Cryptology ePrint Archive: Report 2011/211

Security Evaluation of GOST 28147-89 In View Of International Standardisation

Nicolas T. Courtois

Abstract: GOST 28147-89 is is a well-known 256-bit block cipher which is a plausible alternative for AES-256 and triple DES, which however has a much lower implementation cost. GOST is implemented in standard crypto libraries such as OpenSSL and Crypto++ and is increasingly popular and used also outside its country of origin and on the Internet. In 2010 GOST was submitted to ISO, to become a worldwide industrial encryption standard. Until 2011 researchers unanimously agreed that GOST could or should be very secure, which was summarized in 2010 in these words: despite considerable cryptanalytic efforts spent in the past 20 years, GOST is still not broken". Unhappily, it was recently discovered that GOST can be broken and is a deeply flawed cipher. There is a very considerable amount of recent not yet published work on cryptanalysis of GOST known to us. One simple attack was already presented in February at FSE 2011. In this short paper we describe another attack, to illustrate the fact that there is now plethora of attacks on GOST, which require much less memory, and don't even require the reflection property to hold, without which the recent attack from FSE 2011 wouldn't work. We are also aware of many substantially faster attacks and of numerous special even weaker cases. These will be published in appropriate peer-reviewed cryptography conferences but we must warn the ISO committees right now.

More generally, our ambition is to do more than just to point out that a major encryption standard is flawed. We would like to present and suggest a new general paradigm for effective symmetric cryptanalysis of so called "Algebraic Complexity Reduction" which in our opinion is going to structure and stimulate substantial amounts of academic research on symmetric cryptanalysis for many years to come. In this paper we will explain the main ideas behind it and explain also the precise concept of "Black-box Algebraic Complexity Reduction". This new paradigm builds on many already known attacks on symmetric ciphers, such as fixed point, slide, involution, cycling, reflection and other self-similarity attacks but the exact attacks we obtain, could never be developed previously, because only in the recent 5 years it became possible to show the existence of an appropriate last step for many such attacks, which is a low data complexity software algebraic attack. This methodology leads to a large number of new attacks on GOST, way more complex, better and more efficient than at FSE 2011. One example of such an attack is given in the present paper.

Category / Keywords: Block ciphers, Feistel schemes, key scheduling, self-similarity, reflection attacks, single-key attacks, algebraic attacks, algebraic complexity reduction, black-box reductions

Date: received 2 May 2011, last revised 9 May 2011

Contact author: n courtois at cs ucl ac uk