# Algorithmic techniques in algebraic cryptanalysis and their applications

Makarim, R.H.

# Nederlandse Samenvatting

Neem een polynomiale ring $\mathbb{F}[x_1, \ldots, x_n]$ in variabelen $x_1, \ldots, x_n$ met coëfficienten in een lichaam $\mathbb{F}$ en een gekozen monomiale ordening. Neem een ideaal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ met $I \neq \{0\}$. Een eindige deelverzameling $G$ van het ideaal $I$ wordt een Gröbner basis van $I$ genoemd indien voor alle $f \in I \setminus \{0\}$ er een polynoom $g \in G$ bestaat zodat de leidende term van $g$ de leidende term van $f$ deelt.

Het hoofdonderwerp van dit proefschrift zijn Gröbner-basis algoritmen, dat wil zeggen algoritmen die een Gröbner basis berekenen voor een gegeven ideaal $I \neq \{0\}$ van $\mathbb{F}[x_1, \ldots, x_n]$. Naast de interesse in de algoritmen zelf, worden ook toepassingen van Gröbner-basis algoritmen behandeld in dit proefschrift. Bijvoorbeeld om systemen van vergelijkingen van $\mathbb{F}[x_1, \ldots, x_n]$ over een eindig lichaam $\mathbb{F}$ op te lossen, welke vaak voorkomen in de veiligheidsanalyze van cryptografische systemen.

In hoofdstuk 5 introduceren we een variant Gröbner-basis algoritme genaamd M4GB. Het M4GB algoritme is beschreven op een wijze waarbij de hoog niveau beschrijving geintegreerd is met belangrijke implementatie aspecten, met het doel het algoritme te presenteren zonder het karakter van de implementatie te verliezen. Dit algoritme is namelijk ontworpen om altijd te berekenen op, en bijwerken van, polynomen in staart-gereduceerde vorm met respect tot de huidige tussentijdse basis. Ons nieuwe algoritme berust op een nieuw recursief reduceer algoritme voor polynomen gegeven in de vorm $\mathtt{t} \cdot f$, waar $\mathtt{t}$ en $f$ respectievelijk een term en een niet-nul polynoom zijn in $\mathbb{F}[x_1, \ldots, x_n]$.

In hoofdstuk 6 behandelen we de applicatie van M4GB om meerdere concrete uitdagingen van multivariate kwadratische (MQ) vergelijkingen over eindige lichamen. In het bijzonder heeft M4GB een nieuwe record gezet in de Fukuoka MQ Challenge* voor parameters die gerelateerd zijn aan MQ-gebaseerde cryptografische digitale handtekening systemen. In hetzelfde hoofdstuk analyzeren we ook de verwachte benodigde CPU tijd en geheugen om grotere parameters te kunnen oplossen.

In hoofdstuk 7 demonstreren we een andere applicatie van Gröbner-basis algoritmen om binaire puzzels op te lossen. Een binaire puzzel een Sodokuachtige puzzel waar een waarde in elke cel alleen 0 of 1 mag zijn, in plaats van 1 tot en met 9. Een binaire puzzel is oplosbaar als er elke cel met een waarde gevuld kan worden onder de volgende drie condities:

1. er bestaan geen drie (3) opeenvolgende cellen, danwel verticaal of horizontaal, die dezelfde waarde hebben;
2. het aantal nullen en aantal enen in elke rij of kolom moet gelijk zijn;
3. er mogen geen twee rijen, danwel twee kolommen, gelijk aan elkaar zijn.

De kerngedachte om binaire puzzels op te lossen met Gröbner-basis algoritmen is om de puzzel te zien als een Constraint Satisfaction Problem, waar elke bovenstaande conditie wordt beschreven door een set multivariate polynomen. We introduceren twee methoden om een dergelijke set van polynomen die de oplosbaarheid modeleren te bepalen. De eerste methode is om de condities te modeleren als polynomen over het eindige lichaam $\mathbb{F}_2$. De tweede methode

* `https://www.mqchallenge.org`

modeleert polynomen over $\mathbb{Z}$ of $\mathbb{Q}$. Het voordeel van de tweede methode over de eerste methode is dat het de graad van bepaalde polynomen reduceert ten koste van coefficienten over andere ringen. Een oplossing voor de binaire puzzel kan worden uitgerekend door een Gröbner basis uit te rekenen voor het ideaal gegenereerd door de set polynomen die de drie condities modeleren.

In hoofdstuk 8 leggen we verbanden tussen cryptografische eigenschappen van vectoriële Booleaanse functies en computationele commutatieve algebra. We stellen een ideaaltheoretische karakterisering voor voor noties gerelateerd aan de (niet)lineariteit, differentiaal en autocorrelatie van vectoriële Booleaanse functies. De drie genoemde begrippen houden verband met de lineaire, differentiële en differentieel-lineaire cryptoanalyse van cryptografie primitieven met symmetrische sleutels. De belangrijkste bijdragen zijn de constructie van idealen die nuttig zijn om de algebraïsche implicaties van lineaire, differentiële en differentieellineaire cryptanalyse op een vectoriële Booleaanse functie te analyseren. We laten ook nieuwe benaderingen zien om de bias van een lineaire benadering (inclusief Walsh- en Fourier-transformatie), de waarschijnlijkheid van een differentiaal en de autocorrelatie van de componentfuncties te berekenen met behulp van Gröbner-basis algoritmen.