Periodica Mathematica Hungarica Vol. 65 (2), 2012, pp. 177–192
DOI: 10.1007/s10998-012-2983-8

AGGREGATED DIFFERENTIALS AND CRYPTANALYSIS OF PP-1 AND GOST

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

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

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

(*Received September 29, 2011; Accepted February 13, 2012*)

Abstract

In this paper we look at the security of two block ciphers which were both claimed in the published literature to be secure against differential cryptanalysis (DC). However, a more careful examination shows that none of these ciphers is very secure against... differential cryptanalysis, in particular if we consider attacks with sets of differentials. For both these ciphers we report new perfectly periodic (iterative) aggregated differential attacks which propagate with quite high probabilities.

The first cipher we look at is GOST, a well-known Russian government encryption standard. The second cipher we look at is PP-1, a very recent Polish block cipher. Both ciphers were designed to withstand linear and differential cryptanalysis. Unhappily, both ciphers are shown to be much weaker than expected against advanced differential attacks. For GOST, we report better and stronger sets of differentials than the best currently known attacks presented at SAC 2000 [32] and propose the first attack ever able to distinguish 16 rounds of GOST from random permutation. For PP-1 we show that in spite of the fact, that its S-box has an optimal theoretical security level against differential cryptanalysis [17], [29], our differentials are strong enough to allow to break all the known versions of the PP-1 cipher.

1. Introduction to GOST

GOST 28147-89 is a well-known block cipher and the official encryption standard of the Russian Federation. Its large key size of 256 bits make GOST a plausible

Mathematics subject classification numbers: 94A60, 11T71, 68P25.

Key words and phrases: Block ciphers, GOST, DES, PP-1, S-box design, differential cryptanalysis, sets of differentials, iterative differentials.

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).

0031-5303/2012/$20.00 *Akadémiai Kiadó, Budapest*

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 designed with most serious applications in mind. In addition GOST has a much lower implementation cost than AES or any other comparable encryption algorithm, see [27]. GOST is implemented in standard crypto libraries such as OpenSSL and Crypto++ [26], [18].

Different sets of S-boxes exist for GOST. One set of S-boxes has been published in 1994 as a part of the Russian standard hash function specification GOST R 34.11-94 and according to Schneier [33] 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, it is commonly called just "the GOST cipher" in the cryptographic literature. 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 [26]. Other (secret) S-boxes could be recovered from a chip or implementation, see [31], [20].

2. Introduction to PP-1

The PP-1 cipher was designed at the Poznan University of Technology in Poland (the name derives from the Poznan Polytechnic university) in 2007 [7], [8]. The first version of PP-1 has block length of 64 bits, then also a version with scalable block length which is a multiple of 64 bits was developed. It is not a Feistel cipher but an SPN (substitution-permutation network). The key length to be used in the cipher is equal to length of block or can be twice longer [8]. The PP-1 cipher was clearly designed to withstand linear and differential cryptanalysis (!) and was implemented on various platforms, including side channel protections [8]. The S-box of PP-1 was chosen to have an optimal possible theoretical security level against differential cryptanalysis, see [17], [29]. Yet we will be able to totally break the full 11-round 64-bit version of PP-1 cipher.

Note: A special feature of the cipher is, according to the authors, that it is an involutional SPN, each round is an involution. However the key scheduling prevents the whole cipher from being an involution. This idea of building an involutional cipher has obviously affected the design of PP-1, because it is much harder to design a cipher which has such special and strong properties, and yet to be efficient and secure.

3. GOST and its security

3.1. Short description of 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 need to take into account not only the S-boxes, like in DES, but also the key addition modulo 2^{32}, which implies that their probabilities depend on the key. This is a major difficulty in differential cryptanalysis of GOST. In this paper we summarize the state of the art and report one very significative new result. 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.

3.2. Linear and differential cryptanalysis of GOST

In the well-known Schneier textbook we read: "Against differential and linear cryptanalysis, GOST is probably stronger than DES", see [33]. A basic assessment of the security of GOST against linear and differential cryptanalysis has been conducted in 2000 by Gabidulin et al., see [36], [35]. The results are quite impressive: at the prescribed security level of 2^{256}, 5 rounds are sufficient to protect GOST against linear cryptanalysis. 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 linear cryptanalysis after 6 rounds out of 32. Differential cryptanalysis of GOST seems comparatively easier and has attracted more attention. Moreover, differential cryptanalysis is a much more "practical" attack than linear cryptanalysis: it does not require an astronomical quantity of data to be collected for one single key, which will never occur in practice because nobody encrypts such quantities of data. Differential cryptanalysis works also in a scenario where many different keys are used by different people. It will then allow to break one of these keys. In [35] the authors also estimate that, but here only w.r.t. the security level of about 2^{128}, 7 rounds should be sufficient to protect GOST against differential cryptanalysis. The authors also claim that "breaking the GOST with five or more rounds is very hard". Moreover, Seki and Kaneko [32] show that the straightforward classical differential attack with one single differential characteristic is unlikely to work *at all* for a large 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. [32]), 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 if would propagate with a probability not better than 2^{-360}).

In the same paper [32], more advanced differential attacks on GOST are described. They exploit sets of differentials which follow certain patterns, for example certain S-boxes have zero differentials, other bits have non-zero differentials. These are essentially distinguisher attacks on the weak diffusion of GOST and they differ considerably from the classical differential cryptanalysis: sets of differentials occur naturally with higher probability, and when they occur they give much less exploitable information about the secret keys. The best advanced multiple differential

attack proposed in [32] allows to break between 12 and 17 rounds of GOST depending on the key, some keys being weaker. It is not clear at all, 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 the attack become very hard to distinguish from differences which occur naturally at random.

3.3. How secure is GOST?

There are great many papers about GOST. We only mention the many papers on weak keys in GOST [21], [3], attacks for some well-chosen number of rounds [21], [32], attacks with modular additions removed [3], related-key attacks [22], [19], [30], reverse engineering attacks on S-boxes [31], [20], and at Crypto 2008 the hash function based on this cipher was broken [24]. In all these attacks the attacker has much more freedom than we would allow ourselves.

As far as traditional encryption applications with random keys are concerned, no cryptographically significant attack on this algorithm 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 [27].

4. Aggregated differential attacks on block ciphers

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 Seki and Kaneko's work on GOST exactly the same sorts of differentials are exploited for GOST, see [32]. They 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 Cartesian direct product of two sets $A \times B$.

These types of differentials are also called "almost iterative differentials" in [1], however the word "almost" can be seen as misleading; this is because, as we will see below, for both GOST and PP-1 ciphers, we can have "perfectly" iterative differentials which are perfectly periodic, and can propagate for an arbitrary number of rounds from set A to the same set A.

In addition many but not all of interesting sets of differentials we study are of the following form: some difference bits can be active, some other bits are always inactive. Such sets can also be seen as "truncated differentials" in the sense of [23].

5. Multiple differential attacks on GOST

5.1. Previous results by Saki and Kaneko

This type of differential attack on GOST was introduced in 2000 [32] under the name of "sets of differential characteristics". They exploit sets of differentials, which in addition follow certain patterns, for example certain S-boxes have zero differentials, other bits have non-zero differentials. Such sets of differentials do work extremely well while ordinary DC, as explained in Section 3.2, fails for GOST.

They work for more or less all possible keys, or with a high probability. They work for various S-boxes, and also when S-boxes are chosen at random, see [32]. Moreover, it is easy to see that they will also propagate well and can be detected when the S-boxes are kept secret.

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, will propagate for one round with a probability of about $2^{-5.3}$ and for any key chosen at random. In fact the result is slightly different for even and odd rounds and for specific fixed keys this probability will differ substantially.

Here what we report will already start to differ from the combination of theoretical probabilities given in [32]. 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, with the difference in our experience being almost always helpful for the attacker: better attacks than expected are almost always obtained.

This differential set 0x70707070,0x07070707, described above and in [32], would propagate with a probability of about only 2^{-160} over 32 rounds, (though actually it is better in practice due to propagation through additional differential paths, as we will see below). This is not very good: there are only 2^{64+24} possible differences for a block size of 64-bits. Moreover, a differential of type $0x70707070, 0x07070707$ occurs naturally with probability about 2^{-40}. There will be a lot of false positives in any potential attack using this differential. As far as we know it is not clear how to deal with false positives, and it is generally stated that this type of attacks will not work after a certain number of rounds have been reached, as in [32].

5.2. From distinguishers to key recovery

We should note however that this is only a distinguisher attack, and it is not obvious at all how to use this kind of set of characteristics in key recovery attacks. One method is proposed in [32] and supposes that a specific differential with less

of the "variability", and which is therefore easier to exploit, occurs later in the process. However, we ignore this question for now. The authors of [32] describe a more complex and more detailed attack, and for 12-17 rounds of GOST, this depending on the key, some keys being weaker, they obtain a ratio between false positives and differentials coming from their attack, being bigger than 1. At this moment the attack as described stops working (or rather the authors decided to give up on it).

In this paper we study some different, and arguably better sets of differentials, which propagate with higher probabilities, and where the false positives occur with lower probabilities. In the present version of this paper we still ignore the (very complex) question of key recovery. One needs to connect our "aggregated" sets of differentials with ordinary differentials in the first few, and in the last few rounds. We leave this question for further research. For now it is still NOT known what are the best aggregated differentials for GOST, as the examples we present are clearly better than any previously published, but we believe that further exploration with our software will allow us to find many other interesting aggregated differentials for GOST. Then the question of an optimal key recovery attack will be able to be asked.

5.3. 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. We expect that differentials which are better still will be found very soon.

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:

FACT 1. *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* 4 *rounds of GOST with probability about* $2^{-13.6}$ *on average over all possible keys.*

This probability is an average and it depends on the key, for example if all key bits are equal to 0, this probability is different and is equal to $2^{-13.2}$.

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

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

REMARK 1. Again, for some keys it will be smaller or bigger. For example, if all key bits are equal to 0, a computer simulation gives the probability of $2^{-22.8}$. It appears also that the approximation gives similar results for most keys and we found no keys for which the probability would be significantly worse than $2^{-25.0}$.

REMARK 2. The same kind of improvement, very hard to analyse by theory, but quite substantial and easily visible in practice, also exits for attacks from [32], see Figure 1.

5.4. Propagation for 16 rounds

FACT 3. *The aggregated differential* (Δ, Δ) *produces the same aggregated differential* (Δ, Δ) *after* 16 *rounds of GOST with probability about* 2^{-48} *on average over all possible keys.*

Justification: Here is how this is estimated. In theory if we just compose 2 pieces of 8 rounds, we get 2^{-50}. However, the difference observed between Fact 1 and Fact 2 is an improvement by a factor of $2^{+2.2}$ when the two pieces of GOST are joined together and a number of additional highly probable differentials can occur at the junction. Here the junction is done again, and very roughly we expect that the propagation probability will be about

$$2^{-25+2.2-25} \approx -2^{-48}.$$

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

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

FACT 4. *The* 64*-bit output difference being a member of our set* (Δ, Δ) *occurs naturally with probability about* 2^{-50}.

5.5. Comparison to previous best characteristics applied for 16 rounds

We need to compare our result with the results of Seki and Kaneko [32]. If we apply the probabilities found in [32], 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. Saki and Kaneko do not mention that *all* their current attacks do naturally improve for a

larger number of rounds, due to additional differential paths, and their complexities will be in fact significantly lower than reported in [32].

Similarly, the theory (according to [32]) says that this aggregated differential 0x70707070,0x07070707 will propagate for 16 rounds with a probability of about $2^{-85.3}$. However, by decomposing it as 8+8 rounds we clearly see that it will be at most about 2^{-56} in practice. Unhappily, a differential of type 0x70707070,0x07070707 occurs naturally with probability about 2^{-40}. Here we are not able to distinguish 16 rounds from a random permutation.

Our aggregated differential (Δ, Δ) with $\Delta = 0x80700700$ occurs with a better probability of about 2^{-48} while it 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.

Remark. We can expect that another, better differential distinguisher attack on 16 rounds could also be achieved with methods of [32] by connecting this differential to other differentials at the beginning and at the end, however our attack can also be improved in a similar way. The difference is significant enough to make us believe that more complex attacks derived from our new aggregated characteristics will almost always be better than those derived from the old one.

Aggregated Differential Set	0x70707070,0x07070707	0x80700700,0x80700700
Reference	Seki-Kaneko [32]	this paper
Propagation 2 R	$2^{-8.6}$	$2^{-7.5}$
Propagation 4 R	$2^{-16.7}$	$2^{-13.6}$
Propagation 8 R	$2^{-28.4}$	$2^{-25.0}$
Propagation 16 R	$\geq 2^{-56}$	$\approx 2^{-48}$
Output Δ Occurs Naturally	$2^{-40.0}$	$2^{-50.0}$

Figure 1. *Our new result compared to the best previous result*

6. Short description of PP-1

PP-1 is an SPN (substitution-permutation network). The block length is 64 bits, and there is also a scalable version where the block length is a multiple of 64 bits. The key length is specified to be equal to the block length or twice longer [8]. In this paper we will assume that the key length is equal to the block length. For longer keys our attacks work all the same and will have even much lower complexity compared to the exhaustive search.

The encryption by PP-1 is done through the succession of two layers: the non-linear layer, and the linear layer. The non-linear layer takes a 64-bit input, two

64-bit partial keys, and produces an output on 64 bits. For any given key it is a permutation and an involution. It is depicted in Fig. 2.

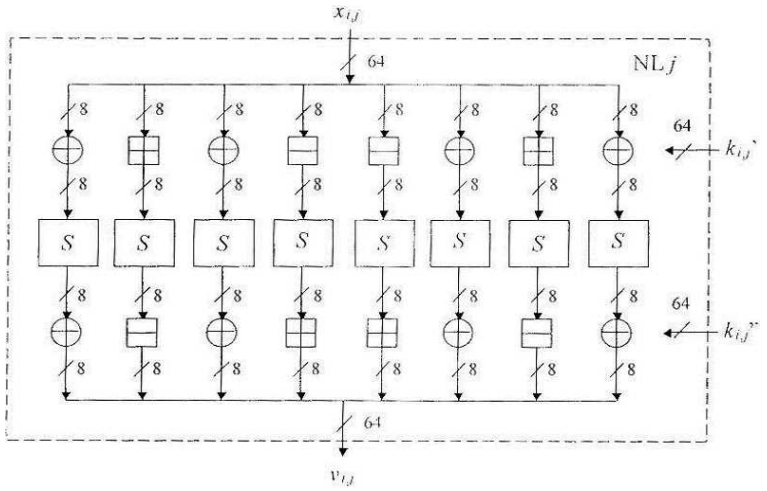

FIGURE 2. *The non-linear keyed substitution layer of PP-1*

The linear layer connects non-linear layers together. For the 64-bit version of the cipher it is depicted in Fig. 3.

Input bits	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Output bits	10	15	18	31	26	47	34	63	42	1	50	17	58	33	2	49
Input bits	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Output bits	12	3	20	19	28	35	36	51	44	5	52	21	60	37	4	53
Input bits	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Output bits	14	7	22	23	30	39	38	55	46	9	54	25	62	41	6	57
Input bits	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
Output bits	16	11	24	27	32	43	40	59	48	13	56	29	64	45	8	61

FIGURE 3. *The linear layer P (a permutation of wires) in the* 64*-bit block versions of PP-1*

From the cryptanalyst point of view, it can be represented in an equivalent way as follows. We pay particular attention to sets of 8 wires which pertain to the same S-box in the non-linear layer, as depicted in Fig. 3. We replace numbers between 1 and 64 by a system with two coordinates of type b3, where the first coordinate denotes the S-box from/to which the given number is connected in previous or next non-linear layer, (a denotes the first S-box, b the second S-box, etc.). The second coordinate will be the bit number in that S-box. For example in Fig. 3 we see that bit 2 will be connected to bit 15. In new coordinates this will be written as $a2 \Rightarrow b7$.

This is shown in Fig. 4.

a1	a2	a3	a4	a5	a6	a7	a8		b2	b7	c2	d7	d2	f7	e2	h7
b1	b2	b3	b4	b5	b6	b7	b8		f2	a1	g2	c1	h2	e1	a2	g1
c1	c2	**c3**	**c4**	c5	c6	c7	c8		b4	a3	**c4**	**c3**	d4	e3	e4	g3
d1	d2	d3	d4	d5	d6	d7	d8	P	f4	a5	g4	c5	h4	e5	a4	g5
e1	e2	e3	e4	e5	**e6**	**e7**	e8	⇒	b6	a7	c6	c7	d6	**e7**	**e6**	g7
f1	f2	f3	f4	f5	**f6**	f7	f8		**f6**	b1	g6	d1	h6	**f1**	a6	h1
g1	g2	g3	g4	g5	g6	g7	g8		b8	b3	c8	d3	d8	f3	e8	h3
h1	h2	h3	h4	**h5**	h6	h7	**h8**		f8	b5	g8	d5	**h8**	f5	a8	**h5**

FIGURE 4. *An alternative representation and analysis of the* 64*-bit permutation P with interesting invariant properties shown in bold*

On this picture we can observe some very interesting invariants. For example, for the third S-box, the output bits c3 and c4, will still be connected to the same S-box in the next round, only swapped. Similar sets of two bits exist for the 5-th, 7-th and the last S-box. We will exploit these invariants in our attacks on PP-1.

We have found the same sort of properties for sets of bits of size 2, for *all* the other versions of the permutation P, for 128, 192 and 256 bits, covering *all possible* variants of PP-1 cipher ever proposed.

REMARK. It seems that it was the idea of building an involutional cipher which has obviously affected a lot the design of PP-1, impacted the security of the cipher. Obviously it is much harder to design a cipher which has such special and strong structural properties. One more time in cryptography we see that "special is dangerous". Not because there will be a suspicion of a hidden backdoor or anything of this kind. But simply because the design of cipher is already very hard, and special ciphers will create additional engineering contraints which will make the cipher much harder to resist the various attacks.

7. The S-box of PP-1

Another weakness of the PP-1 cipher is the use of an "optimal" S-box. Various researchers have studied what will be the best optimal possible theoretical security level of an S-box against differential cryptanalysis, see [17], [29], and in particular this theory was extensively used in the design of AES. From these works we know that for an S-box of size 8×8 bits which is a permutation (especially involution) it is impossible to avoid having in its so-called XOR profile a value as high as 4 (in [7] this parameter is called maxTD). More precisely, there exists some fixed non-zero input XOR difference, and another fixed output non-zero XOR difference, such that the probability of this differential transition will be at least $4/2^8 = 2^{-6}$. Other values which will appear in the differential profile will be 0 (differential attack is not possible) and frequently 2, which means that the transition happens with probability of $2/2^8 = 2^{-7}$. While the presence of values such as 4 cannot be avoided, cf. [17],

[29], [7], it seems that one should not worry about values equal to 2. However all this is pure theory, and things are very different in an actual block cipher. Transitions with probability of $4/2^8$ may never occur in any attack, because they cannot be connected to other "good" differentials. Other transitions which occur with probability of only $2/2^8$ will lead to successful attacks, and moreover many such transitions can be combined in one attack, as we will see later. We see that basing a design of cipher on the mathematical theory of S-boxes and doing this in isolation of how the diffusion will operate in a particular cipher impacts the security of the cipher.

Not all differential transitions are equal, and in practice some differential transitions matter much more. In particular, due to the diffusion, the most important transitions in almost any cipher, will be transitions where the input and out differences have a small Hamming weight. In this respect PP-1 has a weakness, the proposed S-box has several transitions where both the input and output difference have only one active bit. This is shown in Fig. 5.

Input diff. (hex) \ Output diff. (hex)	01_{hex}	02_{hex}	04_{hex}	08_{hex}	10_{hex}	20_{hex}	40_{hex}	80_{hex}
01_{hex}	**2**	0	0	**2**	0	0	2	2
02_{hex}	0	0	2	0	0	2	2	0
04_{hex}	0	2	0	0	2	2	0	0
08_{hex}	**2**	0	0	**2**	2	0	0	0
10_{hex}	0	0	2	2	0	0	0	0
20_{hex}	0	2	2	0	0	0	0	2
40_{hex}	2	2	0	0	0	0	2	2
80_{hex}	2	0	0	0	0	2	2	2

FIGURE 5. *Distribution of one-bit transitions in the PP-1 cipher S-box*

We see that several one-bit transitions, for example, the input difference 0000001_2 or (0x01) which gives an output difference of also 0000001_2 or (0x01), occur with probability $2/2^8 = 2^{-7}$, which is slightly lower than the maximum probability 2^{-6} for this S-box, but these are the transitions that matter, and we will be able to exploit these to construct efficient attacks on a PP-1 cipher.

8. One-round iterative characteristics for the 64-bit version of PP-1

By combining these transitions shown on Fig. 5 with some particularly interesting invariant properties where two bits are connected to the exactly the same two bits (inversed) and to the exactly the same S-box in the next round, which were shown in bold in Fig. 4, it is very easy to find differential attacks for an arbitrary number of rounds on PP-1. In particular we have obtained several very interesting one-round invariant transitions with 1 and 2 active bits which are written in

hexadecimal notation and are shown in Fig. 6

Input difference	00	00	00	00	00	00	00	01	Probability
After non-linear layer	00	00	00	00	00	00	00	08	2^{-7}
After permutation	00	00	00	00	00	00	00	01	1

Input difference	00	00	00	00	00	00	00	08	Probability
After non-linear layer	00	00	00	00	00	00	00	01	2^{-7}
After permutation	00	00	00	00	00	00	00	08	1

Input difference	00	00	00	00	00	84	00	00	Probability
After non-linear layer	00	00	00	00	00	84	00	00	2^{-7}
After permutation	00	00	00	00	00	84	00	00	1

Input difference	00	00	00	00	00	00	00	09	Probability
After non-linear layer	00	00	00	00	00	00	00	09	2^{-7}
After permutation	00	00	00	00	00	00	00	09	1

FIGURE 6. *Best one-round invariant differentials with* 1 *and* 2 *active bits in the* 64*-bit PP-1 cipher*

Now all these transitions can be combined in one single aggregated differential.

9. Aggregated and iterative differential attack on the 64-bit version of PP-1

We recall that *an aggregated differential* A, B is a transition where any non-zero difference $a \in A$ will produce an arbitrary non-zero difference $b \in B$ with a certain probability.

Here is what we obtain for PP-1 by combination of several transitions from Fig. 6.

Input difference	00	00	00	00	00	00	00	01 or 08 or 09	Probability
After non-linear l.	00	00	00	00	00	00	00	08 or 01 or 09	$1.5 \cdot 2^{-6}$
After permutation	00	00	00	00	00	00	00	01 or 08 or 09	1

FIGURE 7. *Our best invariant aggregated differential on the* 64*-bit PP-1 cipher*

By repetition (concatenation) of above almost iterative differential characteristic with itself for 10 rounds we obtain a 10-round characteristic with probability

$$(1.5 \cdot 2^{-6})^{10} = 2^{-54.15}.$$

This means that it can be used for 1R attack on the cipher with block length of 64 bits. However, in the last round we would have only one active S-box, which allows us to recover only one byte of key of last round. In order to find more parts of the last round key we can construct different characteristic with, which is important, higher probability. This is done by iterating our characteristics 9 times, and in the 10-th round, we use the following characteristic (see Fig. 8).

Input difference	00	00	00	00	00	00	00	01 or 08 or 09	Probability
After non-linear layer	00	00	00	00	00	00	00	XX	1
After permutation	01	08	00	04	00	09	01	09	1

FIGURE 8. *A differential characteristic to be used in the* 10*th round*

Thus we obtained a 10-round aggregated differential characteristic of PP-1 cipher, with only one possible output difference, which involves however 6 out of 8 of the S-boxes and occurs with overall probability of

$$(1.5 \cdot 2^{-6})^9 = 2^{-48.74}$$

In this paper we do not study how the key recovery can be handled. Due to different group operations used in the non-linear layers the exact key recovery procedure is quite technical and appears in another paper [25].

10. Cryptanalysis of other versions of PP-1

It is possible to show that all the versions of PP-1 cipher can be broken by using these techniques. How exactly this can be done is out of the scope of this paper and appears in another paper [25]. In Fig. 9 we summarize these very recent attacks from [25]. We also give the minimum number of rounds which is judged sufficient to protect against these attacks.

Block length	64	128	192	256
Number of rounds	11	22	32	43
Number of rounds of characteristic	9+1	20+1	30+1	41+1
Probability of characteristic	$2^{-48.7}$	$2^{-108.3}$	$2^{-162.45}$	2^{-222}
Complexity of attack	2^{50}	2^{110}	2^{164}	2^{224}
Secure number of rounds (min)	12+5	24+5	36+5	48+5

FIGURE 9. *Summary of our attacks on all known versions of PP-1 cipher*

11. Conclusion

Differential cryptanalysis, next to linear and algebraic cryptanalysis are three most fundamental general methods of cryptanalysis of block ciphers. A hasty and simplified analysis showed that the recent PP-1 cipher will certainly be resistant, by design, to differential cryptanalysis. But it isn't. In the same way, Shorin, Jelezniakov and Gabidulin [36], [35] have claimed that GOST is secure against differential cryptanalysis after not much more than 6 rounds, and specifically affirm that "breaking the GOST with five or more rounds is very hard". Moreover, Seki and Kaneko [32] show that the straightforward classical differential attack with one single differential characteristic is unlikely to work *at all* for a large number of rounds of GOST, or would work only for a really negligible fraction of keys.

Unhappily, as shown by Seki and Kaneko, much more powerful differential attacks exist, if one joins several differential attacks together [32]. In this paper we confirm that differential attacks with multiple differentials are indeed quite powerful. We restrict to the class of so-called "aggregated differentials" which are sufficient in our current attacks on GOST and PP-1.

For GOST, we exhibit a differential property which holds for 16 rounds of GOST with a probability of 2^{-48} which is simultaneously lower than the best previous result [32], while simultaneously it has a lower probability of occurring by accident. This is shown in Fig. 1. The new differentials discovered motivate further research on differential cryptanalysis of GOST, to find even better characteristics, and methods to deal with the first few, and the last few rounds. In a series of papers we demonstrate that this leads to attacks on full 32-rounds GOST faster than brute force. Our recent results in this direction can be found in [12], [14], [15].

For the PP-1 cipher, in this paper we exhibit very strong differential characteristics and in another paper [25] we show how to break faster than by brute force every single version of the PP-1 cipher ever proposed. These results are also summarized in Fig. 9.

References

[1] Eli Biham, Vladimir Furman, Michal Misztal and Vincent Rijmen, *Differential Cryptanalysis of Q*, FSE 2002, LNCS 2355, Springer, 2002.

[2] A. Biryukov and D. Wagner, Slide attacks, *Proceedings of FSE'99*, LNCS 1636, Springer, 1999, 245–259.

[3] Alex Biryukov and David Wagner, Advanced slide attacks, *Eurocrypt 2000*, LNCS 1807, Springer, 2000, 589–606.

[4] Christophe De Cannière, GOST article, *Encyclopedia of Cryptography and Security*, 2005, 242–243.

[5] C. Charnes, L. O'Connor, J. Pieprzyk, R. Savafi-Naini and Y. Zheng, *Further comments on GOST encryption algorithm*, Preprint 94-9, Department of Computer Science, The University of Wollongong, 1994.

[6] C. Charnes, L. O'Connor, J. Pieprzyk, R. Savafi-Naini and Y. Zheng, Comments on Soviet encryption algorithm, *Advances in Cryptology* (Eurocrypt'94 Proceedings), LNCS 950 (ed. A. De Santis), Springer, 1995, 433–438.

[7] K. Chmiel, *Differential and linear methods of cryptanalysis of block ciphers* (in Polish), Habilitation dissertation, Poznan, 2009.

[8] K. Chmiel, A. Grocholewska-Czurylo and J. Stoklosa, Involutional block cipher for limited resources, *IEEE GLOBECOM 2008*, 2008, 1–5.

[9] Nicolas Courtois, General principles of algebraic attacks and new design criteria for components of symmetric ciphers, *AES 4*, LNCS 3373, Springer, 2005, 67–83.

[10] Nicolas Courtois, *Algebraic complexity reduction and cryptanalysis of GOST*, Cryptology ePrint Archive, Report 626, 2011, http://eprint.iacr.org/.

[11] Nicolas Courtois, Security evaluation of GOST 28147-89 in view of international standardisation, *Cryptologia*, **36** (2012), 2–13.

[12] Nicolas Courtois, *An improved differential attack on full GOST*, Cryptology ePrint Archive, Report 138, 2012, http://eprint.iacr.org/.

[13] Nicolas Courtois, Gregory V. Bard and David Wagner, Algebraic and slide attacks on KeeLoq, *FSE 2008*, LNCS 5086, Springer, 2008, 97–115.

[14] Nicolas Courtois and Michał Misztal, First differential attack on full 32-round GOST, *ICICS'11*, LNCS series, Springer, accepted.

[15] Nicolas Courtois and Michał Misztal, *Differential cryptanalysis of GOST*, Cryptology ePrint Archive, Report 312, 2011, http://eprint.iacr.org/.

[16] Nicolas Courtois and Josef Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, *Asiacrypt 2002*, LNCS 2501, Springer, 2002, 267–287.

[17] Joan Daemen and Vincent Rijmen, *The Design of Rijndael*, AES – The Advanced Encryption Standard, Springer, Berlin, 2002.

[18] Wei Dai, *Crypto++*, A public domain library, http://www.cryptopp.com.

[19] Fleischmann Ewan, Gorski Michael, Huehne Jan-Hendrik and Lucks Stefan, *Key recovery attack on full GOST block cipher with zero time and memory*, Published as ISO/IEC JTC 1/SC 27 N8229, 2009.

[20] Soichi Furuya, Slide attacks with a known-plaintext cryptanalysis, *ICISC 2001*, LNCS 2288, 2002, 11–50.

[21] Orhun Kara, Reflection cryptanalysis of some ciphers, *Indocrypt 2008*, LNCS 5365, 2008, 294–307.

[22] John Kelsey, Bruce Schneier and David Wagner, Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and triple-DES, *Crypto'96*, LNCS 1109, Springer, 1996.

[23] Lars R. Knudsen, Truncated and higher order differentials, *Fast Software Encryption 1995*, Lecture Notes in Computer Science 1008, Springer Verlag, Berlin, Heidelberg, New York, 1995, 196–211.

[24] Florian Mendel, Norbert Pramstaller, Christian Rechberger, Marcin Kontak and Janusz Szmidt, Cryptanalysis of the GOST hash function, *Crypto 2008*, LNCS 5157, Springer, 2008, 162–178.

[25] Michał Misztal, Differential cryptanalysis of PP-1 cipher, *Workshop on Cryptography and Security Systems* (CSS 2011, September 26-28, 2011, Naleczow, Poland); *Journal Annales UMCS ser. Informatica*.

[26] OpenSSL library, *A Russian reference implementation of GOST implementing Russian algorithms as an extension of TLS v1.0*, OpenSSL 0.9.8, gost89.c, http://www.openssl.org/source/.

[27] Axel Poschmann, San Ling and Huaxiong Wang, 256 bit standardized crypto for 650 GE GOST revisited, *CHES 2010*, LNCS 6225, 2010, 219–233.

[28] J. Pieprzyk and L. Tombak, *Soviet encryption algorithm*, Preprint 94-10, Department of Computer Science, The University of Wollongong, 1994.

[29] Vincent Rijmen, *Cryptanalysis and design of iterated block ciphers*, PhD Thesis, K. U. Leuven, October 1997.

[30] Vladimir Rudskoy, *On zero practical significance of "Key recovery attack on full GOST block cipher with zero time and memory"*, Cryptology ePrint Archive, Report 111, 2010, http://eprint.iacr.org.

[31] Markku-Juhani Saarinen, *A chosen key attack against the secret S-boxes of GOST*, manuscript, 1998.

[32] Haruki Seki and Toshinobu Kaneko, Differential cryptanalysis of reduced rounds of GOST, *SAC 2000, Selected Areas in Cryptography* (eds. Douglas R. Stinson and Stafford E. Tavares), LNCS 2012, Springer, 2000, 315–323.

[33] Bruce Schneier, *Applied Cryptography*, Second Edition, Section 14.1 GOST, John Wiley and Sons, 1996.

[34] Bruce Schneier, The GOST encryption algorithm, *Dr. Dobb's Journal*, **20** (1995), 2.

[35] Vitaly V. Shorin, Vadim V. Jelezniakov and Ernst M. Gabidulin, Linear and differential cryptanalysis of Russian GOST, *Elsevier Preprint*, 2001.

[36] V. V. Shorin, V. V. Jelezniakov, E. M. Gabidulin, *Security of algorithm GOST 28147-89* (in Russian), Abstracts of XLIII MIPT Science Conference (December 8-9, 2000).

[37] I. A. Zabotin, G. P. Glazkov and V. B. Isaeva, *Cryptographic Protection for Information Processing Systems* (in Russian), Government Standard of the USSR, GOST 28147-89, Government Committee of the USSR for Standards, 1989; translated to English by Aleksandr Malchik (English preface co-written with Whitfield Diffie), http://www.autochthonous.org/crypto/gosthash.tar.gz.