0 \\ 4452 & -1964 & 735 & 1 \end{bmatrix}.$$

Come secondo passaggio riduce $\mathbf{M}$ tramite LLL:

$$\mathbf{M}^* = \begin{bmatrix} -2 & 1 & -1 & -4 \\ 3 & 3 & 3 & 1 \\ 0 & 4 & -3 & 3 \\ 7 & -2 & -8 & -2 \end{bmatrix}.$$

Eve a questo punto, secondo quanto definito in sezione 2.4.2, dovrebbe prelevare i primi n valori del vettore riga di $\mathbf{M}^*$ più corto. A causa della composizione del vettore di errore usato in GGH però la selezione del vettore da $\mathbf{M}^*$ risulta essere diversa. In particolare sapendo che $\sigma = 3$ Eve preleverà il vettore riga di forma $[\pm\sigma, \cdots \pm \sigma, 1]$, che non per forza è il vettore più corto di $\mathbf{M}^*$. In questo caso nella matrice è presente un vettore con tale forma, ovvero:

$$\begin{bmatrix} 3 & 3 & 3 & 1 \end{bmatrix} \text{ con conseguente } \mathbf{u} = \begin{bmatrix} 3 & 3 & 3 \end{bmatrix}.$$

Come si può notare $\mathbf{u}$ è uguale al vettore di errore $\mathbf{e}$ utilizzato da Bob nell'esempio 3.1.2, indice del corretto andamento dell'attacco. Come penultimo passaggio Eve calcola il vettore $\mathbf{w}$ più vicino a $\mathbf{c}$:

$$\mathbf{w} = \mathbf{c} - \mathbf{e} = \begin{bmatrix} 4452 & -1964 & 735 \end{bmatrix} - \begin{bmatrix} 3 & 3 & 3 \end{bmatrix} = \begin{bmatrix} 4449 & -1967 & 732 \end{bmatrix}$$

e ottiene infine il messaggio originale $\mathbf{m}$ tramite:

$$\mathbf{m} = \mathbf{w}\mathbf{B}^{-1} = \begin{bmatrix} -48 & 29 & -76 \end{bmatrix}.$$

Contromisure

La principale debolezza di GGH è intrinseca alla sua costruzione: il vettore di errore $\mathbf{e}$ è sempre notevolmente più corto dei vettori nel reticolo. Ciò favorisce quindi un gap di dimensione maggiore nel reticolo incorporato. Tale vulnerabilità viene sfruttata con successo dalla tecnica di incorporamento fino ad una certa dimensione, la quale si colloca tra 250 e 300. Non esiste un modo semplice per risolvere questo problema senza sconvolgere la struttura di GGH, è dunque noto che le istanze CVP derivanti

da tale schema risultano più facili da risolvere rispetto alle istanze CVP generali. L'unica soluzione è anche la più veloce e ovvia: aumentare la dimensione del reticolo oltre 300, in modo da evitare del tutto la possibilità di attacchi analoghi.

3.2.2 Attacco di Nguyen

Questo attacco prende il nome dal suo autore Phong Nguyen[3] il quale, nel 1999, scoprì una vulnerabilità nel crittosistema GGH che permise ad attacchi, come la risoluzione diretta del CVP, di funzionare a dimensioni ancora più elevate di quelle già precedentemente raggiunte. Nguyen notò che la particolare scelta di composizione del vettore di errore in GGH introdusse un "indizio" utilizzabile per ottenere informazioni relative al messaggio $\mathbf{m}$ e addirittura semplificare il CVP del relativo testo cifrato. Richiamando quanto detto nella sezione 3.1:

$$\mathbf{c} = \mathbf{mB} + \mathbf{e} \tag{1}$$

con $\mathbf{e} = \{\pm\sigma\}$. Data la speciale forma di $\mathbf{e}$ è possibile, tramite una precisa scelta di modulo, far scomparire il vettore di errore dall'equazione 1. Definendo quindi un vettore $\mathbf{s} = (\sigma, \ldots, \sigma) \in \mathbb{Z}^n$ e utilizzando come modulo 2σ si ottiene che:

$$\mathbf{e} + \mathbf{s} \equiv 0 \pmod{2\sigma}$$

e di conseguenza:

$$\mathbf{c} + \mathbf{s} \equiv \mathbf{mB} \pmod{2\sigma}.$$

Definendo $\mathbf{cs} = \mathbf{c} + \mathbf{s}$ si arriva ad un sistema modulare di tipo $\mathbf{y} \equiv \mathbf{Bx} \pmod{2\sigma}$ che come unica incognita ha $\mathbf{x}$ (ovvero $\mathbf{m}$). Questa tipologia di sistemi modulari si risolve banalmente quando la matrice $\mathbf{B}$ è invertibile modulo 2σ, permettendo di calcolare direttamente una soluzione unica. Tuttavia, se $\mathbf{B}$ non è invertibile, il processo di risoluzione diventa significativamente più complesso. In queste circostanze, si presentano diverse complicazioni: il sistema può ammettere soluzioni multiple, manca un approccio risolutivo diretto e i metodi di risoluzione devono essere adattati al modulo specifico del sistema in esame. Nguyen, in [3], stabilisce inizialmente che esiste una probabilità significativa che la matrice $\mathbf{B}$ sia invertibile modulo 2σ. Questa dimostrazione implica che in una porzione rilevante dei casi, il sistema modulare può essere risolto in modo diretto e semplice. Quando la matrice non è invertibile invece, Nguyen dimostra come il kernel (e quindi il numero delle soluzioni) sia generalmente molto piccolo. In particolare viene rilevato che solo una parte molto piccola delle matrici modulo 6 (che è il doppio del parametro $\sigma = 3$ suggerito) ha un kernel con più di 12 elementi.
Nguyen conclude quindi che, per la scelta suggerita di parametri (n, σ) e per qualsiasi

testo cifrato $\mathbf{c}$, il sistema lineare ha, molto probabilmente, pochissime soluzioni.
Si denoti con $\mathbf{m}_{2\sigma}$ il messaggio in chiaro modulo 2σ ottenuto risolvendo il precedente sistema modulare. Si supponga ora che $\mathbf{B}$ sia invertibile modulo 2σ, allora il sistema ha una sola soluzione $\mathbf{m}_{2\sigma} = (\mathbf{c} + \mathbf{s})\mathbf{B}^{-1}$. Sottraendo $\mathbf{m}_{2\sigma}\mathbf{B}$ in entrambe le parti dell'equazione 1 si consegue:

$$\mathbf{c} - \mathbf{m}_{2\sigma}\mathbf{B} = \mathbf{m}\mathbf{B} + \mathbf{e} - \mathbf{m}_{2\sigma}\mathbf{B}$$

e, raccogliendo $\mathbf{B}$ nella seconda parte dell'equazione, si ottiene quindi:

$$\mathbf{c} - \mathbf{m}_{2\sigma}\mathbf{B} = (\mathbf{m} - \mathbf{m}_{2\sigma})\mathbf{B} + \mathbf{e}. \tag{2}$$

Un'importante osservazione è che, essendo $\mathbf{m}_{2\sigma}$ congruente a $\mathbf{m}$ modulo 2σ, la differenza $(\mathbf{m}-\mathbf{m}_{2\sigma})$ risulta per definizione divisibile per 2σ. Questa proprietà consente di rappresentare tale differenza come il prodotto tra 2σ e un nuovo intero $\mathbf{m}'$, esprimendola nella forma $\mathbf{m} - \mathbf{m}_{2\sigma} = 2\sigma\mathbf{m}'$, dove $\mathbf{m}'$ costituisce il quoziente intero derivante da questa divisione. E' possibile quindi riscrivere 2 come:

$$\mathbf{c} - \mathbf{m}_{2\sigma}\mathbf{B} = (2\sigma\mathbf{m}')\mathbf{B} + \mathbf{e}$$

e, dividendo per 2σ in entrambe le parti, si ottiene infine:

$$\frac{\mathbf{c} - \mathbf{m}_{2\sigma}\mathbf{B}}{2\sigma} = \mathbf{m}'\mathbf{B} + \frac{\mathbf{e}}{2\sigma}. \tag{3}$$

L'equazione 3 nella sua forma finale mostra una chiara divisione in due parti: la prima rappresenta un punto razionale con tutti gli elementi noti, permettendone così un calcolo diretto; la seconda mantiene la struttura della formula 1, differenziandosi unicamente per la presenza del messaggio $\mathbf{m}'$. Ne consegue quindi che tale equazione può essere letta come un CVP per il quale il vettore di errore $\frac{\mathbf{e}}{2\sigma} \in \{\pm\frac{1}{2}\}^n$ risulta essere molto più piccolo di quello proposto da GGH. Data la relazione tra i due errori, conseguente dal procedimento appena illustrato, se si è in grado di risolvere il ben più semplice CVP posto dall'equazione 3 allora è possibile risolvere anche il CVP originale. In altre parole Nguyen, grazie alla sua intuzione, è riuscito a ridurre l'istanza del CVP di GGH in una più semplice.
L'attacco di Nguyen può essere meglio descritto come una semplificazione del CVP di GGH, semplificazione che può essere sfruttata da algoritmi di risoluzione del CVP come la tecnica di incorporamento. Infatti, una volta risolto il CVP semplificato, si otterrà $\mathbf{m}'$ con il quale sarà possibile calcolare il messaggio originale attraverso:

$$\mathbf{m} = \mathbf{m}_{2\sigma} + 2\sigma\mathbf{m}'.$$

Successivamente alla pubblicazione di GGH nel 1997, vennero pubblicate delle "internet challenges": delle sfide lanciate dagli autori su internet al fine di testare quanto il loro schema fosse sicuro. Le sfide erano composte da 5 istanze di GGH delle quali si era a conoscenza solo del testo cifrato e della chiave pubblica. Ogni sfida era più difficile della precedente, spaziando più precisamente nelle seguenti dimensioni: 200, 250, 300, 350 e 400. Per validare il suo attacco, Nguyen, riuscì a recuperare il messaggio originale in tutte le sfide ad eccezione dell'ultima in dimensione 400, dove ottenne solo informazioni parziali. La sua strategia si articolò in due fasi: per dimensioni fino a 300, impiegò la tecnica di incorporamento con BKZ a blocchi di 20, mentre per le dimensioni superiori combinò lo stesso algoritmo di risoluzione per il CVP con una versione potata di BKZ a blocchi di 60. Per migliorare la stabilità, entrambe le varianti di BKZ furono implementate utilizzando l'aritmetica a virgola mobile. Un problema precedentemente introdotto nella sezione 2.4.2 è l'uso di valori non interi nella costruzione della matrice secondo la tecnica di incorporamento. Infatti, secondo quanto ottenuto nell'equazione 3, $\mathbf{e} \in \{\pm\frac{1}{2}\}^n$ conseguendo quindi che la parte sinistra dell'equazione non sia più un vettore di soli elementi interi. Per risolvere tale problema Nguyen propose due soluzioni:

1. Moltiplicare per 2 l'equazione 3 ottenendo così $\mathbf{e} \in \{\pm 1\}^n$. Ciò però consegue che anche la base pubblica $\mathbf{B}$ sarà moltiplicata per 2 causando un aumento di complessità dei calcoli con reticoli di grandi dimensioni.

2. Aggiungere un vettore costante $\mathbf{s} = (\sigma, \ldots, \sigma)$ e successivamente scalare l'intero sistema per un fattore 2σ. Questa manipolazione matematica semplifica i calcoli, poiché il vettore di errore risultante contiene solo valori 0 o 1. Tuttavia, è importante notare che questa trasformazione comporta un leggero aumento della lunghezza prevista del vettore di errore. Per un esempio più dettagliato si veda [3, Sezione 5]

Esempio 3.2.2. (Esempio dell'attacco di Nguyen a GGH tramite incorporamento) Siano $(\mathbf{B}, \sigma)$ e $\mathbf{c}$ rispettivamente chiave pubblica e testo cifrato utilizzati tra Alice e Bob nell'esempio 3.1.2. Si supponga che Eve abbia intercettato il testo cifrato e la chiave pubblica. Eve, venuta a conoscenza della scoperta di Nguyen, tenta così di decifrare il messaggio cifrato sfruttando tale informazione. Eve innanzitutto verifica se la base pubblica $\mathbf{B}$ sia invertibile modulo 2σ. Per fare ciò calcola $\det(\mathbf{B}) = 781$ e controlla se esso sia coprimo con $2\sigma = 6$. Scopre così che $\mathbf{B}$ è effettivamente invertibile, di conseguenza, il sistema modulare ha un'unica soluzione, che può essere determinata direttamente:

$$(\mathbf{c} + \mathbf{s})\mathbf{B}^{-1} \equiv \mathbf{m} \pmod{2\sigma}$$

$$\mathbf{m}_{2\sigma} = (\mathbf{c} + \mathbf{s})\mathbf{B}^{-1} \pmod{2\sigma}$$

$$\mathbf{m}_{2\sigma} = \left(\begin{bmatrix} 4452 & -1964 & 735 \end{bmatrix} + \begin{bmatrix} 3 & 3 & 3 \end{bmatrix} \right) \begin{bmatrix} 1 & 1 & 5 \\ 3 & 2 & 5 \\ 3 & 1 & 0 \end{bmatrix} \pmod{2\sigma} = \begin{bmatrix} 0 & 5 & 2 \end{bmatrix}.$$

Eve, ottenuto $\mathbf{m}_{2\sigma}$, procede con il calcolare il CVP semplificato tramite l'equazione 3. Dato che vuole utilizzare la tecnica di incorporamento per risolverlo nel passaggio successivo, moltiplica per 2 la frazione in modo da liberarsi di valori con la virgola. Tale moltiplicazione andrà poi riflessa su $\mathbf{B}$ anche nei passaggi successivi all'estrazione del vettore $\mathbf{e}$.

$$\mathbf{c}^* = 2\Big(\frac{\mathbf{c} - \mathbf{m}_{2\sigma}\mathbf{B}}{2\sigma}\Big) = \begin{bmatrix} 1659 & -743 & 211 \end{bmatrix}.$$

Ora che Eve ha ottenuto un'istanza semplificata del CVP originale, procede con gli stessi passaggi presentati nell'esempio 3.2.1, ma utilizzando il nuovo $\mathbf{c}^*$ invece che $\mathbf{c}$.

$$\mathbf{M} = \begin{bmatrix} 145 & -73 & -23 & 0 \\ -39 & 21 & 16 & 0 \\ -165 & 80 & 11 & 0 \\ 1659 & -743 & 211 & 1 \end{bmatrix}.$$

Nell'esempio 3.2.1 Eve usò LLL come algoritmo di riduzione. In questo attacco, per una maggiore sicurezza, decide di usare BKZ. Ottiene quindi la matrice:

$$\mathbf{M}^* = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 6 & -3 & -2 \\ 3 & -1 & 6 & -6 \\ 9 & 0 & -6 & -4 \end{bmatrix} \quad \text{con} \quad \mathbf{e} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}.$$

Dopo aver costruito il vettore $\mathbf{u}$, Eve è ora in grado di calcolare $\mathbf{m}'$, ricordandosì però che ora è necessario raddoppiare $\mathbf{B}$.

$$\mathbf{m}' = (\mathbf{c}^* - \mathbf{u})(2\mathbf{B})^{-1} = \begin{bmatrix} -8 & 4 & -13 \end{bmatrix}.$$

Eve, come ultimo passaggio, decifra il messaggio originale tramite:

$$\mathbf{m} = \mathbf{m}_{2\sigma} + 2\sigma\mathbf{m}' = \begin{bmatrix} 0 & 5 & 2 \end{bmatrix} + \left(6 \begin{bmatrix} -8 & 4 & -13 \end{bmatrix} \right) = \begin{bmatrix} -48 & 29 & -76 \end{bmatrix}.$$

Contromisure

Nguyen stesso propose delle modifiche allo schema originale in [3, Sezione 7] per contrastare la vulnerabilità da lui scoperta e riparare lo schema GGH. La vulnerabilità principale del sistema è riconducibile alla particolare struttura del vettore di errore $\mathbf{e}$, come definito dagli autori in [5]. Per mitigare questo problema, un approccio

intuitivo consiste nel modificare l'intervallo dei possibili valori che le componenti del vettore possono assumere. Specificamente, Nguyen propose di adottare un intervallo più ampio $[-\sigma, \ldots, +\sigma]$, in sostituzione del più ristretto insieme $\pm\sigma$ originariamente utilizzato. Il nuovo vettore di errore risolve con successo la vulnerabilità sfruttata da Nguyen, ma rende il vettore stesso più corto, aumentando così il gap del reticolo incorporato e rendendo lo schema più vulnerabile ad attacchi basati su tecnica di incorporamento.

3.2.3 Attacco basato su informazioni parziali

Per quanto la vulnerabilità scoperta da Nguyen renda molto più facile l'attacco a GGH, essa non si rivelò sufficiente per dimensioni superiori a 400. A tal proposito nel 2010, Moon Sung Lee e Sang Geun Hahn[15], proposero un attacco in grado di rompere la barriera dimensionale a cui i precedenti attacchi si fermarono. Mentre sia questo attacco che quello di Nguyen mirano a semplificare il CVP, essi differiscono nel metodo: Nguyen riduce la lunghezza del vettore di errore $\mathbf{e}$, mentre questo nuovo approccio aumenta la lunghezza del vettore più corto nel reticolo definito dalla base pubblica. Per fare ciò però è necessario che un numero k di valori del messaggio originale siano noti, tale conoscenza risulta essere possibile solo in alcuni casi. Il metodo su cui si basa l'attacco è il seguente.
Sia $\mathbf{m}^1$ il vettore composto dai primi k degli n valori di $\mathbf{m}$ (noti) e sia $\mathbf{m}^2$ il vettore composto dai restanti valori di $\mathbf{m}$. Similmente, sia $\mathbf{B}^1$ la matrice composta dalle prime $\mathbf{k}$ righe della base pubblica $\mathbf{B}$ e sia $\mathbf{B}^2$ la matrice composta dalle righe rimanenti di $\mathbf{B}$. Allora si ha che:

$$\mathbf{c} = \mathbf{mB} + \mathbf{e} = (\mathbf{m}^1\ \mathbf{m}^2)\begin{pmatrix}\mathbf{B}^1\\ \mathbf{B}^2\end{pmatrix} + \mathbf{e} = \mathbf{m}^1\mathbf{B}^1 + \mathbf{m}^2\mathbf{B}^2 + \mathbf{e}$$

da cui si deriva:

$$\mathbf{c} - \mathbf{m}^1\mathbf{B}^1 = \mathbf{m}^2\mathbf{B}^2 + \mathbf{e}. \tag{4}$$

Data l'assunzione iniziale, la prima componente dell'equazione 4 è conosciuta. La seconda componente, analogamente all'equazione 3 discussa in precedenza, può essere ricondotta a una versione semplificata del CVP originale. Tuttavia, in questo caso, il problema è definito su un reticolo $\mathcal{L}(\mathbf{B}_2)$ che è un sottoinsieme del reticolo originale $\mathcal{L}(\mathbf{B})$, ma distinto da esso. La risoluzione del nuovo CVP implica la risoluzione dell'istanza originale del problema. Tale affermazione sussiste in quanto il rango della matrice su cui viene risolta risulta essere $n - k$ e quindi molto più piccola dell'originale. Per validare il loro metodo, gli autori di [15] applicarono l'attacco alla sfida rimanente in dimensione 400, sfruttando anche la vulnerabilità scoperta da Nguyen. Il corretto funzionamento richiedeva la determinazione di k valori del

messaggio originale. Sapendo che il messaggio era composto da 400 numeri interi $\mathbf{m} = (\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{400})$, con $\mathbf{m}_i \in [-128, 127]$, e che $\mathbf{m}_1 \bmod 6 = 5$ grazie alle informazioni parziali rilevate da Nguyen, si dedusse l'esistenza di sole 43 possibilità per $\mathbf{m}^1 = (\mathbf{m}_1)$, ovvero $(-127), (-121), \ldots, (125)$. Questa deduzione permise di restringere significativamente lo spazio di ricerca per l'attacco, rendendo il metodo più efficace e praticabile. In conclusione quindi, gli autori di [15], riuscirono a rompere la challenge in dimensione 400 avendo a dispozione un solo valore del messaggio originale.

Contromisure

Dato l'utilizzo della vulnerabilità scoperta da Nguyen al fine di indovinare valori del messaggio originale è logico pensare che la contromisura proposta da Nguyen sia sufficiente al fine di proteggere l'algoritmo da questo attacco. Questa affermazione risulta vera, ma solo se effettivamente non c'è una perdita di informazione relativa al messaggio originale. In [15] viene discussa la possibilità di un attacco alle challenge 350 e 400 senza utilzzare la tecnica di Nguyen. Gli autori scoprirono che per decifrare con successo il messaggio originale, era necessario fare supposizioni su 9 e 17 valori (k) per le rispettive sfide. Considerando che lo schema GGH originale definisce i valori del messaggio nell'intervallo $[-128, +127]$, indovinare un singolo elemento richiederebbe 2^8 tentativi, mentre per k elementi sarebbero necessari $2^{(8k)}$ tentativi. Risulta evidente che un approccio di questo tipo sarebbe impraticabile sia in termini di tempo che di risorse computazionali.

Capitolo 4

Migliorare GGH usando la Forma Normale di Hermite

Considerando i vari attacchi discussi nella sezione 3.2 e le note vulnerabilità del crittosistema GGH, è evidente che, per un suo utilizzo sicuro, la dimensione delle chiavi deve essere almeno superiore a 400. Tuttavia, una tale dimensione comporta complessità spaziali e temporali tali da rendere il crittosistema poco competitivo rispetto ad altri attualmente in uso come RSA o DSS. Nel 2001, Daniele Micciancio [6] ha proposto una versione migliorata del crittosistema basata sulla forma normale di Hermite, nota come GGH-HNF. Questo schema mira ad aumentare sia le performance che la sicurezza in comparazione alle risorse necessarie rispetto alla versione originale di GGH.

4.1 Struttura e funzionamento di GGH-HNF

Sulla base di quanto precedentemente esposto nella sezione 3.1, in GGH il messaggio originale $\mathbf{m}$ viene codificato in un vettore $\mathbf{x}$ appartenente al reticolo, e il testo cifrato risulta come $\mathbf{c} = \mathbf{xB} + \mathbf{e}$. Le ottimizzazioni sviluppate da Micciancio hanno portato a una modifica di questo approccio. Invece di generare in maniera casuale sia il vettore $\mathbf{x}$ che la base $\mathbf{B}$, Micciancio ha scelto di codificare il messaggio direttamente nel vettore di errore $\mathbf{e}$, procedendo con un approccio deterministico per la generazione dei precedentemente citati parametri. Questa scelta nasce dalla difficoltà nel generare vettori e basi random che abbiano una sicurezza intrinseca e dimostrabile. Questa difficoltà si ripercuote sulla sicurezza del crittosistema: $\mathbf{B}$ scelta casualmente rilascia spesso informazioni parziali relative a $\mathbf{R}$ permettendo così una facile riduzione di essa. Per superare questo problema, Micciancio decide di non generare più $\mathbf{B}$ tramite la costruzione di matrici unimodulari casuali moltiplicate per $\mathbf{R}$. Invece, opta per un approccio deterministico basato sulla forma normale di Hermite (HNF) di $\mathbf{R}$. La forma

normale di Hermite è una rappresentazione canonica e unica per una data matrice, ottenuta mediante operazioni elementari di riga e colonna. Essa presenta una struttura triangolare e garantisce che gli elementi sulla diagonale principale siano ordinati in modo decrescente. Poiché l'HNF è unica per ogni reticolo la chiave pubblica $\mathbf{B}$ non rivela informazioni sulla chiave privata $\mathbf{R}$, se non il reticolo $\mathcal{L}$ che genera. Inoltre, qualsiasi informazione su $\mathbf{R}$ che possa essere efficacemente calcolata da $\mathbf{B}$ può essere altrettanto efficacemente calcolata a partire da qualsiasi altra base $\mathbf{B}'$ che genera lo stesso reticolo $\mathcal{L}$. Questo perché $\mathbf{B} = \mathrm{HNF}(\mathbf{R}) = \mathrm{HNF}(\mathbf{B}')$.
Ottenuto $\mathbf{B}$ è necessario quindi calcolare un vettore $\mathbf{xB}$ appartenente al reticolo che verrà poi aggiunto a $\mathbf{e}$ come da equazione 1. L'idea migliore sarebbe scegliere il vettore in modo casuale e uniforme, ma questa scelta non è praticabile. Tuttavia, Micciancio in [6, Sezione 4.1] dimostra che tale risultato può essere ottenuto mediante il semplice calcolo di $\mathbf{x} = \mathbf{e} \bmod \mathbf{B}$. Quindi, invece di aggiungere a $\mathbf{e}$ un vettore casuale $\mathbf{xB}$, si riduce $\mathbf{e}$ modulo la base pubblica. Data la particolare struttura della matrice $\mathbf{B}$ nella sua forma HNF, questo calcolo risulta particolarmente semplice da effettuare. Partendo da un vettore $\mathbf{x}$ inizialmente nullo, si può calcolare un valore di $\mathbf{x}$ alla volta, iniziando dall'ultimo componente $\mathbf{x}_n$, tramite la seguente formula:

$$\mathbf{x}_i = \left\lfloor \frac{\mathbf{e}_i - \sum_{j=i+1}^{n-1} \mathbf{B}_{j,i}\mathbf{x}_j}{\mathbf{B}_{i,i}} \right\rfloor \tag{5}$$

e ottenere infine:

$$\mathbf{c} = \mathbf{e} - \mathbf{xB}. \tag{6}$$

Come si può notare le due equazioni 1 e 6 sono diverse, ma come dimostrato in [6, Sezione 4.3] esse garantiscono lo stesso livello di sicurezza.
Un ulteriore cambiamento, conseguente dalla scelta di Micciancio di usare $\mathbf{e}$ come vettore rappresentante il messaggio, è la totale mancanza di un fattore di bilanciamento, ruolo che nella versione originale del crittosistema veniva ricoperto da σ. Il processo di decifratura infatti, basato sulla tecnica di arrotondamento di Babai, rimane invariato. Pertanto, quanto detto in sezione 3.1.1, è ancora vero anche per GGH-HNF: il crittosistema è probabilistico e necessità di un parametro per bilanciarne la probabilità di decifratura con chiave pubblica e privata. Nella versione originale di GGH, σ, veniva derivato direttamente dalla base privata e veniva utilizzato come parametro assoluto per la costruzione di $\mathbf{e}$.
In GGH-HNF invece, Micciancio, decide di creare un nuovo parametro ρ derivandolo sempre dalla base privata, ma con un approccio differente. La base privata $\mathbf{R}$ viene ortogonalizzata utilizzando l'algoritmo di Gram-Schmidt, producendo la base

ortogonale $\mathbf{R}^*$. Successivamente ρ è calcolato attraverso:

$$\rho = \frac{1}{2} min_i \|\mathbf{r}_i^*\|_2.$$

ρ rappresenta un raggio di correzione: se la lunghezza del vettore di errore è minore di questo raggio la decifratura avrà successo. Poiché la base privata è conosciuta esclusivamente dal destinatario, è essenziale che il parametro ρ sia incluso nella chiave pubblica, insieme alla base pubblica $\mathbf{B}$. Questa inclusione è fondamentale affinché il mittente possa generare messaggi appropriati, codificandoli nel vettore di errore $\mathbf{e}$. In questo modo, il mittente può assicurarsi che i messaggi cifrati siano compatibili con i parametri di decifratura del destinatario, garantendo che possano essere decifrati correttamente utilizzando la base privata del ricevente.
Un'ultima modifica proposta riguarda la generazione di $\mathbf{R}$. Mentre GGH optava per la creazione di una matrice rettangolare successivamente moltiplicata per una matrice casuale, Micciancio suggerisce un metodo diverso basato sui suoi esperimenti. Il nuovo approccio consiste nel generare direttamente una matrice casuale i cui elementi sono interi compresi nell'intervallo $[-n, \ldots, n]$. A questa matrice viene poi applicata una riduzione LLL. Gli esperimenti provarono che questo metodo produce basi con un ρ sufficientemente grande, più precisamente $\rho = \frac{n}{2}$.

4.1.1 Esempio pratico

Esempio 4.1.1. (Esempio di funzionamento di GGH) Sia $\mathbf{R}$ la base privata di Alice definita nell'esempio 3.1.2. Sia $\mathbf{B}$ la forma normale di Hermite di $\mathbf{R}$:

$$\mathbf{B} = \mathrm{HNF}(\mathbf{R}) = \begin{bmatrix} 1 & 0 & 327 \\ 0 & 1 & 1322 \\ 0 & 0 & 1363 \end{bmatrix}.$$

Se si dovesse calcolare il rapporto di Hadamard di $\mathbf{B}$ si otterrebbe che $\mathcal{H}(\mathbf{B}) = 0.01322$ che è ancora minore di quello relativo alla base pubblica dell'esempio 3.1.2, facendo intuire quanto l'HNF sia utile per la generazione di basi reticolari di bassa qualità.
Alice procede col calcolare il ρ della sua chiave privata ottenendo $\rho = 3.99242$ e conclude con la generazione della sue sue due chiavi:

$$\mathbf{K}_{private} = (\mathbf{R}, \mathbf{R}^{-1}) \quad \text{e} \quad \mathbf{K}_{public} = (\mathbf{B}, \rho).$$

Bob vuole ora mandare un messaggio ad Alice. Inizia con il selezionare un vettore $\mathbf{e}$ la cui lunghezza sia minore del ρ di Alice:

$$\mathbf{e} = \begin{bmatrix} 1 & 1 & 2 \end{bmatrix} \quad \text{con} \quad \|\mathbf{e}\|_2 = 2.44948.$$

Una volta ottenuto $\mathbf{e}$, Bob, calcola il testo cifrato attraverso le equazioni 5 e 6:

$$\mathbf{c} = \mathbf{e} - \mathbf{xB} = \begin{bmatrix} 1 & 1 & 2 \end{bmatrix} - \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 327 \\ 0 & 1 & 1322 \\ 0 & 0 & 1363 \end{bmatrix} = \begin{bmatrix} 0 & 0 & -1647 \end{bmatrix}.$$

Alice, una volta ricevuto $\mathbf{c}$, utilizza la sua chiave privata per decifrarlo attraverso la tecnica di arrotondamento di Babai:

$$\mathbf{x} = \lfloor \mathbf{cR}^{-1} \rceil = \begin{bmatrix} -40 & -5 & -121 \end{bmatrix} \text{ ed } \mathbf{e} = \mathbf{c} - \mathbf{xR} = \begin{bmatrix} 1 & 1 & 2 \end{bmatrix}.$$

Si supponga ora che Eve, una volta intercettato il testo cifrato e la chiave pubblica, tenti di ottenere il messaggio originale usando solo la base $\mathbf{B}$:

$$\mathbf{e}' = \mathbf{c} - (\lfloor \mathbf{cB}^{-1} \rceil \mathbf{B}) = \begin{bmatrix} 0 & 0 & -284 \end{bmatrix}.$$

È possibile osservare una significativa differenza tra $\mathbf{e}$ ed $\mathbf{e}'$, dimostrando ancora una volta l'aumento di sicurezza apportato dall'uso della forma normale di Hermite. Inoltre è possibile verificare che $\mathbf{B}$ non è in grado di correggere l'errore $\mathbf{e}$ attraverso il calcolo del suo ρ, il quale, è pari a 0.50042.
Mentre nell'esempio precedente (esempio 3.1.2) il messaggio decifrato $\mathbf{m}'$ mostrava poche cifre di distanza dal messaggio originale $\mathbf{m}$, in questo caso la situazione cambia notevolmente, presentando differenze molto più marcate.

4.2 Limiti pratici di GGH-HNF

GGH-HNF riesce a risolvere i problemi di GGH con successo, riuscendo a diventarne una variante migliorata a tutti gli effetti. Nelle conclusioni di [6], Micciancio suggerisce che una dimensione di 500 potrebbe offrire un livello di sicurezza adeguato, mantenendo al contempo una dimensione delle chiavi accettabile grazie all'impiego della forma normale di Hermite. Sfortunatamente però le supposizioni di Micciancio si rivelarono troppo ottimistiche.
Nel Gennaio del 2004 Christoph Ludwig stilò un report tecnico [16] nel quale crittoanlizzò GGH-HNF e ne testò i suoi limiti pratici.

Generazione delle chiavi

Una serie di esperimenti vennero condotti sulla generazione delle chiavi di GGH-HNF. Il lavoro si è concentrato su diverse dimensioni dei reticoli, fino a 475, con un caso speciale in dimensione 800. Per le chiavi private, il processo più impegnativo è stato la riduzione LLL delle basi scelte casualmente. Secondo gli esperimenti di Ludwig

questo ha richiesto fino a 58 minuti nelle dimensioni più alte. Molto più pesante invece il dato riguardante la generazione della chiave pubblica: il miglior algoritmo a disposizione impiegò 4 ore. Per quanto riguarda il caso in dimensione 800 i tempi rilevati furono di 4 ore e mezza per la chiave privata e 46 ore per quella pubblica.

Cifratura e decifratura

Come descritto precedentemente, la particolare struttura della forma normale di Hermite consente una cifratura molto veloce. Ciò venne confermato dai test di Ludwig i quali impiegarono in media solo 0.29 secondi in dimensione 800. Le cose cambiano drasticamente con la decifratura: a causa dell'ortogonalizzazione Gram-Schmidt e della precisione richiesta, lo spazio occupato e il tempo richiesto per i calcoli cresce a livelli non accettabili. Gli esperimenti richiedettero 40 minuti per ortogonalizzare e rispettivamente 13 e 73 minuti per decifrare in dimensione 475 e 800. E' però importante precisare che Ludwig utilizzò il metodo del piano più vicino di Babai che restituisce una soluzione più precisa, ma contemporaneamente richiede più tempo per trovarla a causa della sua complessità computazionale maggiore.

Attacchi a GGH-HNF

Gli attacchi a GGH-HNF coinvolsero reticoli di dimensioni fino a 280, impiegando vettori di errore la cui lunghezza variava dal 10% al 100% del ρ. Gli algoritmi di riduzione impiegati spaziarono da LLL a diverse varianti di BKZ. L'algoritmo LLL dimostrò efficacia in dimensione 280 con vettori di errore corti, ma si rivelò inefficace per dimensioni pari o superiori a 180 con vettori più lunghi. L'incremento della dimensione del reticolo rese necessario l'impiego di BKZ con blocchi fino a 60 per mantenere l'efficacia degli attacchi. Utilizzando una tecnica di estrapolazione basata sui risultati sperimentali ottenuti, Ludwig è riuscito a prevedere l'efficacia degli attacchi su dimensioni più elevate, che non erano state direttamente testate. Questo ha fornito una visione sulla sicurezza futura del sistema. Considerando scenari di complessità esponenziale e subesponenziale, Ludwig ha suggerito che per garantire la sicurezza del GGH-HNF sarebbero necessarie dimensioni del reticolo di almeno 800, un valore significativamente superiore rispetto alle stime iniziali di Micciancio, che si attenevano su una dimensione di 500.

E' ovvio che i valori riportati da Ludwig portino alla comune considerazione che le basse performance di GGH-HNF su alte dimensioni lo rendano praticamente non utilizzabile, soprattutto dopo che le estrapolazioni fatte hanno indicato la necessità di dimensioni superiori a 800. E' però importante precisare che, dato l'avanzamento della tecnologia, tali dati siano ormai obsoleti. Come mostrano i dati sperimentali presentati in sezione **??**(sezione futura), grazie ai nuovi algoritmi è possibile generare

e decifrare chiavi con molte meno risorse spaziali e temporali di quelle richieste negli anni della pubblicazione dell'algoritmo, ormai venti anni fa.

Bibliografia

[1] de Barros Charles Figueredo e Menasché Schechter Luis, "GGH May Not Be Dead after All," Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, 21941-590 Rio de Janeiro RJ, 2015

[2] Galbraith Steven, "Mathematics of Public Key Cryptography", seconda edizione, Ottobre 2018

[3] Nguyen Phong, "Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97," Advances in Cryptology — CRYPTO' 99, 45 rue d'Ulm, 75230 Paris Cedex 05, France, pagine 288–304, 1999

[4] Babai László, "On Lovász' Lattice Reduction e the Nearest Lattice Point Problem," Combinatorica, vol. 6, no. 1, pagine 1–13, 1986

[5] Goldreich Oded, Goldwasser Shafi e Halevi Shai, "Public-key Cryptosystems from Lattice Reduction Problems," Advances in Cryptology — CRYPTO '97, pagine 112–131, 1997

[6] Micciancio Daniele, "Improving Lattice Based Cryptosystems Using the Hermite Normal Form," Lecture Notes in Computer Science, 9500 Gilman Drive, La Jolla, CA 92093 USA, pagine 126–145, 2001

[7] Micciancio Daniele e Regev Oded, "Lattice-based Cryptography," Post-Quantum Cryptography, pagine 147–191, 2009

[8] Aharonov Dorit e Regev Oded, "Lattice Problems in NP ∩ coNP", CiteSeer X (The Pennsylvania State University), 2009

[9] Micciancio Daniele e Goldwasser Shafi, "Complexity of Lattice Problems: a cryptographic perspective", The Kluwer International Series in Engineering and Computer Science, Boston, Massachusetts, Kluwer Academic Publishers, volume 671, 2002

[10] Silverman Joseph H., Pipher Jill e Hoffstein Jeffrey, "An introduction to mathematical cryptography", seconda edizione, Springer, Undergraduate texts in mathematics, 2008

[11] Lenstra Arjen Klaas, Lenstra Hendrik Willem e László Lovász, "Factoring polynomials with rational coefficients", Mathematlsche Annalen, Springer, volume 261, pagine 515-534, 1982

[12] Nguyen Phong e Damien Stehlé, "Floating-point LLL revisited", LNCS, Springer, volume 3494, pagine 215-233, 2005

[13] Schnorr Claus Peter e M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems", Mathematical Programming, volume 66, pagine 181-199, 1994

[14] Schnorr Claus Peter e H. H. Hörner, "Attacking the Chor-Rivest cryptosystem by improved lattice reduction", Proc. of Eurocrypt'95, Springer-Verlag, volume 921, pagine 1-12, 1995

[15] Moon Sung Lee e Sang Geun Hahn, "Cryptanalysis of the GGH Cryptosystem", Mathematics in Computer Science, volume 3, pagine 201-208, 2010

[16] Ludwig Christoph, "The Security and Efficiency of Micciancio's Cryptosystem", Technische Universität Darmstadt Germany, 2004