An Integral Distinguisher on Grøstl-512 v3*

Marine Minier[1] and Gaël Thomas[2]

[1] Université de Lyon, INRIA
INSA-Lyon, CITI, F-69621, Villeurbanne, France
marine.minier@insa-lyon.fr
[2] XLIM (UMR CNRS 7252), Université de Limoges
123 avenue Albert Thomas, 87060 Limoges Cedex - France
gael.thomas@unilim.fr

Abstract. This paper presents an improved integral distinguisher using 2^{913} computations against an 11-round version of the compression function of the SHA-3 candidate Grøstl-512 with the round 3 parameters. The original result presented in [18] was enhanced through the use of different integral properties.

Keywords: Hash functions, cryptanalysis, integral distinguishers, SHA-3 competition.

1 Introduction

The entire cryptographic community has been waiting until last October for the outcome of the SHA-3 competition[1]. Among the finalists, Grøstl [13] is a surviving proposal designed by P. Gauravaram et al. It is based on AES transformations and outputs 256 or 512 bits of hash according to the Grøstl-256/512 version.

During the second round, Grøstl has attracted a significant amount of cryptanalysis. For example, T. Peyrin presented rebound distinguishers against full version of the compression function Grøstl-256 [20]. This is one of the main reasons that forced the Grøstl designers to modify the parameters of Grøstl for the SHA-3 round 3. In the remainder of this paper, we refer to this last version as Grøstl v3 whereas the previous version is called Grøstl v2. Results against the compression function of Grøstl-256 v3 include a semi-free-start collision against 6 rounds that uses 2^{180} computations [22], a pseudo preimage against 8 rounds that uses $2^{507.32}$ computations [21], a rebound distinguisher against 10 rounds that uses 2^{392} computations [14], and an integral distinguisher against 11 rounds that requires 2^{953} computations [18]. In this paper, we improve this last distinguisher leading to an integral distinguisher on 11 rounds of the compression function of Grøstl-512 v3 with a complexity of 2^{913} computations.

* This work was partially supported by the French National Agency of Research: ANR-11-INS-011.

[1] see for example: http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

G. Paul and S. Vaudenay (Eds.): INDOCRYPT 2013, LNCS 8250, pp. 50–59, 2013.

This paper is organized as follows: Section 2 introduces related work, notations of the paper and the description of Grøstl-512; Section 3 describes the integral distinguisher against Grøstl-512 v3 reduced to 11 rounds and finally Section 4 concludes this paper.

2 Related Work and Notations

2.1 Integral Attacks

Integral cryptanalysis was first introduced against the Square block cipher in the original paper [6] in the unknown key setting to retrieve information on some key bytes. Then, it was applied to AES in the original submission paper [7,8]. The original integral property on AES was extended by one round by Ferguson et al. in [10].

After those first attacks, many ciphers especially the ones that use a SPN structure have been studied with regard to this kind of distinguishers. Among all the integral cryptanalyses proposed in the literature, we could cite the attacks against SAFER [2], CRYPTON [9] and more recently on PRESENT [5]. The different Rijndael versions (Rijndael-192 and Rijndael-256) have also been attacked using integral properties [15,11]. Other contributions also analyze the general framework of Integral cryptanalysis and especially focus on the conditions that a block cipher must fulfill to be attacked using this method [17,3]. In [17], L. Knudsen and D. Wagner analyze integral cryptanalysis as a dual to differential attacks particularly applicable to block ciphers with bijective components. A first-order integral cryptanalysis considers a particular collection of m words in the plaintexts and ciphertexts that differ on a particular component. The aim of this attack is thus to predict the values in the sums (i.e. the integral) of the chosen words after a certain number of rounds of encryption. The same authors also generalize this approach to higher-order integrals: the original set to consider becomes a set of m^d vectors which differ in d components and where the sum of this set is predictable after a certain number of rounds. The sum of this set is called a d-th order integral.

More recently, in [16] Integral cryptanalysis has been proposed in the new model called known key settings where the key is known to the attacker. In the same settings, compression functions of hash functions could also be analyzed and some distinguishers have been proposed against SHA-3 candidates also using integral properties. Consider for instance integral distinguishers on the compression functions of Hamsi-256 [1,19] and Keccak [4].

2.2 Notations

In the remainder of this paper, we use the consistent notations introduced in [17] and extend them for expressing word-oriented integral attacks. For a d-th order integral, we have:

- The symbol 'C' (for "Constant") in the i-th entry, means that the values of all the i-th words in the collection of texts are equal.

- The symbol 'P' (for "Permutation") means that all words in the collection of texts are different.
- The symbol '?' means that the sum of words cannot be predicted.
- The symbol 'P^d' corresponds to the components that participate in a d-th order integral, i.e. if a word can take m different values then $\mathcal{P}^d$ means that in the integral, the particular word takes all values exactly m^{d-1} times.
- The symbol '0' means that the sum of all values is zero.

2.3 Description of the Grøstl-512 Hash Function

Grøstl [12] is a SHA-3 candidate designed by Guaravaram *et al.*, notably Grøstl-256 outputs hash values of lengths 224 and 256 bits whereas Grøstl-512 outputs hash values of lengths 384 or 512 bits. We focus on Grøstl-512. It is an iterated hash function with a compression function built from two distinct permutations P and Q. A t-block message (after padding) $(M_1, \cdots, M_t)$ is hashed by computing successive chaining values H_i using the compression function $f(H_{i-1}, M_i)$ and then applying the output transformation $g(H_t)$ as follows:

$$\begin{aligned} H_0 &= IV \\ H_i &= f(H_{i-1}, M_i) = H_{i-1} \oplus P(H_{i-1} \oplus M_i) \oplus Q(M_i) \text{ for } 1 \leq i \leq t \\ h &= g(H_t) = trunc(H_t \oplus P(H_t)) \end{aligned}$$

where $trunc(\cdot)$ denotes the function that truncate its input by returning only the last 384 (or 512) bits.

The two permutations P and Q are constructed using the wide trail strategy, their design is very similar to AES with a fixed key input. Both permutations of the compression function of Grøstl-512 act on a 1024-bit state represented as a 8×16 matrix of bytes and have 14 rounds. The round transformations of Grøstl-512 are the following ones:

- AddRoundConstant (AC) adds a round-dependent constant to the state of P and Q.
- SubBytes (SB) is the non-linear layer that applies the AES Sbox to each byte of the state.
- ShiftBytes (ShB) rotates the bytes of row j in the following way: 0 for $j = 1$, 1 for $j = 2, \cdots 6$ for $j = 7$ and 11 for $j = 8$ for the P permutation and the shifted values are 1, 3, 5, 11, 0, 2, 4, 6 for the Q permutation.
- MixBytes (MB) is the linear diffusion layer where each column of the state is multiplied by a constant matrix B.

Note that the differences between Grøstl-512 v2 and the new version of Grøstl-512, Grøstl-512 v3 are localized in the two transformations AddRoundConstant and ShiftBytes.

3 Description of the 11-Round Distinguisher of the Grøstl-512 v3 Compression Function

3.1 The Divide-and-Conquer Method to Find Integral Properties

In [18], the authors propose a divide-and-conquer method to efficiently find integral properties on several rounds of an AES-like cipher or hash function. Their method works as follows: first, find some integral properties that sum to 0 before the last MixColumns (or MixBytes) operation. Then, combine several integral properties that sum together to 0 on a complete column and apply the MixColumns (or MixBytes) operation to fulfill the integral property. One thus obtain finally an integral property on a complete number of rounds.

3.2 Integral Properties for P and Q in the Forward Direction

We apply this method to the case of Grøstl-512 v3 and we find, for P and Q, the integral properties for 3.5 rounds shown in Fig. 1. In fact, we find the following integral properties with two active bytes for P:

- when the two active bytes are in position (0,0) and (1,1), then after 3.5 rounds, the bytes on three shifted columns have their sum equal to 0. This property also holds for two active bytes at positions (3,0) and (4,1); (5,0) and (6,1); (0,1) and (5,6); (7,1) and (0,6); (7,0) and (1,6). All those properties lead to three zero-sum shifted columns.

and the following integral properties with two active bytes for Q:

- when the two active bytes are in position (0,0) and (5,1), then after 3.5 rounds, the bytes on three shifted columns have their sum equal to 0. This property also holds for two active bytes at positions (1,0) and (6,1); (2,0) and (7,1); (4,0) and (0,1); (3,0) and (0,6); (3,1) and (4,6); (4,1) and (2,6). All those properties lead to three zero-sum shifted columns.

Thus, we can combine those two bytes 3.5-round integral properties to mount integral properties on 4 rounds with respectively 12 active bytes for P and 14 active bytes for Q using the divide-and-conquer method of [18]. The deduced integral properties for P and Q are shown in Fig. 2. We are hence able to distinguish P and Q from random permutations using respectively 2^{96} and 2^{112} chosen texts that sum to 0 at byte level on three particular columns (i.e. on 192 bits) after four applications of the round function of P (respectively Q). This distinguisher has a complexity equal to 2^{96} cipher operations for P and 2^{112} cipher operations for Q.

Following the work of [15], we extended by two rounds at the beginning those 4-round integral properties using first a 24-th order integral property and second a 104-th order integral property as shown on Fig 3. We were able to distinguish P and Q from random permutations using 2^{832} chosen texts that sum to 0 at byte level on three particular columns (i.e. on 192 bits) after six applications of the round function of P (respectively Q). This distinguisher has a complexity equal to 2^{832} cipher operations.

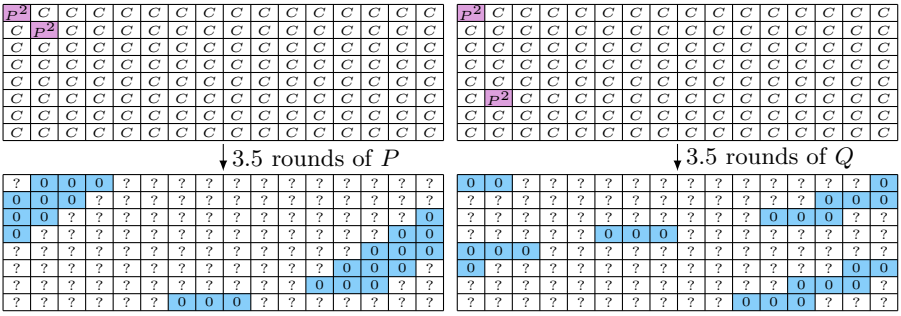

Fig. 1. The 3.5-round P integral property with 2 active bytes on the left and the 3.5-round Q integral property with 2 active bytes on the right

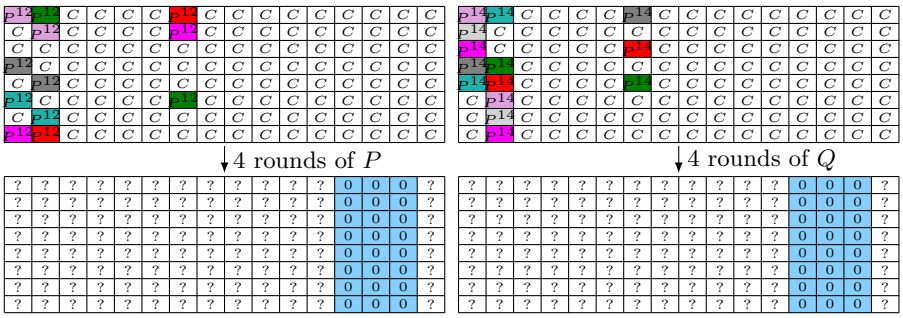

Fig. 2. The 4-round P integral property with 12 active bytes on the left and the 4-round Q integral property with 14 active bytes on the right

3.3 Integral Properties for P and Q in the Backward Direction

Let us now analyze which integral properties exist for the backward direction. We use the backward integral property already described in [19], a 2nd order integral property on 3 backward rounds presented in Fig. 4.

This property leads to a distinguisher on 3 backward rounds where the sums taken at byte level over all the inputs on the three shifted columns marked in blue in Fig. 4 are equal to 0. It requires 2^{16} chosen texts to work and has a complexity equal to 2^{16} cipher operations. This property could be extended by first one round and second two backward rounds at the beginning using a 80th order integral property as shown on Fig. 5. This leads to an integral distinguisher that uses 2^{640} chosen texts with a complexity equal to 2^{640} cipher operations to test if the sums taken at byte level over $3 \times 8 \times 8 = 192$ bits are equal to 0 or not.

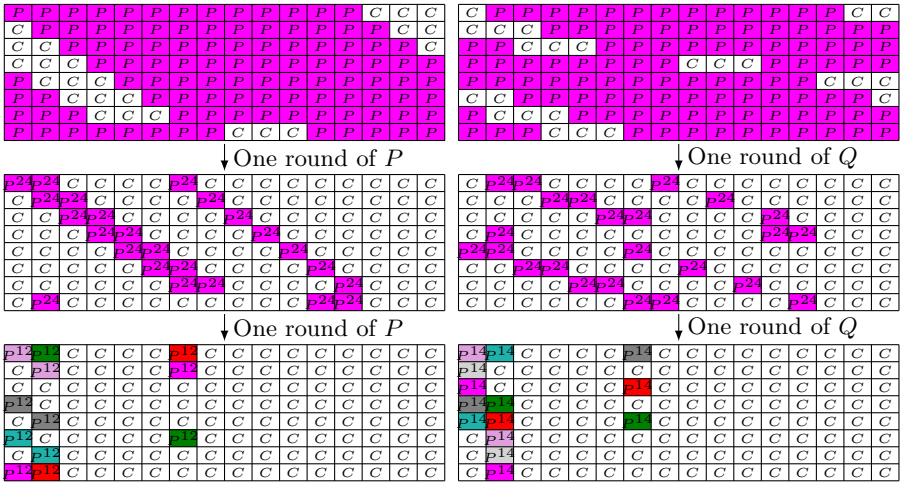

Fig. 3. The two added rounds of the integral property with 104 active bytes, for P on the left and Q on the right

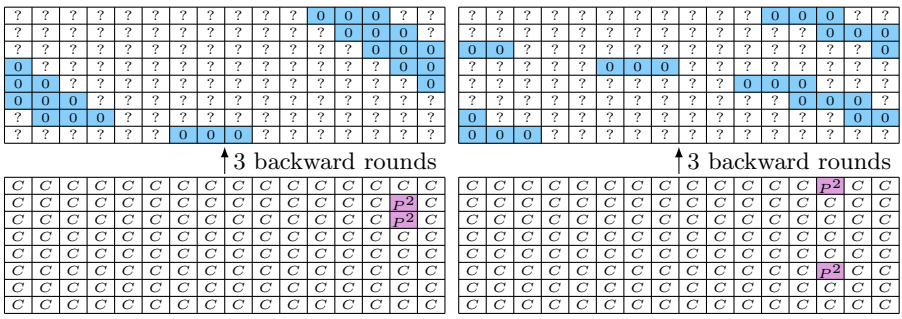

Fig. 4. The 2nd order Integral property on 3 backward rounds of P (left) and Q (right)

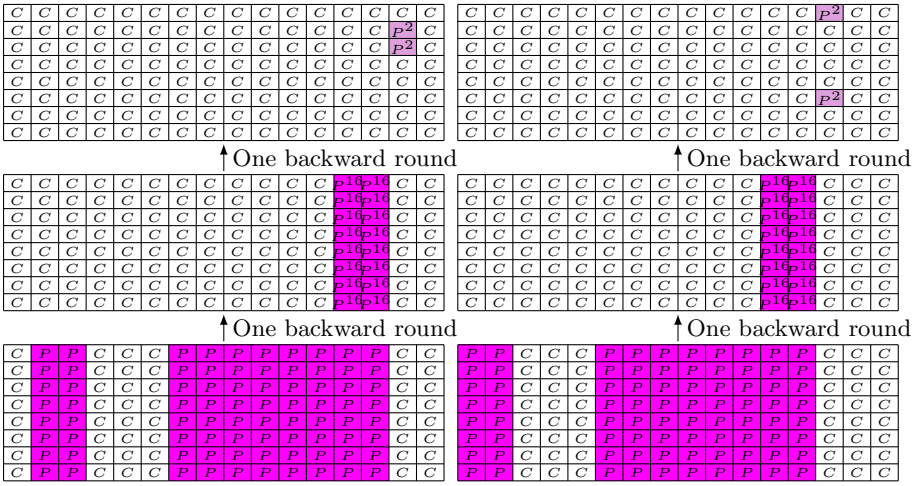

Fig. 5. The two added rounds of the P integral property with 80 active bytes on the left and the two added rounds of the Q integral property with 80 active bytes on the right

3.4 Distinguisher on 11 Rounds of the Compression Function of Grøstl-512 v3

We combined those two properties (in the backward and in the forward directions) starting from both the middle of P and the middle of Q to build a structural property on the compression function of Grøstl-512 when 11 rounds are considered (see Fig. 6). For the permutation P, start from the middle with 2^{912} middletexts with 114 active bytes (the other are taken equal to a constant) then, go backward on five rounds to obtain inputs that sum to 0 on 3 shifted columns and go forward on 6 rounds to obtain outputs that sum to 0 on 3 columns. Do the same for the permutation Q. Using Q, get the 2^{912} corresponding M_t messages. Using those messages and the inputs of P, compute the corresponding 2^{912} H_{t-1} values. Those 2^{912} values also verify that their sums taken over all 2^{912} values on 6 bytes are equal to 0 (due to the linearity of the XOR operation and considering the intersection of all 0-sum bytes). Considering the knowledge of H_{t-1}, of the outputs of P and of the outputs of Q, the corresponding H_t values are such that the sums taken over all the 2^{912} values on the intersection of the 6 common bytes (for the backward direction) and of the 3 columns (for the forward direction) are equal to 0. In other words, the sum taken over all the 2^{912} outputs of the compression function is null at 4 byte positions whereas the corresponding inputs H_{t-1} and M_t have 0-sum on 6 bytes (see Fig. 7).

Thus, we have exhibited a structural property of the Grøstl-512 compression function when P and Q are limited to 11 rounds. The computational cost of this property is about 2^{913} cipher operations with modest memory requirements to

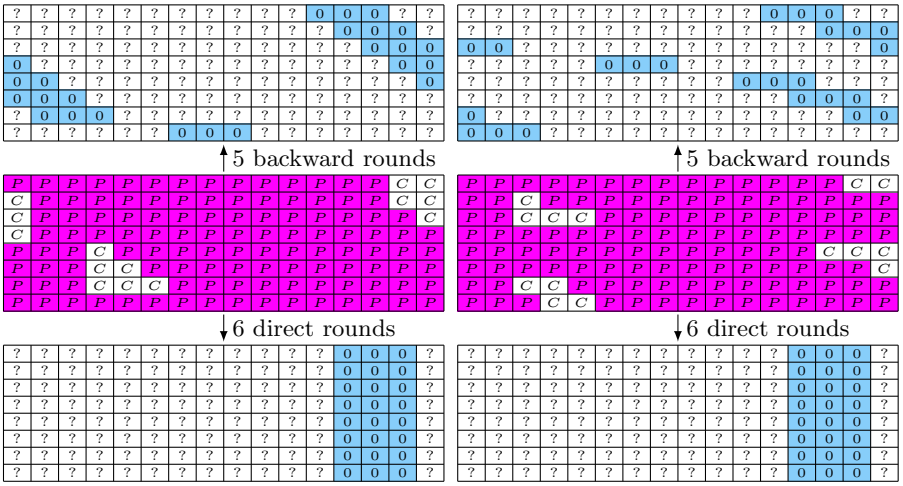

Fig. 6. Complete property on 11 rounds of P (on the left) and of Q (on the right) starting from the middle with a 114th order integral property

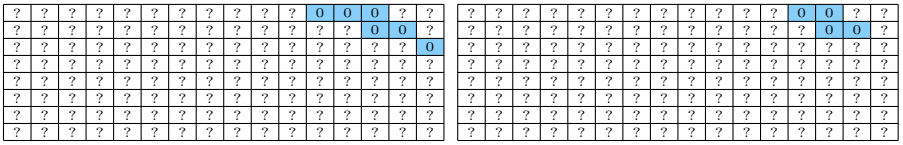

Fig. 7. Position of the 6 zero-sum bytes for H_{t-1} and M_t (left), and the 4 zero-sum bytes for H_t (right)

find some 0-sums at particular positions (4 bytes at the output of the compression function and 6 bytes at the input). This new structural property improves the one described in [18] that reaches 11 rounds also with a complexity equal to 2^{953} cipher operations.

Table 1. Summary of distinguishers against the compression function of Grøstl-512 v3

Nb rounds	Type of Attack	Time	Memory	Source
6	Semi-free-start Collision	2^{180}	2^{64}	[22]
8	Pseudo Preimage	$2^{507.32}$	2^{507}	[21]
10	Rebound Distinguisher	2^{392}	2^{64}	[14]
11	Integral Distinguisher	2^{953}	small	[18]
11	Integral Distinguisher	2^{913}	small	this paper

4 Conclusion

In this paper, we have improved the integral properties exhibited on the compression function of Grøstl-512 v3 presented in [18]. Table 1 sums up the main distinghuishers against the compression function of Grøstl-512 v3.

References

1. Aumasson, J.-P., Käsper, E., Knudsen, L.R., Matusiewicz, K., Ødegård, R., Peyrin, T., Schläffer, M.: Distinguishers for the compression function and output transformation of hamsi-256. In: Steinfeld, R., Hawkes, P. (eds.) ACISP 2010. LNCS, vol. 6168, pp. 87–103. Springer, Heidelberg (2010)
2. Biryukov, A., De Cannière, C., Dellkrantz, G.: Cryptanalysis of SAFER++. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 195–211. Springer, Heidelberg (2003)
3. Biryukov, A., Shamir, A.: Structural cryptanalysis of SASAS. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 394–405. Springer, Heidelberg (2001)
4. Boura, C., Canteaut, A., De Cannière, C.: Higher-Order Differential Properties of Keccak and *Luffa*. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 252–269. Springer, Heidelberg (2011)
5. Collard, B., Standaert, F.-X.: A statistical saturation attack against the block cipher PRESENT. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 195–210. Springer, Heidelberg (2009)
6. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher Square. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997)
7. Daemen, J., Rijmen, V.: AES proposal: Rijndael. In: The First Advanced Encryption Standard Candidate Conference. N.I.S.T (1998)
8. Daemen, J., Rijmen, V.: The Design of Rijndael. Springer (2002)
9. Vitek, J., Bijnens, G., Rijmen, V., Preneel, B.: Attack on Six Rounds of Crypton. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 46–59. Springer, Heidelberg (1999)
10. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.L.: Improved cryptanalysis of rijndael. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 213–230. Springer, Heidelberg (2001)
11. Galice, S., Minier, M.: Improving integral attacks against Rijndael-256 up to 9 rounds. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 1–15. Springer, Heidelberg (2008)
12. Gauravaram, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: Grøstl – a SHA-3 candidate. Submission to NIST, Round 1/2 (2008)
13. Gauravaram, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: Grøstl addendum. Submission to NIST, Round 2 (2009)
14. Jean, J., Naya-Plasencia, M., Peyrin, T.: Improved rebound attack on the finalist Grøstl. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 110–126. Springer, Heidelberg (2012)
15. Nakahara Jr., J., de Freitas, D.S., Phan, R.C.-W.: New multiset attacks on Rijndael with large blocks. In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS, vol. 3715, pp. 277–295. Springer, Heidelberg (2005)

16. Knudsen, L.R., Rijmen, V.: Known-key distinguishers for some block ciphers. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 315–324. Springer, Heidelberg (2007)
17. Knudsen, L.R., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
18. Li, Y., Wu, W., Dong, L.: Integral distinguishers of JH and Grøstl-512. Journal of Electronics (China) 29, 94–102 (2012)
19. Minier, M., Phan, R.C.-W., Pousse, B.: Integral distinguishers of some SHA-3 candidates. In: Heng, S.-H., Wright, R.N., Goi, B.-M. (eds.) CANS 2010. LNCS, vol. 6467, pp. 106–123. Springer, Heidelberg (2010)
20. Peyrin, T.: Improved differential attacks for ECHO and Grøstl. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 370–392. Springer, Heidelberg (2010)
21. Wu, S., Feng, D., Wu, W., Guo, J., Dong, L., Zou, J.: (Pseudo) Preimage attack on round-reduced Grøstl hash function and others. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 127–145. Springer, Heidelberg (2012)
22. Schläffer, M.: Updated differential analysis of Grøstl, Grøstl website (January 2011)