Advanced Differential Cryptanalysis and GOST Cipher

Nicolas T. Courtois Theodosis Mourouzis

University College London, UK

Abstract

Differential Cryptanalysis (DC) is one of the oldest known attacks on block ciphers and there is no doubt that it has influenced the design of encryption algorithms very deeply, ever since the 1970s. DC is based on tracking of changes in the differences between two messages as they pass through the consecutive rounds of encryption. However DC remains poorly understood.

In this paper we survey some of our research on the differential cryptanalysis of GOST. GOST cipher is the official encryption standard of the Russian federation. It has military-grade 256-bit keys and until recently it had a very solid reputation. It is also an exceptionally economical cipher implemented in OpenSSL and by some large banks. In 2010 it was submitted to ISO to become a global industrial standard.

In his textbook written in the late 1990s Schneier wrote that against differential cryptanalysis, GOST is "probably stronger than DES". In fact Knudsen have soon proposed more powerful advanced differential attacks however to this day most people get it wrong. In the most recent survey paper about advanced differential cryptanalysis and specifically in the context of ciphers with small blocks such as GOST, [Albrecht-Leander 2012] we read: "Truncated differentials, [...] in some cases allow to push differential attacks one or two rounds further". In fact we can gain not 2 but much closer to 20 rounds. For the default set of S-boxes our best differential attack on GOST has complexity of 2^{179} which is also the best single key attack on GOST cipher ever found. For other S-boxes the adaptation is possible but not straightforward.

Key Words: Block ciphers, GOST, differential cryptanalysis, sets of differentials, truncated differentials, non-linearity, S-boxes

Mathematics in Defence 2013

1 Introduction

GOST is a well-known Russian government standard block cipher. It has a 256 bits key which can be potentially further extended with secret S-boxes. This makes it a military-grade cipher and GOST is the official encryption standard of the Russian Federation. It appears that GOST is used by large banks such as Sberbank and the Central Bank of Russian Federation. It became an Internet standard [15] and it is a part of many crypto libraries such as OpenSSL and Crypto++ [16, 22]. In recent years it was increasingly popular and used outside its country of origin [18]. It is frequently praised for its exceptionally low implementation cost in hardware [18] which makes it a cheaper alternative for the major industrial standards such as AES and triple DES. Accordingly in 2010 GOST was submitted to ISO to become an international standard [18, 5].

Until 2010 the consensus in the research community was that “despite considerable cryptanalytic efforts spent in the past 20 years” GOST is not broken [18, 5]. However, as soon as it was submitted to ISO, it has attracted more attention from serious cryptanalysts. GOST got “academically” speaking broken and some 50 distincts attacks on GOST faster than brute force have been proposed, cf. [5, 11] and many other. This includes new advanced differential attacks [20, 6, 7, 8, 12, 11]. This is particularly interesting because Differential Cryptanalysis (DC) is one of the oldest classical attacks on modern ciphers. It is very widely known and studied, and it has guided cipher designers ever since the 1970s [3]. Our research shows that differential cryptanalysis remains poorly understood.

2 GOST And Differential Cryptanalysis

In his textbook written in the late 1990s Schneier wrote that against differential cryptanalysis, GOST is “probably stronger than DES” [21]. Moreover in 2000 Russian researchers claimed that breaking GOST with five or more rounds is “very hard” and explain that as few as 7 rounds out of 32 are sufficient to protect GOST against differential cryptanalysis [13]. All this is maybe true if we only look at simple differential attacks with single differentials such as Biham-Shamir attacks on DES [2]. GOST appears to be secure in the standard historical Biham-Shamir formulation of DC with single differences on the full state: we look at bitwise XORs of 64-bit words and the probabilities that certain particular differences could be invariant and propagate inside the cipher with a large probability. Interestingly, in 2000 Seki and Kaneko [20], explained that in GOST a basic differential attack with one single difference is unlikely to work **at all** for a larger number of rounds. This is due to the fact that unlike for DES, in GOST, differential characteristics for one round, typically work only for a fraction of keys, and this fraction is likely to rapidly decrease with the number of rounds, see [20]). However the study of differential cryptanalysis of DES is highly misleading [2]. It is possible to see that for many ciphers substantially better attacks can be obtained with sets of differentials.

2.1 Advanced Differential Attacks

In particular we have "truncated differential" attacks introduced by Knudsen [17] as early as 1994. Similar attacks are shown to exist for GOST as early as in 2000 by the same Japanese authors Seki and Kaneko [20]. These early advanced multiple differential attacks allowed to break about 13 rounds of GOST, see [20]. It was later discovered that these exact sets of differentials propagate with probabilities much higher than expected, see [7, 8]. Since 2011 we have discovered and published a number of better/stronger differential properties of GOST cipher than those of [20].

To this day, cryptographic literature badly underestimates the power of such attacks. For example in the most recent paper specifically about advanced differential cryptanalysis with many differentials, and which specifically looks at ciphers with small block which is the case for GOST [1], we read that: "Truncated differentials, [...] in some cases allow to push differential attacks one or two rounds further." Our research on GOST shows that we gain not 2 but much closer to 20 rounds [12]. This is a truly huge improvement knowing that the security of ciphers grows in general exponentially with the number of rounds.

2.2 The Most Basic Result

We consider differences with respect to the bitwise XOR. Following [7, 8] we define *an aggregated differential* A, B as the transition where any non-zero difference $a \in A$ will produce an arbitrary non-zero difference $b \in B$. In particular we consider the case when A is a set of all possible non-zero differentials contained within a certain mask. This can also be seen as a special case of "Truncated Differentials" [17] which are defined as fixing the difference not on all but a subset of data bits. A small technicality is that we explicitly exclude all-zero differentials from our sets of differences. For example for

$$\Delta = 0x80700700$$

we consider a set of all differences on 32 bits with between 1 and 7 active bits (but not 0) and where the "active" bits are contained within the mask 0x80700700. Similarly we denote by (Δ, Δ) a set of difference on 64 bits with up to 14 active bits, including also differences which are all zero in one half. There are $2^{14}-1$ differences in this set and we have $|A| = |B| = 2^{14}-1$.

Following [6, 7] for the default set of GOST S-boxes, the set of differentials (Δ, Δ) with uniform sampling of all differences it allows, produces an element of the same aggregated differential set (Δ, Δ) after 8 rounds of GOST with probability about $2^{-25.0}$.

3 Conclusion

A common misconception is that the choice of S-boxes allows to make a cipher more secure against differential cryptanalysis. In fact there is no evidence that they do. On this question opinions vary very substantially. Courtois has claimed in March 2012 [12] that the security of GOST depends essentially on the internal connections of the cipher and much less on S-boxes, while Russian advocates of GOST [19] have claimed in July 2012 that *S-boxes heavily affect security* and *with "good" S-boxes the attack fails.* A number of recent results tend to show that none of the alternative versions of GOST is really much more secure against advanced differential attacks.

Table 1: Some recent results with sets of 14 bits and 8 rounds cf. [10]

Set Name	Set	P(8R)
default set [21]	78000078 07070780	$2^{-24.0}$
ISO 18033-3 proposal	80000707 20707000	$2^{-22.7}$

However this sort of question does not have a definite final answer. Advanced differential attacks have very substantial combinatorial complexity. There is no straightforward metric to compare various differential properties. Their propagation probabilities cannot always be multiplied for more rounds. Additional properties such as symmetry may be required [12].

In order to address these problems we have been able to refine the Knudsen approach and propose a new refined form of an advanced differential attack. We introduce *General Open Sets* which partition the classical truncated attacks into disjoint sub-sets based on the very specific internal structure of the cipher [9]. This allows us to construct new families of distinguishers for 20 and more rounds of GOST [9]. Then taking into the account the weak key schedule of GOST, full 32-round GOST can be broken, cf. [12]. Our best differential attack on GOST has complexity of 2^{179} which is also the best single key attack on GOST cipher ever found.

References

[1] Martin Albrecht and Gregor Leander: *An All-In-One Approach to Differential Cryptanalysis for Small Block Ciphers,* preprint available at `eprint.iacr.org/2012/401/`.

[2] Eli Biham, Adi Shamir, *Differential Cryptanalysis of DES-like Cryptosystems,* Journal of Cryptology, vol. 4, pp. 3-72, IACR, 1991.

[3] Matt Blaze, *"Re: Reverse engineering and the Clipper chip",* Newsgroup post at `sci.crypt`, 15 August 1996, `https://groups.google.com/group/sci.crypt/msg/5cd14a329372cc5a`

[4] Nicolas Courtois: *The Best Differential Characteristics and Subtleties of the Biham-Shamir Attacks on DES,* On `eprint.iacr.org/2005/202`.

[5] Nicolas Courtois: *Security Evaluation of GOST 28147-89 In View Of International Standardisation,* Cryptologia, Vol. 36 Iss. 1 pp. 2-13, 2012.

[6] Nicolas Courtois, Michał Misztal: *Aggregated Differentials and Cryptanalysis of PP-1 and GOST,* In CECC 2011, Periodica Mathematica Hungarica Vol. 65 (2), pp. 1126, 2012.

[7] Nicolas Courtois, Michał Misztal: *First Differential Attack On Full 32-Round GOST,* in ICICS'11, pp. 216-227, Springer LNCS 7043, 2011.

[8] Nicolas Courtois, Michał Misztal: *Differential Cryptanalysis of GOST,* In Cryptology ePrint Archive, Report 2011/312. 14 June 2011, `http://eprint.iacr.org/2011/312`.

[9] Nicolas T. Courtois, Theodosis Mourouzis: *Enhanced Truncated Differential Cryptanalysis of GOST,* in SECRYPT 2013, 10th International Conference on Security and Cryptography Reykjavik, Iceland, July 29-31, 2013

[10] Nicolas T. Courtois, Theodosis Mourouzis: *Propagation of Truncated Differentials in GOST,* accepted at SECURWARE 2013, The Seventh International Conference on Emerging Security Information, Systems and Technologies, August 25 - 31, 2013 - Barcelona, Spain

[11] Nicolas Courtois: *Algebraic Complexity Reduction and Cryptanalysis of GOST,* Preprint 2010-2013, available at `http://eprint.iacr.org/2011/626`

[12] Nicolas Courtois: *An Improved Differential Attack on Full GOST*, In Cryptology ePrint Archive, Report 2012/138. 15 March 2012, `http://eprint.iacr.org/2012/138`.

[13] Vitaly V. Shorin, Vadim V. Jelezniakov and Ernst M. Gabidulin: *Linear and Differential Cryptanalysis of Russian GOST*, Preprint submitted to Elsevier Preprint, 4 April 2001

[14] I. A. Zabotin, G. P. Glazkov, V. B. Isaeva: *Cryptographic Protection for Information Processing Systems,* Government Standard of the USSR, GOST 28147-89.

[15] Vasily Dolmatov, Editor, RFC 5830: *GOST 28147-89 encryption, decryption and MAC algorithms,* IETF. ISSN: 2070-1721. March 2010. `http://tools.ietf.org/html/rfc5830`

[16] A Russian reference implementation of GOST implementing Russian algorithms as an extension of TLS v1.0. is available as a part of OpenSSL library. The file gost89.c contains eight different sets of S-boxes and is found in OpenSSL 0.9.8 and later: `http://www.openssl.org/source/`

[17] Lars R. Knudsen: *Truncated and Higher Order Differentials,* In FSE 1994, pp. 196-211, LNCS 1008, Springer.

[18] 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.

[19] Vladimir Rudskoy, Andrey Dmukh: *Algebraic and Differential Cryptanalysis of GOST: Fact or Fiction,* In CTCrypt 2012, 2 July 2012, Nizhny Novgorod, Russia. An extended abstract is available at: `https://www.tc26.ru/invite/spisokdoc/CTCrypt_rudskoy.pdf`. Slides are available at: `https://www.tc26.ru/documentary%20materials/CTCrypt%202012/slides/CTCrypt_rudskoy_slides_final.pdf`

[20] H. Seki and T. Kaneko: *Differential Cryptanalysis of Reduced Rounds of GOST. In SAC 2000, LNCS 2012, pp. 315-323, Springer, 2000.*

[21] Bruce Schneier: Section 14.1 GOST, in *Applied Cryptography,* Second Edition, John Wiley and Sons, 1996. ISBN 0-471-11709-9.

[22] Wei Dai: Crypto++, contains a reference C++ implementation of GOST and test vectors, `http://www.cryptopp.com`