# First Differential Attack on Full 32-Round GOST*

Nicolas T. Courtois[1] and Michał Misztal[2]

[1] University College London, Gower Street, London, UK
n.courtois@cs.ucl.ac.uk

[2] Military University of Technology, Kaliskiego 2, Warsaw, Poland
mmisztal@wat.edu.pl

**Abstract.** GOST 28147-89 is a well-known block cipher and the official encryption standard of the Russian Federation. A 256-bit block cipher considered as an alternative for AES-256 and triple DES, having an amazingly low implementation cost and thus increasingly popular and used [12,15,13,20]. Until 2010 researchers have written that: “despite considerable cryptanalytic efforts spent in the past 20 years, GOST is still not broken”, see [15] and in 2010 it was submitted to ISO 18033 to become a worldwide industrial encryption standard. In 2011 it was suddenly discovered that GOST is insecure on more than one account. There is a variety of recent attacks on GOST [3,7]. We have reflection attacks [14,7], attacks with double reflection [7], and various attacks which do not use reflections [7,3]. The final key recovery step in these attacks is in most cases a software algebraic attack [7,3] and sometimes a Meet-In-The-Middle attack [14,7].

In this paper we show that GOST is NOT SECURE even against (advanced forms of) differential cryptanalysis (DC). Previously Russian researchers postulated that GOST will be secure against DC for as few as 7 rounds out of 32 [9,19] and Japanese researchers were already able to break about 13 rounds [18]. In this paper we show a first advanced differential attack faster than brute force on full 32-round GOST.

**Keywords:** Block ciphers, GOST, differential cryptanalysis, sets of differentials, aggregated differentials, iterative differentials.

## 1 Introduction on GOST

GOST 28147-89 was standardized in 1989 [10] and is an official standard for the protection of confidential information in Russia, and formerly in the Soviet Union. Several specifications in English are also is available [11,12]. Unlike DES which could only be used to protect unclassified information, and like AES, GOST allows to protect also classified and secret information apparently without

* This work was supported by Polish Ministry of Science and Higher Education under research project Nr O R00 0111 12 and by the European Commission under the FP7 project number 242497 Resilient Infrastructure and Building Security (RIBS).

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 216–227, 2011.

any limitations, which is explicitly stated by the Russian standard, see the first page of [11]. Therefore GOST is much more than a Russian equivalent of DES, and its large key size of 256 bits make GOST a plausible alternative for AES-256 and 3-key triple DES. The latter for the same block size of 64 bits offers keys of only 168 bits. Clearly GOST is a very serious military-grade cipher.

The GOST S-boxes can be secret and they can be used to constitute a secondary key which is common to a given application, further extending key size to a total of 610 bits. Two sets of GOST S-boxes have been explicitly identified as being used by the two of most prominent Russian banks and financial institutions cf. [19,13]). The Russian banks need to securely communicate with tens of thousands of branches to protect assets worth many hundreds of billions of dollars against fraud.

One set of S-boxes known as "GostR3411_94_TestParamSet" [13] was published in 1994 as a part of the Russian standard hash function specification and according to Schneier [19] this set is used by the Central Bank of the Russian Federation. This precise version of GOST 28147-89 block cipher is the most popular one, and it is commonly called just "the GOST cipher" in the cryptographic literature. In this paper we concentrate on this set of S-boxes. The most complete current reference implementation of GOST which is of genuine Russian origin and is a part of OpenSSL library, contains eight standard sets of S-boxes [13]. Other (secret) S-boxes could possibly be recovered from a chip or implementation, see [17,8].

### 1.1 GOST Is Very Competitive

In addition to the very long bit keys GOST has a much lower implementation cost than AES or any other comparable encryption algorithm. For example in hardware GOST 256 bits requires less than 800 GE, while AES-128 requires 3100 GE, see [15]. Accordingly in 2010 GOST was submitted to ISO to become a worldwide encryption standard. ISO is still in the process of standardizing GOST at the time of writing.

## 2 Security of GOST

GOST was widely studied in the literature and while it is widely understood that the structure of GOST is in itself quite weak, for example compared to DES, and in particular the diffusion is not quite as good, it was however always stipulated that this should be compensated by a large number of 32 rounds cf. [9,19,18] and also by the additional non-linearity and diffusion provided by modular additions [9,16]. As far as traditional encryption applications of GOST with random keys are concerned, until 2011, no cryptographically significant single-key attack on GOST was ever found, which was summarized in 2010 in these words: "despite considerable cryptanalytic efforts spent in the past 20 years, GOST is still not broken", see [15].

In the well known Schneier textbook written in the late 1990s we read: "Against differential and linear cryptanalysis, GOST is probably stronger than

DES", see [19]. Then in 2000 Russian researchers claimed that "breaking the GOST with five or more rounds is very hard". and explain that as few as 5 to 7 rounds are sufficient to protect GOST against linear and differential cryptanalysis. In the same year, Japanese researchers [18], explain that in addition, such straightforward classical differential attack with one single differential characteristic are unlikely to work **at all** for a larger number of rounds. This is due to the fact that they only work for a fraction of keys, likely to rapidly decrease with the number of rounds, see [18]).

Yet in the same paper [18], more advanced differential attacks on GOST are described. They show how to break about 13 rounds of GOST and until now it was not clear if these attacks can be extended in any way to a larger number of rounds such as full 32 rounds, because partial internal differences generated in such attack become very hard to distinguish from differences which occur naturally at random. These questions are the central topic in this paper.

### 2.1 Recent Attacks on GOST

A new attack which finally breaks GOST, was very recently presented at FSE 2011, see [14]. A related but different, simpler and faster attack, appears in [7]. Many other new attacks have been recently developed, see [3,7].

## 3 Linear and Differential Cryptanalysis of GOST

### 3.1 Previous Research and Application to GOST

A basic assessment of the security of GOST against linear cryptanalysis (LC) and differential cryptanalysis (DC) has been conducted in 2000 by Gabidulin *et al*, see [9]. The results are quite impressive: at the prescribed security of level of $2^{256}$, 5 rounds are sufficient to protect GOST against LC. Moreover, even if the S-boxes are replaced by identity, and the only non-linear operation in the cipher is the addition modulo $2^{32}$, the cipher is still secure against LC after 6 rounds out of 32. In [9] the authors also estimate that, but here only w.r.t. the security level of about $2^{128}$, roughly about 7 rounds should be sufficient to protect GOST against DC.

### 3.2 Classical Biham-Shamir DC Attacks and GOST

The difficulty is explained by the Japanese researchers in 2000 [18]. If we consider the straightforward classical differential attack with one single differential characteristic it is in fact **unlikely to work at all** for a larger number of rounds.

This is due to the fact that when we study reasonably "good" iterative differential characteristics for a limited number of rounds (which already propagate with probabilities not better than $2^{-11.4}$ per round, cf. [18]), we realize that they only work for a fraction of keys smaller than half. For full 32-round GOST such an attack with a single characteristic would work only for a negligible fraction of keys of about $2^{-62}$ (and even for this tiny fraction it would propagate with a probability not better than $2^{-360}$).

### 3.3 Advanced Differential Attacks on GOST

This however does not prevent more advanced differential attacks on GOST which are the central topic in this paper. They have been introduced in 2000 in the same already cited Japanese paper [18]. They can be seen in two different ways, either as attacks which use sets of differentials as they are formalized in [18], or more specifically, as it is the case for the most interesting attacks of this type known (from [18] and in this paper), as attacks in which differentials are truncated, so that the best sets of differentials actually follow certain patterns, for example certain bits or whole S-boxes have zero differentials, and only some bits are active and have non-zero differentials.

### 3.4 Previous Advanced DC Attack on GOST

The best key recovery attack proposed in [18] has the

1. An initial extension with a small number of active bits at the input.
2. An iterative set of differentials with 24 active bits which can propagate for an arbitrary number of rounds.
3. A final extension differential with again a much smaller number of active bits,
4. A method for key recovery with guessing some key bits.

Attacks with sets of differentials can be applied to other ciphers, for example Q [1] and more recently PP-1 [5]. Our final key recovery method uses the key scheduling of GOST and thus is different than in previously published works [18,1,5].

In [18] the main iterative set of differentials occur naturally with higher probability of $2^{-50}$, which is not negligible anymore like in DES [2]. We are no longer dealing with exceptional events which never happen by accident, and which when they happen, happen for a specific reason and yield a lot of information when they happen, like in DES [2]. For GOST, when some differentials in a set are attained, there is a lot of ambiguity about why exactly they are attained, and such events give much less exploitable information about the secret keys than in DC for DES [2].

**Summary.** The best advanced multiple differential attack proposed in [18] allows to break between 12 and 17 rounds of GOST depending on the key, some keys being weaker. In this paper we greatly improve on the state of the art and develop the first differential attack on full 32 rounds.

## 4 From GOST to New Differential Attacks on GOST

GOST is a block cipher with a simple Feistel structure, 64-bit block size, 256-bit keys and 32 rounds. Each round contains a key addition modulo $2^{32}$, a set of 8 bijective S-boxes on 4 bits, and a simple rotation by 11 positions.

Differential characteristics in GOST, need to take into account not only the S-boxes, like in DES, but also the key addition modulo $2^{32}$, which makes that their probabilities depend on the key. In this paper we summarize the state of the art and report some very important new results. The (very technical) explanation on how to obtain this type of results through extended computer simulations is outside the scope of this paper and will appear elsewhere.

## 5 Vocabulary: Aggregated Differentials

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 $b \in B$ with a certain probability.

In the previous work on GOST exactly the same sorts of differentials are exploited for GOST, see [18]. The are called "sets of differential characteristics" however this would suggest that any set of characteristics is possible, for example $a \Rightarrow b$ and $a' \Rightarrow b'$ could be permitted but not $a \Rightarrow b'$. This is an unnecessarily general notion. Our notion of Aggregated Differentials only allows "sets of differential characteristics" which are in a Cartezian direct product of two sets $A \times B$.

Similar sets of differentials are also called "almost iterative differentials" in [1], however the word "almost" can be seen as misleading, because here and elsewhere [1,5] we will have "perfectly" iterative differentials, which are perfectly periodic, and can propagate for an arbitrary number of rounds, from set $A$, to exactly the same set $A$.

## 6 Multiple Differential Attacks on GOST

This attack on GOST was introduced in 2000 [18]. For example the difference of type 0x70707070,0x07070707, where each 7 means an arbitrary difference on 3 bits, plus extra rules to exclude all-zero differentials, propagates for one round with a probability of about $2^{-5.3}$. Here what we report will already start to differ from the combination of theoretical probabilities given in [18]. This is because it is very hard to predict what really happens with complex sets of differentials by theory. In fact it is rather impossible for complex differentials which could propagate over many rounds, to enumerate all possible differential paths which could at the end produce one of the differentials in our set. Moreover they strongly depend on the key. Therefore the more rounds we have, the more the actual (experimental) results will differ from predictions. Moreover the difference is in our experience almost always beneficial to the attacker: as we will see below, better attacks than expected are almost always obtained.

### 6.1 New Results

Many very good characteristics exist for GOST. Here we give one example. This example has been constructed by hand by the authors from differential characteristics of various S-boxes and already reported in one paper [5]. Consider the following differential set:

$$\varDelta = 0x80700700$$

by which we mean all differences with between 1 and 7 active bits (but not 0) and where the active bits are contained within the mask 0x80700700. Similarly, an aggregated differential $(\varDelta, \varDelta)$ means that we have 14 active bits, and that any non-zero difference is allowed. There are $2^{14} - 1$ differences in this set of ours. The following fact can be verified experimentally:

**Fact 6.2.** *The aggregated differential $(\varDelta, \varDelta)$ with uniform sampling of all differences it allows, produces an element of the same aggregated differential set $(\varDelta, \varDelta)$ after 4 rounds of GOST with probability about $2^{-13.6}$ on average over all possible keys.*

Importantly, for 8 rounds the result is better than the square of $2^{-13.6}$ which would be $2^{-27.2}$. It is:

**Fact 6.3.** *The aggregated differential $(\varDelta, \varDelta)$ (again with uniform sampling) produces the same aggregated differential $(\varDelta, \varDelta)$ after 8 rounds of GOST with probability about $2^{-25.0}$ on average over all possible keys.*

### 6.4 Propagation for 16 Rounds

**Fact 6.5.** *The aggregated differential $(\varDelta, \varDelta)$ produces the same aggregated differential $(\varDelta, \varDelta)$ after 16 rounds of GOST with probability about $2^{-48}$ on average over all possible keys.*

*Justification:* A more precise result need to be obtained by computer simulations.

This needs to be compared to the probability that the output difference set $(\varDelta, \varDelta)$ will also occur naturally. In this set there are exactly 50 inactive bits where the difference must always be 0. Therefore:

**Fact 6.6.** *The 64-bit output difference being a member of our set $(\varDelta, \varDelta)$ occurs naturally with probability about $2^{-50}$.*

### 6.7 Detailed Comparison New vs. Previous Results

We need to compare our result with the Japanese paper [18] from 2000. If we apply the probabilities found in [18], in theory, we expect that the difference of type 0x70707070,0x07070707 will propagate for 8 rounds with a probability of about $2^{-42.7}$. Our simulations show it is **much** higher. It is about $2^{-28.4}$ in practice.

Our aggregated differential $(\varDelta, \varDelta)$ with $\varDelta = 0x80700700$ propagates with a better probability of about $2^{-48}$, while the output difference in this set occurs naturally with probability of about $2^{-50}$. Clearly with the new method we are able to distinguish 16 rounds of GOST from a random permutation. Some of these results were already reported in [5]. Further values have less precision and are extrapolations.

| Input Aggregated Differential | 0x70707070,0x07070707 | 0x80700700,0x80700700 |
|---|---|---|
| Output Aggregated Differential | 0x70707070,0x07070707 | 0x80700700,0x80700700 |
| Reference | Seki-Kaneko [18] | this paper and [5] |
| Propagation 2 R | $2^{-8.6}$ | $2^{-7.5}$ |
| Propagation 4 R | $2^{-16.7}$ | $2^{-13.6}$ |
| Propagation 6 R | $2^{-24.1}$ | $2^{-18.7}$ |
| Propagation 8 R | $2^{-28.4}$ | $2^{-25.0}$ |
| Propagation 10 R | $2^{-35}$ | $2^{-31.1}$ |
| Propagation 12 R | $2^{-43}$ | $2^{-36}$ |
| Propagation 14 R | $2^{-50}$ | $2^{-42}$ |
| Propagation 16 R | $2^{-56}$ | $2^{-48}$ |
| Propagation 18 R | $2^{-62}$ | $2^{-54}$ |
| Propagation 20 R | $2^{-70}$ | $2^{-60}$ |
| Propagation 22 R | $2^{-77}$ | $2^{-66}$ |
| Output $\Delta$ Occurs Naturally | $2^{-40.0}$ | $2^{-50.0}$ |

**Fig. 1.** Our results and further extrapolations vs. previous results

### 6.8 An Initial Extension

It appears that the best single differential suitable for the initial extension for $(\Delta, \Delta)$ is one which does not modify anything in the first round, and one which will only affect the highest bit in the modular addition in the second round which does not generate any carries. This differential is $(0x80000000, 0x00000000)$.

In the following table we report some results which are computed as follows: for smaller number of rounds $X$ they are computed experimentally. For a larger $X$ and for all possible decompositions $X = Y + Z$ we consider that for the first $Y$ rounds we have achieved the iterative set from the initial set, and for the remaining $Z$ rounds we apply one of the exact results from Table 1 above. Due to the method these results are rather conservative estimations. We compare these results to those obtained assuming that one used the initial extension from [18] which again are exact results for up to 8 rounds, and beyond we again give lower bounds and based on a decomposition of $X = Y + Z$ rounds with $Y$ rounds being as in Table 2 and $Z$ being the main iterative piece as in Table 1, where we report the best lower bound obtain by such decomposition which again is a conservative estimation.

## 7 A Final Extension

In this section we propose a final extension with less active bits which seems to work well for various numbers of rounds.

| Input Aggregated Differential | 0x00000700,0x00000000 | 0x80000000,0x00000000 |
|---|---|---|
| Output Aggregated Differential | 0x70707070,0x07070707 | 0x80700700,0x80700700 |
| Reference | Seki-Kaneko [18] | this paper |
| Propagation 2 R | $2^{-1.4}$ | $2^{-0.4}$ |
| Propagation 4 R | $2^{-5.6}$ | $2^{-6.2}$ |
| Propagation 6 R | $2^{-11.5}$ | $2^{-12.2}$ |
| Propagation 8 R | $2^{-20.1}$ | $2^{-20.5}$ |
| Propagation 10 R | $2^{-28}$ | $2^{-24.6}$ |
| Propagation 12 R | $2^{-34}$ | $2^{-30.3}$ |
| Propagation 14 R | $2^{-41}$ | $2^{-36}$ |
| Propagation 16 R | $2^{-46}$ | $2^{-42}$ |
| Propagation 18 R | $2^{-55}$ | $2^{-47}$ |
| Propagation 20 R | $2^{-61}$ | $2^{-53}$ |
| Propagation 22 R | $2^{-66}$ | $2^{-59}$ |
| Output $\Delta$ Occurs Naturally | $2^{-40.0}$ | $2^{-50.0}$ |

**Fig. 2.** Some results with our initial extension

**Fact 7.1.** *The ordinary differential* $(0x80000000, 0x00000000)$ *produces a non-zero differential in the set* $(0x00000100, 0x80600200)$ *after 20 rounds of GOST with probability roughly at least about* $2^{-58}$ *on average over all possible keys.*

*Justification:* Currently we have no good method to estimate this probability. We consider an affine model. Our best aggregated differential which is $(0x80000000, 0x00000000) \Rightarrow (0x00000100, 0x80600200)$ Experimental results obtained for 8, 10 and 12 rounds are respectively $2^{23.6}$, $2^{28.4}$, and $2^{33.2}$. If we extrapolate from the last two values we get that maybe for 20 rounds the result could be $2^{-28.4-4.8\cdot(20-10)/2} \approx 2^{-52}$. Being conservative we postulate it is at least $2^{-58}$ due to the propagation (cases with many intermediate differentials of small Hamming weight) and another $2^{-59}$ which occur by accident because we have 59 inactive bits in $(0x00000100, 0x80600200)$. We do not have enough computing power to confirm this result. **This result is inexact.** A better method to estimate this probability needs to be developed in the future.

### 7.2 Our Distinguisher For 20 Rounds

We can note that the aggregated differential $(0x00000100, 0x80600200)$ has 5 active bits and occurs naturally with probability $2^{-59}$. In contrast the propagation we predict is expected to occur with probability of about $2^{-58}$ (with many intermediate differentials of small Hamming weight).

We are finally able to distinguish 20 rounds from a random permutation. We study this distinguisher in more details.

For a random permutation, if we consider $2^{63}$ possible pairs with an input difference $(0x80000000, 0x00000000)$, about $2^4 = 2^{63-59}$ pairs will have an output difference in the desired form in $(0x00000100, 0x80600200)$ purely by accident (a collision on 59 bits in the last round, arbitrary differentials in the middle of the computation).

In the case of the actual 20 rounds of GOST we expect that there will be another and additional number of about $2^5 = 2^{63-58}$ "good" pairs and with output difference in $(0x80700700, 0x80700700)$ and with many intermediate differentials of small Hamming weight. It is essential to understand that the overlap between these sets of $2^4$ and $2^5$ pairs should be most of the time negligible, because we are well below the birthday paradox bound for two sets to overlap.

Therefore in our attacks on 20 rounds we expect to get about $2^4$ pairs when the key guessed is incorrect, and about $2^4+2^5$ when it is correct. Can we distinguish between these two cases?

The standard deviation for the number of cases (collisions on 59 bits which occur by accident) can be computed as a sum of $2^{63}$ independent random variables equal to 1 with probability $2^{-59}$ and the result is $2^2$. Our additional $2^5$ cases amounts to 8 standard deviations. By applying the central limit theorem and assuming that our sum of $2^{63}$ independent random variables is Gaussian, and by applying the Gauss error function we obtain that the probability that by accident the number reaches a threshold of $2^4 + 2^5$ when it is correct, which is outside 8 standard deviations, is about $2^{-50}$. In contrast if the permutation has these additional pairs which come from the propagation of our differential, we expect to be above the threshold of $2^4 + 2^5$ with probability $2^{-1}$.

This is the basis of our attack and this distinguisher will be used to filter out a large proportion of wrong assumptions on GOST keys.

**Future Work:** Our aggregated output differential is in fact a collection of $2^5-1$ ordinary differentials, and the frequency of these differentials is not uniform. Thus better distinguishers can probably be developed. However this is **not** very easy because the distribution strongly depends on the key.

## 8 Key Recovery Attacks on Full 32-Round GOST

The key property which makes that we can substantially reduce the number of rounds in full 32-round GOST is that the order of 32-bit words in the key schedule is inversed in the last 8 rounds. In the fist 8 rounds we have:

$$k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7, \ldots$$

In the last 8 rounds we have:

$$\ldots, k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0$$

Thus for example if we guess $k_0, k_1, k_2, k_3, k_4, k_5$ we are left with only 20 rounds inside GOST. Then the simplest attack one can think of based on Fact 7.1 would work as follows:

### 8.1 First Differential Attack on GOST Faster Than Brute Force

For each 192-bit guess $k_0, k_1, k_2, k_3, k_4, k_5$ and for each of $2^{64}$ P/C pairs for 32 rounds, we compute the first 6 rounds forwards, and the last 6 rounds backwards.

Thus we get $2^{64}$ P/C pairs for 20 rounds. This would require a total time spent in this step of about $2^{192} \cdot 2^{64} \cdot 12/32$ GOST encryptions which is $2^{254.6}$ GOST encryptions, slightly less than brute force but not much less. Then we can discard a proportion about $2^{-50}$ of keys on 192 bits. Remaining key bits are found by brute force.

**Summary.** This attack requires $2^{64}$ KP and allows to break full 32-round GOST in time of about $2^{254.6}$ GOST encryptions for a success probability of 50 %. This is faster than brute force.

## 9 Conclusion

In 2000 Russian researchers claimed that as few as 7 rounds out of 32 would protect GOST against differential cryptanalysis, see [9]. In the same year two Japanese researchers [18], show that approximatively 13 rounds can be broken by joining several differential characteristics together [18]. More recently it was shown that the characteristics from [18] propagate better than expected, for example they allows to easily distinguish 12 rounds from a random permutation, see Fig. 2 and [5]. Ne and better sets of differentials able to distinguish 16 rounds of GOST were proposed in [5]. In this paper we extend previous results with suitable initial and final extensions and show how to distinguish 20 rounds of GOST from a random permutation, cf. Fact 7.1. From here, given the weakness in ordering of round keys in GOST, we develop a first differential attack on full 32-round GOST which is (only slightly) faster than brute force.

GOST is a standardized block cipher intended to provide a military level of security and to protect the communications for the government, the military, large banks and other organisations. Designed in the Soviet times, it remains today the official encryption standard of the Russian Federation. While in the United States DES could be used ONLY for unclassified documents, GOST "does not place any limitations on the secrecy level of the protected information", see [11]. GOST is a very economical cipher in hardware implementation, cf. [15]. In 2010 GOST was submitted to ISO to become an international standard and it is still in the process of being standardized at the time of writing. It is extremely rare to see such a cipher being broken by a mathematical attack faster than brute force.

The attack presented in this paper is just a sketch and a proof of concept. There is no systematic method known to find good aggregated differential characteristics. We have been conservative in estimations of probabilities and these probabilities alone require more work or/and more simulations to be computed exactly. We have also estimated that it is possible to lower the time complexity of this attack to about $2^{226}$ by a more progressive guessing of key bits, and filtering out pairs which cannot occur. Due to the lack of space, and the necessity to do more work on exact probabilities, these more complex attacks need more space and attention and will be developed in future publications. Some further but still early results are reported in [4].

## References

1. Biham, E., Furman, V., Misztal, M., Rijmen, V.: Differential Cryptanalysis of Q. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 174–186. Springer, Heidelberg (2002)
2. Biham, E., Shamir, A.: Differential Cryptanalysis of the Full 16-Round DES. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 487–496. Springer, Heidelberg (1993)
3. Courtois, N.T.: Security Evaluation of GOST 28147-8. View Of International Standardisation, document officially submitted to ISO in May 2011. In: Cryptology ePrint Archive, Report 2011/211, May 1 (2011), `http://eprint.iacr.org/2011/211/`
4. Courtois, N.T., Misztal, M.: Differential Cryptanalysis of GOST. In: Cryptology ePrint Archive, Report 2011/312, June 14 (2011), `http://eprint.iacr.org/2011/312`
5. Courtois, N.T., Misztal, M.: Aggregated Differentials and Cryptanalysis of PP-1 and GOST. In: 11th Central European Conference on Cryptology, Post-proceedings Expected to Appear in Periodica Mathematica Hungarica
6. Courtois, N.T.: General Principles of Algebraic Attacks and New Design Criteria for Cipher Components. In: Dobbertin, H., Rijmen, V., Sowa, A. (eds.) AES 2005. LNCS, vol. 3373, pp. 67–83. Springer, Heidelberg (2005)
7. Courtois, N.T.: Algebraic Complexity Reduction and Cryptanalysis of GOST. Preprint, submitted to Crypto 2011, later split in several papers, a short and basic version exactly as submitted to Asiacrypt (2011), `http://www.nicolascourtois.com/papers/gostac11.pdf`
8. Furuya, S.: Slide Attacks with a Known-Plaintext Cryptanalysis. In: Kim, K.-c. (ed.) ICICS 2001. LNCS, vol. 2288, pp. 214–225. Springer, Heidelberg (2002)
9. Shorin, V.V., Jelezniakov, V.V., Gabidulin, E.M.: Linear and Differential Cryptanalysis of Russian GOST. Preprint submitted to Elsevier Preprint, April 4 (2001)
10. Zabotin, I.A., Glazkov, G.P., Isaeva, V.B.: Cryptographic Protection for Information Processing Systems, Government Standard of the USSR, GOST 28147-89, Government Committee of the USSR for Standards (1989) (in Russian, Translated to English in [11])
11. An English translation of [10] by Aleksandr Malchik with an English Preface co-written with Whitfield Diffie, can be found at, `http://www.autochthonous.org/crypto/gosthash.tar.gz`
12. Dolmatov, V. (ed.): RFC 5830: GOST 28147-89 encryption, decryption and MAC algorithms, IETF (March 2010) ISSN: 2070-1721, `http://tools.ietf.org/html/rfc5830`
13. 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/`
14. Isobe, T.: A Single-Key Attack on the Full GOST Block Cipher. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 290–305. Springer, Heidelberg (2011)
15. Poschmann, A., Ling, S., Wang, H.: 256 Bit Standardized Crypto for 650 GE – GOST Revisited. In: Mangard, S., Standaert, F.-X. (eds.) CHES 2010. LNCS, vol. 6225, pp. 219–233. Springer, Heidelberg (2010)
16. Charnes, C., O'Connor, L., Pieprzyk, J., Safavi-Naini, R., Zheng, Y.: Comments on Soviet Encryption Algorithm. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 433–438. Springer, Heidelberg (1995)

17. Saarinen, M.-J.: A chosen key attack against the secret S-boxes of GOST (1998) (unpublished manuscript)
18. Seki, H., Kaneko, T.: Differential Cryptanalysis of Reduced Rounds of GOST. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 315–323. Springer, Heidelberg (2001)
19. Schneier, B.: Section 14.1 GOST. In: Applied Cryptography, 2nd edn. John Wiley and Sons (1996) ISBN 0-471-11709-9
20. Dai, W.: Crypto++, a public domain library containing a reference C++ implementation of GOST and test vectors, `http://www.cryptopp.com`