Cryptology ePrint Archive: Report 2011/669

Small Linearization: Memory Friendly Solving of Non-Linear Equations over Finite Fields

Christopher Wolf and Enrico Thomae

Abstract: Solving non-linear and in particular Multivariate Quadratic equations over finite fields is an important cryptanalytic problem. Apart from needing exponential time in general, we also need very large amounts of memory, namely $\approx Nn^2 $ for n variables, solving degree D, and $N \approx n^D$. Exploiting systematic structures in the linearization matrix, we show how we can reduce this amount of memory by n^2 to $\approx N$. For practical problems, this is a significant improvement and allows to fit the overall algorithm in the RAM of \emph{one} machine, even for larger values of n. Hence we call our technique Small Linearization (sl).

We achieve this by introducing a probabilistic version of the F$_5$ criterion. It allows us to replace (sparse) Gaussian Elimination by black box methods for solving the underlying linear algebra problem. Therefore, we achive a drastic reduction in the algorithm's memory requirements. In addition, Small Linearization allows for far easier parallelization than algorithms using structured Gauss.

Category / Keywords: implementation / MQ problem, Algebraic Attacks, Equation Solver, F5, Buchberger

Date: received 6 Dec 2011, last revised 14 Dec 2011

Contact author: chris at Christopher-Wolf de, enrico thomae@rub de

Available formats: PDF | BibTeX Citation

Version: 20111216:180408 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]