Algebraic and Differential cryptanalysis of GOST: Fact or Fiction

Vladimir Rudskoy, Andrey Dmukh

In 2010 GOST was submitted to ISO to become a part of international encryption standard ISO/IEC 18033-3. This fact stimulated intense research and lead to appearance of many papers devoted to cryptanalysis of GOST utilizing different analytic techniques. Some of the results reduced theoretical security of GOST[1, 2, 6, 7], while others[3, 8, 4, 5, 9] are only of a speculative nature. In this talk we will focus on latter «results» of N. Courtois et al., witch can be devided into two major groups: algebraic attacks and differential attacks.

Algebraic attack. Algebraic attacks are defined as attacks in which the problem of key recovery is written as a problem of solving a large system of Boolean algebraic equations. Algebraic attacks consist of two major steps.

The first step is called «Algebraic complexity reduction». At this step the attacker exploits self-similarity of GOST. In assumptions on existence of input-output (I/O) pairs of a certain kind and using self-similarity and its consequences, such as reflection and fixed point properties, the problem of attacking encipherment transformation is reduced to a problem of attacking 8 rounds of the algorithm. More precisely, given a large (2^{32} - 2^{64}) amount of known or chosen I/O pairs for the encryption transformation, several (1-4) I/O pairs for 8 rounds are obtained.

There are many different reductions presented; some are applicable to all keys and some use weak key families. There is a severe technical mistake in the best attack with weak keys. In our talk we investigate the impact of this mistake on the overall attack complexity.

At the second step the attacker represents the 8 round transformation as a system of multivariate polynomial equations. The attacker then tries to solve this system and hence recover the key using the obtained I/O pairs at the first step. Neither of the papers contains a full description and a proof of the second step complexity estimates. Author claims some «facts» instead which regard the complexity of the second step for GOST cipher, and estimates the overall complexity of attacks basing on these facts. These facts are claimed as experimental results, and some of them indeed can be experimentally achieved. However, most of the attacks are based on a «fact», which seems fictitious.

We scrutinize the validity of denoted «facts» and consider alternative technique for the second step. We show that usage of well-grounded algorithms and estimates instead of **fictitious** ones heavily increases time and memory requirements and therefore reduces the significance of these attacks.

Differential attack An attempt to mount a differential attack on GOST appeared recently[4, 5, 9]. This attack makes use of so-called «aggregated differentials». Firstly, an experimental differential characteristic for a small number of rounds is presented. All consequent analysis, as in the case of algebraic attacks, is based on unproved «facts» (or fictions).

Obviously, any differential attack strongly depends on the differential properties of the set of S-boxes. According to GOST 28147-89 standard, the S-boxes are not defined. The authors considered the set from Russian standard hash function specification GOST R 34.11-94. According to the latter standard, this set should be used only for test purposes. Although authors «are not certain if it is possible at all to make a cipher such as GOST

secure against differential cryptanalysis by changing only the S-boxes» and constantly allege to standardization of GOST as a part of ISO 18033-3, they avoid analyzing the set of S-boxes which was specified in the draft of amendment 1 of this standard.

Taking on trust the unproved hypothesis and estimating probabilities of differential characteristics just the same way the authors did, we analyze applicability of the attack on GOST with the mentioned set of S-boxes. «Surprisingly», we see that the attack is not applicable, and hereby we claim that appropriate choice of S-boxes makes GOST secure against differential cryptanalysis.

Bibliography

[1] O. Kara, Reflection Cryptanalysis of Some Ciphers, In Indocrypt 2008, LNCS 5365, pp. 294-307, 2008.

[2] T. Isobe, A Single-Key Attack on the Full GOST Block Cipher, In FSE 2011, Fast Software Encryption, Springer LNCS, 2011.

[3] N. Courtois, Security Evaluation of GOST 28147-89 In View Of International Standardisation, http://eprint.iacr.org/2011/211/.

[4] N. Courtois, M. Misztal, First Differential Attack On Full 32-Round GOST, in ICICS'11, pp. 216-227, Springer LNCS 7043, 2011.

[5] N. Courtois, M. Misztal, Differential Cryptanalysis of GOST, http://eprint.iacr.org/2011/312.

[6] I. Dinur, O. Dunkelman, A. Shamir, Improved Attacks on Full GOST, http://eprint.iacr.org/2011/558

[7] B. Zhu, G. Gong, Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2, http://eprint.iacr.org/2011/619

[8] N. Courtois, Algebraic Complexity Reduction and Cryptanalysis of GOST, http://eprint.iacr.org/2011/626/.

[9] N. Courtois, An Improved Differential Attack on Full GOST, http://eprint.iacr.org/2012/138