Cryptology ePrint Archive: Report 2011/626

Algebraic Complexity Reduction and Cryptanalysis of GOST

Nicolas T. Courtois

Abstract: GOST 28147-89 is a well-known Russian government encryption standard. Its large key size of 256 bits at a particularly low implementation cost make that it is widely implemented and used, in OpenSSL and elsewhere. In 2010 GOST was submitted to ISO to become an international standard. 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 keys generated at random are concerned, until 2011 no cryptographically significant attack on GOST was found. In this paper we present several new attacks on full 32-rounds GOST. Our methodology is derived from the idea 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/MITM attack on 8 or less rounds. Overall we obtain some 40 distinct attacks faster than brute force on the full 32-round GOST and we provide five nearly practical attacks on two major 128-bit variants of GOST (cf. Table 6). Our single key attacks are summarized in Table 2 p.14 and Table 4 p.84 and attacks with multiple keys in Table 3 page 80.

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

Publication Info: 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 Dec 2012

Contact author: courtois at minrank org