Розглядаються дві схеми побудови колізійних rebound атак на Grostl-подібні алгоритми гешування. Пропонується підхід до визначення потрібної кількості циклів для забезпечення стійкості до розглянутих атак. Запропонований підхід застосовується до алгоритму Купина, який прийнято в якості українського національного стандарту гешування ДСТУ 7564:2014. Доводиться, що наявність 5 і більше циклів в кожному з перетворень P і Q цього алгоритму гешування робить його стійким до атаки «зміни напрямку» (rebound attack)

Ключові слова: алгоритм гешування, Grostl, Rijndael-подібні перетворення, колізійна атака, rebound атака

Рассматриваются две схемы организации коллизионных rebound атак на Grostl-подобные алгоритмы хеширования. Предлагается подход к определению необходимого количества циклов в преобразованиях для обеспечения стойкости к рассматриваемым атакам. Предложенный подход применяется к алгоритму Купина, принятому в качестве украинского национального стандарта хеширования ДСТУ 7564:2014. Доказывается, что наличие 5 и более циклов в каждом из преобразований P и Q этого алгоритма хеширования делает его стойкими к атаке «изменения направления» (rebound attack)

Ключевые слова: алгоритм хеширования, Grostl, Rijndael-подобные преобразования, коллизионная атака, rebound атака

UDC 004.056.55
DOI: 10.15587/1729-4061.2017.117684

DEVELOPMENT OF THE APPROACH TO PROVING THE SECURITY OF GROSTL-LIKE HASHING ALGORITHMS TO REBOUND ATTACKS

V. Ruzhentsev
Doctor of Technical Sciences, Associate Professor
Department of information technologies security
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
E-mail: viktor.ruzhentsev@nure.ua
Y. Onishchenko
PhD, Associate Professor*
E-mail: onischenko1980@gmail.com
V. Svitlychnyi
PhD, Associate Professor*
E-mail: vit.svet@ukr.net
*Department of cybersecurity
Kharkiv National University of Internal Affairs
L. Landau ave., 27, Kharkiv, Ukraine, 61080

1. Introduction

Many modern cryptographic primitives, including hashing functions, use Rijndael-like ciphers as a construction element. For example, such hash functions are Whirlpool, Grostl [1], ECHO and Ukrainian standard DSTU 7564:2014 (Kupyna) [2]. The Kupyna was adopted as the Ukrainian standard DSTU 7564:2014 in 2015. Several papers devoted to the analysis of the security of the Kupyna algorithm were published after it was adopted as a standard [3, 4]. This algorithm uses the Rijndael-like block cipher Kalyna [5, 6] as the basic transformation. The block cipher Kalyna was also adopted as the Ukrainian national standard in 2015 (DSTU 7624: 2014). The high-level structure of the compression function is identical to the one used in the Grostl algorithm. A detailed analysis of the Grostl algorithm within the framework of the SHA-3 competition showed that the most effective collision attacks on this hash function with a reduced number of rounds are rebound attacks [7–11]. These attacks use truncated byte differentials (BDs) or truncated byte differential characteristics (BDCs).

Thus, the actual problems are, first, the selection of the criteria for these BDs or BDCs for known collision attacks and, second, the development of methods for determination of the necessary number of rounds in the hashing algorithms to ensure resistance to known rebound attacks. The solution of these problems is the purpose of this work.

2. Literature review and problem statement

The main difference between cryptanalysis of hash functions and cryptanalysis of block ciphers is that there are no keys in hash algorithms unknown to the cryptanalyst, instead, constants are used. Thus, a known-key model is usually used in the hashing algorithms analysis.

Using this model, the cryptanalyst tries to implement one of the following scenarios:

1) show that the value of the hash function differs from random – distinguisher attack;

2) construct a message that has a given hash value – the first preimage attack;

3) construct a message that has the same hash value as the known message – the second preimage attack;

4) construct two messages that have the same hash value – the collision attack.

For the hashing algorithm with the hash code size w, the complexity of the brute force attacks of the first preimage, the second preimage, and the collision is 2^w, 2^w, and $2^{w/2}$, respectively. The hashing algorithm provides resistance to some analytical attacks in the case when the complexity

of this attack is higher than the complexity of brute force attacks.

Many of attack scenarios on hash functions are similar to ideas of differential cryptanalysis and can be described in corresponding terms. For example, the problem of constructing a preimage is the problem of finding two messages which have nonzero input difference and zero output difference. The problem of constructing a collision is the task of finding two messages that have a nonzero difference and their hash codes form a zero difference. The scheme of difference transformation in terms of differential cryptanalysis is called the differential characteristic, or, as in the case of differential attacks on Rijndael-like ciphers, the byte differential characteristic (BDC). The work [12] is devoted to the analysis of BDCs, byte differentials and their probabilities for Rijndael-like ciphers. In [13], an attempt to generalize these results for block ciphers in general was made, and a model of ciphers provably secure against truncated differential attacks was proposed. The results obtained in these papers about the upper bounds of the probabilities of BDCs and byte differentials can also be used in the security analysis of the Grostl-like hashing algorithms.

The absence of unknown keys in hashing algorithms makes it possible to begin the right pair searching for the selected differential or differential characteristics from any internal round. Right pair search is the most effective when it starts from the places where the difference propagation has a low probability. This idea is used in the rebound attack, which was proposed in [7] during the analysis of SHA-3 competition participating algorithms including Grostl. Later, several works offered different improvements of this attack. Thus, it was proposed in [8] to consider a two-round Rijndael-like transformation as a set of 32-to-32 bits substitutions. This made it possible to increase the number of rounds of the attack. In [9], an "internal differential" variant of attacks was proposed. This attack used the similarity of the P and Q transformations in the first version of the Grostl algorithm. After the modernization of the Grostl algorithm (in [1], an improved algorithm is presented), the final known variant of the collision attack was proposed in [10]. A fundamentally new scheme for constructing a rebound attack was proposed in [11]. The attack from [11] is the most effective for the considered kind of hashing algorithms at the moment.

The Kupyna hash algorithm [2] was adopted as the Ukrainian standard DSTU 7564:2014 in 2015. This algorithm uses base transformations of the Kalyna block cipher (the Ukrainian standard DSTU 7624:2014). As compared with other hashing algorithms, Kupyna has a high-level structure similar to Grostl. Several papers on Kupyna security analysis have already been published [3,4] since its adoption. The preimage attack and the collision attack performed according to the scheme from [9] were proposed in [3]. Modification of the attack from [9] was also proposed in [4].

At the same time, the presence of attack descriptions in [3, 4, 7–11] does not answer the questions about the possible further improvement of rebound attacks for Grostl-like hashing algorithms and about the approach to determining the necessary number of rounds to ensure resistance to these attacks. The work is devoted to the search for answers to these questions.

3. The aim and objectives of the study

The aim of this work is to research properties of BDC, which can be used in different kinds of rebound attacks, and to propose the ways of proving the security of Grostl-like hash algorithms against collision rebound attacks.

To achieve this aim, it is necessary to accomplish the following objectives:

– to analyze known collision attacks on Grostl-like hashing algorithms and detect the necessary conditions for performing these attacks;

– to determine the boundary numbers of rounds in the transformations P and Q, which are necessary to ensure security;

– to perform a security proving for the Kupyna algorithm against collision rebound attacks.

4. Grostl-like hashing algorithms and the Kupyna algorithm

The traditional general scheme for generating the hash value (Fig. 1) and the compression function scheme from the Grostl algorithm [1] (Fig. 2) were taken as a basis for building the Kupyna algorithm.

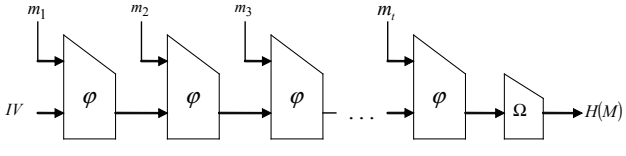

Fig. 1. The traditional general scheme for generating the hash value

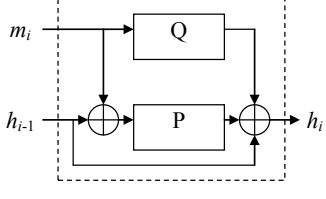

Fig. 2. The scheme of compression function ϕ for the Grostl algorithm

In Fig. 1:

m_i – blocks of messages;

IV – initial vector;

φ – compression function;

W – the transformation, which consists in discarding the upper half of the digits;

$H(M)$ – hash value.

In Fig. 2:

h_i – variable, the value of which is obtained by processing the i-th block of the message, $h_0=IV$;

P and Q are Rijndael-like block encryption algorithms, in which constants are used instead of the round keys.

Rijndael-like ciphers it mean ciphers with four main transformations of Rijndael in each round. These transformations are: byte substitution ByteSub (BS); cyclic shift of rows in the matrix representing the data block by a different number of bytes – ShiftRows (SR); multiplying each column of the matrix representing the data block by a fixed matrix – MixColumns (MC); adding a data block

with a subkey of the appropriate size – AddKey. Depending on the size of the block, the number and size of the columns may vary.

There are two kinds of the Kupyna hashing algorithm: Kupyna-256 with the 256-bit hash value and block size for *P* and *Q* transformations of 512 bits and Kupyna-512 with a hash size of 512 bits and a block size for *P* and *Q* transformations of 1024 bits. *P* and *Q* transformations of Kupyna-256 contain 10 rounds, for Kupyna-512 – 14 rounds.

As the *P* and *Q* transformations, modifications of the Rijndael-like block cipher Kalyna [5, 6] are used. For the 512-bit block, the same transformations as the Kalyna cipher are used in the *P* and *Q* transformations, but instead of the round key addition, addition with constants is performed. Constants are different for the *P* and *Q* transformations. Moreover, addition with constants in the transformation *P* is performed using the XOR operation, and addition by modulo 2^{64} is performed in the *Q* transformation.

Grostl-like hashing algorithms will be called algorithms that use the same compression scheme as the Grostl algorithm (Fig. 2), and the *P* and Q transformations are Rijndael-like.

The main differences of Kupyna from Grostl are the following:

1) using of modular addition instead of XOR in the *Q* transformation;

2) using of similar shift values in ShiftRows of *P* and *Q* transformations;

3) key constants used in *P* and *Q* transformations are different in all bytes;

4) using of 4 different non-algebraically built substitutions in SubBytes.

A more detailed description of Kupyna can be found in [2–4].

5. Rebound attacks on Groesl-like hashing algorithms

Any known rebound attack uses the byte differential characteristic (BDC). The construction of the right pair in rebound attacks is performed in two stages, which are called inbound and outbound. These phases correspond to different parts of BDC. The inbound part often covers a part of BDC which has the lowest probability. The outbound parts should have a high probability. Selection of the right pair starts with the inbound part. Then, each pair that satisfies the inbound part of BDC, is checked against the outbound parts. It can be two outbound parts: initial and final.

There are two known schemes for organizing rebound attacks for the Grostl algorithm. In the first scheme, the right pair must contain the same input and output differences. We denote the number of active bytes at the input and output as *a* and represent such BDC as $a \to ... \to a$. This type of BDC covers *P* and *Q* transformations and it is used in the attacks [7, 8, 10]. Fig. 3 explains the considered scheme of organization of a rebound attack.

The message blocks M_0 have a non-zero difference in the shaded bytes in Fig. 3. Next, in the attack, the pairs of blocks that match the inbound part of the BDC are searched. Then the found pair is checked for compliance with the outbound parts of the BDC. In the case of matching, the difference in the blocks obtained at the output of the transformations P and Q is verified (in Fig. 3 these blocks are on the right). If the output differences are the same, a collision pair is built: the message blocks M_0 can be added to the beginning of any message, and the messages received as a result of this addition will have the same hash code.

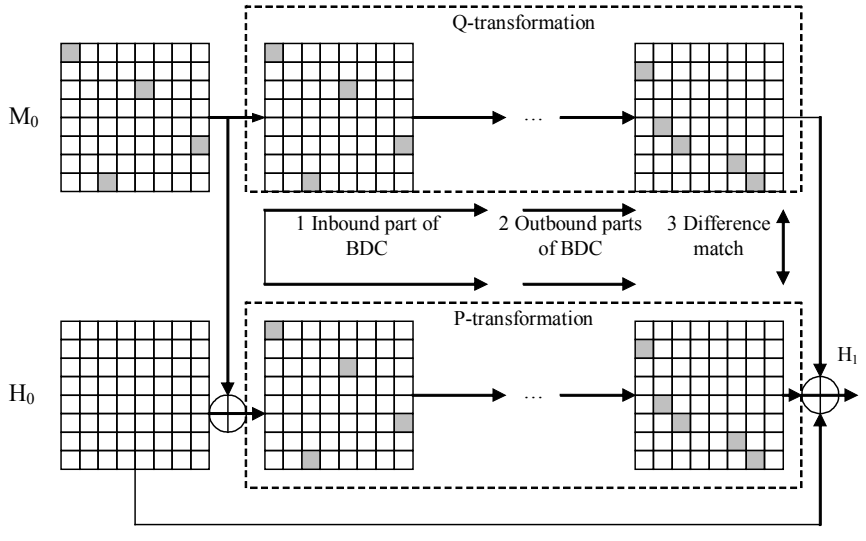

Fig. 3. Scheme of organization of a rebound attack $a \to ... \to a$

The second scheme of the attack was proposed in [11]. BDC contains all active bytes at the input and some number of active bytes at the output. We denote this number as *a*. The BDC covers only the P transformation in this scheme. The active output bytes contain the equal difference with bytes at the corresponding positions at the input. Addition of input and output values results to zero difference in these bytes. The goal of the second scheme is to reset all the input active bytes in a few iterations. Fig. 4, taken from [11], explains the attack.

Note that in this case, the input difference is fixed and cannot be selected in the process of constructing a pair in contrast to the first scheme of BDC. The second scheme of BDC will be denoted as $m^2 \to ... \to a$. Fig. 5 illustrates one iteration of this scheme of attack.

The process of assessment of the expected number of right (collision) pairs was clearly explained in [6]. To determine the expected number of right pairs for selected BDC N_{pairs_BDC}, it is necessary, first, to determine the total number of input pairs N_{pairs_inp} which can be constructed for the input difference, second, multiply this number by the probability of the selected BDC P_{BDC}, and, third, multiply it by the probability of a full match of the input and output differences P_{match}, i. e.:

$$N_{pairs\_BDC} = N_{pairs\_input} \cdot P_{BDC} \cdot P_{match}. \quad (1)$$

The attack is effective if the expected number of pairs calculated in accordance with (1) is at least 1, and the complexity is not higher than the complexity of the brute force attack.

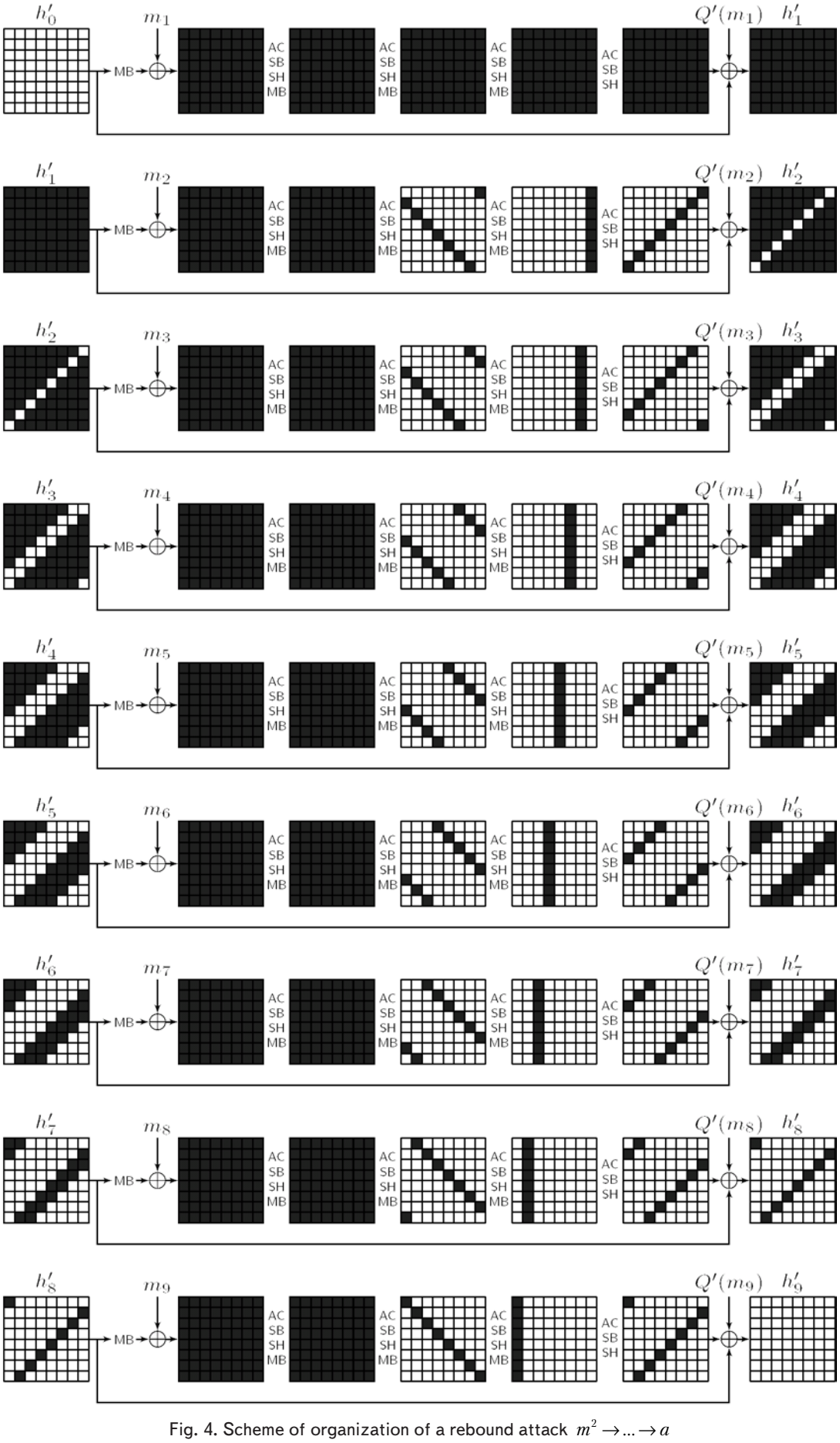

Fig. 4. Scheme of organization of a rebound attack $m^2 \to ... \to a$

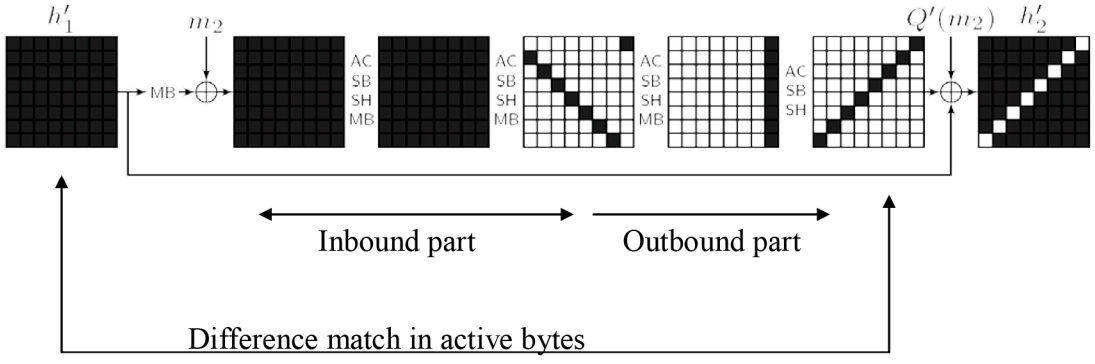

Fig. 5. One iteration of the scheme of organization of a rebound attack $m^2 \to ... \to a$

6. Development of the approach to determine the required number of rounds to ensure the security against rebound attacks

The proposed approach to security estimation is as follows. On the one hand, in accordance with the above-formulated criterion of security, the value of the expression (1) must be less than 1. On the other hand, there are known restrictions on the probability of BDC and byte differentials for Rijndael-like ciphers from [12, 13]. Using this knowledge, we will try to determine the boundary number of rounds for the inbound and outbound parts of the BDC, in which the known rebound attacks will not be effective.

The Grostl-like hash algorithm which uses a Rijndael-like block cipher with a block size of $m \times m$ bytes will be considered in this section. General restrictions for BDCs which could be used in $a \to ... \to a$ and $m^2 \to ... \to a$ schemes of rebound attack will be analyzed here.

6. 1. The restrictions for BDC used

In accordance with the proposed model [13] of Rijndael-like ciphers with 3 or more rounds secure from truncated differential attacks, the probability of BDC can not be higher than

$$p_{rand} \approx \left(2^{-8}\right)^u,$$

where u is the number of inactive bytes in the output difference. Thus, if BDC contains more than three rounds, its probability P_{BDC}:

$$P_{BDC} \le p_{rand} = 2^{-8(m^2-a)}.$$

6. 1. 1. BDC $a \to ... \to a$

For the scheme $a \to ... \to a$, $P_{match} = 2^{-8a}$. The maximum number of input pairs is

$$N_{pairs_{input}} = 2^{8a} \cdot 2^{8m^2} = 2^{8m^2+8a}.$$

By substituting these values in the expression (1), we will get the maximum possible number of right pairs for the selected BDC

$$N_{pairs_{BDC}} = 2^{8a}.$$

Assuming that the expected number of right pairs for the selected BDC should be not less than 1, it is possible to determine the limit value for the BDC probability under these conditions:

$$P_{\text{BDC}} \ge 2^{-8a} \cdot p_{rand} = 2^{-8m^2}. \quad (1)$$

Now, some structural features of BDC on the basis of the presented restrictions on the BDC probability can be selected. To do this, we define the probabilities of major difference transitions that can occur in the BDC (Table 1).

Table 1

Probabilities of difference transitions

Difference transitions	Number of active bytes in the input difference	Number of active bytes in the output difference	Probabilities of difference transitions
$m^2 \to m$	m^2	m	$P_{m^2 \to m} = 2^{-8(m^2-m)} = 2^{-8m^2+8m}$
$m \to 1$	m	1	$P_{m \to 1} = 2^{-8(m-1)} = 2^{-8m+8}$
$b \to (b-1)$	b	$b-1$	$P_{b \to (b-1)} \approx 2^{-8}$

The following statements about the BDC structure can be proved using the expressions (2) and the data from Table 1.

Statement 1. For the scheme $a \to ... \to a$, BDC, which is used in an attack, may not contain two or more difference transitions $m^2 \to m$.

Statement 2. For the scheme $a \to ... \to a$, BDC, which is used in an attack, may not contain 1 difference transitions $m^2 \to m$ and 2 or more difference transitions $m \to 1$.

Statement 3. For the scheme $a \to ... \to a$, BDC, which is used in an attack, may not contain 1 transition $m^2 \to m$, 1 transition $m \to 1$ and 2 or more transitions $b \to (b-1)$ for any b: $2<b<m^2$.

6. 1. 2. BDC $m^2 \to ... \to a$

For this scheme, the input BDC difference has a fixed value, so the number of possible input pairs is $N_{pairs\_input} = 2^{8m^2}$.

Match probability is $P_{match} = 2^{-8a}$.

If the BDC contains 3 or more rounds, then in accordance with the proposed model [13] of Rijndael-like ciphers secure from truncated differential attacks, the maximum BDC probability is limited by p_{rand}, i. e.:

$$P_{BDC} \le p_{rand} = 2^{-8(m^2-a)}.$$

By substituting these values to the expression (1), we will get the maximum possible number of right pairs for the selected type of BDC $N_{pairs\_BDC} = 1$.

The main conclusion is that the probability of BDC $m^2 \to ... \to a$ must be maximum $P_{BDC} = p_{rand} = 2^{-8(m^2-a)}$. Otherwise, the expected number of right pairs would be less than 1.

6. 2. Estimation of the maximum number of rounds for the inbound part of BDC

Table 2 summarizes the complexities of construction of the right pairs for the inbound part of BDC, which often has the structure $m \to m^2 \to ... \to m^2 \to m$.

Table 2

Complexities of construction of the right pairs for the inbound part of BDC

Number of rounds in the inbound part	Complexity
2	2^4
3	2^{8m}
4	2^{4m^2}

Estimations were obtained by using papers [7–11].

The data from Table 2 show that the inbound part can cover at most 4 rounds. However, the complexity in the case of 4 rounds is too high (for the block size of w bits, the complexity is $2^{w/2}$). Only the 3-round inbound part can be used in most cases.

These estimations are fair for both considered types of BDC.

In almost all known attacks with the scheme of BDC $a \to ... \to a$, the scheme of the inbound phase is

$$m \to m^2 \to ... \to m^2 \to m.$$

We can estimate the maximum number of pairs which could be built for the inbound part of BDC:

$$N_{pairs_{BDC_{inbound}}} = N_{pairs\_input\_inbound} \cdot P_{BDC\_inbound} =$$
$$= 2^{8m^2+8m} \cdot 2^{-8m^2+8m} = 2^{16m}. \quad (3)$$

The scheme of the inbound phase for BDC $m^2 \to ... \to a$ is $m^2 \to ... \to m^2 \to m$. The maximum number of pairs which could be built for such inbound part of BDC is:

$$N_{pairs_{BDC_{inbound}}} = 2^{8m^2} \cdot 2^{-8m^2+8m} = 2^{8m}. \quad (4)$$

6. 3. Estimation of the maximum number of rounds for the outbound part of BDC

6. 3. 1. BDC $a \to ... \to a$

The BDC with the inbound part

$$m \to m^2 \to ... \to m^2 \to m$$

is considered here.

Even if the outbound parts of BDC will have the maximum probability

$$P_{BDC_{outbound}} = 1,$$

then, with $P_{match} = 2^{-8a}$ and $N_{pairs_{BDC_{inbound}}} = 2^{16m}$ (3), the expected number of pairs will be

$$N_{pairs\_BDC} = 2^{16m-8a}.$$

This means that for at least one right pair to exist even if $P_{BDC\_outbound} = 1$, the following condition must always hold

$$a < 2m. \quad (5)$$

Now, we define a restriction on the probability of the outbound part of BDC. If we denote the probability of the outbound part of BDC as

$$P_{BDC_{outbound}} = 2^{-8x},$$

then the expected number of right pairs will be

$$N_{pairs_{BDC}} = 2^{16m-8a-8x},$$

and it must be greater than 1. It means that the following condition must hold: $x \le 2m - a$.

Now we consider possible values of the parameter a in (5). Since the inbound part has a structure

$$m \to m^2 \to ... \to m^2 \to m$$

that has by m active bytes at its outputs, we consider two situations: the first – $m<a<2m$; the second – $a<=m$.

The first situation: $m<a<2m$.

In this case, the input of the first MC transformation and the output of the last MC transformation of BDC must have at least 2 active columns (because a is bigger than m). According to [12, 13], for each of the $2m-a$ passive output bytes of the MC, the probability of BDC will decrease by about 2^8 times. Then the expected number of pairs for BDC will be

$$N_{pairs\_BDC} = 2^{16m-8a} \cdot 2^{-8(2m-a)} \cdot 2^{-8(2m-a)} = 2^{-16m+8a}.$$

This number is significantly lower than 1 as the condition (5) holds. Hence, the situation where $m<a<2m$ is impossible.

The second situation: $a<m$.

In this case, the following statement is true.

Statement 4. In the case of $a \to ... \to a$ BDC with

$$m \to m^2 \to ... \to m^2 \to m$$

inbound part, the outbound part of BDC can not contain any single MC transformation with more than one active column.

Proof. Suppose that the initial or the final part of the BDC has MC transformation with two active columns, and at the end and at the beginning of BDC a ($a<m$) active bytes must be obtained. For each of the $2m-a$ passive bytes at the output of the BDC, the probability will decrease by 2^8 times. In the second half of the outbound part, reduction of the number of active bytes from m to a must also occur. Then, taking into account $P_{match} = 2^{-8a}$, the number of right pairs for the inbound part of BDC

$$N_{pairs\_BDC\_inbound} = 2^{16m},$$

the expected number of pairs for the whole BDC will be

$$N_{pairs\_BDC} = 2^{16m-8a} \cdot 2^{-8(2m-a)} \cdot 2^{-8(m-a)} = 2^{-8m+8a}.$$

As $a<m$, the value N_{pairs_BDC} is much less than 1 and it is hard to find a right pair in this case. With the increase in the number of active columns in the outbound parts of the BDC,

the expected number of pairs will decrease even more. The statement is proved.

Now, using the statement 4, we can estimate the maximum possible number of rounds for the outbound part. In accordance with the scheme of the inbound part of BDC, there are m active bytes at the beginning of each of the two outbound parts of BDC. It can be seen that the following sequence of transformations could be performed until we have only one active column: MC_0–AC_1–SB_1–SR_1–MC_1–AC_2–SB_2–SR_2, where the output of MC_0 is the output of the inbound part of BDC. The MC_1 outputs m active bytes and SR_2 puts them to different columns.

By reducing the probability by $2^{8(m-1)}$ times, this sequence can be extended for another one round: MC_0–AC_1–SB_1–SR_1–MC_1–AC_2–SB_2–SR_2–MC_2–AC_3–SB_3–SR_3. In this case, MC_1 performs the transition from m active bytes to 1 with probability $2^{-8(m-1)}$; MC_2 makes a transition 1 to m and SR_3 distributes these m bytes to different columns. Similar discourses can be used for the movement in the opposite direction from the exit of the inbound part to the top of BDC. It can be seen that the following sequence of transformations could be performed until we have only one active column:

$$MC_0^{-1} - AC_1^{-1} - SB_1^{-1} - SR_1^{-1} - \\ -MC_1^{-1} - AC_2^{-1} - SB_2^{-1} - SR_2^{-1} - MC_2^{-1}.$$

By reducing the probability by $2^{8(m-1)}$, times this sequence can be extended for another one round:

$$MC_0^{-1} - AC_1^{-1} - SB_1^{-1} - SR_1^{-1} - MC_1^{-1} - AC_2^{-1} - \\ -SB_2^{-1} - SR_2^{-1} - MC_2^{-1} - AC_3^{-1} - SB_3^{-1} - SR_3^{-1} - MC_3^{-1}.$$

To summarize the presented arguments, neither the initial nor the final part of the outbound part of BDC can not contain 3 or more rounds of complete transformation.

The same conclusion can be made in a different way, using the proposed model of ciphers protected from truncated differential attacks from [13]. In accordance with this model, for the BD probabilities for Rijndael-like ciphers with 3 or more rounds and with a such a block structure, the boundary value of probability is

$$p_{rand} \approx \left(2^{-8}\right)^u,$$

where u is the number of passive bytes in the output difference. In the considered type of BDC, $u=m^2-a$. Taking into account

$$P_{match} = 2^{-8a}$$

and the number of right pairs for the inbound part of BDC $N_{pairs\_BDC\_inbound} = 2^{16m}$ (3), we can obtain the expected number of correct pairs

$$N_{pairs\_BDC} = 2^{16m-8a} \cdot 2^{-8(m^2-a)} = 2^{-8m^2+16m}. \quad (6)$$

If $m>2$, the expression (6) is much less than 1, and it means that an attack is impossible.

The following statement summarizes the results obtained in this subsection.

Statement 5. In the case of $a \to ... \to a$ BDC with $m \to m^2 \to ... \to m^2 \to m$ inbound part, the following conditions must hold for the outbound part of BDC:

1) $a<=m$, where a is a number of active bytes at the input and output of BDC;

2) neither the initial nor the final outbound parts of BDC can not contain more than 3 full rounds.

6. 3. 2. BDC $m^2 \to ... \to a$

The feature of this type of BDC is that the input difference is fixed and it has many active bytes. Therefore, the probability that exactly this difference can be obtained at the start of BDC from some right pairs for the inbound part of BDC is very low. For this reason, in a certain attack scenario [11], the initial outbound part of BDC is absent. Thus, BDC consists of two parts: the inbound part and the outbound final part.

According to the conclusion in subsection 6.1.2, the BDC probability should be approximately equal to p_{rand}. Therefore, if the inbound part has the scheme

$$m^2 \to ... \to m^2 \to m,$$

the final number of active bytes should be not higher than m to get at least one right pair. As it was shown in the previous subsection 6.3.1, after the transition m^2 to m bytes, it is possible to save the situation with only 1 active column without loss of probability during the transformations MC0–AC1–SB1–SR1–MC1–AC2–SB2–SR2, where the output of MC0 is the output of the inbound part of BDC.

The following statement summarizes the results obtained for the outbound part of BDC $m^2 \to ... \to a$.

Statement 6. In the case of $m^2 \to ... \to a$ BDC with

$$m^2 \to ... \to m^2 \to m$$

inbound part, the following conditions must hold for outbound part of BDC:

1) $a<=m$;

2) the final outbound part of BDC can not contain 2 or more full rounds.

7. Security estimation of Kupyna hash algorithm

Security estimation of Kupyna was performed using the statements 5 and 6.

The first scheme of collision rebound attack on Grostl has been shown in [7]. Used in this scheme BDC covers the transformations P and Q and we note such BDC as $a \to ... \to a$ in this work. Statement 5 can be used to estimate the necessary number of rounds to achieve resistance to the rebound attack. The maximum number of rounds is 3 for the inbound part and 2.5+2.5=5 for the outbound parts. So, the overall number of rounds is 8 for P and Q transformations. Thus, each of P and Q transformations may contain 4 rounds at most.

The second scheme of attack was proposed in [11]. In this scheme BDC $m^2 \to ... \to a$ should cover the transformation P. Statement 6 can be used to estimate the necessary number of rounds to achieve resistance to the rebound attack. The maximum number of rounds will be 3 for the inbound part and 1.5 for the outbound parts. So, the overall number of rounds is 4.5 for the P transformation. Thus, each of P and Q transformations may contain 5 rounds to be secure against the second scheme of rebound attack.

8. Comparison with known results about security of Grostl-like hashing algorithms to collision rebound attacks

The main research results are statements 5 and 6, proven for Grostl-like hashing algorithms, which determine the minimum number of rounds necessary to ensure resistance to collision rebound attacks discussed in the paper.

The conclusion about the security of Kupyna and Grostl to rebound attacks with the scheme of BDC $a \to ... \to a$ fully agrees with known results from the works [7–10]. The best known such attack allows building a collision with less complexity than the brute force attack for the case where the P and Q transformations contain 3 rounds each.

The rebound attacks presented in the works [3,4] on 5-rounds Kupyna and in [11] on 5-rounds Grostl with the scheme $m^2 \to ... \to a$ disagree with the presented results because the BDC with the expected number of right pairs 2^{-56} is used in these attacks. To compensate such a low probability of BDC, the length of the message was increased. As a result, the authors estimate that the collision may be constructed for messages that contain 2^{59} blocks, which is almost impossible to implement in practice. Thus, in our opinion, the presented results are consistent with the known.

The practical significance of the proposed approach is that it allows determining the necessary number of rounds at which the collision rebound attack will not be effective for Grostl-like hashing algorithms.

The first defect of the proposed approach is that only the version of the Rijndael-like cipher with the block size of $m \times m$ bytes is analyzed, but in practice other variants may also occur. The second defect is related to the fact that the used constraints on the probability of BDC from [12, 13] were obtained for Rijndael-like ciphers that used the XOR-addition operation with a key, while in the Q transformation of the Kupyna algorithm, addition by modulo 2^{64} is used. In some cases, these differences may lead to inaccurate results for the scheme $a \to ... \to a$ of attack. Elimination of these defects will be the aim of future research.

9. Conclusions

1. Two schemes of organization of collision rebound attacks on Grostl-like hashing algorithms are considered in the work. The necessary conditions for effective attacks are defined for these schemes:

1) the complexity must be lower than the complexity of brute force attacks;

2) the value of the expression (1) must be greater than 1.

2. The boundary number of rounds in the transformations P and Q, which is necessary for ensuring security, is determined. For both considered attack schemes, the inbound part of the BDC can not contain more than 3 rounds. The boundary number of rounds in the outbound parts of the BDC is determined for the scheme $a \to ... \to a$ in the statement 5, and for the scheme $m^2 \to ... \to a$ in the statement 6.

3. The developed approach to security estimation of Grostl-like hashing algorithms to collision rebound attacks is applied to the Kupyna-256 algorithm. The presence of 5 or more rounds in each of the P and Q transformations of this hash algorithm makes it resistant to rebound attacks.

References

1. Groestl – a SHA-3 candidate [Electronic resource]. – Available at: http://www.groestl.info
2. Oliynykov, R. A new standard of Ukraine: The Kupyna hash function [Electronic resource] / R. Oliynykov, I. Gorbenko, O. Kazymyrov, V. Ruzhentsev, O. Kuznetsov, Y. Gorbenko et. al. // Cryptology ePrint Archive. – 2015. – Available at: http://eprint.iacr.org/2015/885
3. Dobraunig, C. Analysis of the Kupyna–256 Hash Function [Electronic resource] / C. Dobraunig, M. Eichlseder, F. Mendel // Cryptology ePrint Archive. – 2015. – Available at: http://eprint.iacr.org/2015/956
4. Zou, J. Cryptanalysis of the Round-Reduced Kupyna Hash Function [Electronic resource] / J. Zou, L. Dong // Cryptology ePrint Archive. – 2015. – Available at: http://eprint.iacr.org/2015/959
5. Granger, R. On the discrete logarithm problem in finite fields of fixed characteristic [Electronic resource] / R. Granger, T. Kleinjung, J. Zumbrägel // Cryptology ePrint Archive. – 2015. – Available at: https://eprint.iacr.org/2015/685
6. Oliynykov, R. Results of Ukrainian national public cryptographic competition [Text] / R. Oliynykov, I. Gorbenko, V. Dolgov, V. Ruzhentsev // Tatra Mountains Mathematical Publications. – 2010. – Vol. 47, Issue 1. doi: 10.2478/v10127-010-0033-6
7. Mendel, F. The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl [Text] / F. Mendel, C. Rechberger, M. Schläffer, S. S. Thomsen // Lecture Notes in Computer Science. – 2009. – P. 260–276. doi: 10.1007/978-3-642-03317-9_16
8. Gilbert, H. Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations [Text] / H. Gilbert, T. Peyrin // Lecture Notes in Computer Science. – 2010. – P. 365–383. doi: 10.1007/978-3-642-13858-4_21
9. Peyrin, T. Improved Differential Attacks for ECHO and Grøstl [Text] / T. Peyrin // Lecture Notes in Computer Science. – 2010. – P. 370–392. doi: 10.1007/978-3-642-14623-7_20
10. Schlaffer M. Updated Differential Analysis of Groestl [Electronic resource] / M. Schlaffer // Groestl website. – 2011. – Available at: http://groestl.info/groestl-analysis.pdf
11. Mendel, F. Collision Attack on 5 Rounds of Grøstl [Text] / F. Mendel, V. Rijmen, M. Schläffer // Lecture Notes in Computer Science. – 2015. – P. 509–521. doi: 10.1007/978-3-662-46706-0_26
12. Ruzhentsev, V. Towards Provable Security of Rijndael-Like Spn Ciphers Against Differential Attacks [Text] / V. Ruzhentsev, V. Dolgov // Tatra Mountains Mathematical Publications. – 2012. – P. 53, Issue 1. doi: 10.2478/v10127-012-0046-4
13. Ruzhentsev, V. The conditions of provable security of block ciphers against truncated differential attack [Text] / V. Ruzhentsev // Studia Scientiarum Mathematicarum Hungarica. – 2015. – Vol. 52, Issue 2. – P. 176–184. doi: 10.1556/012.2015.52.2.1307