AOC

Algebraically Cryptanalyzing AOCs – Open Research Questions

by Jan Ferdinand Sauer   Jun 30, 2021   0 Comment

The project about algebraically cryptanalyzing AOCs has run its course. As is usually the case in research, there are a lot more questions left to answer. I have listed some of the more interesting ones below – if you are looking for inspiration, this might be a starting point.

- The most pressing question is to find lower complexity bounds for Gröbner basis computations.
- A polynomial system gives rise to various similar but distinct concepts in trying to capture the complexity of a Gröbner basis computation – for example the Hilbert Regularity[1], the First Fall Degree, the Solving Degree, and others. Systematizing and relating the different definitions and concepts would greatly reduce confusion, helping not only newcomers but also experts.
- It is generally assumed that computing a Gröbner basis for a polynomial system without any underlying structure is about as hard as it can get. Discovering structure, for example of a weighted homogeneous kind, then using the appropriate monomial order for computing the Gröbner basis, might speed up the computation. It is unknown how to discover structure like this.
- It might be possible to divide a Gröbner basis attack for a keyed primitive into an offline and an online phase. In the offline phase, the plaintext and ciphertext are left as a variable, and the ideal of the polynomial system is of positive dimension. In the online phase, the acquired plaintext and ciphertext are plugged into the pre-computed Gröbner basis, and the key is derived. The details, feasibility, and overhead of such an approach are unclear.
- Gröbner basis algorithm F_5 has shown that the complexity of computing a Gröbner basis for a given set of polynomials can be characterized by the syzygy module for that set. It is believed that computing the syzygy module is as hard as computing the Gröbner basis, but whether this is actually the case is unknown.
- Furthermore, it would be interesting to know if we can derive a polynomial system's degree of regularity[2] given its syzygy module.
- AOCs use MDS matrices to mix the different state elements. Computing a Gröbner basis for the cipher can be seen as an unmixing of these transformations. It might be possible to incorporate an AOC's MDS matrix[3] into the monomial order to counteract the mixing.
- There a bunch of open questions surrounding the Gröbner Walk. Can we find an upper bound on the number of cones in the Gröbner fan? (How) does the number of cones relate to the size of the staircase? Is the shape of the fan characteristic for a certain cipher? How does its performance to FGLM compare on systems derived from an AOC? Can we estimate the fastest path to one of the *lex* orders?

Many more questions regarding Gröbner bases still don't have an answer, but this list has probably raised enough questions for a few years worth of research.

Footnotes

1. corresponding to one of multiple "Degree of Regularity" ↩
2. after clearly having specified *which* degree of regularity; see also the second bullet point ↩
3. or its inverse? The transpose? ↩

Jan Ferdinand Sauer

Website: https://asdm.gmbh

Leave a Reply

Logged in as Jan Ferdinand Sauer Logout

Comment

Submit