RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 13 / 22. Januar 2013

AUFGABE 1:
Sei $V_1 \supset V_2 \supset V_3 \supset \ldots$ eine absteigende Kette affiner Varietäten über einem beliebigen Körper $\mathbb{F}$. Zeigen Sie, dass die Kette stationär wird: Es gibt ein $N \geq 1$, so dass $V_i = V_N$ fÃ¼r alle $i \geq N$.

AUFGABE 2:
Sei $\mathbb{F} = \mathbb{C}$ der Körper der komplexen Zahlen. Wir betrachten folgendes Gleichungssystem in $\mathbb{F}[X_1, \ldots, X_n]$:

$$\begin{aligned} f_1 &:= X_1^2 - 1 = 0 \\ f_2 &:= X_2^2 - X_1 = 0 \\ f_3 &:= X_3^2 - X_2 = 0 \\ &\ldots \\ f_n &:= X_n^2 - X_{n-1} = 0 \end{aligned}$$

Wie sieht $V(f_1, \ldots, f_n)$ aus? Geben Sie eine Gröbnerbasis für $I = I(f_1, \ldots, f_n)$ an für $>_{\texttt{deglex}}$ und für $>_{\texttt{lex}}$. Sind Ihre Gröbnerbasen reduziert? Wie sieht eine reduzierte Gröbnerbasis aus? Was ändert sich, wenn man die letzte Gleichung f_n durch $\widetilde{f_n} = (X_n - 2)^2 - X_{n-1} = 0$ ersetzt.

Aufgaben 3 und 4 auf Hausübung verlegt

AUFGABE 3:
Sei $>$ eine Monomordnung und sei $I = \langle g_1, \ldots, g_m \rangle \subset \mathbb{F}[X_1, \ldots, X_n]$ ein Ideal, wobei $G = \{g_1, \ldots, g_m\}$ nicht notwendig Gröbnerbasis. Wähle $1 \leq i \leq m$ und setze $\widetilde{G} = G \setminus \{g_i\} \cup \{\overline{g_i}^{G \setminus \{g_i\}}\}$ (wie im Algorithmus `Reduziere Gröbner`). Zeigen Sie:

(a) $I = \langle G \rangle = \langle \widetilde{G} \rangle$

(b) $\langle \mathrm{LM}(G) \rangle \subset \langle \mathrm{LM}(\widetilde{G}) \rangle$

Welche Konsequenz(en) und Verbesserungsmöglichkeiten ergeben sich dadurch für den Buchberger-Algorithmus?

AUFGABE 4:
Betrachten Sie folgendes Erzeugendensystem für ein Ideal, das ein Subset-Sum Problem formalisiert:

$$\begin{aligned} f_1 &:= X_1^2 - X_1 \\ f_2 &:= X_2^2 - X_2 \\ f_3 &:= X_3^3 - X_3 \\ f_4 &:= X_1 + 3X_2 + 4X_3 - 5 \end{aligned}$$

Wie sieht das entsprechende Subset-Sum Problem aus? Wie muss die reduzierte Gröbnerbasis für $I = \langle f_1, f_2, f_3, f_4 \rangle \subset \mathbb{F}[X_1, X_2, X_3]$ aussehen? Berechnen Sie diese mit dem Buchberger-Algorithmus. Die Monomordnung sei dabei so, dass $X_1 > X_2 > X_3$ (mehr braucht man in diesem Fall nicht zu wissen). $\mathbb{F}$ sei dabei als $\mathbb{Q}$ oder $\mathbb{F}_{11}$ gewählt (warum?).