Cryptology ePrint Archive: Report 2011/626

Algebraic Complexity Reduction and Cryptanalysis of GOST

Nicolas T. Courtois

Abstract: GOST 28147-89 is a well-known block cipher and the official encryption standard of the Russian Federation. Its large key size of 256 bits at a particularly low implementation cost make GOST a plausible alternative for AES-256 and 3-key triple DES. The latter for the same block size of 64 bits offers keys of only 168 bits. All these algorithms are widely used, in particular in the financial industry. GOST is implemented in OpenSSL and other crypto libraries, and is increasingly popular also outside its country of origin. In 2010 GOST was submitted to ISO, to become an international standard. In theory 256-bit keys could remain secure for 200 years. GOST was analysed by Schneier, Biham, Biryukov, Dunkelman, Wagner, various Australian, Japanese, and Russian scientists, and all researchers seemed to agree that it looks quite secure. Though the internal structure of GOST seems quite weak compared to DES, and in particular the diffusion is not quite as good, it is always stipulated that this should be compensated by a large number of 32 rounds and by the additional non-linearity and diffusion provided by modular additions. At Crypto 2008 the hash function based on this cipher was broken. Yet as far as traditional encryption applications with single random keys are concerned, and until 2011, no cryptographically significant attack on this algorithm was found. One reflection attack with very large memory requirements was presented at FSE 2011. In this paper we present several attacks on full 32-rounds GOST two of which are substantially faster and all of which require much less memory. Our attacks belong to the family of conditional algebraic attacks on block ciphers: which can be defined as attacks in which the problem of key recovery is written as a problem of solving a large system of algebraic equations, and where the attacker makes some "clever" assumptions on the cipher which lead to an important simplification in the algebraic description of the problem, which makes it solvable in practice if the assumptions hold. Our methods work by black box reduction and allow to literally break the cipher apart into smaller pieces and reduce breaking GOST to a low data complexity software algebraic attack on only 8 rounds (sometimes less). Overall we obtain more than 10 different attacks faster than brute force on the full 32-round GOST (the best six results are given in Table 2) and ten more attacks on several different classes of weaker or special keys. This is shown in Table 3 and in Table 5 where we present five very nearly practical attacks breaking two principal 128-bit variants of GOST known from the literature.

Category / Keywords: Block ciphers, Feistel schemes, GOST, ISO 18033, key scheduling, self-similarity, advanced slide attacks, fixed points, reflection attacks, black-box reductions, low-data complexity attacks, algebraic attacks on block ciphers

Publication Info: Not published, earlier versions which contain a subset of this work were submitted to Crypto 2011 and Asiacrypt 2011

Date: received 19 Nov 2011, last revised 5 Jan 2012

Contact author: courtois at minrank org

Available formats: PDF | BibTeX Citation

Note: This is our "master paper" which describes a new general methodology for block cipher cryptanalysis through a reduction to a low-data complexity key recovery attack and more than 20 different attacks on GOST obtained with this methodology. It is here for reference, to establish priority, and to show the big picture how all these attacks are related to each other. Most of these attacks were developed in the period September 2010-February 2011 when an original 28-pages version of this paper with five distinct attacks which break GOST faster than brute force was submitted to Crypto 2011. In May 2011 a much shorter version of it was submitted to Asiacrypt 2011 and it contained two distinct attacks with time complexity of 2^216, this second attack method was last month borrowed by Shamir at al, who present an alternative faster last step for this precise attack, and obtain an overall faster attack in 2^192 see http://eprint.iacr.org/2011/558. This paper actually contains an attack with even lower complexity, 2^185, though it is not exactly a single-key attack therefore not everybody will agree that it is better than the most recent 2^192 result. Most of the attacks presented here have an experimental software last step which can certainly still be improved.

Version: 20120106:002650 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]