Propagation of Truncated Differentials in GOST

Nicolas T. Courtois
University College London,
Gower Street, London, UK
n.courtois@cs.ucl.ac.uk

Theodosis Mourouzis
University College London,
Gower Street, London, UK
theodosis.mourouzis.09@ucl.ac.uk

***Abstract*—GOST 28147-89 is a well-known block cipher with 256-bit keys. Its excessively low implementation cost makes it a plausible alternative for major industrial cryptographic algorithms such as 3-DES and AES-256. In 2010, GOST was submitted to ISO to become a part of the international encryption standard ISO/IEC 18033-3. This stimulated intense research by the cryptographic community and lots of new attacks were developed which reduce its 256-bit security level. These recent attacks against full GOST belong to two main categories: complexity reduction attacks and advanced differential attacks. In differential cryptanalysis, the essential task is the exploration of the exponentially large space of differentials in a systematic way and the construction of complex distinguisher attacks. In this paper, we study the GOST cipher in the well-known theory framework of Markov cipher, which is a basis of many works on differential cryptanalysis. However, we prove that GOST is NOT a Markov cipher though in approximation it still seems to behave like one. We propose a heuristic black-box methodology for efficient discovery of interesting sets of differentials in GOST and we show that results better than any previously known can be obtained with this methodology. However, different sets will be the best possible solutions for various numbers of rounds and more work is needed in order to improve the best known single-key attacks on GOST and adapt them to other sets of S-boxes.**

Keywords*—*differential cryptanalysis, block ciphers, GOST, S-boxes, diffusion, optimization problems, truncated differentials, aggregated differentials

I. INTRODUCTION

GOST 28147-89 encryption algorithm is the state standard of Russian Federation and it is widely used for encrypting confidential documents. It is implemented in many crypto libraries such as OpenSSL and Crypto++ [15], [19] and is one of the Internet data security standards. In 1989, it was standardized and became an official standard for protection of confidential information. The specification of the cipher was kept secret until 1994 when it was declassified and published [24]. The first international translation was done in 1994 by Malchik and Diffie [18].

Until 2010, most researchers would agree that despite considerable cryptanalytic efforts spent in the past 20 years, GOST is still not broken. The very large 256-bit security level of GOST and its excessively competitive low implementation cost made it a plausible alternative to all major standard cryptographic algorithms such as 3-DES or AES [19]. 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 general, all these attacks fall in two main categories: differential attacks [7], [11], [12], [13] and complexity reduction attacks [6], [10], [14], where an attacker reduces the problem of attacking the full GOST to a simpler problem of attacking a smaller number of rounds. We have reflection attacks, attacks with double reflections, self-similarity attacks and advanced differential attacks and combinations of these attacks. The main aim of a differential attack is to distinguish a certain number of rounds of GOST from a random permutation on 64 bits and then some key bits can be recovered by following some extra steps. The construction of such distinguishers can be seen as a series of optimization problems which need to be solved for each variant of GOST. Additionally, the exponentially large space of differentials makes the systematic search computationally infeasible and thus some hidden combinatorial structure of the cipher needs to be explored. Courtois and Misztal developed an advanced differential attack with complexity which was later improved to 2^{179} against the full 32-round 256-bit GOST. This attack is based on constructing distinguishers for 20 rounds and by solving a series of combinatorial optimization problems [7], [12].

This paper is structured as follows. In Section II we briefly describe the specifications of the GOST block cipher and its variants. In Section III we study GOST with respect to the well-known notion of Markov cipher. Informally, a Markov cipher is a cipher where the probability of a propagation of a specific difference does not depend on the input plaintexts and does depend only on the XOR of the plaintexts. We prove that GOST is NOT a Markov cipher and try to see how much this cipher deviates from this ideal cipher notion. Early results suggest that it still behaves as a Markov cipher from the practical point of view.

In Section IV, we define a form of set differential cryptanalysis on GOST cipher by introducing some special sets constructed based on the internal connections between S-boxes from round to round.

Finally in Section V, we describe a heuristic methodology for finding sets of differentials whose propagation deviates from what expected in case of a random permutation on 64-bits. Such sets of differentials can later be used to build distinguishers for a larger number of rounds, cf. [7], [9]. More importantly we provide a precise analysis, important insights and theory, on the propagation of interesting differentials in GOST, both from the point of view of advanced differential attacks and combined differential-algebraic attack approaches. This can be exploited further for developing many advanced differential attacks against full cipher and for improving numerous already known attacks in these two families [10].

Copyright (c) IARIA, 2013.   ISBN: 978-1-61208-298-1

II. 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, as shown in *Figure* 1.

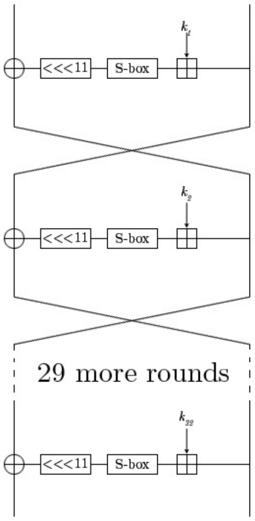

Fig. 1. Diagram of GOST cipher, 32-rounds of a Feistel network to encrypt a 64-bit plaintext using a 256-bit key

Each round of GOST contains and combines a series of logical and arithmetic operations as shown in *Figure* 2. Initially, we have a key addition modulo 2^{32}, then we have a substitution function which consists of 8 different 4-bit to 4-bit S-boxes and the output is then rotated by 11 positions to the left.

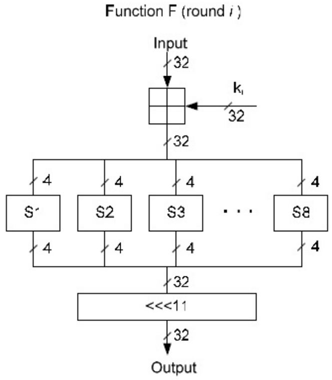

Fig. 2. Detailed description of the round function F_I used in GOST

Thus the image of any input $P = L||R$ after a single round of GOST, where L, R the left and right 32-bit halves respectively, is given by

$$(L, R) \rightarrow (R, L \oplus F_i(R)) \tag{1}$$

GOST block cipher consists of three main components; the key schedule, the S-boxes and the internal connections between them. We briefly discuss them in the next subsections.

A. Key Schedule

The 256-bits of key K are divided into eight consecutive 32-bit words $k_0, k_1, .., k_7$. 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* I.

TABLE I. 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
$k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7$	$k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0$

Its very simple key schedule makes it suitable for cryptanalysis.

B. S-boxes

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. Thus, the effective key size is increased to 610 by the addition of this extra $354 * (log_2(16!^8))$ bits of information. However, this information can be recovered in approximately 2^{32} encryptions by a chosen-key attack [21].

C. Internal Connections

Let S_i for $i = 1, 2, ..., 8$ be the i-th S-box used in each round as shown in *Figure* 3. Then we can number the inputs of the S-box S_i by integers from $4i+1$ to $4i+4$ out of $1, .., 32$ and its outputs are numbered according to their final positions after the rotation by 11 positions.

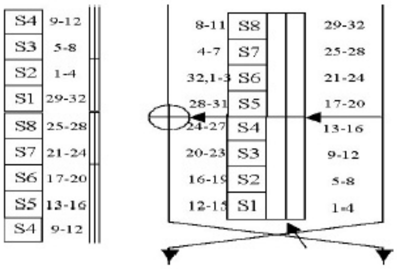

Fig. 3. The connections between different S-boxes from round to round inside GOST

For example the inputs of $S6$ are 20,21,22,23 and the outputs are 32,1,2,3. Such connections are of major cryptanalytic importance as they describe how these S-boxes interact within the general structure of the cipher.

III. Markov Cipher

The concept of Markov block cipher is a very important theory concept in the development and study of differential and linear cryptanalysis [1], [16], [17].

Informally, in a Markov block cipher the average difference propagation probability over each round is independent of the rounds's text input. There are numerous examples of Markov cipher including DES, Rijndael, Camelia and many others.

In spite of the progress in mathematical foundations of differential and linear cryptanalysis, there are still difficulties in analyzing and obtaining security proofs for non-Markov cipher, like GOST due to lack of adequate mathematical methods accounting for the structure and irregular properties of non-Markov cipher.

Definition 1: An iterated cipher round function $Y = f(X, Z)$ is a Markov cipher if there is a group operation $\otimes$ for defining differences such that, for all choices of α ($\alpha \neq e$) and ($\beta \neq e$), $P(\Delta Y = \beta | \Delta X = \alpha, X = \gamma)$ is independent of γ when the subkey Z is uniformly random.

If an iterated cipher is Markov and its round subkeys are independent then the sequence of differences at each round output forms a Markov chain.

Definition 2: We say that X may cause Y with probability p by the function F if for a fraction p of all the possible input pairs encrypted by all the possible subkeys values in which the input XOR of the F equals to X, the output XOR equals Y. If $p > 0$ we denote this by $X \rightarrow Y$.

In the rest of this section we will study GOST with respect to its Markov and non-Markov properties. We consider differences with respect to the bitwise XOR operation.

Let $X^{(i)} = L^{(i)} || R^{(i)}$ for $i = 1, 2$ be two distinct plaintexts.

Then the round function G maps $X^{(i)}$ to

$Y^{(i)} = R^{(i)} || (L^{(i)} \oplus ROT^{11} S(L^{(i)} \boxplus R^{(i)}))$

Xoring the two outputs we have

$\Delta Y = Y^{(1)} \oplus Y^{(2)}$

$= (R^{(1)} \oplus R^{(2)}) ||$

$(L^{(1)} \oplus L^{(2)} \oplus ROT^{11}(S(K \boxplus R^{(1)}) \oplus S(K \boxplus R^{(2)})))$

$= (\Delta Y^R) ||$

$(\Delta Y^L \oplus ROT^{11}(S(K \boxplus R^{(1)}) \oplus S(K \boxplus R^{(2)})))$

As we prove below GOST is not a Markov cipher but it can be a Markov cipher if the modular 2^{32} addition $\boxplus$ is replaced by the bitwise XOR operation $\oplus$.

Theorem 1: GOST is a Markov cipher if the modular 2^{32} addition $\boxplus$ is replaced by the bitwise XOR operation $\oplus$

Proof: To prove this lemma it is suffices to prove the property for each of the S-boxes.

For each input XOR $S'_E = S_E \oplus {S^*}_E$ there exist $S'_I = S'_E$ regardless of the key since $(S_E \oplus K) \oplus (({S^*}_E \oplus K))$ is independent of key.

Suppose that there exist exactly k pairs $\{(S_I^i, {S^*}_I^i)\}_{1 \leq i \leq k}$ to the S-boxes such that $S_E \oplus {S^*}_E = X$ and the output XOR is Y, cf. 4

Fix a pair input $(P_E, {P^*}_E)$ such that $P_E \oplus {P^*}_E = X$. There exists unique K for each i such that $P_E \oplus K = S_I^i$ which forces ${P^*}_E \oplus K = {S^*}_I^i$. However, $X = P_E \oplus {P^*}_E = (S_I^i \oplus K) \oplus ({S^*}_I^i \oplus K) = S_I^i \oplus {S^*}_I^i$ is not affected by key addition and comes for free.

Thus we have that the XOR output will be Y for a fix pair of inputs for exactly k keys and thus this version of GOST with XOR bitwise operation instead of modular addition is a Markov cipher.

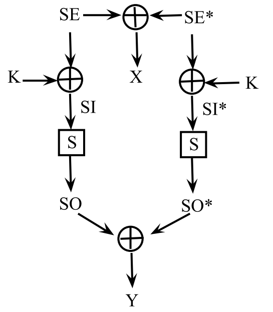

Fig. 4. The output given two input pairs for modified GOST

Theorem 2: GOST is **NOT** a Markov cipher

Proof: Suppose that there exist exactly k pairs $\{(S_I^i, {S^*}_I^i)\}_{1 \leq i \leq k}$ to the S-boxes such that $S_E \oplus {S^*}_E = X$ and the output XOR is Y, cf. 5.

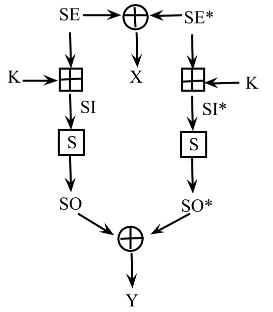

Fig. 5. The output given two input pairs for actual GOST

We follow the same methodology as before and we fix a pair input $(P_E, {P^*}_E)$ such that $P_E \oplus {P^*}_E = X$. Let l be the number of keys that follow the input and output difference property.

There exists unique K for each i such that $P_E \boxplus K = S_I^i$. However, now ${P^*}_E \boxplus K = {S^*}_I^i$ is not ensured by the same value of K as in general $(\alpha \oplus \beta) \boxplus \gamma \neq \alpha \oplus (\beta \boxplus \gamma)$.

We have $l = m$ is not always true and thus GOST is **NOT** a Markov cipher.

Remark - Another Proof: There is another way to disprove this result, it is by concrete analysis of concrete attacks. We sketch one such proof by conter-example on a very specific example which is dictated by our pragmatic cryptanalysis work. We have computed by simulation the probability $P(\Delta Y \in 0x8070070080700700 | \Delta Y \in 8070070080700700)$ over randomly selected keys and plaintexts and it is approximately equal to $2^{-3.73}$. Additionally, we computed some probabilities $P(\Delta Y \in 0x8070070080700700 | \Delta Y \in 8070070080700700, X = X_0)$ for fixed plaintext X_0 and we observed that they are not equal to $2^{-3.73}$ proving also experimentally that GOST is not a Markov cipher. For example for $X_0 = 0x000031A90F4A3312$ the probability equals to $2^{-3.61}$ and for $X_0 = 0x0000001000000010$ equals to $2^{-3.89}$. However, the difference between these probabilities is approximately equal to $|2^{-3.61} - 2^{-3.89}| \simeq 0.014$ which shows that GOST still is a somehow Markov cipher with a margin of error which is only about 10 $\%$. Moreover, we know from our Theorem 1 and 2 that this is due to the presence of the modular addition mod 2^{32}. Overall, we still conjecture that techniques applied to normal Markov cipher can be applied to GOST and lead to approximate but essentially valid cryptographic results.

IV. Advanced Differential Cryptanalysis

Differential cryptanalysis (DC) is one of the oldest known attacks on block ciphers. Biham and Shamir were the first to describe this method and applied it to DES algorithm, see [3], [4]. DC is based on tracking of changes in the differences between two messages as they pass through the consecutive rounds of encryption.

We apply an advanced form of differential cryptanalysis to GOST. We consider differences with respect to the bitwise XOR operation (and we still do apply them to the standard GOST cipher which also uses modular additions). 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.

We need to experimentally determine the probabilities of these transitions from A to B for different number of rounds. This is achieved by carrying out lots of simulations and aggregating the results obtained in each simulation until the probability value converges to its actual value. According to the 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 reasonable precision. As the number of trials is increased, it is going to become closer to the expected value and the deviation can be predicted according to the Gauss Error Function.

We consider the following differential set: $\Delta = 0x80700700$ 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 (Δ, Δ) 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 for the version of GOST which uses GostR3411-94-TestParamSet set of S-boxes:

Experimental Facts: The aggregated differential (Δ, Δ) with uniform sampling of all differences it allows, produces an element of the same aggregated differential set (Δ, Δ) after:

1) 1 round of GOST with probability $P_1 = 2^{-3.73}$ on average over all possible keys
2) 4 rounds of GOST with probability $P_4 = 2^{-13.6}$ on average over all possible keys
3) 8 rounds of GOST with probability $P_8 = 2^{-25.0}$ on average over all possible keys

We partition the space of differences (Δ, Δ) into 63 disjoint classes. All these sets of differentials are constructed based on the connections between the S-boxes so they need to be re-invented for each new variant of GOST. In the next chapter, we explain our heuristic methodology for finding such differentials.

V. Direct Black-Box Discovery Method for Truncated Differential Attacks on GOST

In classical differential cryptanalysis, such as Biham-Shamir attacks on DES, [3], [4], the process of discovery of best differential attacks is rather straightforward. In advanced differential attacks however, the potential number of different sets of differences which could be mapped to other arbitrary differences makes systematic exploration impossible. Some heuristics are needed which basically group together similar differentials into sets of differentials of certain type, cf. [9].

In our work, we are basically looking for differential sets which are very similar to those already known from [11], [12], [22]. However, we do not want to follow the heuristics from [7] such as looking at "loops" of S-boxes which are connected to each other, because we believe that better attacks exist which do not exhibit this sort of regular structure. Ultimately what matters are the best differential properties we can find.

Our heuristic pseudo-code for finding new interesting attacks on GOST is as follows:

1) We select at random set of say 14 bits. This seems to be about right size, previous attacks have used sets of 14-24 bits [7], [11], [22].
2) We work in black-box way for a fixed number of rounds for example between 4 and 8.
3) For each set we run a simulation of whether flipping some random difference within the set of 14 active bits results in output difference in which the bits which differ are also a subset of these 14 bits.
   In other words we are studying an invariant truncated differential property for e.g. 8 rounds of GOST.
4) We use a variant of method called method of "Structures" by Biham and Shamir [3]. More precisely we fix the 64-14 bits and consider a fraction but not all possible plaintexts with such fixed 64-14 bits, and look at how many ciphertext also share the same 64-14 bits. This method gives a quadratic speedup: the number of pairs with suitable difference we see here is the square of the number of actual encryptions which we need to carry.
5) Thus we can measure the probability with sufficient precision to see which sets are within heuristically 2^{-5} form the best know set of 14 bits.
6) We keep a database of 100 best sets of 14 bits at any moment. The sets are ranked based on the observed propagation probability.
7) During the attack we mix fully random sets of 14 bits with sets obtained by flipping up to 4 bits in the 100 already found sets.
8) In this way we progressively update our set of 100 best results.
9) At the end we stop and run a much longer simulation to see which out of 100 is really the best, because at no moment during the above discovery process we know these probabilities with sufficient precision.

For the time being we have obtained the following quite remarkable and surprising results.

TABLE II. SOME SETS OF 14 BITS WITH PROPAGATION BELOW 2^{-25} FOR 8 ROUNDS

Set Name	Set	P(8R)
GostR3411_94_Test	78000078 07070780	$2^{-24.0}$
GostR3411_94_CryptoPro	00030780 703A0010	$2^{-22.8}$
Gost28147_Test	60707800 00000507	$2^{-22.2}$
Gost28147_CryptoPro A	70780000 80030780	$2^{-23.8}$
Gost28147_CryptoPro B	C0707000 00000707	$2^{-23.0}$
Gost28147_CryptoPro C	03070780 78000010	$2^{-25.3}$
Gost28147_CryptoPro D	70707000 80000207	$2^{-25.0}$
GostR3411_94_Sberbank	80080207 80707800	$2^{-22.4}$
ISO 18033-3 proposal	80000707 20707000	$2^{-22.7}$
GOST-P proposal	50703800 00000707	$2^{-25.2}$

A. *Early Results With Our Simple Algorithm*

First of all, it is possible to see that on the strict basis of results for 8 rounds, one can find better results than currently known not only for the default sets of S-boxes, but for absolutely every other known set of S-boxes. Our results are shown in Table II.

This is quite remarkable because it shows that other sets of S-boxes are maybe not stronger. Unhappily, the best results for 8 rounds are not necessarily the best results for other numbers of rounds. We give one detailed below. The aggregated differential $(0x78000078, 0x07070780)$ with uniform sampling of all input differences, produces an element of the same aggregated differential set with 4 or 8 rounds with the following probabilities on average over all possible keys:

1) For 4 rounds of GOST with probability $P_4 = 2^{-13.8}$. This is NOT as good as $P_4 = 2^{-13.6}$ for the previous set (Δ, Δ), however for 8 rounds it will be otherwise.
2) After 8 rounds of GOST we obtain probability $P_8 = 2^{-24.0}$ on average over all possible keys which is strictly better than $P_8 = 2^{-25.0}$ for the previous set (Δ, Δ).
3) This however does NOT mean that it will be better for 10 rounds. In fact for 10 rounds we obtain less than 2^{-35} which is not as good as $P_{10} = 2^{-31.0}$ with the previous set (Δ, Δ). see [12].

We see that discovery of interesting iterative invariant attacks on 8 rounds of GOST cannot rely on heuristic combination of 8=4+4 rounds, and that our new result is not very good for 4 rounds yet now becomes the best ever found for 8 rounds which however does NOT guarantee it is the best for 10 rounds. This justifies our black-box methodology but also shows that it is difficult to find a solution which works for various numbers of rounds.

B. *Propagation of New Sets*

It is interesting to see if for new sets we can observe the same sort of behavior as before, which amounts to saying that few paths in a certain transition graph dominate the whole attack for many rounds, which will be the best currently known attack. For the new property we have made the following observations which show that in many aspects the new attacks are similar to the old ones yet more irregular. Moreover, the entropy of states deeply inside the cipher is quite low. This suggests that in all cases design further advanced combined attacks such as differential-algebraic attacks [2] or attacks with simultaneous differentials cf. [8]. Below we show what we call the "dominating path" in the transition graph for our new discovery set of 14 bits which shows that special cases may happen quite frequently.

$$0R : 7000007007070000$$
$$1R : 0707000000000070$$
$$2R : 0000007007000000$$
$$3R : 0700000000000000$$
$$4R : 0000000007000000$$
$$5R : 0700000000000070$$
$$6R : 0000007007070000$$
$$7R : 0707000070000000$$
$$8R : 7000000007070780$$

In one propagation for 8 rounds (and similarly for any number of rounds) we have observed that the specification of input and output sets being $(0x78000078, 0x07070780)$ as above, with uniform sampling of all input differences, we have observed that for about 2^{-2} of the time, the above sets of differential sets are simultaneously satisfied at every round. Moreover, only few such paths amount for a majority of all events which are observed.

VI. CONCLUSION

GOST is an important government and industrial block cipher which is widely used and implemented in standard crypto libraries such as OpenSSL, Crypto++ and also in RSA Security products. GOST is a 32-round Feistel cipher with 64-bit blocks and 256-bit key. Until 2010, there were no serious attacks on full GOST which may threaten its 256-bit level security and thus it was submitted to ISO for standardization. This stimulated the cryptographic community to carry out a more extensive security analysis of GOST and as a result of this many new attacks were developed.

Most differential attacks of GOST are based on the construction of a distinguisher for a reduced version of GOST from a random permutation on 64-bits. This is combined with many additional complex technical steps to recover the full key. However, the construction of the initial distinguisher is difficult to achieve. It is based on the exploration of the exponentially large space of differentials for finding interesting patterns which propagate for a large number of rounds, and on combinations of such properties, see also [9].

In this paper, we study the fundamental question of how such differential attacks propagate inside the cipher. This question is fundamental both in order to enable efficient heuristic discovery of similar attacks, and in order to improve existing distinguisher attacks by more precise statistical analysis or by combination [9]. In order to study this question, one first needs to answer the question whether GOST is a Markov cipher. This question is about whether (at least on average over the keys) the differential transitions can be seen as events which are independent on the input value, and happen with more or less stable probabilities. We have answered this question by negative: we prove mathematically that GOST is NOT a Markov cipher. However, from the practical point what matters is how much these probabilities will vary, and not for individual differentials, but really for the most interesting sets of differentials such as used in the best known differential attacks on GOST [7]. To this more pragmatic question our current answer is positive: it seems that GOST behaves like a Markov cipher in practice with deviations of about 10 % which question however deserves a further study.

The next important question is can we find better attacks on GOST? In this respect, in this paper we have not followed some regularly shaped sets from previous papers and we have introduced a new simple heuristic methodology for finding differentials of more irregular shape efficiently. We have applied this methodology to the main historical version of GOST and have found properties which are substantially stronger than in previous works, event though it remains very difficult to find differential sets which work equally well for various numbers or rounds, as a result of which we claim that almost certainly one can improve the best currently known single key attack on GOST in 2^{179} from [7] though the exact further adaptation of the attack to any new set requires a lot of attention to detail, see [7], [9]. However, we are now able to improve the central property which allows to construct such attacks. More such results will appear in the extended version of this paper.

Moreover, we have discovered that the internal propagation inside GOST cipher for properties we studied is quite remarkable. All cases we have studied in details lead to quite strong events inside the cipher which basically amounts to paths in a graph with very few dominant paths accounting for a larger proportion of all interesting events. This leads to surprisingly low entropy of differences inside the cipher which fact is already explicitly exploited in several differential-complexity reduction-algebraic attacks in [10] and is expected to lead to many interesting advanced differential-algebraic [2] and simultaneous differential attacks [8]. This sort of low entropy facts are already exploited in several attacks on GOST in [10].

REFERENCES

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

[2] Martin R. Albrecht, Carlos Cid: *Algebraic Techniques in Differential Cryptanalysis*, In FSE 2009, LNCS, pp.193-208, Springer, 2009.

[3] E. Biham and A. Shamir: *Differential Cryptanalysis of the Full 16-round DES* In: Crypto'92, Springer-Verlag, 487, 1992.

[4] E. Biham and A. Shamir: *Differential Cryptanalysis of DES-like Cryptosystems* Extended Abstract. In: Crypto'90,Springer-Verlag, 2., 1990.

[5] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann and M.J.B. Robshaw: *PRESENT: An Ultra-Lightweight Block Cipher* CHES 2007, LNCS 4727, pp. 450466, Springer, 2007.

[6] N.T. Courtois: *Security Evaluation of GOST 28147-89 In View Of International Standardisation.* In Cryptologia, Volume 36, Issue 1, pp. 2-13, 2012.

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

[8] Nicolas T. Courtois: *T*he Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime, In SECRYPT 2009 International Conference on Security and Cryptography: pp. 331-338. INSTICC Press 2009.

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

[10] N.T. Courtois: *Algebraic Complexity Reduction and Cryptanalysis of GOST.* In Cryptology ePrint Archive, Report 2011/626, 2011.

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

[12] N.T. Courtois and M. Misztal: *First Differential Attack On Full 32-Round GOST.* In ICICS'11, pp. 216-227, Springer LNCS 7043, 2011.

[13] N.T. Courtois and M. Misztal: *Differential Cryptanalysis of GOST.* In Cryptology ePrint Archive, Report 2011/312, 2011.

[14] I. Dinur, O. Dunkelman and A. Shamir:*Improved Attacks on Full GOST.* FSE 2012, LNCS 7549, pp. 9-28, 2012.

[15] GOST: *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/.* , 2005.

[16] L.R. Knudsen: Block Ciphers The Basics, Spring 2011, https://www.cosic.esat.kuleuven.be/ecrypt/courses/albena11/slides/LRK-basics.pdf.

[17] X. Lai and J. Massey:*Markov Ciphers and Differential Cryptanalysis.* In Eurocrypt'91, LNCS 547, Springer-Verlag, pp.17-38, 1991.

[18] A. Malchik and W. Diffie:*English Translation,Cryptographic Protection for Information Processing Systems, Government Standard of the USSR,GOST 28147-89.* autochthonous.org/crypto/gosthash.tar.gz, 1994.

[19] A. Poschmann, S. Ling and H. Wang: *256 Bit Standardized Crypto for 650 GE GOST Revisited.* In CHES 2010, LNCS 6225, pp. 219-233, 2010.

[20] V. Rudskoy and A. Chmora: *Working draft for ISO/IEC 1st wd of amd1/18033-3.* In Russian Block Cipher GOST, ISO/IEC JTC 1/SC 27 N9423, MD5=feb236fe6d3a79a02ad666edfe7039aa , 2011.

[21] M. J. Saarinen: *A chosen key attack against the secret S-boxes of GOST.* Unpublished manuscript, 1998.

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

[23] B. Schneier: *Applied Cryptography.* Section 14.1 GOST, 2nd Edition, In John Wiley and Sons,1996.

[24] I.A. Zabotin, G.P. Glazkov and V.B. Isaeva: *Cryptographic Protection for Information Processing Systems, Government Standard of the USSR,GOST 28147-89.* Government Committee of the USSR for Standards, 1989.