New Frontiers in Symmetric Cryptanalysis

Nicolas T. Courtois
University College of London

September 21, 2007

Short Abstract:

In this talk we will present recent advances in experimental algebraic cryptanalysis of block ciphers. The progress has been very fast in the recent years and two major attack methods have been discovered: ElimLin and conversion to SAT. Both, in spite of their extreme simplicity, almost always give much better results than any previously known Gröbner bases attack, that seem to have developed in the wrong direction. We argument that attention must be shifted from solving systems of equations at a high degree and avoiding reduction to 0, to solving different and much larger systems, that are nevertheless easier to solve. The main limitation of current algebraic attacks remains the same: they all 'hit the wall' very quickly when the number of rounds increases. Nevertheless we are making some progress and we have just started studying a vast space of cryptographic attacks with very low plaintext requirements that has never been explored before, and that is rich in possibilities.

Remark: The following web page allows to download prominent examples of equations used in cryptanalysis of block ciphers:
`www.cryptosystem.net/aes/toyciphers.html`