Yeh, Jenny Yuan-Chun; Cheng, Chen-Mou; Yang, Bo-Yin
Operating degrees for XL vs. $F_4/F_5$ for generic $MQ$ with number of equations linear in that of variables. (English) Zbl 1290.94140

Summary: We discuss the complexity of $MQ$, or solving multivariate systems of $m$ equations in $n$ variables over the finite field $F_q$ of $q$ elements. $MQ$ is an important hard problem in cryptography. In particular, the complexity to solve overdetermined $MQ$ systems with randomly chosen coefficients when $m = cn$ is related to the provable security of a number of cryptosystems.

In this context there are two basic approaches. One is to use XL (“eXtended Linearization”) with the solving step tailored to sparse linear algebra; the other is of the many variations of Jean-Charles Faugère’s $F_4/F_5$ algorithms.

Although $F_4/F_5$ has been the de facto standard in the cryptographic community, it was proposed [B.-Y. Yang et al., Information and communications security. 6th international conference, ICICS 2004. Lect. Notes Comput. Sci. 3269, 401–413 (2004; Zbl 1109.94353)] that XL with Sparse Solver may be superior in some cases, particularly the generic overdetermined case with $m/n = c + o(1)$.

At the steering committee meeting of the post-quantum cryptography workshop in 2008, Johannes Buchmann listed several key research questions to all post-quantum cryptographers present. One problem in $MQ$-based cryptography, he noted, is “if the difference between the operating degrees of XL (with-sparse-solver) and $F_4/F_5$ approaches can be accurately bounded for random systems.”

We answer in the affirmative when $m/n = c + o(1)$, using saddle point analysis:

1. For instances with randomly drawn coefficients, the degrees of operation of XL and $F_4/F_5$ has the most pronounced differential in the large-field, “barely overdetermined” ($m - n = c$) cases, where the discrepancy is $\propto \sqrt{n}$.
2. In most other types of random systems with $m/n = c + o(1)$, the expected difference in the operating degrees of XL and $F_4/F_5$ is constant which can be evaluated mathematically via asymptotic analysis.

Our conclusions are partially backed up using tests with Maple, MAGMA, and an XL implementation featuring Block Wiedemann as the sparse-matrix solver.

For the entire collection see [Zbl 1275.94006].

MSC:
94A60 Cryptography
68P25 Data encryption (aspects in computer science)
68W30 Symbolic computation and algebraic computation

Keywords:
sparse solver; Gröbner basis; XL; MQ; asymptotic analysis; $F_4$/ $F_5$

Software:
Maple

Full Text: DOI