Advanced Truncated Differential Cryptanalysis of GOST Block Cipher

Theodosis Mourouzis
Department of CS, University College London, WC1E 6BT

tmourouz@cs.ucl.ac.uk

Nicolas Courtois
Department of CS, University College London, WC1E 6BT

n.courtois@ucl.ac.uk

Nikos Komninos
Department of CS, City University London, EC1V 0HB

nikos.komninos.1@city.ac.uk

Abstract

Differential Cryptanalysis (DC) is one of the oldest and most powerful techniques in the area of symmetric cryptanalysis. It is a chosen plaintext attack and its discovery was attributed to Eli Biham and Adi Shamir in the later 1980's since they were the first to publish a differential attack against the FEAL block cipher and then a similar attack against DES [5, 6]. However, according to a member of the original IBM DES team, Don Coppersmith, this technique was already known to IBM as early as 1974, and defending against DC had beem a design goal [4]. In addition, some other sources state that NSA was aware also of this technique and it was decided that since it should be kept secret.

In DC, the main task is to study how the differences propagate inside the cipher and discover some interesting propagations which occur with sufficiently good probability and can be used to distinguish a given number of rounds of the cipher from a random permutation. These differences expose the non-uniform distribution of some output differences given one or several input differences.

The method of DC was studied by many cryptographers and many enhancements have been proposed, which make this technique even more powerful. The most important one is by Knudsen who proposed advanced forms of DC based on truncated differentials [7, 8]. A truncated differential is a collection of (non-zero) differences instead of a single difference [7, 8]. Thus, the problem of studying single differences is transformed to the problem of studying the propagation of sets of differences. However, the space now becomes exponentially large and thus the study is infeasible in practise, unless some shortcuts are found based on the very specific structure of the given encryption algorithm. Importantly, many block ciphers which were supposed to be secure against naive DC, they were broken faster than brute-force based on truncated differential techniques. It is not easy to claim that a cipher is secure against this technique, since exhausting all possible combinations of sets of differences is infeasible and so far there was no theory which provides a measure of security against truncated DC. We plan to provide such a theory in our future studies.

In this paper, we study the security of GOST block cipher and its variants with respect to advanced forms of DC and especially using the notion of truncated differentials. Seki and Kaneko in 2011 have applied this notion to break around 13 rounds of GOST but no extension to an attack against the full cipher was feasible under their constructions [12].

GOST is a military-grade cipher which was designed by the former Soviet Union. It is the official encryption standard of the Russian federation given the number 28147-89 by the Government Committee for Standards of the USSR and it is used by large banks and implemented in many standard cryptography libraries such as, OpenSSL, Crypto++ and RSA security products. It is a 256-bit symmetric-key block cipher that operates on 64-bit blocks

[1]. It follows the Feistel Network design paradigm for block ciphers and has a very simple round function consisting of XORs, substitutions (S-boxes), rotations and modular additions which applied for 32 rounds.

Except of its military-grade 256-bit key and in theory it could be secure for 200 years, GOST has also an amazingly low hardware implementation. GOST requires approximately one fourth of the size of the circuit needed for AES-128 and DES. Thus, it seems to be a plausible alternative for AES-256 and 3-DES [2].

With respect to its security analysis, according to the Russian standard, GOST is safe to be used for encrypting secret and classified information and does not limit the security level. More precisely, at the beginning of the standard it states that " GOST satisfies all cryptographic requirements and does not limit the grade of security information to be protected".

In addition, according to Bruce Schneier [3], GOST is probably stronger than DES with respect to DC. Except of Schneier, many other prominent cryptographers and ISO cryptography experts have studied GOST and all seemed to agree that it could be or should be secure, since no better way to break it except brute force was known. Gabidulin et al, were the first who conducted a basic assessment of the security of GOST against linear and differential cryptanalysis [18]. As they have very naively claimed, 7 rounds are sufficient for a 128-bit level security against DC and that even if the S-boxes are replaced by the Identity map it is still secure at this level [18].

Until 2010, all researchers in the cryptographic community claimed that " despite considerable cryptanalytic efforts spent in the past 200 years, GOST is still not broken". Since GOST seems to offer a perfect balance between security and efficient implementation, when GOST was submitted to ISO 18033-3. By the same year of submission, many attacks against the full block cipher were discovered and presented in several conferences; reflection attacks, attacks based on double reflections, related-key attacks and advanced differential attacks [13, 14, 15, 16]. In 2011, we have discovered and published some interesting and very strong truncated differential properties of GOST and some other of its variants by introducing a refinement of Knudsen's approach which partitions the classical truncated differentials into disjoint sub-sets. In particular Courtois and Mourouzis have introduced the notion of general open sets which are sets constructed based on the connections between the S-boxes from round to round and are of partitioning type [9]. Then, using a black-box evolutionary algorithm [10, 17], they discovered interesting 8-round propagations, which can be combined effectively and produce distinguishers for 20 rounds of GOST. The notion of general open sets shows that good truncated differential properties can be found for all variants of GOST and that they mainly depend on the connections between S-boxes from round to round and not on their values.

In particular, Courtois and Mourouzis presented very strong statistical 20 round distinguisher for three different variants of GOST [9]; TestParamSet, CryptoProParamSet and ISO 18033-3. All these sets are of major importance since they are implemented in many standards and used by many organizations. The first one appears as the default set of S-boxes used in all available implementations. The second one is used in the hash function implementation and by many large bank organizations, while the last one is the one which is believed to be the strongest and was suggested in the ISO standardization process to become a global industrial standard. Extending a statistical distinguisher to an attack against the full block cipher is a non-trivial task and involves a series of optimization and combinatorial sub-tasks to be considered and solved. In fact, it is never guaranteed that it will succeed. Courtois extended a 20 round distinguisher to a full attack against the GOST cipher which uses the set of S-boxes TestParamSet of time complexity approximately 2^{179} GOST encryptions, memory complexity of about 2^{64} and using the full code-book [16]. In order to achieve the extension, he exploited the self-similarity of the cipher due to the very weak schedule and the poor diffusion for a limited number of rounds, up to 8 rounds.

In this paper, we use the ideas presented by Courtois and Mourouzis to study the security of two variants of GOST, which are considered as the simpler and most secure variants [9]; the one with the S-boxes replaced by the Identity Map and the ISO version which is assumed to be the strongest one. The advanced differential attacks we present are of the form of Depth-First Key search, which uses a 20 round distinguisher in the middle (or equivalently 26-round distinguisher for the simpler version of GOST with Identity Map) [11]. The main idea is that we consider a partition of the 32 rounds by placing in the middle the constructed distinguisher. Then, based on the weak diffusion we can extend these very strong statistical distinguishers to efficiently good filters for some external rounds. Then, by guessing some key bits for external rounds and determining some plaintext and ciphertext pairs of specified input-output differences we can extend the construction to an attack against the full block cipher. Thus, the technique we apply is a generic cryptanalytic framework of First-Search key search type which involves several optimization tasks obtained from the specific structure of the given encryption algorithm.

The results we obtain are remarkable and they reflect how powerful the differential attacks are, if appropriate ad-hoc heuristics are found and several non-trivial optimization tasks are considered and solved based on the structure of the very specific encryption algorithm we study. Using the entire codebook, we present an attack of time complexity approximately 2^{160} GOST encryptions against the full 32 rounds of the simplest GOST variant and an attack of time complexity approximately $2^{244.4}$ GOST encryptions against the full 32 rounds of the GOST submitted to ISO [11]. Even more importantly, the attacks we present are always subject to improvements if better solutions are found to the underlying optimization steps we consider. These attacks can be seen as new parametric form of advanced differential attacks, where several optimization and combinatorial sub-tasks are considered.

References

[1] Aleksandr Malchik, *An English translation of GOST Standard by Aleksandr Malchik with an English Preface co-written with Whitfield Diffie* , 1994.

[2] Axel Poschmann, San Ling and Huaxiong Wang, *256 Bit Standardized Crypto for 650 GE GOST Revisited* , In CHES 2010, LNCS 6225, pp. 219-233, 2010.

[3] Bruce Schneier, *Applied Cryptography, Second Edition* ,John Wiley and Sons, 1996.

[4] Don Coppersmith, *The Data Encryption Standard (DES) and its strength against attacks* , IBM Journal of Research and Development 38 (3): 243. doi:10.1147/rd.383.0243, 1994.

[5] Eli Biham and Adi Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, ISBN: 0-387-97930-1, 3-540-97930-1, 1993.

[6] Eli Biham and Adi Shamir, *Differential cryptanalysis of the full 16-round DES* , In Advances in Cryptology, CRYPTO 92, E. F. Brickel, Ed.,vol. 740 of Lecture Notes in Computer Science, pp. 487 496, 1992.

[7] Lars Knudsen, *Truncated and higher order differentials* , In Fast Software Encryption, pp. 196-211, Springer Berlin Heidelberg, 2011.

[8] Lars Knudsen and Matthew Robshaw, *The Block Cipher Companion* , Springer Berlin Heidelberg, 1995.

[9] Nicolas T. Courtois and Theodosis Mourouzis, *Enhanced Truncated Differential Cryptanalysis of GOST*, In SECRYPT, 2013.

[10] Nicolas T. Courtois and Theodosis Mourouzis, *Propagation of Truncated Differentials in GOST* , In SECURWARE, 2013.

[11] Theodosis Mourouzis, *Optimizations in Algebraic and Differential Cryptanalysis* , PhD Thesis, University College London , 2014.

[12] Haruki Seki and Toshinobu Kaneko, *Differential cryptanalysis of reduced rounds of GOST* , In Selected Areas in Cryptography, pp. 315-323, Springer Berlin Heidelberg, 2001.

[13] Takanori Isobe, *A single-key attack on the full GOST block cipher*, In Fast Software Encryption, pp. 290-305, Springer Berlin Heidelberg, 2011.

[14] Nicolas T. Courtois, *Security Evaluation of GOST 28147-89 In View Of International Standardisation*, IACR Cryptology ePrint Archive, 2011.

[15] Nicolas T. Courtois, *Algebraic Complexity Reduction and Cryptanalysis of GOST*, IACR Cryptology ePrint Archive, 2011.

[16] Nicolas T. Courtois, *An Improved differential attack on full GOST*, IACR Cryptology ePrint Archive , 2012.

[17] Nicolas T. Courtois, Theodosis Mourouzis, Michal Misztal, Jean-Jacques Quisquater and Guangyan Song, *Can GOST Be Made Secure Against Differential Cryptanalysis?*, In Cryptologia Journal , 2013.

[18] Vitaly Shorin, Vadim Jelezniakov and Ernst Gabidulin, *Linear and differential cryptanalysis of Russian GOST*, Electronic Notes in Discrete Mathematics 6, pp. 538-547 , 2001.