Algorithmic techniques in algebraic cryptanalysis and their applications

Makarim, R.H.

English Summary

Let $\mathbb{F}[x_1, \ldots, x_n]$ be a multivariate polynomial ring in variables $x_1, \ldots, x_n$ with coefficients in a field $\mathbb{F}$ and a chosen monomial ordering. Let $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an ideal such that $I \neq \{0\}$. A finite subset G of the ideal I is said to be a Gröbner basis of I if for all $f \in I \setminus \{0\}$ there exists a polynomial $g \in G$ such that the leading term of g divides the leading term of f.

The primary subject in this thesis are Gröbner-basis algorithms, i.e., algorithms that compute a Gröbner basis for a given ideal $I \neq \{0\}$ of $\mathbb{F}[x_1, \ldots, x_n]$. In addition to the interest in the algorithms themselves, the work in this thesis also covers applications of Gröbner-basis algorithms. For instance, to solve systems of equations of $\mathbb{F}[x_1, \ldots, x_n]$ over a finite field $\mathbb{F}$, which often arise in the security analysis of cryptographic schemes.

In Chapter 5 we introduce a variant Gröbner basis algorithm called M4GB. The M4GB algorithm is described in a way that unifies high-level description together with its main implementation aspects, with the goal to present it without obscuring the nature of its implementation. It is namely designed to consistently operate on and maintain polynomials in tail-reduced form with respect to the current intermediate basis. Our new algorithm relies on a new recursive reduction algorithm for polynomials given in the form $\mathtt{t} \cdot f$, where $\mathtt{t}$ and f are a term and a non-zero polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ respectively.

In Chapter 6 we present the application of M4GB to solve several concrete challenges of multivariate quadratic (MQ) problems over finite fields. In particular M4GB sets a new record in the Fukuoka MQ challenge* for parameters that represent the public-key in MQ-based digital signature algorithms. In the same chapter we also analyze the expected required CPU time and memory to solver larger parameters.

In Chapter 7 we demonstrate another application of Gröbner-basis algorithms to solve binary puzzles. A binary puzzle is a Sudoku-like puzzle with an entry in each cell taken from the set $\{0, 1\}$ instead of $\{0, 1, \ldots, 9\}$. A binary puzzle is solvable if there exists an assignment for each cell that satisfies all three constraints:

1. there exists no three (3) consecutive cells, both vertically and horizontally, which are filed with the same value;
2. the number of zeros and ones in each row and column must be equal;
3. every two distinct rows (resp. columns) must not be equal.

The main idea to solve binary puzzles using Gröbner bases algorithms is to view it as a constraint satisfaction problem where each constraint above is represented by a set of multivariate polynomials. We introduce two approaches for the derivation of such a set of polynomials that represent the solvability of a binary puzzle. The first approach is to model the constraints as polynomials over $\mathbb{F}_2$. The second one is to model the polynomials over $\mathbb{Z}$ or $\mathbb{Q}$. The advantage of the latter approach than the former is it reduces the degree of some polynomials at the expense of defining the coefficients over different rings. A solution for the binary puzzle is obtained by computing a Gröbner basis of the ideal generated by the polynomials that represent the three constraints.

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

In Chapter 8 we establish connections among cryptographic properties of vectorial Boolean functions and computational commutative algebra. We propose ideal-theoretic characterization for notions related to the (non)linearity, differential, and autocorrelation of vectorial Boolean functions. The three mentioned notions are related to the linear, differential, and differential-linear cryptanalysis of symmetric-key cryptography. The primary contributions are the construction of ideals that are useful to analyse the algebraic implications of linear, differential, and differential-linear cryptanalysis on a vectorial Boolean function. We also exhibit new approaches to compute the bias of a linear approximation (including Walsh and Fourier transform), the probability of a differential, and the autocorrelation of the component functions using Gröbner bases algorithms.