RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 3 / 2. November 2011 / Abgabe bis spätestens 9. November 2011, 10 Uhr in dem Kasten auf NA 02

Wir wollen zeigen, dass der Gauss-Algorithmus stets eine minimale Basis $\mathbf{b}_1, \mathbf{b}_2$ erzeugt, d.h. $\|\mathbf{b}_i\| = \lambda_i$ für $i = 1, 2$.

Algorithm 1 Gauss-Reduce

Eingabe: Gitterbasis $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^n$ mit $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$
Ausgabe: Minimale Basis $\mathbf{b}_1, \mathbf{b}_2$

```
μ* ← ⟨b1,b2⟩ / ⟨b1,b1⟩
while |μ*| > 1/2 do
    b2 ← b2 − ⌊μ*⌉ b1
    if ||b1|| > ||b2|| then
        Vertausche b1 und b2.
    end if
    μ* ← ⟨b1,b2⟩ / ⟨b1,b1⟩
end while
return b1, b2
```

AUFGABE 1 (5 Punkte)**:**

Wir nennen eine Basis $\mathbf{B} = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix} \in \mathbb{R}^{2\times n}$ *Gauss-reduziert* genau dann, wenn $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ und $|\mu^*| \leq \frac{1}{2}$ für $\mu^* := \frac{\langle \mathbf{b}_1, \mathbf{b}_2 \rangle}{\langle \mathbf{b}_1, \mathbf{b}_1 \rangle}$ gilt. Zeigen Sie:

(a) $\mathbf{B}$ Gauss-reduziert $\Rightarrow \|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \|\mathbf{b}_2 - \mu\mathbf{b}_1\|$ für alle $\mu \in \mathbb{Z}$.

Hinweis: Zeigen Sie zunächst (geometrisch), dass $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \|\mathbf{b}_1 \pm \mathbf{b}_2\|$. Betrachten Sie dann die Abbildung $f(\mu) = \|\mathbf{b}_2 - \mu\mathbf{b}_1\|^2$ wie in Aufgabe 1 aus der Präsenzübung. In welchem Bereich nimmt f sein Minimum an und wie verhält sich f wenn man sich vom Minimum wegbewegt?

(b) $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \|\mathbf{b}_2 - \mu\mathbf{b}_1\|$ für alle $\mu \in \mathbb{Z} \Rightarrow \|\mathbf{b}_i\| = \lambda_i$ für $i = 1, 2$.

Hinweis: Betrachten Sie beliebiges $\mathbf{v} = \alpha_1\mathbf{b}_1 + \alpha_2\mathbf{b}_2$. Für $\alpha_2 \neq 0$ führen Sie Division mit Rest von α_1 bzgl. α_2 durch.

(c) Beweisen Sie, dass die Ausgabe von `Gauss-Reduce` stets eine minimale Basis ist.

Hinweis: Benutzen Sie Teil (a) und (b).

AUFGABE 2 (5 Punkte)**:**
Seien $a_1, \ldots, a_n \in \mathbb{Z}$. Geben Sie eine Basismatrix $\mathbf{B}$ für das Gitter

$$L := \{\mathbf{z} \in \mathbb{Z}^n \ : \ a_1 z_1 + \ldots + a_n z_n = 0\}$$

an und zeigen Sie $L = \text{span}(B)$. Berechnen Sie $\dim(L)$.

AUFGABE 3 (5 Punkte)**:**
Seien $a_1, a_2, \ldots, a_n, S \in \mathbb{N}$ mit $S = \sum_{i=1}^{n} a_i x_i$ für unbekannte $x_i \in \{0, 1\}$. Sei $A := \max\{a_1, \ldots, a_n\}$. Konstruieren Sie einen Algorithmus `linearcomb`, der in Zeit $\mathcal{O}(n^2 \log^2 A)$ ganze Zahlen $y_1, y_2, \ldots, y_n \in \mathbb{Z}$ findet mit

$$\sum_{i=1}^{n} y_i a_i = S.$$

Begründen Sie die Laufzeit und beweisen Sie die Korrekheit.

Hinweis: Beachten Sie, dass $\text{ggT}(a_1, \ldots, a_n)$ die Summe S teilt. Benutzen Sie eine verallgemeinerte Variante von Aufgabe 4 aus der Präsenzübung.

AUFGABE 4 (5 Punkte)**:**
Beweisen Sie für Satz 45 aus dem Skript die beiden Behauptungen:

(a) $\mathbf{d}$ ist ein nächster Gittervektor zum Targetvektor $\mathbf{y}'$.

(b) Jeder Gittervektor in L, der Abstand exakt $\sqrt{n/4}$ zum Targetvektor $\mathbf{y}'$ hat, ist von der Form $(y_1 - x'_1, \ldots, y_n - x'_n)$ mit $s = \sum_{i=1}^{n} x'_i a_i$ und $x'_i \in \{0, 1\}$.

BONUSAUFGABE 5 (10 Punkte)**:**
Implementieren Sie den Reduktionsbeweis von *Subset-Sum* auf *CVP* (siehe Satz 45) und berechnen Sie eine Lösung für $\mathbf{a}, S$ für die Dateien `a.sobj` und `S.sobj` (alternativ siehe `SS_cvp.txt`). Zusätzlich sind zwei Parameter $n = 80$ (Dimension) und $b = 30$ (maximale Bitgröße der Gewichte a_i) gegeben.
Gehen Sie hierbei wie folgt vor:

(i) Implementieren Sie den Algorithmus `linearcomb` aus Aufgabe 3 und berechnen Sie $\mathbf{y}$ mit $\sum_i y_i a_i = S$.

(ii) Schreibe Sie eine Prozedur `gen_basis(y,a,n,b)`, die eine Basis $\mathbf{B}$ zum durch die Gleichung $a_1 z_1 + \ldots + a_n z_n = 0$ definierten Gitter gemäß Aufgabe 2 erzeugt. Erweitern Sie die Basis um den zusätzlichen Basisvektor $\mathbf{y}$ und fügen Sie eine Spalte $(0, \ldots, 0, 2^b)$ ein[1].

(iii) Führen Sie eine LLL-Reduktion auf $\mathbf{B}$ durch. Dies geht in sage mit dem Befehl `B.LLL()`. Die ersten n Koordinaten des letzte Basisvektors der reduzierten Basis liefern eine Lösung $\mathbf{x}$ für das Subset-Sum Probelm $\mathbf{a}, S$. Testen Sie auf Korrektheit $\langle \mathbf{a}, \mathbf{x} \rangle = S$ und Zulässigkeit der Lösung $\mathbf{x} \in \{0, 1\}^n$.

[1]Wir haben somit ein Gitter erzeugt, welches den Targetvektor $\mathbf{y}$ erweitert um eine große Konstante 2^b als Gittervektor enthält. Wir verzichten auf die zusätzliche Transformation $\mathbf{y}' = \mathbf{y} - \frac{1}{2}(1, \ldots, 1)$ aus der Reduktion, denn die Eingabeinstanz kann bereits so gelöst werden. Die große Konstante 2^b sorgt dafür, dass der Basisvektor $(\mathbf{y}, 2^b)$ nicht zur Längenreduktion benutzt wird. Wenn wir diese Basis LLL-reduzieren, erhalten wir als letzten Basisvektor schliesslich den relativ kurzen Gittervektor $\mathbf{y} + \sum_i \alpha_i \mathbf{b}_i$, d.h. $\mathbf{v} = \sum_i \alpha_i \mathbf{b}_i$ ist ein Gittervektor (des Originalgitters) nahe zu $\mathbf{y}$.