A crossbred algorithm for solving Boolean polynomial systems

Antoine Joux, University of Paris VI

We consider the problem of solving multivariate systems of Boolean polynomial equations: starting from a system of m polynomials of degree at most d in n variables, we want to find its solutions over F_2. Except for $d = 1$, the problem is known to be NP-hard, and its hardness has been used to create public cryptosystems; this motivates the search for faster algorithms to solve this problem. After reviewing the state of the art, we describe a new algorithm and show that it outperforms previously known methods in a wide range of relevant parameters. In particular, it can be used to solve all the Fukuoka Type I MQ challenges, culminating with the resolution of a system of 148 quadratic equations in 74 variables in less than a day (and quite a lot of luck).