Re-linearization and Elimination of Variables in Boolean Equation Systems

Bjørn Møller Greve[1,2], Håvard Raddum[2] and Øyvind Ytrehus[2].

[1]Norwegian Defence Research Establishment (FFI),[2]Simula@UiB
bjorn-moller.greve@ffi.no, {haavardr,oyvindy}@simula.no

This work is motivated by applications in cryptanalysis. Assume that for a given cipher, a plaintext P and the corresponding ciphertext C are known, and the encryption key K is unknown. K can be determined by solving the equation system associated with the encryption $E_K(P) = C$. In a round-based encryption process extra auxiliary variables need to be introduced at each round to keep equations simple. For a strong cipher the resulting equation system must be nonlinear, contain many variables and be hard to solve.

In [1], we presented a new algorithm for eliminating auxiliary variables, while limiting the degree of the ensuing modified equations. The current work extends this by instead of bounding the degree at the lowest possible while eliminating, we let the maximum allowed degree be a chosen parameter m.

Generalizing the approach in [1], the input of the new algorithm consists of a sequence of *elimination sets* $F^m, \ldots, F^2$ of Boolean equations of degrees $m, \ldots, 2$, respectively. We also show how one can improve the results obtained in [1] by multiplying the target elimination variable onto selected polynomials. This technique produces more useful polynomials than what the previous approach does, and is linked to earlier solving strategies such as the XL-algorithm. However, here we do not multiply with *all* variables, only the target variable at each elimination step. We give a theoretic proof of why this works.

Each of the elimination steps produces new equations, which may have higher degree than the original ones. By design, we *discard* equations of degree greater than m to control the overall complexity. As in [1], the generalized algorithm contains a *normalization* step, where we remove many monomials containing the target variable. After normalization a large set of monomials cannot appear in the different sets, which may help to produce new polynomials of degree $\leq m$. A new algorithm where the maximum degree m is not kept constant is also presented. Here we start with a small value of m, and increase this maximum degree only after a number of elimination steps have been carried out, when the algorithm detects too big solution space expansion. In this way we keep the complexity low as long as possible, without expanding the solution space.

We then discuss the trade-off between the number of variables, the number of equations, and m to show when re-linearization may work after only eliminating a few variables. This gives a combinatorial description of when these systems re-linearize, and when the algorithm can actually solve the input system of equations after a few steps.

Finally, to demonstrate the algorithm and verify the bounds for re-linearization, we apply it to systems representing some small-scale block ciphers. We examine for which cases we produce polynomials of low degree only in variables from K, and when the method of re-linearization breaks these ciphers faster than exhaustive search. It is worth to note that some of the polynomials only in K-variables are of lower degrees than one would expect.

References

1. B.Greve, H.Raddum, G.Fløystad, Ø.Ytrehus *Solving polynomial systems over Boolean rings by elimination of variables*, to be presented at Boolean Functions and their Applications (BFA), 2017.