Enhanced Truncated Differential Cryptanalysis of GOST

Nicolas T.Courtois[1], Theodosis Mourouzis[1] and Michał Misztal[2]
[1]*Department of Computer Science, University College London, Gower Street, London, U.K.*
[2]*Military University of Technology, Kaliskiego 2, Warsaw, Poland*
{*n.courtois, tmourouz*}*@cs.ucl.ac.uk, mmisztal@wat.edu.pl*

Keywords: Block Ciphers, GOST, S-boxes, ISO 18033-3, Differential Cryptanalysis, Sets of Differentials, Distinguisher, Gauss Error Function, Aggregated Differentials, Truncated Differentials.

Abstract: GOST is a well-known block cipher implemented in standard libraries such as OpenSSL, it has extremely low implementation cost and nothing seemed to threaten its high 256-bit security [CHES 2010]. In 2010 it was submitted to ISO to become a worldwide industrial standard. Then many new attacks on GOST have been found in particular some advanced differential attacks by Courtois and Misztal with complexity of 2^{179} which are based on distinguishers for 20 Rounds. In July 2012 Rudskoy *et al* claimed that these attacks fail when the S-boxes submitted to ISO 18033-3 are used. However, the authors failed to consider that these attacks need to be re-optimized again for this set of S-boxes. This is difficult because we have exponentially many sets of differentials.

In this paper we present a basic heuristic methodology and a framework for constructing families of distinguishers and we introduce differential sets of a special new form dictated by the specific regular structure of GOST. We look at different major variants of GOST and we have been able to construct a distinguisher for 20 round for CryptoParamSetA and similar results for the new version of GOST submitted to ISO which is expected to be the strongest (!). Therefore there is absolutely no doubt that these versions of GOST are also broken by the same sort of attacks.

1 INTRODUCTION

GOST 28147-89 encryption algorithm is the state standard of the Russian Federation and it expected to be widely used in Russia and elsewhere (GOST, 2005; A. Poschmann and Wang, 2010). It was standardized in 1989 and first it became an official standard for the protection of confidential information. However the specification of the cipher kept confidential until 1994 when it was declassified, published (I.A. Zabotin and Isaeva, 1989) and translated to English (Malchik and Diffie, 1994). It is described in several more recent Internet standards, like (Dolmatov, 2010) and (V. Popov and Leontie, 2006).

According to Russian standard, GOST is safe to be used for encrypting classified and secret information without any limitation (Malchik and Diffie, 1994). Until 2010 most researchers would agree that "despite considerable cryptanalytic efforts spent in the past 20 years, GOST is still not broken", and moreover its large military-grade key size of 256 bits and its amazingly low implementation cost made it a plausible alternative to all standard encryption algorithms such as 3-DES or AES (A. Poschmann and Wang, 2010). It appears that never in history of industrial standardization, we had such a competitive algorithm in terms of cost vs. claimed security level.

Accordingly in 2010 it was submitted to ISO 18033-3 to become a worldwide industrial standard. This has stimulated intense research and lead to the development of many interesting new cryptanalytic attacks. In fact, ISO standards underpin our industry data security applications and when a cryptographic algorithm is submitted to ISO and it is flawed, it is our obligation to find these flaws and publish them, otherwise our economy and critical infrastructures would be at risk.

There are two main categories of attacks on GOST: attacks with complexity reduction which reduce the attack to an attack on a smaller number of rounds (Courtois, 2011b; Courtois, 2011a; Isobe, 2011; Itai Dinur and Shamir,), and differential attacks (Courtois and Misztal, 2012; Courtois, 2012) which reduce the attack to the problem of distinguishing a certain number of rounds of GOST from a random permutation.

In this paper we present fundamental methodology for constructing general families of distinguish-

ers on reduced-round GOST. The design of the distinguisher is a highly nontrivial optimization step which needs to be solved in order to be able to find a working differential attack against the complete full round cipher. Unhappily the number of potential attacks with sets of differential is very large and there is no hope to explore it systematically. In order to tackle the astronomical complexity of this task we introduce the new notion of "*general open sets*" which allows us to consider "similar" differentials together. It is a compromise between the study of individual differentials (infeasible) and truncated differentials (Knudsen, 1994) which sets are already too large. Our new notion is a major refinement of truncated differential cryptanalysis of practical importance which allows for efficient discovery of better advanced differential distinguisher attacks on GOST.

In July 2012 Russian researchers have claimed that this attack will not work for the new version of GOST which is expected to be the strongest, see (Rudskoy and Dmukh, 2012). However this claim is not correct, and there is a major methodological flaw in their reasoning. One cannot just apply the attack to the new S-boxes directly, one needs to re-optimize the attack for other sets of S-boxes. We basically need to re-discover it from scratch because no efficient method for exploration of all possible sets of differentials is at sight. In this paper we are going to refine the basic attacks from (Courtois and Misztal, 2011), propose better and more powerful distinguishers and methodology.

2 GOST BLOCK CIPHER

GOST is a block cipher with a simple 32-round Feistel structure which encrypts a 64-bit block using a 256-bit key, see *Figure* 1

Each round of GOST contains a key addition modulo 2^{32}, a set of 8 bijective S-boxes on 4 bits and a simple rotation by 11 positions to the left. The image of any 64-bit block of the form $L||R$ (where L and R the left and the right half respectively) after 1 round of GOST is given by:

$$(L,R) \rightarrow (R, L \oplus F_i(R)) \qquad (1)$$

where F_i is the internal function used in each round as shown in *Figure* 2.

In the following subsections we describe in details the main components of GOST; key schedule, S-boxes and the internal connections between its S-boxes.

GOST has a very simple key schedule. The 256-bit key is divided into eight 32-bit words $k_0, k_1, .., k_7$

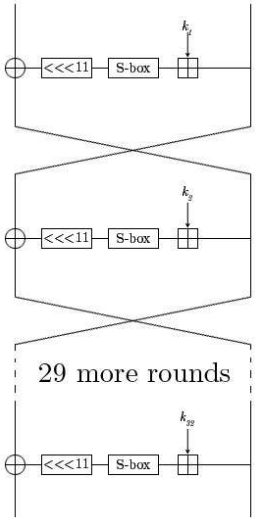

Figure 1: Diagram of GOST cipher, 32-rounds of a Feistel network to encrypt a 64-bit plaintext using a 256-bit key.

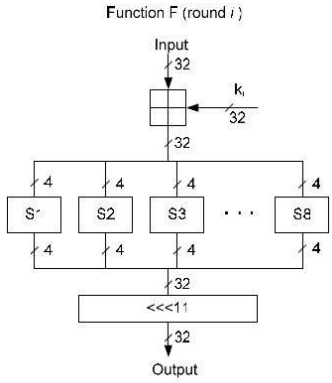

Figure 2: Detailed description of the round function F_I used in GOST.

where the first 24 rounds use the keys in this order and only the last 8 rounds use them in the reverse order, as shown in *Table* 1.

Table 1: Key schedule in GOST.

R1-R8	R9-R16
$k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7$	$k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7$
R17-R24	R25-R32
$k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7$	$k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0$

Each round function makes use of 8 4-bit to 4-bit S-boxes. According to the Russian standard, these S-boxes can be kept secret and as they contain about $354 * (log_2(16!^8))$ bits of secret information they increase the effective key size to 610 bits. However, a chosen-key attack can reveal the content of the S-Boxes in approximately 2^{32} encryptions (Saarinen, 1998).

In this paper we apply our methodology to

GOST and in particular we report concrete results on two set of S-boxes; GostR3411-94-TestParamSet which is used by the Central Bank of the Russian Federation (Schneier, 1996) and Gost28147-CryptoProParamSetA. However, our general methodology can be applied to any set of S-boxes.

3 ENHANCING DIFFERENTIAL CRYPTANALYSIS

Differential cryptanalysis (DC) is one of the oldest known attacks on block ciphers. In cryptographic literature it was first described and analysed by Biham and Shamir and applied to DES algorithm, see (Biham and Shamir, 1992; Biham and Shamir, 1990). DC is based on tracking of changes in the differences between two messages as they pass through the consecutive rounds of encryption. In his textbook written in the late 1990s Schneier writes that: "Against differential and linear cryptanalysis, GOST is probably stronger than DES", see (Schneier, 1996). However Knudsen and other researchers have soon proposed more powerful advanced differential attacks (Knudsen, 1994). Such attacks were applied to GOST as early as in 2000, (Seki and T.Kaneko, 2000) showing that Schneier was wrong, and since 2011 many much stronger differential properties have been found, cf. (Courtois and Misztal, 2011) and many other.

We aim to evaluate the resistance of GOST against advanced forms of differential cryptanalysis of GOST algorithm, and we are in fact going to propose new forms of advanced differential attacks which are going to be special versions of attacks with sets of differential and "aggregated differentials" from (Courtois and Misztal, 2012) and a refinement of truncated differentials of (Knudsen, 1994).

In the rest of this section we provide our heuristic methodology for constructing a family of distinguishers for some variants of GOST block cipher, including the GOST-ISO version. In order to be able to discover new interesting attacks on GOST we need a suitable definition. We are going to introduce a new form of differential sets, which is designed to be a practical compromise between the study of sets of individual differentials (infeasible) and truncated differentials (too simple) and which allows for efficient discovery of advanced differential attacks on GOST which are going to be better than previously studied attacks due to the larger degree of freedom introduced.

3.1 Aggregated and Truncated Differentials in GOST

All differences in our differential attacks are considered with respect to the bitwise XOR operation. We employ the notation and terminology as previously defined in (Courtois and Misztal, 2012).

Definition 3.1.1. (Aggregated Differentials)**.** Transition where any non-zero difference $a \in A$ will produce an arbitrary non-zero difference $b \in B$ with a certain probability.

Particularly we consider the case when A is a set of all possible non-zero differentials contained within a certain mask. This can also be studied as a special case of *Truncated Differentials*, which are defined as xoring the difference not on all but a subset of data bits, see (Knudsen, 1994).

Additionally, each mask is constructed according to the structure of each variant of GOST and this is the basic reason why the attack fails when it is applied in exactly the same way on all variants of GOST as claimed in (Rudskoy and Dmukh, 2012). The following definition of *General Open Sets* is fundamental to understand how the Courtois-Misztal attack needs to be re-designed for each new variant of GOST and captures exactly the basic ideas implemented behind this attack.

Definition 3.1.2. (General Open Sets)**.** We define a General Open Set as a string Q of 16 characters on the alphabet 0,7,8,F and by definition this general open set is a set of differences $X \in Q$ on 64-bits which

1. are "under" Q by which we mean that $Sup(X) \subseteq Sup(Q)$, where $Sup(X)$ is the set of bits at 1 in X
2. AND in each of the up to 16 substrings in the specification which are not 0 but any of 7,8,F, there is at least one "active" bit at 1.

In other words these are special sorts of truncated differentials with "holes": some subsets which have been removed. These removed subsets can be seen as unions of other General Open Set classes. Moreover all these sets are disjoint and partition the whole space of all possible 64-bit differentials.

The main reason why we have this very special alphabet 0,7,8,F is the internal connections of GOST cipher: we group together bits which are likely to be flipped to together.

It is very important to notice that a General Open Set encoded by 8070070080700700 is NOT the same set of differentials as in previous papers on this topic. Previous works included all open sets "under" the current set, or in other words they do not exclude special cases and much simpler differentials, which is

also how the truncated differentials work. However in our work we need to exclude these cases because they lead to vastly different propagation probabilities, and different patterns, and we want to produce better, more refined distinguishers and attacks. It is possible to see that previous research uses sets which we now are going to call closed sets as follows.

Definition 3.1.3. (Closure Of Differential Sets)**.** The closure of a differential set X is denoted by $[X]$. $[X]$ is the union of all open sets below X.

For example the closure of 8070070080700700, denoted as $[8070070080700700]$ consists of $2^{14}-1$ elements (zero-differential is excluded only).

There are 2^{32} open sets for 64-bit blocks and many occur with very low probability. This allows us to reduce the complexity and model the propagation of differentials in Courtois-Misztal attacks in a more refined way. Earlier notions of *truncated differentials* (Knudsen, 1994) and earlier Japanese differential attacks on GOST and also most Courtois and Misztal attacks are all unions of our new General Open Sets. However we can also now consider new arbitrary unions of open sets and propose new attacks which will be more refined and stronger than previous attacks. For example we are able to improve the recent Courtois-Misztal distinguisher for 20 rounds of GOST which used "closed sets".

3.2 Propagation through GOST

Our new methodology and definitions needs some sort of validation to see if they are really interesting to be studied in the case of GOST cipher. In this section we illustrate the propagation of the input difference $(80000000, 00000000)$ through different rounds of GOST which uses the set of S-boxes "GostR3411-94-TestParamSet". We are interested in transitions where the output difference lies within the mask $(80700700, 80700700)$. This is equivalent to considering 64-1 disjoint open sets, all under $(80700700, 80700700)$, which are judged particularly interesting due to previous attacks, and for which it is feasible to study them in more detail and trace some transition graphs with probabilities. We basically are studying an interesting subset of a much larger graph with 2^{32} General Open Sets. On the following figures each box represents one of these 64-1 non-empty classes. The boxes with a larger frame represent the possible output difference after some rounds of GOST, while other open sets (other boxes) cannot yet be achieved at all at this step. The width of each box is proportional to the logarithm of the probability for the output differential to fall within this specific open set, after $1, 2, 3, \ldots$ rounds, which was computed by

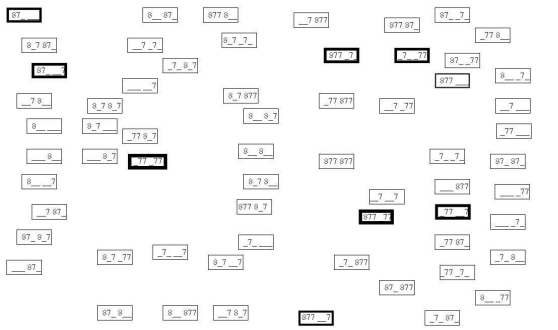

Figure 3: Propagation of $(80000000, 00000000)$ after 7R of GOST.

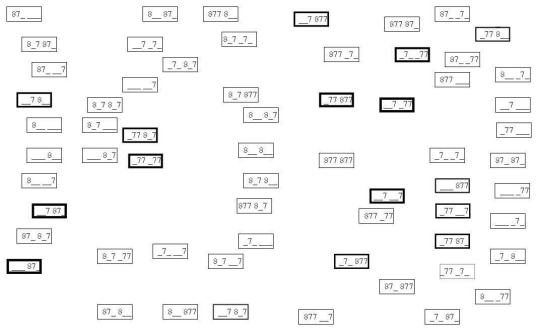

Figure 4: Propagation of $(80000000, 00000000)$ after 8R of GOST.

computer simulations.

As we observe from the figures the input differential even after 8 rounds of GOST is still more probable to be mapped to some very specific open sets. *Figure* 5 represents the entropy of the output difference variable for each round of GOST. We see that the entropy initially is low as expected for small number of rounds and then it increases more or less uniformly reaching close to 12.31 after 7 rounds. For 8 rounds and more we expect the entropy to be close to 14 and the probability distribution will tend to a uniform distribution.

These graphs and entropy figures can be seen as a sort of validation of our methodology: our sets seem to capture very well the fact that not all differences inside earlier attacks are ever attained, we are likely to attain only very specific open sets, and therefore we can construct more precise and refined distinguisher attacks on GOST than ever before.

4 DISCOVERY OF NEW ADVANCED ATTACKS ON GOST

In the previous works distinguishers were constructed as invariant closed sets to closed sets propagations,

Round	Entropy
0	0.0
1	0.0
2	2.81
3	5.61
4	5.72
5	8.19
6	10.92
7	12.31

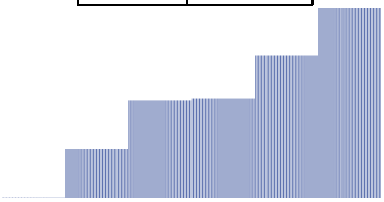

Figure 5: The Entropy estimation and plot after 1-7 rounds of GOST starting from the input set 8000000000000000.

and were frequently evaluated heuristically and split in several pieces. However the nature of closed sets is such that they contain many open sets for which the propagation probabilities are not at all the same with important discrepancies. As we advance in the study of such attacks we need to dis-aggregate the previous attacks into unions of many different transitions for open sets, and we expect that in this way we can construct more powerful attacks, and also we can evaluate the propagation probabilities in previous attacks with better precision.

In present work we still omit several interesting questions, for example how good properties for 8 rounds of GOST can be discovered at all. In (Courtois, 2012) some heuristics for that are provided. It still not even clear for example which properties are good and which one are "better" and why. For example is a property on 1 bit difference which propagates for 9 rounds with probability 2^{-35} any better than a weaker property with $2^{14}-1$ differences which propagates fro 9 rounds with probability 2^{-29}? This is however precisely the point. For 8 rounds we do NOT have an objective measure of scientific achievement. However for 20 rounds we do have one. Distinguishers can be rated on what is the advantage: how many standard deviations we are at from the behavior of a random permutation? A higher figure allows to reject a higher percentage of key in a cryptographic attack. We want to construct a practical theory of advanced differential attacks on GOST and this explains why we look at 20 rounds precisely.

4.1 Methodology

In this section we briefly describe our methodology for constructing good distinguishers for some rounds of GOST cipher. Distinguisher is an algorithm that is able of distinguishing a given cryptographic primitive such as a block cipher from a random permutation (or from a random mapping for or hash function). Not every distinguisher can be transformed into a key recovery attack on the cipher (or to recover some of the plaintext bits). However the existence of an efficient distinguisher always means the cryptographic primitive in question is weak and for example it would not be considered by ISO as a serious candidate for standardization. For advanced differential attacks, the construction of such a distinguisher is typically the most difficult step involved when developing an attack on a given cipher.

Figure 6 illustrates how our methodology works for constructing a distinguisher for n rounds of a given block cipher. The methodology is based on searching highly likely (compared to the natural probability) transitions between general open sets for different numbers of rounds.

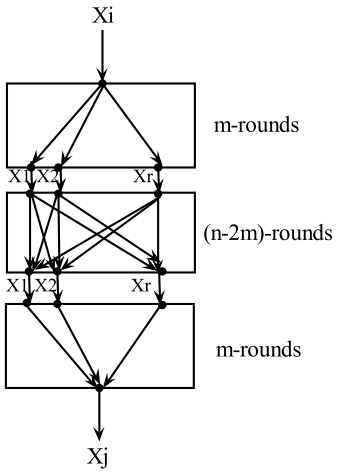

Figure 6: Representation of construction of a general distinguisher for n rounds seen as a combinatorial problem.

As a first step, we need to experimentally determine the probabilities of transitions between *general open sets* as described in the previous section for some m round, additional $n-2m$ rounds, and next m rounds of the cipher as shown on *Figure* 6 (in total we have n rounds). According to the **Law of Large Numbers** Central Limit Theorem because our experience is repeated many times, the average number of suitable events observed by the attacker is approximated by the Gaussian with good precision. As more trials are performed by the attacker, it is going to become closer and closer to the expected value The law ensures stable long-term results for random events. and the deviation can predicted according to the Gauss Error Function.

For each input/output X_i/X_j we compute by simulations the expected average number of events for a random key by:

$$E_{i,j} = \sum_{m,n} \#Events \quad (2)$$

$$= \sum_{m,n} \left(\frac{\#(X_i)}{2^{64}}.P(i \to m).P(m \to n).P(n \to j)\right) \quad (3)$$

Theorem 3.2.1. For a permutation on 64-bits we expect that the expected number of events for an input/output pair X_i/X_j for open sets X_i, X_j is given by:

$$E_{ref} = \frac{\#X_i.\#X_j}{2} \quad (4)$$

Proof. We have in total ${C_2}^{2^{64}} \simeq 2^{127}$ possible pairs (P,C). The total number of ordered 64-bit input/output differences $(\Delta X, \Delta Y)$ is 2^{128}. Thus for a random permutation on 64-bits the expected number of events for an input/output pair X_i/X_j for open sets X_i, X_j is given by $\#(P,C).P(\Delta X \in X_i, \Delta Y \in X_j) = 2^{127}.\frac{\#X_i.\#X_j}{2^{128}} = \frac{\#X_i.\#X_j}{2}$.

The key question is how a differential attack on GOST can cope with false positives. We have differentials which occur naturally for an arbitrary permutation on 64-bits and in this case we expect to have E_{ref} pairs (P_i, P_j) with such differences. According to Central Limit Theorem this number can be approximated by a Gaussian with a standard deviation $\sqrt{E_{ref}}$.

Additionally we have differentials which occur due to propagation of small Hamming weight differentials for n rounds of GOST. Under this scenario we expect to have $(E_{i,j} + E_{ref} - E_{ir})$ such pairs (P_i, P_j), where E_{ir} is the number of events which can happen in both cases; random permutation on 64-bits and also a reduced-round version of GOST.

However, E_{ir} is negligible since if we assume that the first and last m-rounds as shown in *Figure* 6 is m-rounds of GOST while the middle $n-2m$ is a random permutation we get that this input/output difference X_i/X_j occurs naturally with probability approximately $(100.2^{-50})^2$ which is close to zero due to our construction of our differential.

A distinguisher on n rounds must be constructed in such a way such that the intersection between these two sets is negligible and thus we are able to distinguish n rounds of GOST from a random permutation.

Thus the advantage (ADV) an attacker has to distinguish the cipher from a random permutation is approximately computed as follows:

$$ADV = \frac{|(E_{i,j} + E_{ref} - E_{ir}) - E_{ref}|}{\sqrt{E_{ref}}} \quad (5)$$

Thus what we really obtain here is $\frac{|(E_{i,j}|}{\sqrt{E_{ref}}}$.

In the next subsections we apply our methodology and we present some really good distinguishers for 20 rounds that we have constructed for two different variants of GOST block cipher; GostR3411-94-TestParamSet and Gost28147-CryptoProParamSetA.

5 Results and Concrete Optimizations

5.1 GostR3411-94-TestParamSet

In this section we present the results obtained when our methodology is applied to the GOST which uses the set of S-boxes as described in *Table* 2.

Table 2: The set of S-boxes named id-GostR3411-94-TestParamSet.

Order	id-GostR3411-94-TestParamSet
1	4,10,9,2,13,8,0,14,6,11,1,12,7,15,5,3
2	14,11,4,12,6,13,15,10,2,3,8,1,0,7,5,9
3	5,8,1,13,10,3,4,2,14,15,12,7,6,0,9,11
4	7,13,10,1,0,8,9,15,14,4,6,12,11,2,5,3
5	6,12,7,1,5,15,13,8,4,10,9,14,0,3,11,2
6	4,11,10,0,7,2,1,13,3,6,8,5,9,12,15,14
7	13,11,4,1,3,15,5,9,0,10,14,7,6,8,2,12
8	1,15,13,0,5,7,10,4,9,2,3,14,6,11,8,12

Result 5.1.1.

8780070780707000
↓ (10R)
[8070070080700700]
↓ (10R)
8070700087800707

is a 20 rounds distinguisher for this variant of GOST.

Justification. For a typical permutation on 64-bits (does not have to be a random permutation, it can be GOST with more rounds) we expect that there are $2^{27.1}$ pairs (P_i, P_j) with such differences. The distribution of this number can be approximated by a Gaussian with a standard deviation $2^{13.55}$.

For 20 rounds of GOST and for a given random GOST key, there exists two disjoint sets of $2^{27.1} + 2^{18.2}$ such pairs (P_i, P_j).

The distribution of the sum can be approximated by a Gaussian with an average of about $2^{27.1} + 2^{18.2}$ and the standard deviation of $2^{13.55}$

None of the $2^{18.2}$ pairs (P_i, P_j) is a member of the $2^{27.1}$ occurring naturally. For any of these cases which occur naturally, we have a non-zero input differential 8780070780707000. By a computer simulation we

obtain that a differential of type [8070070080700700] can occur at 10 rounds from the beginning with probability $2^{-29.4}$. Similarly it can occur 10 rounds from the end but with probability $2^{-29.4}$. Overall we expect only about $2^{-29.4-29.4+27.1} = 2^{-31.7}$ pairs (P_i, P_j) on average will have the propagation characteristic as shown. Therefore the two sets are entirely disjoint with high probability. This gives us an *ADV* of approximately 25.8 standard deviations.

5.2 Gost28147-CryptoProParamSetA

In this section we present the results obtained when our methodology is applied to the GOST which uses the set of S-boxes as described in *Table* 3.

Table 3: The set of S-boxes named Gost28147-CryptoProParamSetA.

Order	Gost28147-CryptoProParamSetA
1	10,4,5,6,8,1,3,7,13,12,14,0,9,2,11,15
2	5,15,4,0,2,13,11,9,1,7,6,3,12,14,10,8
3	7,15,12,14,9,4,1,0,3,11,5,2,6,10,8,13
4	4,10,7,12,0,15,2,8,14,1,6,5,13,11,9,3
5	7,6,4,11,9,12,2,10,1,8,0,14,15,13,3,5
6	7,6,2,4,13,9,15,0,10,1,5,11,8,14,12,3
7	13,14,4,1,7,0,5,10,3,12,8,15,6,2,9,11
8	1,3,10,9,5,11,4,15,8,6,7,14,13,0,2,12

Result 5.2.1.

$$\begin{array}{c} 0770070077777770 \\ \downarrow (10R) \\ [7007070070070700] \\ \downarrow (10R) \\ 7777777007700700 \end{array}$$

is a 20 rounds distinguisher for this variant of GOST, where [7007070070070700] is a closed set.

Justification: For a typical permutation on 64-bits (does not have to be a random permutation, it can be GOST with more rounds) we expect that there are $2^{55.1}$ pairs (P_i, P_j) with such differences. The distribution of this number can be approximated by a Gaussian with a standard deviation $2^{27.55}$.

For 18 rounds of GOST and for a given random GOST key, there exists two disjoint sets of $2^{55.1} + 2^{33.0}$ such pairs (P_i, P_j).

None of the $2^{33.0}$ pairs (P_i, P_j) is a member of the $2^{55.1}$ occurring naturally. For any of these cases which occur naturally, we have a non-zero input differential 0770070077777770. By a computer simulation we obtained the probability for a differential of type [7007070070070700] to occur at 10 rounds from the beginning and Similarly to occur 10 rounds from the end. Overall we expect only about $2^{1.47}$ pairs (P_i, P_j) on average will have the propagation characteristic as shown. Therefore the two sets are entirely disjoint with high probability. This gives us an *ADV* of approximately 42.24 standard deviations.

6 CONCLUSIONS

GOST is an important government and industrial block cipher with a 256-bit key which is widely used implemented in standard crypto libraries such as OpenSSL and Crypto++ (GOST, 2005). Until 2010 there was not attacks on GOST when used in encryption such as advanced differential attacks.

The most difficult step involved in all these advanced differential attacks on full GOST is the design of a distinguisher for some 20 Rounds using differentials of special form constructed based on the connections between the S-boxes (Courtois and Misztal, 2011).

In this paper we have for the first time proposed a methodology which allows for efficient discovery of "good" attacks of this type.

In order to achieve this we have introduced a fundamental notion of "*general open sets*", which are special sets consisting of 32-bit strings which are dictated by the structure of GOST. The methodology we provide regarding the construction of reduced-round distinguishers can be seen as a series of advanced combinatorial optimization problems which is obtained by studying the low-level structure of GOST: the S-boxes and the connections between them, then we study how differentials from various open sets can only lead to other very specific open sets with high probability, and then we construct distinguishers for more rounds.

Our methodology is validated by the construction of very good distinguishers for 20 rounds for two variants of GOST; "GostR3411-94-TestParamSet", and "Gost28147-CryptoProParamSetA".

This paper introduces important enhancements and new forms of advanced differential attacks which can be applied to any block cipher in order to improve known attacks such as Knudsen truncated differential attacks and Seki-Kaneko-Misztal-Courtois attacks on GOST and many other.

REFERENCES

A. Poschmann, S. L. and Wang, H. (2010). 256 bit standardized crypto for 650 ge gost revisited. In *In CHES 2010, LNCS 6225, pp. 219-233*.

Biham, E. and Shamir, A. (1990). Differential cryptanalysis of des-like cryptosystems. In *Extended Abstract. In: Crypto'90,Springer-Verlag, 2*.

Biham, E. and Shamir, A. (1992). Differential cryptanalysis of the full 16-round des. In *In: Crypto'92, Springer-Verlag, 487*.

Courtois, N. (2011a). Algebraic complexity reduction and cryptanalysis of gost. In *Cryptology ePrint Archive, Report 2011/626*.

Courtois, N. (2011b). Security evaluation of gost 28147-89 in view of international standardisation. In *In Cryptologia, Volume 36, Issue 1, pp. 2-13, 2012. http://www.tandfonline.com/toc/ucry20/36/1 An earlier version which was ocially sub-mitted to ISO in May 2011 can be found at http://eprint. iacr.org/2011/211/*.

Courtois, N. (2012). An improved differential attack on full gost. In *In Cryptology ePrint Archive, Report 2012/138. 15 March 2012, http://eprint. iacr.org/2012/*.

Courtois, N. and Misztal, M. (2011). First differential attack on full 32-round gost. In *in ICICS'11, pp. 216-227, Springer LNCS 7043*.

Courtois, N. and Misztal, M. (2012). Aggregated differentials and cryptanalysis of pp-1 and gost. In *CECC 2011, 11th Central European Conference on Cryptology. In Periodica Mathematica Hungarica Vol. 65(2), pp. 1126, DOI:10.1007/s10998-012-2983-8, Springer*.

Dolmatov, V. (2010). Rfc 5830: Gost 28147-89 encryption, decryption and mac algorithms. In *IETF. ISSN: 2070-1721*.

GOST (2005). 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/.

I.A. Zabotin, G. G. and Isaeva, V. (1989). Cryptographic protection for information processing systems, government standard of the ussr,gost 28147-89. In *Government Committee of the USSR for Standards*.

Isobe, T. (2011). A single-key attack on the full gost block cipher. In *In FSE 2011, pp. 290-305, Springer LNCS 6733*.

Itai Dinur, O. D. and Shamir, A. Improved attacks on full gost. In *FSE 2012, LNCS 7549, pp. 9-28*.

Knudsen, L. (1994). Truncated and higher order differentials. In *In FSE 1994, pp.196-211, LNCS 1008, Springer*.

Malchik, A. and Diffie, W. (1994). English translation: Cryptographic protection for information processing systems, government standard of the ussr,gost 28147-89. In *http://www.autochthonous.org/ crypto/gosthash.tar.gz*.

Rudskoy, V. and Dmukh, A. (2012). Algebraic and differential cryptanalysis of gost: Fact or fiction. In *In CTCrypt 2012, Workshop on Current Trends in Cryptology, affiliated with 7th International Computer Science Symposium in Russia (CSR-2012), 2 July 2012, Nizhny Novgorod, Russia. Full papers will be submitted and published in a special issue of Russian peer-review journal Mathematical Aspects of Cryptography*.

Saarinen, M. (1998). A chosen key attack against the secret s-boxes of gost. In *Unpublished manuscript*.

Schneier, B. (1996). Section 14.1 gost, in applied cryptography, second edition. In *John Wiley and Sons*.

Seki, H. and T.Kaneko (2000). Differential cryptanalysis of reduced rounds of gost. In *In SAC 2000, LNCS 2012, pp. 315-323, Springer*.

V. Popov, I. K. and Leontie, S. (2006). Rfc 4357: Additional cryptographic algorithms for use with gost 28147-89, gost r 34.10-94,gost r 34.10-2001, and gost r 34.11-94 algorithms. In *http://tools.ietf.org/html/rfc4357*.