Annales UMCS Informatica AI XI, 2 (2011) 9–24
DOI: 10.2478/v10065-011-0006-7

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

Differential cryptanalysis of PP-1 cipher

Michał Misztal*

Institute of Mathematics and Cryptology, Cybernetics Faculty,
Military University of Technology
ul. S. Kaliskiego 2, 00-908 Warsaw, Poland

Abstract

In this paper we present a differential attack on the block cipher PP-1 which was designed at Poznan University of Technology. Complexity of the attack is smaller than that of brute force attack for every version of the cipher (for every block length). The attack is possible is spite of the fact that the S-box exhibits optimal security against the differential cryptanalysis. The attack is based on the fact that the design of the cipher S-box and permutation were constructed independently. The permutation operates on individual bits, and in the XOR profile table of S-box 1 bit to 1 bit transitions are possible. It allows constructing a simple one-round differential characteristic which is "almost" iterative with the probability $1.5 \cdot 2^{-6}$. By 9 times concatenation of the characteristic and its relaxation in the last round we obtained a 10-round characteristic with the probability 2-48.7. Using this characteristic with 1R attack makes differential cryptanalysis of full 11-round cipher with complexity smaller than exhaustive search possible. By carefully exploiting similar characteristics it is possible to find analogous attacks on different versions of cipher PP-1, with higher a larger of rounds.

1. Introduction

Differential cryptanalysis [**1**] is, next to linear cryptanalysis [**2, 3**] and algebraic attacks [**4**] one of three fundamental, general methods of cryptanalysis of

*E-mail address: mmisztal@wat.edu.pl

block ciphers [**5**]. This method has been known since 90' and modern block ciphers should be invulnerable to it. However, some new block ciphers are vulnerable to this attack, for example Q cipher [**6, 7**]. The aim of the paper is to show that even completely new designed block ciphers can be attacked with differential cryptanalysis if they are not carefully constructed. The flaw of PP-1 cipher attacked here is an independent design of nonlinear layer (S-boxes) and linear layer (permutation). Applied permutation operates on individual bits, but independently designed involutional S-box shows in its XOR profile that differential transitions with only one active bit on input to one active bit on output are possible. It means that diffusion in the cipher is quite poor. This observation allows finding differential characteristics with one active S-box in every round. Concatenation of three one-round iterative characteristics with the probability 2^{-7} each allows constructing almost iterative characteristic with the probability $1.5 \cdot 2^{-6}$. Extension of the iterative characteristic to 9 rounds and extra extension with the last round allows finding a 10-round differential characteristic with the probability $2^{-48.7}$. This characteristic can be used in 1R attack on the full 11-round version of the cipher with complexity lower than exhaustive search complexity 2^{64}. Its extension to 21, 31 and 42 rounds allows attacking the cipher with the block length 128, 192 and 256 bits respectively, as well. Some preliminary results on iterative differential cryptanalysis of the most basic version of PP-1 cipher are presented in [**8**]. In this paper we extend these early results to actual attacks on the full PP-1 cipher.

PP-1 cipher was designed at Poznan University of Technology (name is derived from Poznań Politechnique - in Polish) in 2007 [**9, 10**]. The first version of PP-1 has the block length of 64 bits, then also a version with a scalable block length which is a multiple of 64 bits was developed. The special feature of the cipher is, according to the authors that it is an involutional SPN (substitution-permutation network). More detailed description of the cipher is given in Section 2. In Section 3 we present four one-round, iterative differential characteristics, and a method to concatenate two of them to construct an almost iterative characteristic. In Section 4 we give method of extension this one-round characteristic to 10 rounds, and also some improvements of the method. In Section 5 we present differential attack on PP-1 cipher with 11 rounds which uses the characteristic. Section 6 gives some conclusions, in which we discuss the security of PP-1 cipher with bigger number of rounds.

2. Description of PP-1 cipher

The PP-1 cipher was designed at Poznan University of Technology [**9, 10**]. It allows encryption of plaintexts of the length being an arbitrary multiplicity

of 64 bits. The cipher is involutional SPN (substitution-permutation network). It means that, non-linear layer (S-boxes) as well as linear (permutation) are involutions and may be used for encryption and decryption. The non-linear layer is presented in Fig. 1.

The non-linear layer transforms the 64-bit input block to the same length output block with a twice longer key (128-bit round key). It uses the operations: XOR, arithmetic sum and subtraction (see Fig. 1) and involutional S-box S of the size 8 8 bits. For the versions of PP-1 with the block length of multiplicity of 64 bits, the non-linear layer is used in parallel for each 64-bit input block and requires the round key to be twice longer than the block length.

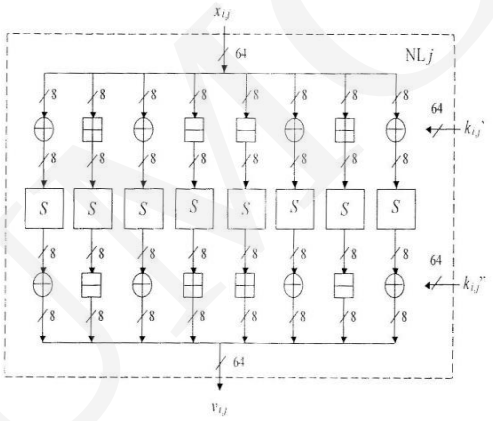

Fig. 1. Scheme of non-linear layer of PP-1 cipher.

After the non-linear layer in the PP-1 cipher linear (involutional again) operation is applied. It is a permutation P which operates with the full length of the block. The permutation for the version with 64-bit block is presented in Table 1. Odd rows in the table give subsequently input bits, and under them (even rows) positions on which the input bits goes in output. So, according to the table the first bit goes to position 10, the second to 15, and so on.

In order to show the influence of permutation P on the dependencies between output bits of non-linear layer of one round and input bits to non-linear layer of next round the permutation P is presented in the following, equivalent way (Table 2).

Subsequent input bytes to permutation P are written in rows and denoted with the letters from a to h. They correspond to output bytes to subsequent S-boxes of non-linear layer (a - the output form first S-box, b - the second, and so on). Bits in those bytes are denoted with the digits from 1 to 8. Bit $a1$ denotes the first output bit from the first S-box and goes to (according to Table 2.) bit

Table 1. Permutation P as PP-1 cipher for the block length $n = 64$.

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

Table 2. Permutation P in tables of the size 8×8 bits ($n = 64$).

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**

$b2$, which means the second input bit to second S-box in the next round, which is 10th output bit from permutation P. It is consistent with Table 1.

One can see that every row of input table is transformed by permutation P into only two different columns of output table. This fact will not be used directly in the differential attack described below, but it cannot be considered as an advantage of the permutation. It is rather a flaw, because input bits are permuted in a schematic way and not optimally diffused. But the main flaw of the permutation, applied in the attack is the fact that the output bits from one S-box may go to input bits of the same S-box, for example $c3$ to $c4$ and inversely (involution), similarly $e6$ to $e7$, $f1$ to $f6$ and $h5$ to $h8$.

For the versions of the cipher with a longer block length the permutation P is defined by a special dedicated algorithm [**9, 10**]. The algorithm is supposed to provide similar properties for permutation of bits in blocks of arbitrary length (multiplicity of 64 bits), and should provide also the involution property.

In this paper we omit the detailed description of this algorithm, and study directly the relevant permutations obtained with this algorithm for the three

principal block sizes of 64, 128 and 256 bits relevant to the three main versions of PP-1 cipher. These are given in Table 3 through Table 5 together with some observations shown in bold which are relevant to our attacks.

Table 3. Permutation P for the tables of the size 8×8 bits ($n = 128$).

a1	a2	a3	a4	a5	a6	a7	a8		b2	d7	c2	h7	d2	l7	e2	p7
b1	b2	b3	b4	b5	b6	b7	b8		f2	a1	g2	e1	h2	i1	i2	m1
c1	c2	c3	c4	c5	c6	c7	c8		j2	a3	k2	e3	l2	i3	m2	m3
d1	d2	d3	d4	d5	d6	d7	d8		n2	a5	o2	e5	p2	i5	a2	m5
e1	e2	e3	e4	e5	e6	e7	e8		b4	a7	c4	e7	d4	i7	e4	m7
f1	f2	f3	f4	f5	f6	f7	f8		f4	b1	g4	f1	h4	j1	i4	n1
g1	g2	g3	g4	g5	g6	g7	g8		j4	b3	k4	f3	l4	j3	m4	n3
h1	h2	h3	h4	h5	h6	h7	h8	P	n4	b5	o4	f5	p4	j5	a4	n5
i1	i2	i3	i4	i5	i6	i7	i8	⇒	b6	b7	c6	f7	d6	j7	e6	n7
j1	j2	j3	j4	j5	j6	j7	j8		f6	c1	g6	g1	h6	k1	i6	o1
k1	k2	k3	k4	k5	k6	k7	k8		j6	c3	k6	g3	l6	k3	m6	o3
l1	l2	l3	l4	l5	l6	l7	l8		n6	c5	o6	g5	p6	k5	a6	o5
m1	m2	m3	m4	m5	m6	m7	m8		b8	c7	c8	g7	d8	k7	e8	o7
n1	n2	n3	n4	n5	n6	n7	n8		f8	d1	g8	h1	h8	l1	i8	p1
o1	o2	o3	o4	o5	o6	o7	o8		j8	d3	k8	h3	l8	l3	m8	p3
p1	p2	p3	p4	**p5**	p6	p7	**p8**		n8	d5	o8	h5	**p8**	l5	a8	**p5**

Table 4. Permutation P for the tables of the size 8×8 bits ($n = 192$).

a1	a2	a3	a4	a5	a6	a7	a8		b2	f7	c2	l7	d2	r7	e2	x7
b1	b2	b3	b4	b5	b6	b7	b8		f2	a1	g2	g1	h2	m1	i2	s1
c1	c2	c3	c4	c5	c6	c7	c8		j2	a3	k2	g3	l2	m3	m2	s3
d1	d2	d3	d4	d5	d6	d7	d8		n2	a5	o2	g5	p2	m5	q2	s5
e1	e2	e3	e4	e5	e6	e7	e8		r2	a7	s2	g7	t2	m7	u2	s7
f1	f2	f3	f4	f5	f6	f7	f8		v2	b1	w2	h1	x2	n1	a2	t1
g1	g2	g3	g4	g5	g6	g7	g8		b4	b3	c4	h3	d4	n3	e4	t3
h1	h2	h3	h4	h5	h6	h7	h8		f4	b5	g4	h5	h4	n5	i4	t5
i1	i2	i3	i4	i5	i6	i7	i8		j4	b7	k4	h7	l4	n7	m4	t7
j1	j2	j3	j4	j5	j6	j7	j8		n4	c1	o4	i1	p4	o1	q4	u1
k1	k2	k3	k4	k5	k6	k7	k8		r4	c3	s4	i3	t4	o3	u4	u3
l1	l2	l3	l4	l5	l6	l7	l8	P	v4	c5	w4	i5	x4	o5	a4	u5
m1	m2	m3	m4	m5	m6	m7	m8	⇒	b6	c7	c6	i7	d6	o7	e6	u7
n1	n2	n3	n4	n5	n6	n7	n8		f6	d1	g6	j1	h6	p1	i6	v1
o1	o2	o3	o4	o5	o6	o7	o8		j6	d3	k6	j3	l6	p3	m6	v3
p1	p2	p3	p4	p5	p6	p7	p8		n6	d5	o6	j5	p6	p5	q6	v5
q1	q2	q3	q4	q5	q6	q7	q8		r6	d7	s6	j7	t6	p7	u6	v7
r1	r2	r3	r4	r5	r6	r7	r8		v6	e1	w6	k1	x6	q1	a6	w1
s1	s2	s3	s4	s5	s6	s7	s8		b8	e3	c8	k3	d8	q3	e8	w3
t1	t2	t3	t4	t5	t6	t7	t8		f8	e5	g8	k5	h8	q5	i8	w5
u1	u2	u3	u4	u5	u6	u7	u8		j8	e7	k8	k7	l8	q7	m8	w7
v1	v2	v3	v4	v5	v6	v7	v8		n8	f1	o8	l1	p8	r1	q8	x1
w1	w2	w3	w4	w5	w6	w7	w8		r8	f3	s8	l3	t8	r3	u8	x3
x1	x2	x3	x4	**x5**	x6	x7	**x8**		v8	f5	w8	l5	**x8**	r5	a8	**x5**

We observe that both permutations P for bigger block lengths have one property which is the same as in the 64-bit version from Table 10. In all cases, the last S-box fifth bit is exchanged with the eighth bit, which is marked in the above tables in bold.

Table 5. Permutation P for the tables of the size 8×8 bits ($n = 256$).

a1	a2	a3	a4	a5	a6	a7	a8		b2	h7	c2	p7	d2	x7	e2	ϕ7
b1	b2	b3	b4	b5	b6	b7	b8		f2	a1	g2	i1	h2	q1	i2	y1
c1	c2	c3	c4	c5	c6	c7	c8		j2	a3	k2	i3	l2	q3	m2	y3
d1	d2	d3	d4	d5	d6	d7	d8		n2	a5	o2	i5	p2	q5	q2	y5
e1	e2	e3	e4	e5	e6	e7	e8		r2	a7	s2	i7	t2	q7	u2	y7
f1	f2	f3	f4	f5	f6	f7	f8		v2	b1	w2	j1	x2	r1	y2	z1
g1	g2	g3	g4	g5	g6	g7	g8		z2	b3	α2	j3	β2	r3	χ2	z3
h1	h2	h3	h4	h5	h6	h7	h8		δ2	b5	ε2	j5	ϕ2	r5	a2	z5
i1	i2	i3	i4	i5	i6	i7	i8		b4	b7	c4	j7	d4	r7	e4	z7
j1	j2	j3	j4	j5	j6	j7	j8		f4	c1	g4	k1	h4	s1	i4	α1
k1	k2	k3	k4	k5	k6	k7	k8		j4	c3	k4	k3	l4	s3	m4	α3
l1	l2	l3	l4	l5	l6	l7	l8		n4	c5	o4	k5	p4	s5	q4	α5
m1	m2	m3	m4	m5	m6	m7	m8		r4	c7	s4	k7	t4	s7	u4	α7
n1	n2	n3	n4	n5	n6	n7	n8		v4	d1	w4	l1	x4	t1	y4	β1
o1	o2	o3	o4	o5	o6	o7	o8		z4	d3	α4	l3	β4	t3	χ4	β3
p1	p2	p3	p4	p5	p6	p7	p8	P	δ4	d5	ε4	l5	ϕ4	t5	a4	β5
q1	q2	q3	q4	q5	q6	q7	q8	$\Rightarrow$	b6	d7	c6	l7	d6	t7	e6	β7
r1	r2	r3	r4	r5	r6	r7	r8		f6	e1	g6	m1	h6	u1	i6	χ1
s1	s2	s3	s4	s5	s6	s7	s8		j6	e3	k6	m3	l6	u3	m6	χ3
t1	t2	t3	t4	t5	t6	t7	t8		n6	e5	o6	m5	p6	u5	q6	χ5
u1	u2	u3	u4	u5	u6	u7	u8		r6	e7	s6	m7	t6	u7	u6	χ7
v1	v2	v3	v4	v5	v6	v7	v8		v6	f1	w6	n1	x6	v1	y6	δ1
w1	w2	w3	w4	w5	w6	w7	w8		z6	f3	α6	n3	β6	v3	χ6	δ3
x1	x2	x3	x4	x5	x6	x7	x8		δ6	f5	ε6	n5	ϕ6	v5	a6	δ5
y1	y2	y3	y4	y5	y6	y7	y8		b8	f7	c8	n7	d8	v7	e8	δ7
z1	z2	z3	z4	z5	z6	z7	z8		f8	g1	g8	o1	h8	w1	i8	ε1
α1	α2	α3	α4	α5	α6	α7	α8		j8	g3	k8	o3	l8	w3	m8	ε3
β1	β2	β3	β4	β5	β6	β7	β8		n8	g5	o8	o5	p8	w5	q8	ε5
χ1	χ2	χ3	χ4	χ5	χ6	χ7	χ8		r8	g7	s8	o7	t8	w7	u8	ε7
δ1	δ2	δ3	δ4	δ5	δ6	δ7	δ8		v8	h1	w8	p1	x8	x1	y8	ϕ1
ε1	ε2	ε3	ε4	ε5	ε6	ε7	ε8		z8	h3	α8	p3	β8	x3	χ8	ϕ3
ϕ1	ϕ2	ϕ3	ϕ4	**ϕ5**	ϕ6	ϕ7	**ϕ8**		δ8	h5	ε8	p5	**ϕ8**	x5	a8	**ϕ5**

This property of two bits of the last S-box being mapped to the same two bits of the same S-box in the same round is systematically exploited in our attacks on different versions of PP-1.

The PP-1 cipher is an iterative which alternates the non-linear layer and a (linear) permutation P. These two transformations form one round of the cipher and are performed many times. The number of repetitions or rounds depends on the block length. Numbers of rounds for different versions of cipher are shown in Table 6. Block lengths are not limited to the values 256 bits, as we mentioned before the PP-1 cipher may operate on the block lengths being an arbitrary (finite) multiplicities of 64 bits. Specific versions with the blocks longer than 256 bits have not been yet specified and are therefore outside the scope of this work.

Table 6. Number of rounds of PP-1 cipher for different block lengths.

Block length	64	128	192	256
Number of rounds	11	22	32	43

The length of the key used in the cipher is equal to that of block or it is twice longer [**10**]. In our attack we assume that the key length is equal to the block length. We omit the discussion of these twice longer keys as our attacks will have a similar complexity which will therefore be much lower than the exhaustive search.

3. One-round, almost iterative differential characteristic

As already mentioned the main observation used in the differential attack on the PP-1 cipher was the fact that non-linear and linear layers of the cipher were designed without consideration of how they will work together. The main flaw of the cipher is composition of bit permutation and S-box, in which one-bit to one-bit transitions are possible. A second flaw we will exploit is the possibility of transformation in permutation P of individual bits without change of S-box (see bits marked in bold in Tables 2–5). These properties allow to find a one-round iterative characteristic, or even several such characteristics with the same probability, and then combining three of them to form an "almost" iterative characteristic with higher probability.

The base of each differential attack is a construction of XOR profile for S-box(es) [**1, 9, 6, 11, 5**]. The S-box used in the PP-1 cipher was not selected randomly, but it was constructed to be an involution and possibly most resistant to differential and linear cryptanalysis. From theory [**12, 13**] we know, that the S-box of the size 8×8 bits which is a permutation (especially involution) in the best case must have the smallest maximum 4 in XOR profile (in paper [**9**] this parameter is called maxTD). It means that the probability of a non-trivial transition could be at most $4/2^8 = 2^{-6}$. Greater values should not appear in the XOR profile. Now the case with the S-box maximally resistant to differential attack is dealt with in the PP-1 cipher. In the XOR profile which is not entirely presented here due to its size, one can find only entries (except the trivial transition $(0 \rightarrow 0)$) 4, 2 and 0. In spite of the fact that the S-box of PP-1 cipher is optimal i.e. maximally resistant to differential attack, its combination with permutation P allows such an attack. The reason is the fact mentioned earlier that in the S-box one-bit transitions are possible. The XOR profile restricted to only one-bit transitions is presented in Table 7.

Table 7. Distribution of one-bit transitions in the S-box from PP-1.

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

As we can see from the above table, several one-bit transitions are possible, but none of them has the maximum value in the entire XOR profile which is 4. It means that certain one-bit transitions for example transition of 0000001_2 (01_{hex}) to 0000001_2 (01_{hex}) occurs with the probability $2/2^8 = 2^{-7}$ which is slightly lower than the maximum probability 2^{-6}.

We are especially interested in those S-boxes in which input and output are combined with the round key by the XOR operation, these are S-boxes a, c, f and h (see Fig. 1). For other S-boxes the round key is combined by the operations of arithmetic sum or subtraction. These operations in the differential attack based on the differential (linear) operation of XOR are non-linear and must be analysed like other non-linear operations for example S-boxes. It is possible to analyse transitions of these arithmetic operations only for the most significant bits, because these bits behave as for the XOR operation. This diminishes our possibilities of analysis to some extent. So, we focus only on the S-boxes a, c, f and h. For one of them, we search such one-bit transition (see Table 7), for which permutation P does not activate in the next round S-boxes which do not belong to our required set of S-boxes a, c, f and h. For that purpose the most convenient way is to use these bits in permutation P, which does not change the S-box in the next round. These are transition of $c3$ to $c4$, $e6$ to $e7$, $f1$ to $f6$ or $h5$ to $h8$, as well as their inversions. As follows from the above we must reject at once transition of $e6$ to $e7$, because the S-box e (fifth) is "surrounded" with arithmetic operations. Of the other three transitions only those of the fifth bit (08_{hex}) to the eighth bit (01_{hex}) and opposite, for the eighth S-box h are possible (according to Table 1). Therefore we obtain two similar (we call them involutional symmetric) one-round iterative differential characteristics presented in Table 8.

By using the above transitions of permutation P which does not change the S-box (these are transitions of $c3$ to $c4$, $f1$ to $f6$ or $h5$ to $h8$) we can also

Table 8. One-round, iterative differential characteristics (with one bit).

Input difference	00	00	00	00	00	00	00	01	Probability
Diff. after the non-linear layer	00	00	00	00	00	00	00	08	2^{-7}
Difference after permutation	00	00	00	00	00	00	00	01	1

Input difference	00	00	00	00	00	00	00	08	Probability
Diff. after the non-linear layer	00	00	00	00	00	00	00	01	2^{-7}
Difference after permutation	00	00	00	00	00	00	00	08	1

find one-round iterative two-bit differential characteristics. The bits $c3$ and $c4$ fixed to 1 form the byte 30_{hex}, but differential transition $30 \rightarrow 30$ is not possible in the analysed S-box. However, the bits $f1$ and $f6$ form the byte 84_{hex}, the bits $h5$ and $h8$ form the byte 09_{hex}, and these transitions $84 \rightarrow 84$ and $09 \rightarrow 09$ respectively are possible in the analysed S-box, both of them again with the probability 2^{-7}. That observation gives us two more one-round iterative characteristics collected in Table 9.

Table 9. One-round, iterative differential characteristics (with two bits).

Input difference	00	00	00	00	00	84	00	00	Probability
Diff. after the non-linear layer	00	00	00	00	00	84	00	00	2^{-7}
Difference after permutation	00	00	00	00	00	84	00	00	1

Input difference	00	00	00	00	00	00	00	09	Probability
Diff. after the non-linear layer	00	00	00	00	00	00	00	09	2^{-7}
Difference after permutation	00	00	00	00	00	00	00	09	1

The main advantage of these characteristics is the fact, that they are iterative and can be concatenated an arbitrary number of times of course with the cost of multiplying the probability. A disadvantage of these characteristics is, however, the fact that they do not exploit the best differential transitions of the S-box with the probability 2^{-6}. It would be especially important in iterating (concatenating) these characteristics for many rounds. Such transitions with the maximal probability, which could be used in a similar way, have not been found.

To improve the probability of one-round characteristic we can use already mentioned property of "involutional symmetry" of our first two characteristics (Table 8), the second two-bit characteristic in Table 9 and extra one-bit transitions from the XOR profile of the S-box (Table 7). Namely, there is no problem if in the S-box h differential input 01 goes to output 01 or 09, differential input

08 goes to output 08 or 09, and differential input 09 goes to output 01 or 08. Such transitions are possible with the probability 2^{-7} (see Table 7 and the XOR profile of the S-box). In that way the first characteristic in Table 8 becomes the second in that table or the second in Table 9 or vice-versa. Thus we obtain one-round almost iterative characteristic (analogous to those from the attack on Q cipher [**7**]) illustrated in Table 10.

Table 10. One-round, almost iterative differential characteristic.

Input difference	00	00	00	00	00	00	00	01 or 08 or 09	Probability
Diff. after the non-linear layer	00	00	00	00	00	00	00	08 or 01 or 09	$1.5{\cdot}2^{-6}$
Difference after permutation	00	00	00	00	00	00	00	01 or 08 or 09	1

The probability of the above characteristic is $3 \cdot 2^{-7} = 1.5 \cdot 2^{-6}$, since we allow transitions of 01 to 08 or 01 or 09, similarly 08 to 01 or 08 or 09 and 09 to 01 or 08 or 09. It is an almost iterative characteristic, since output does not have to be the same as input, but it can be concatenated for an arbitrary number of rounds. The term 'almost iterative' comes from the conclusions of paper [**7**]. A similar technique is used for the GOST cipher [**14**]. In that paper the authors have called this technique 'a set of differential characteristics'. A detailed discussion about the terminology related to the sets of differentials used in our attacks on PP-1, compared to the sets which occur in attacks on other ciphers, for example for the Russian GOST cipher, can be found in [**8**].

4. Extension of characteristic to 10 rounds

Extension by repetition (concatenation) of the above almost iterative differential characteristic (Table 10) for 10 rounds gives us characteristic with the probability $\left(1.5 \cdot 2^{-6}\right)^{10} = 2^{-54.15}$ which means that it can be used for 1R attack on the cipher with the block length of 64 bits. But, in the last round we would have only one active S-box, which allows to recover only one byte of the last round key. In order to find more parts of the last round key we can construct different characteristics with, which is important, higher probability.

Namely, we can relax the above characteristic in the last round. It will increase its probability because in the last round we allow transition to the arbitrary (with the probability 1) output. Let us recall here once more (Table 11) permutation P for the tables of the size 8×8 bits which illustrates the dependencies between input bits and output bits of individual S-boxes (Table 2). If we focus the on S-box h we can see (based on the fact emphasized earlier), that after permutation P the bits of S-box h appear as outputs only in the fifth and

eighth columns. Moreover, we can see that these bits do not appear in the third and fifth rows (value in bold in Table 11).

Table 11. Permutation P for the tables of the size 8×8 bits ($n = 64$).

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	$\Rightarrow$	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**

Thus we can observe that if only S-box h is active, then after permutation P in the next round six S-boxes can be active (all except the third and the fifth ones), and these active S-boxes will have one or two active bits (only on the fifth and/or eighth bit) (according to Table 11). It means that if we assume that in one before last round S-box h is active, and in the last round transition in the S-box is arbitrary (with the probability 1), then after permutation P in the last round at most six S-boxes could be active, and these active S-boxes would have only one or two active bits in input. Such relaxation of the characteristic with the active S-box h is presented in Table 12.

Table 12. One (final)-round extension of characteristic.

Input difference	00	00	00	00	00	00	00	01 or 08 or 09	Probability
Diff. after non-linear layer	00	00	00	00	00	00	00	XX	1
Difference after permutation	01	08	00	04	00	09	01	09	1

XX means here an arbitrary value, for which in rows 01, 08 or 09 of the XOR profile we have an entry different from 0. From the set of 8 bits before permutation P from one to eight bits could be active. Moreover, in the next round for the S-boxes a, b and g if respective one bit is inactive, then the entire S-box is inactive. S-boxes c and e are always inactive.

After nine concatenations of almost iterative characteristic (from Table 13) and after concatenation with the final characteristic (Table 12) we get 10-round differential characteristic of PP-1 cipher with the probability $2^{-48.7}$. The full 10-round characteristic used in the attack on 11 rounds of PP-1 is shown in Table 13.

Table 13. 10-round differential characteristic of PP-1 cipher with the probability $2^{-48.7}$.

Input difference	0 0	0 0	0 0	0 0	0 0	0 0	0 0	01 or 08 or 09	Probability
Diff. after non-linear layer	0 0	0 0	0 0	0 0	0 0	0 0	0 0	08 or 01 or 09	$1{,}5 \cdot 2^{-6}$
Difference after permutation	0 0	0 0	0 0	0 0	0 0	0 0	0 0	01 or 08 or 09	1

Repeated 9 times

Input difference	00	00	00	00	00	00	00	01 or 08 or 09	Probability
Diff. after non-linear layer	00	00	00	00	00	00	00	XX	1
Difference after permutation	01	08	00	04	00	09	01	09	1

Iterative characteristic from the first part is repeated 9 times.

5. Attack on 64-bit version (11 rounds)

Differential attack on 11 rounds of PP-1 is now possible with the characteristic given in Table 13 in the following way. First we construct a set of plaintexts whose difference on the eighth byte is equal to 01, 08 or 09. To reduce the number of plaintexts used, we use a dedicated structure called quartet [**1**]. We begin with a randomly chosen plaintext M1, and then the next three plaintexts are determined in the following way:

$$M_2 = M_1 \oplus 00\,00\,00\,00\,00\,00\,00\,01$$
$$M_3 = M_1 \oplus 00\,00\,00\,00\,00\,00\,00\,08$$
$$M_4 = M_1 \oplus 00\,00\,00\,00\,00\,00\,00\,09.$$

These four plaintexts give us six pairs, two pairs with each value from our characteristic, since:

$$M_1 \oplus M_2 = M_3 \oplus M_4 = 00\,00\,00\,00\,00\,00\,00\,01$$
$$M_1 \oplus M_3 = M_2 \oplus M_4 = 00\,00\,00\,00\,00\,00\,00\,08$$
$$M_3 \oplus M_2 = M_1 \oplus M_4 = 00\,00\,00\,00\,00\,00\,00\,09.$$

By encrypting only four plaintexts, we get six pairs with a required input difference. If we wanted to get these pairs in a standard way, we would have to generate and encrypt 12 plaintexts. Using these structures reduces complexity of our attack three times.

We encrypt the structure with a full, 11-round version of PP-1, using the same key (a chosen plaintext attack). In this way we get four ciphertexts. At the beginning we permute each of the ciphertexts with an inverse P permutation (which is equal to permutation P, being an involution). What we get are blocks after the last non-linear layer. We search among them for the pairs which follow

our characteristic. The first condition for a good pair is that it has the inactive S-boxes c and e. To identify such pairs, we sort all ciphertexts (after inverse P permutation P) by the 3-rd and the 5-th bytes. If we find a pair in a structure - or several pairs - with the same values on these two bytes, we analyze this pair further. The probability of having two equal bytes in one block is 2^{16}, while we have six pairs in one structure - so in each structure we can find at most one pair satisfying this condition. If we do not find such a pair, we generate another structure. If such pair occurs, we move to the next phase - recovering a part of the last round subkey. We look for these 8-bit parts of the 11-th round subkey, which undergo the XOR operations after the S-boxes a, f and h. This makes together $3 \times 8 = 24$ key bits.

Table 14. Possibilities of using differential characteristic in the last round.

S-box	a	b	c	d	e	f	g	h
Input difference	01	08	00	04	00	09	01	09
Operation after the S-box layer	$\oplus$	-	$\oplus$	+	+	$\oplus$	-	$\oplus$
Usage	Ka	none	filtering	none	filtering	Kf	none	Kh

Table 14 shows the possibilities of using our differential characteristic for individual S-boxes in the last round of the cipher. As mentioned earlier, the S-boxes c and e are inactive (input differences are equal to zero), so they may be used for an initial filtration (finding pairs which follow our characteristic among all generated structures). For the S-boxes b, d and g used in the cipher arithmetic operations make differential cryptanalysis of these blocks impossible. We cannot find the 8-bit part of the last round subkey for these S-boxes. We are left only with the S-boxes a, f and g. For them we can find the parts (bytes) of the 11-th round subkey denoted here as Ka, Kf and Kh respectively. For each of these three S-boxes we perform a typical key recovery procedure [**1, 11, 15**]. Using cipertexts (after inversion of permutation P) of plaintext pairs, in which the third and the fifth bytes are inactive (initial filtration) and using outputs given from the differential characteristic (Table 14) we look for a candidate for round subkeys (24 bits). For the S-boxes f and h we take into account the fact that outputs of characteristic can be only one- or two-bit values. Therefore for these S-boxes a number of the obtained candidate round subkeys may be three times larger than for the S-box a. It is also possible that one of the three S-boxes is inactive, and this does not result in rejection of the analysed pair. We reject the analysed pair (extra filtration) if for any of three S-boxes during the analysis we get impossible transition in the XOR profile.

The characteristic which was used (Table 13) has the probability $2^{-48.7}$. So, for this characteristic right pairs will appear once on $2^{48.7}$ generated pairs. For

our characteristic we can generate structures with four plaintexts (quartets), and in each such structure we have six different pairs compatible with input of the characteristic. Hence, finding one right pair requires $2^{48.7}/6 \approx 2^{46.1}$ structures. Since, finding one right pair is not enough to recover the 24-bit part of subkey we need more (2 or 3) right pairs. Hence, in the attack we have to use about 2^{48} structures. The complete algorithm of the attack in pseudo-code form is given below.

Algorithm 1. Algorithm of the attack in the pseudo-code form:

I. We initialize a table with 2^{24} entries for counter L of candidate keys with zeros;
II. For 2^{48} structures:
   1. We generate four plaintexts M (according to a given receipt of quartet);
   2. We get ciphertexts C;
   3. Each ciphertext undergoes permutation P, so let $T = P(C)$;
   4. Initial filtration. By sorting of T blocks we search for pairs equal on the third and the fifth bytes.
   5. If such pairs do not occur in the structure we generate a next structure (go to 1), or for every pair which has this property we analyse the pair, it is for the S-boxes a, f and h:
      a. If a given S-box is inactive (output difference is zero) we go to the next S-box;
      b. Extra filtration. If output difference (from T) cannot be obtained from the S-box for any input differences taken from the characteristic (for S-box a: 01, for S-boxes f and h: 01, 08 or 09) then we reject the pair and go back to 5;
      c. Finding candidate keys. For a given S-box, output difference (from T) and input differences (like in the sub-point b) we find candidate keys.
   6. For every three S-boxes we concatenate the obtained candidate 8-bit keys to 24-bit values. For every 24-bit value of key obtained in that way we increment a respective value in the counter L.
III. We search for the maximum value in the counter L. It corresponds to the 24-bit of correct three-byte part of 11^{th} round subkey.
IV. If in the counter L there is no unique maximum we generate more structures (go to 1).

Based on the above pseudo-code and the previous analysis we claim that complexity of the presented attack on the full 11-round version of PP-1 cipher is 2^{50} (encryption of 2^{48} structures with four plaintexts each). The result of the attack is 24-bits (three bytes) of the second part of 11th round subkey.

6. Conclusions

In the paper we presented a differential attack on the full 11-round 64-bit version of PP-1 cipher. Its complexity is 2^{50} encryptions with the cipher. It

finds 24 bits of the last round key. In this attack we constructed a 10-round differential characteristic which is nine times concatenation of one-round almost iterative characteristic and "relaxed" final characteristic (this is again similar to the technique used for the GOST cipher [**14**]). Subsequently, almost iterative one-round characteristic is combination of three different one-round iterative characteristics. These one-round characteristics are a consequence of designing a non-linear part of the cipher apart from linear permutation.

These iterative characteristics can be naturally concatenated for an arbitrary number of rounds, and their probability allows conducting a similar attack on the version of the cipher with a longer block length and consequently, a larger number of rounds (see Table 6). In the cipher with longer blocks permutation P is different, but preserves property of exchange of the fifth and the eighth bits in the last S-box (see value in bold in Tables 3–5). Thanks to it, the proposed one-round almost iterative characteristic can be applied to every version of the cipher, with our difference transitions being used always in the last S-box. For the cipher with a 128-bit block (22 rounds) we can concatenate our almost iterative characteristic 20 times, for the 192-bit version (32 rounds) 30 times, and for the 256-bit version (43 rounds) 41 times. By applying the suggested relaxation in the last round we obtain in every above case a characteristic which covers one round less than the full cipher. The probabilities of such characteristics and complexities of attacks on different block length versions are given in Table 15.

Table 15. Probabilities of characteristics of PP-1 cipher with different block lengths.

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

The above analysis shows that the number of rounds suggested for the structure of PP-1 block cipher in every version is insufficient for securing the cipher from a differential attack. To achieve a security level of the cipher on which complexity of a differential attack with the characteristic proposed in the paper would be higher than that of exhaustive search, a number of rounds in the 64-bit version should be at least 12+security margin, because only 12 times concatenation of a given characteristic has the probability (2^{-65}) too small to

perform an attack. Furthermore, a security margin should be at least 4, 5 rounds, because it would prevent the cipher from techniques based on relaxation of characteristic in the last round or adding an extra "free" first round (like in the attack on the full 16-rounds version on DES [**1**]).

In this paper we extend the attacks and the methodology of [**8**] to all versions of PP-1 cipher ever proposed, and explain how this type of advanced differential properties can be extended and exploited in practice to recover the actual keys of all existing variants of PP-1 cipher.

References

[1] Biham E., Shamir A., Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, New York (1993).
[2] Matsui M., Linear Cryptanalysis Method for DES Cipher, EuroCrypt '93, Springer-Verlag (1993).
[3] Matsui M., The first experimental Cryptanalysis of the Data Encryption Standard, CRYPTO '94, Springer-Verlag (1994).
[4] Courtois N. T., Pieprzyk J., Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, AsiaCrypt 2002, Springer-Verlag (2002).
[5] Misztal M., Methods of cryptanalysis of block ciphers,(in polish). Bulletin WAT Cryptology part IV, Warszawa (2004).
[6] McBride L., Q: A Proposal for NESSIE v2.00, submission to NESSIE (2000).
[7] Biham E., Furman V., Misztal M., Rijmen V., Differential Cryptanalysis of Q, FSE 2002, LNCS 2355, Springer-Verlag (2002).
[8] Courtois N. T., Misztal M., Aggregated Differentials and Cryptanalysis of PP-1 and GOST, To appear in 11th Central European Conference on Cryptology (2011), 30 June - 2 July, Debrecen, Hungary.
[9] Chmiel K., Differential and linear methods of cryptanalysis of block ciphers, (in polish), Habilitation dissertation, Poznań (2009).
[10] Chmiel K. Grocholewska-Czuryło A., Stokłosa J., Involutional Block Cipher for Limited Resources, IEEE "GLOBECOM" (2008) – proceedings.
[11] Misztal M., Practical differential cryptanalysis of DES reduced to 8 rounds, (in polish). Bulletin WAT Cryptology part I, Warszawa (1999).
[12] Deamen J., Rijmen V., The Design of Rijndael, Springer-Verlag (2002).
[13] Rijmen V., Cryptanalysis and design of iterated block ciphers, PhD Thesis, October (1997), K.U.Leuven.
[14] Seki H., Kaneko T., Differential Cryptanalysis of Reduced Rounds of GOST, SAC 2000, Springer-Verlag LNCS 2012 (2001): 315.
[15] Misztal M., The S/N ratio in differential cryptanalysis of 9 rounds of DES, Journal of Telecommunications and Information Technology (JTIT) 3 (2006): 49.