Research Journal of Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 149-159, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.149.159
© 2013 Academic Journals Inc.

Cryptanalysis of SHA-3 Candidates: A Survey

Shilpa Chauhan, Rajeev Sobti, G. Geetha and Sami Anand
Lovely Professional University, Punjab, India

Corresponding Author: Shilpa Chauhan, Lovely Professional University, Punjab, India

ABSTRACT

The final round SHA-3 candidate algorithms are BLAKE, Skein, Groestl, Keccak and JH. This study brings together all the cryptanalysis performed on the five finalist algorithms in the Cryptographic Hash Algorithm Competition organized by NIST. In this study, one section for each candidate algorithm is dedicated to discuss the cryptanalysis results in detail. The timeline of the attacks, the manner in which it was attacked, analysis of the attacks and the success rate of the authors are elaborated in this study. A great deal of contributions is made by the cryptanalysts all around the globe and we have compiled all the results together with our own criticisms to take a better view of the cryptanalysis status of SHA-3 finalists.

Key words: Attack, blake, skein, groest, keccak, pre-image, collision, near-collision, distinguisher

INTRODUCTION

All The Hash functions were first introduced in late 1970s. In the next two decades, a notable increase in number of hash functions was observed but the more the number of hash functions the more were security flaws in these functions. Hash functions found large number of applications and MD5 and SHA-1 both were named as “Swiss army knives” of cryptography. Wang cryptanalyzed MD5 in 2004 and present results in his paper titled “Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD” to such a level that finding collisions became very easy. Differential collision attack and time complexity will be used for finding collisions in MD5 compression (Xie and Feng, 2009). Authors also concluded that, a 2-bit weak input difference is found to be able to construct a practical 1-block collision attack on MD5. Recent advancement in SHA-1 cryptanalysis is introduction of a new collision attack against SHA-1, with a theoretical attack complexity of 2^{51} hash function calls. Schneier (2009) writes in his blog Schneier on Security-“The great truism of cryptanalysis: attacks always get better, they never get worse. The next Standard in line that is SHA-2 is also cryptanalyzed to a considerable level now. Sasaki *et al.* (2009), proposed meet-in-the-middle preimage attacks for SHA-256 and SHA-512; time complexity for 41-step SHA-256 is $2^{253.5}$ compression function operations and the memory requirement is 2^{16}*10 words. The time complexity for 46-step SHA-512 is 2^{511}.5 compression function operations and the memory requirement is 2^{3}*10 words. The most recent attack proposed on SHA-2 was in 2011 by Khovratovich *et al.* (2011a), where 52-round attack on the SHA-256 compression function and a 57-round attack on the SHA-512 compression function were shown possible.

NIST announced a public competition in November 2007 named Cryptographic Hash Algorithm Competition in response to advancing cryptanalysis of Hash Functions, with a goal to select a new hash function family by 2012 which will augment Secure Hash Standard. Initially 64 entries were made: 51 made it to first round, 14 made it to the second round and five made it to the third and final round. On December 9, 2010 the five algorithms named BLAKE, Grøstl, JH, Keccak and Skein advanced to final round (NIST, 2012).

To receive maximum feedback on five finalists, NIST planned a one-year public comment period and made an open call to cryptographers from around the world to contribute to security and performance analysis of SHA-3 finalists. We have compiled the cryptanalysis of five finalist algorithms. In this study, cryptanalysis is performed on the final round SHA-3 candidate algorithms like BLAKE, Skein, Groestl, Keccak and JH. The timeline attacks, analysis of various attacks and the success rate are elaborated.

CRYPTANALYSIS STATUS OF BLAKE

Ji and Liangyu (2009), found collision and preimage attacks for BLAKE with compression function reduced to 2.5 rounds by analyzing the round function and message permutation where, for BLAKE -224, -256, -384 and -512, free-start collision attacks have complexities 2^{96}, 2^{112}, 2^{160} and 2^{224}; preimage attacks have complexities 2^{209}, 2^{241}, 2^{355} and 2^{481}, respectively.

Guo and Matusiewicz (2009) published round reduced near-collision attack on 2^{32} bits for the compression of BLAKE-256 up to 4 middle rounds, with complexity 2^{56}.

Wang *et al.* (2009) claimed that preimage attacks are applicable to all the variants (round-reduced) of BLAKE family (using Splice-and-cut, Partial-matching and Partial-fixing) and for BLAKE-256 preimage attacks with complexity 2^{252} and memory requirements 2^{8} were presented.

Aumasson *et al.* (2010) establishing differential properties of the core function G, found out preimage on 1.5 rounds (2^{128} in BLAKE-32) and they also figured out specific impossible differentials for 5 rounds of BLAKE-256 and 6 rounds of BLAKE-512. The team modified G to find near-collisions for the compression function with 4 specific rounds, in 2^{56} trials.

Mouha *et al.* (2010) proposed a software toolkit for the automation of differential cryptanalysis of cryptographic primitives based on operations addition, rotation and xor (ARX) to assist the cryptanalysts and during the same period Su *et al.* (2010a), proposed near-collision attacks on BLAKE -256, -512, -512 (compression functions) reduced to 4, 4, 5 middle rounds with complexity 2^{21}, 2^{16} and 2^{216}, respectively.

Vidali *et al.* (2010) cryptanalyzed the toy version BLOKE and BRAKE to reinforce the concept of using permutations in original version BLAKE and usage of padding bits in the same (BLOKE and BRAKE are toy versions of BLAKE).

Turan and Uyan (2010) published near-collision attacks for round-reduced compression function of BLAKE-256 for 1.5 and 2 rounds on 209 and 184 bits, respectively with complexity 2^{26}. Late in December, Ming *et al.* (2010) by combining meet-in-the-middle technology and differential properties of compression function of BLAKE evidenced that the BLAKE family is strongly resistance to many attacks.

Biryukov *et al.* (2011) proposed distinguishers for the compression function of BLAKE-256 reduced to 7 rounds with complexity 2^{232} and for keyed permutation (BLAKE-256 reduced to 8 rounds) with complexity 2^{242}.

Khovratovich *et al.* (2011b) proposed distinguisher for 10 rounds of the permutation of compression function of BLAKE.

May 2011, Aumasson *et al.* (2011) introduced distinguisher for the permutation of BLAKE-256 reduced to 4 middle rounds, with complexity 2^{64}.

Again Dunkelman and Khovratovich (2011) presented distinguisher for the permutation of BLAKE-256 reduced to 6 middle rounds, with complexity 2^{456}.

In August, Gligoroski (2011), showing Bananb target collisions for Skein claimed that he can find the collisions for BLAKE and other candidate algorithms very easily.

Late in November Chang *et al.* (2011), gave security proof on indiffrentiability of BLAKE.

CRYPTANALYSIS STATUS OF SKEIN

Skein is SHA-3 candidate algorithm given by team of Bruce Schneier. It is the one and only candidate algorithm that has no cryptanalysis results yet to be obtained on the complete hash function though underlying building blocks have been cryptanalyzed by the cryptanalysts in the best possible ways. Following is the report on Skein hash function family cryptanalysis:

- Aumasson *et al.* (2009a, b) gave an improved cryptanalysis on Threefish. Threefish is the tweakable block cipher at the core of Skein, defined with a 256-, 512-and 1024-bit block size. This team of cryptanalysts gave new result on Threefish-512 instance. The results are: 16 rounds: near collisions in 2^6 (459-bit), 17 rounds: near collisions in 2^{24} (434-bit), 21 rounds: distinguisher in 2^4, 21 rounds: impossible differential, 23 rounds: key recovery in 2 ;^{274}24 rounds: key recovery in 2^{431}, 25 rounds: key recovery in 2^{441}
- Aumasson *et al.* (2009a, b) for the first time applied key-recovery boomerang attack to an "ARX" algorithm and boomerang technique to known-key distinguishers. The results they came up with are-a distinguisher on 35-round Threefish-512 and a key recovery attack on 32 rounds, related-key boomerang distinguisher works on up to 33 rounds of Threefish-256
- Khovratovich and Nikolic (2010) in February using Rotational Cryptanalysis technique analyzed the security of systems based on modular addition, rotation and xor (ARX systems). The primitive chosen for the practical implementation was Threefish (the core algorithm of Skein). Rotational attacks on Threefish-256,-512,-1024 (39/42/43.5 rounds out of 72/72/80 rounds) are the best attacks on this primitive. A rotational pair of Three fishcipher texts can be obtained faster than for a random permutation, which provides both a distinguisher and a key recovery attack
- During second round the submitters released a new version of Skein and the only modification was updated rotation constants. Chen and Jia (2009) gave related-key distinguishers on round-reduced Threefish-512 based on new rotation constants using modular differential method and with these distinguishers mounted related-key boomerang key recovery attacks on Threefish-512 reduced to 32, 33 and 34 rounds
- Gligoroski (2010) came up with an interesting analysis that double-pipe designs of Skein i.e., Skein-512-256 and Skein-1024-512 are not suffering from the defects of narrow-pipe compression functions that are extended to the infinite domain. Kaminsky (2010), analyzed the statistical properties of Skein to check on nonrandom behavior. There were three different types of statistical tests among which independence test resulted into nonrandom behavior in Skein
- McKay and Vora (2010) showed that pseudo-linear approximations were applicable to ARX ciphers and as an example eight and twelve round approximations for the Threefish-256 block cipher were presented. During the same phase Gligoroski (2011), demonstrated Bananb Target Collisions for Skein using NIST KAT files
- Su *et al.* (2010b) in December found out that computational complexity of near-collision attacks on 24-round compression functions of Skein-256, Skein-512 and Skein-1024 have a complexity of 2^{60}, 2^{230} and 2^{395}, respectively. Khovratovich *et al.* (2010) combined the rotational cryptanalysis with the rebound attack and as a result rotational collisions for about 53/57 out of the 72 rounds of the Skein-256/512 compression function were obtained

- In May 2011, Khovratovich *et al.* (2011a), applied meet-in-the-middle attack to Skein-512 to obtain a computational complexity enhancement for its full 72-round version. The full preimage is found with complexity $2^{511.2}$

CRYPTANALYSIS STATUS OF GROESTL

Mendel *et al.* (2009a) in February 2009 proposed the rebound attack, a new tool for the cryptanalysis of hash functions and applied the rebound attack to the SHA-3 submission Groestl, which leads to an attack on 6 rounds of the Groestl-256 compression function with a complexity of 2^{120} and memory requirements of about 2^{64}.

In March 2009, Mendel *et al.* (2009b) improved and extended the rebound attack and presented the first attack on 7 rounds for the Groestl-256 output transformation and improved the semi-free-start collision attack on 6 rounds.

In February 2010, Gilbert and Peyrin (2010) improved the rebound and start-from-the-middle attacks on AES-like permutations. In this the Super-Sbox cryptanalysis was introduced which very often improves upon the classical rebound or start-from-the-middle attacks both in terms of efficiency and simplicity. The results were obtained on Groestl.

Mendel *et al.* (2010) after one year, in March 2010, came up with a collision attack on 4/10 rounds of the Groestl-256 hash function and 5/14 rounds of the Groestl-512 hash functions. Also the reduced round attacks on versions of the compression function of Groestl-256 and Groestl-512 (7/10 and 7/14) were presented.

Peyrin (2010) gave the improved cryptanalysis of Groestl. A new technique, the internal differential attack, was presented and he also exploited the recently introduced Super-Sbox attacks. These findings have cryptanalyzed Groestl to such a level that a distinguishing attack for the full (10 rounds) Groestl-256 compression function or internal permutations could be mounted.

Exploiting the start-from-the-middle variant of the rebound technique, Ideguchi *et al.* (2009) put forward collision attacks on the Grøstl -256 hash function reduced to 5 and 6 out of 10 rounds with time complexities 2^{48} and 2^{112}, respectively. Semi-free-start collision attacks on the Grøstl -224 and -256 hash functions reduced to 7 rounds and the Grøstl -224 and -256 compression functions reduced to 8 rounds were given.

Sasaki *et al.* (2010) in December 2010 gave non-full-active Super-Sbox analysis detecting non-ideal properties of the 8-round Grøstl -256 permutation with a practical complexity and extending the approach to an improvement on a semi-free-start collision attack on the 7-round Grøstl -512 compression function.

Schlaffer (2011) presented one more application of Rebound attacks on the initial submission to the tweaked version of Groestl. Cryptanalyzed the round-reduced hash function and compression function for collisions on Groestl-256 (3/10 rounds) and Groestl-512 (6/14 rounds).

In May 2010, Naya-Plasencia (2010) gave some more contributions to improved rebound attacks and Groestl is one among the candidates under analysis.

CRYPTANALYSIS STATUS OF KECCAK

The Keccak hash function has been cryptanalyzed in a lot different manner than any other SHA-3 final round candidate. The internal and external affairs are both conducive to cryptanalysis. One set of results comes from the Home organized KECCAK Crunchy Crypto Collision and Pre-image Contest (by submitters). Submitters challenged public for 96 reduced-round Keccak instances, 48 preimage and 48 collision, out of which six preimage challenges and eight collision challenges are already met. All the preimage results are submitted by Morawiecki and Srebrny, 2010), collectively found the collisions. Preimage challenge is solved till second round [Keccak [r = 1440, c = 160, Nr = 2]] and collision challenge is solved till fourth round [Keccak [r = 1440, c = 160, Nr = 4]]. The solutions on the cryptanalysis can be easily obtained by a simple mailing procedure given on the website.

The third party cryptanalysis consists of a lot more results contributed by the worldwide cryptanalysts. The cryptanalysis on Keccak is as follows:

- In April Aumasson and Khovratovich (2009) in their publication First Analysis of Keccak showed the application of automated cryptanalysis tools to the core permutation of Keccak. In their findings they claimed that the proposed 13 rounds (by submitters) are sufficient to present structural distinguishers and 9 rounds against collisions
- Lathrop (2009) in his master's thesis demonstrated that if the maximum degree of Keccak's output polynomials is, then a cube attack might be practical against up to 7 rounds of 224 or 256 bit Keccak
- Aumasson and Meier (2009) in September 2009, came up with a new type of distinguisher called zero-sum distinguisher and applied it to reduced versions of the Keccak-f. The results were-practical and deterministic distinguishers on up to 9 rounds and shortcut distinguishers on up to 16 rounds were obtained
- In January 2010, Boura and Canteaut (2010a) extended the findings of Aumasson and Meier to 18 rounds (the zero-sum property) and in the same month submitters. Bertoni *et al.* (2010, 2011), increased the security margin of Keccak By increasing the number of rounds from 18 to 24
- In August 2010, Boura and Canteaut (2010b) extended zero-sum distinguishers to 20 rounds and during the same time in CRYPTO'10, Boura *et al.* (2011) presented Beware of optimistic weather forecast, in which possibility of extension of the zero-sum distinguishers to the full 24-round version was discussed
- In October 2010, Morawiecki and Srebrny (2010) gave SAT-based preimage analysis of reduced Keccak hash functions and found a preimage for the 3-round Keccak-f [1600] with 40 unknown message bits. Boura *et al.* (2010) found a new bound for the degree of iterated permutations which led to zero-sum distinguishers for the full Keccak-f permutation
- In January 2011, Duan and Lai (2012) improved the zero-sum distinguisher of full 24 rounds Keccak-f permutation by lowering the size of the zero-sum partition from 2^{1590} to 2^{1579}
- In November of 2011, Duc *et al.* (2012) obtained a practical distinguisher for 6 rounds of the Keccak-f [1600] permutation and in the end an 8-round distinguisher for the Keccak-f [1600] internal permutation with a complexity of $2^{491.47}$

CRYPTANALYSIS STATUS OF JH

Cryptanalysis reports on JH were obtained pretty earlier than all other candidates of Hash Competition but the graph lowered later on as compared to other candidates' cryptanalysis reports' statistics.

The first cryptanalysis paper on JH was presented in 2008 by Mendel and Thomsen (2008) showing a generic preimage attack on JH-512. It uses some properties in the design principles of JH-512 which do not exist in other hash functions. A preimage for JH-512 with a total complexity of about $2^{510.3}$ (over the space of 2^{1024} elements) compression function evaluations was found.

During the same year, Bagheri (2008) claimed an attack that can find pseudo-collisions and pseudo-second preimages in JH.

During 2009 very less contribution was made in the cryptanalysis of JH and the one was by Wu (2009), author gives a complexity analysis for the findings of Mendel and Thomsen (2008) pointing that the cost of the collision search is the most expensive part in their attack. He claimed that their attack requires at least $2^{510.3}$ compression function computations, $2^{510.6}$ memory ($2^{516.6}$ bytes), 2^{524} memory accesses and 2^{524} comparisons. Such complexity is far more expensive than brute force attack which requires 2^{512} compression function computations and almost no memory. As per observations by Wu (2009) 1024-bit hash value in JH plays an important role in defending such attack.

Rijmen *et al.* (2010) applied rebound attack to JH hash function family for d = 4 and d = 8 obtaining a semi-free-start collision for 16 rounds (out of 35.5) of JH for all hash sizes with $2^{179.24}$ compression function calls. The same attack was then extended to 19 rounds and a 1008-bit semi-free-start near-collision was found on the JH compression function with $2^{156.77}$ compression function calls, $2^{152.28}$ memory access and $2^{143.70}$-bytes of memory.

Bhattacharyya *et al.* (2010) analyzed JH in the in differentiability framework. Considering the assumption that the underlying permutation is a random permutation, JH mode of operation with specific padding rule is in differentiable from a Random Oracle. A modified (chopped bits) version JH' was analyzed taking into consideration the in differentiability with optimal bounds. A distinguisher for JH mode without length padding was presented. At last a preimage attack with 2^{507} complexity was obtained.

Turan and Uyan (2010) using hill climbing methods evaluated the near-collision resistance of JH and found 820/1024-bit near-collisions for 10-round compression function of JH.

Naya-Plasencia (2010) demonstrates how to reduce the complexities of the rebound attacks on JH.

CRITICISMS

Cryptanalysts all across the world have tried to perform attacks on five candidate algorithms using both conventional as well as state-of-the-art techniques. Substantial success has been achieved but sill a greater part is to be worked on. Our survey show how well these algorithms have been analyzed.

Collision attacks have been performed on BLAKE compression function reduced to 2.5 rounds with complexities (free-start collision attacks) 2^{96}, 2^{112}, 2^{160} and 2^{224} for BLAKE -224, -256, -384 and -512, respectively whereas using collision attacks Groestl hash function is cryptanalyzed till 5 and 6 (total 10) rounds (with complexities 2^{48} and 2^{112}, respectively) for Groestl-256 and 5 (total 14) rounds for Groestl -512. Compression function of Groestl-256 and Groestl-512 (8/10 and 7/14) are also prone to collision attacks and Keccak collision challenge is solved till fourth round [Keccak [r = 1440, c = 160, Nr = 4]].

Preimage attack on BLAKE is performed with compression function reduced to 2.5 rounds with complexities 2^{209}, 2^{241}, 2^{355} and 2^{481} for BLAKE -224, -256, -384 and -512, respectively. The same attack on BLAKE -256 hash function till 1.5 rounds with complexity 2^{128} was presented whereas a preimage for the 3-round Keccak-f [1600] with 40 unknown message bits is found and added to that, on JH, a preimage attack with 2^{507} complexity was obtained.

Near collision attacks are found on a 4-round compression function of BLAKE-32, 4-round and 5-round compression functions of BLAKE-64 with computational complexity 2^{21}, 2^{16} and 2^{216},

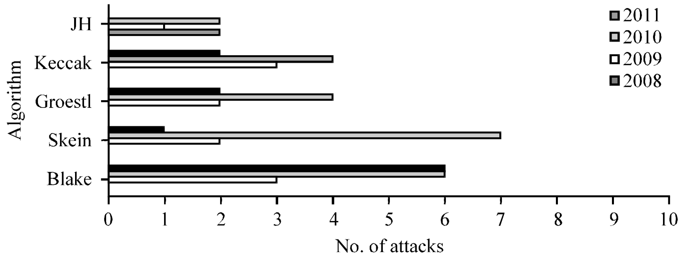

Fig. 1: Comparison graph of number of attacks

respectively whereas, the best attack on JH compression function was a semi-free-start near-collision attack on 19 rounds and a 1008-bits with $2^{156.77}$ compression function calls, $2^{152.28}$ memory accesses and $2^{143.70}$-bytes of memory.

Distinguishers were proposed for the permutation of BLAKE-256 reduced to 4 middle rounds, with complexity 2^{64} whereas in the case of Skein a distinguisher on 35-round Threefish-512 and a key recovery attack on 34 rounds, related-key boomerang distinguisher works on up to 33 rounds of Threefish-256. Zero-sum distinguishers on up to 24 rounds and shortcut distinguishers on up to 16 rounds for reduced permutations of Keccak-f were proposed and obtained and a distinguisher for JH mode without length padding was presented.

All the analysis results obtained on each and every algorithm were calculated based on different assumed parameters. The number of attacks from 2008-till date on the SHA-3 finalists is depicted in Fig. 1 in Appendix. The graph reveals that Skein Hash algorithm is susceptible to more number of attacks than the other SHA-3 finalists (Manuel, 2008).

CONCLUSION

The four years of Cryptographic Hash Algorithm Competition have given ample amount of opportunities to submitters so as to strengthen their algorithm and present it in a form never before. Cryptanalysts are given one more year (public comments' period) to cryptanalyze the algorithm using conventional, state-of-the-art and novel techniques. All the five candidates are cryptanalyzed well in advance even before the final selection. These results will play their role in making a decision when considering the robustness of the algorithm. The proposed attacks might be both feasible and possible.

The analysis done on the algorithms is definitely going to leave an impact on every aspect for the selection of final algorithm. To make the winner algorithm more and more attack resistant, the organizing body can make a separate committee of cryptanalysts associated with the algorithm's analysis. The tasks assigned to this committee will be to peer-review the updated algorithm and provide the suggestions to make it more robust, if necessary.

Even in the review stage, these algorithms have received ample amounts of entries analyzing them. There is a long way to go for the finalist but we have to wait and watch until the final results are out.

REFERENCES

Aumasson, J.P. and D. Khovratovich, 2009. First analysis of Keccak. NIST Mailing List. https://131002.net/data/papers/AK09.pdf

Aumasson, J.P. and W. Meier, 2009. Zero-sum distinguishers for reduced Keccak-f and for the core functions of Luffa and Hamsi. Rump Session CHES, September, 2009. https://131002.net/data/papers/AM09.pdf

Aumasson, J.P., C. Calik, W. Meier, O. Ozen, R.C.W. Phan and K. Varici, 2009a. Improved cryptanalysis of skein. Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security, December 6-10, 2009, Tokyo, Japan, pp: 542-559.

Aumasson, J.P., W. Meier and R. Phan, 2009b. Improved analysis of threefish. The FSE 2009 Rump Session, February 24, 2009. http://fse2009rump.cr.yp.to/412a260c7d5a7a99ccb6e2c874a94718.pdf

Aumasson, J.P., J. Guo, S. Knellwolf, K. Matusiewicz and W. Meier, 2010. Differential and invertibility properties of BLAKE. http://eprint.iacr.org/2010/043.pdf.

Aumasson, J.P., G. Leurent, W. Meier, F. Mendel and N. Mouha *et al.*, 2011. Tuple cryptanalysis of ARX with application to BLAKE and Skein. Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, May 15-19, 2011, Tallinn, Estonia, pp: 1-13.

Bagheri, N., 2008. Pseudo-collision and pseudo-second preimage on JH. NIST Mailing List, November 29, 2008.

Bertoni, G., J. Daemen, M. Peeters and G. Van Assche, 2011. The Keccak sponge function family. http://keccak.noekeon.org/crunchy0.html

Bertoni, G., J. Daemen, M. Peeters and G.V. Assche, 2010. Note on zero-sum distinguishers of Keccak-f. NIST Mailing List. http://keccak.noekeon.org/NoteZeroSum.pdf

Bhattacharyya, R., A. Mandal and M. Nandi, 2010. Security analysis of the mode of JH Hash function. Proceedings of the 17th International Workshop on Fast Software Encryption, February 7-10, 2010, Seoul, Korea, pp: 168-191.

Biryukov, A., I. Nikolic and A. Roy, 2011. Boomerang attacks on BLAKE-32. Proceedings of the 18th International Workshop on Fast Software Encryption, February 13-16, 2011, Lyngby, Denmark, pp: 218-237.

Boura, C. and A. Canteaut, 2010a. A zero-sum property for the Keccak-f permutation with 18 rounds. Proceedings of the IEEE International Symposium on Information Theory Proceedings, June 13-18, 2010, Austin, TX., USA., pp: 2488-2492.

Boura, C. and A. Canteaut, 2010b. Zero-sum distinguishers for iterated permutations and application to Keccak-f and hamsi-256. Proceedings of the 17th International Workshop on Selected Areas in Cryptography, August 12-13, 2010, Waterloo, Ontario, Canada, pp: 1-17.

Boura, C., A. Canteaut and C.D. Canniere, 2010. Beware of optimistic weather forecast. Proceedings of the 30th Annual Cryptology Conference, August 15-19, 2010, Santa Barbara, CA., USA.

Boura, C., A. Canteaut and C. De Canniere, 2011. Higher-order differential properties of Keccak and Luffa. Proceedings of the 18th International Workshop on Fast Software Encryption, February 13-16, 2011, Lyngby, Denmark, pp: 252-269.

Chang, D., M. Nandi and M. Yung, 2011. Indifferentiability of the hash algorithm BLAKE. Proceedings of the 14th IACR International Conference on Practice and Theory of Public Key Cryptography, March 6-9, 2011, Taormina, Italy, pp: 1-14.

Chen, J. and K. Jia, 2009. Improved related-key boomerang attacks on round-reduced Threefish-512. Cryptology ePrint Archive: Report 2009/526, http://eprint.iacr.org/2009/526.pdf

Duan, M. and X. Lai, 2012. Improved zero-sum distinguisher for full round Keccak-f permutation. Chin. Sci. Bull., 57: 694-697.

Duc, A., J. Guo, T. Peyrin and L. Wei, 2012. Unaligned rebound attack: Application to Keccak. Proceedings of the 19th International Workshop on Fast Software Encryption, March 19-21, 2012, Washington, DC., USA., pp: 402-421.

Dunkelman, O. and D. Khovratovich, 2011. Iterative differentials, symmetries and message modification in BLAKE-256. Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, May 15-19, 2011, Tallinn, Estonia, pp: 1-13.

Gilbert, H. and T. Peyrin, 2010. Super-Sbox cryptanalysis: Improved attacks for AES-like permutations. Proceedings of the 17th International Workshop on Fast Software Encryption, February 7-10, 2010, Seoul, Korea, pp: 365-383.

Gligoroski, D., 2010. Narrow-pipe SHA-3 candidates differ significantly from ideal random functions defined over big domains. NIST Mailing List. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.180.5902&rep=rep1&type=pdf

Gligoroski, D., 2011. Practical demonstration of Bananb Target Collisions for Skein with NIST KAT files (slides). Rump Session CRYPTO, http://www.specialist-online-dictionary.com/video/writing/video/ad-nZPeh0dk/Practical-demonstration-of-Bananb-Target-Collisions-for-Skein-with-NIST-KAT-files.html

Guo, J. and K. Matusiewicz, 2009. Round-reduced near-collisions of BLAKE-32. Proceedings of the Western European Workshop on Research in Cryptology, July 7-9, 2009, Graz, Austria.

Ideguchi, K., E. Tischhauser and B. Preneel, 2009. Improved collision attacks on the reduced-round grostl hash function. Proceedings of the 13th International Conference on Information Security (ISC'10), Springer-Verlag, pp: 1-16.

Ji, L. and X. Liangyu, 2009. Attacks on round-reduced BLAKE. Cryptology ePrint Archive: Report 2009/238, http://eprint.iacr.org/2009/238.pdf

Kaminsky, A., 2010. Cube test analysis of the statistical behavior of CubeHash and Skein. Cryptology ePrint Archive: Report 2010/262, http://eprint.iacr.org/2010/262.pdf

Khovratovich, D. and I. Nikolic, 2010. Rotational cryptanalysis of ARX. Proceedings of the 17th International Conference on Fast Soft Wear Encryption, Volume 6147, February 7-10, 2010, Seoul, Korea, pp: 333-346.

Khovratovich, D., I. Nikolic and C. Rechberger, 2010. Rotational rebound attacks on reduced skein. Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology, Volume 6477, December 5-9, 2010, Singapore, pp: 1-19.

Khovratovich, D., C. Rechberger and A. Savelieva, 2011a. Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family. Cryptology ePrint Archive: Report 2011/286, http://eprint.iacr.org/ 2011/286.pdf

Khovratovich, D., G. Leurent and M. Naya-Plasencia, 2011b. Observations on BLAKE (slides). Technical Report: MSR-TR-2011-43, Microsoft Research, http://research.microsoft.com/apps/pubs/default.aspx?id=147172

Lathrop, J., 2009. Cube attacks on cryptographic hash functions. Masters Thesis, Rochester Institutwe of Technology.

Manuel, S., 2008. Classification and generation of disturbance vectors for collision attacks against SHA-1. Cryptotology ePrint Archive: Report 2009/223, http://eprint.iacr.org/2008/469.pdf

McKay, K.A. and P.L. Vora, 2010. Pseudo-linear approximations for ARX Ciphers: With application to threefish. Cryptology ePrint Archive: Report 2010/282, http://eprint.iacr.org/2010/282.pdf

Mendel, F. and S.S. Thomsen, 2008. An observation on JH-512. https://ehash.iaik.tugraz.at/uploads/archive/d/da/20081216134423!Jh_preimage.pdf

Mendel, F., C. Rechberger, M. Schlaffer and S.S. Thomsen, 2009a. The rebound attack: Cryptanalysis of reduced whirlpool and grostl. Proceedings of the 16th International Workshop on Fast Software Encryption, February 22-25, 2009, Leuven, Belgium, pp: 260-276.

Mendel, F., T. Peyrin, C. Rechberger and M. Schlaffer, 2009b. Improved cryptanalysis of the reduced grostl compression function, ECHO permutation and AES block cipher. Proceedings of the 16th Annual International Workshop on Selected Areas in Cryptography, August 13-14, 2009, Alberta, Canada, pp: 16-35.

Mendel, F., C. Rechberger, M. Schlaffer and S.S. Thomsen, 2010. Rebound attacks on the reduced grostl hash function. CT-RSA. http://www2.mat.dtu.dk/people/S.Thomsen/MendelRST-fse09.pdf

Ming, M., H. Qiang and S. Zeng, 2010. Security analysis of BLAKE-32 based on differential properties. Proceedings of the International Conference on Computational and Information Sciences, December 17-19, 2010, Chengdu, Sichuan, China, pp: 783-786.

Morawiecki, P. and M. Srebrny, 2010. A SAT-based preimage analysis of reduced Keccak hash functions. Cryptology ePrint Archive: Report 2010/285, http://eprint.iacr.org/2010/285.pdf

Mouha, N., V. Velichkov, C. De Canniere and B. Preneel, 2010. Toolkit for the differential Cryptanalysis of ARX-based cryptographic constructions. Proceedings of the Workshop on Tools for Cryptanalysis, June 22-23, 2010, KU Leuven, pp: 125-126.

NIST, 2012. Cryptographic hash algorithm competition. National Institute of Standard and Technology (NIST), USA. http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

Naya-Plasencia, M., 2010. How to improve rebound attacks. http://eprint.iacr.org/2010/607.pdf

Peyrin, T., 2010. Improved differential attacks for ECHO and Grostl. Proceedings of the 30th Annual Cryptology Conference on Advances in Cryptology, August 15-19, 2010, Santa Barbara, CA., USA., pp: 370-392.

Rijmen, V., D. Toz and K. Varici, 2010. Rebound attack on reduced-round versions of JH. Proceedings of the 17th International Workshop Fast Software Encryption, February 7-10, 2010, Seoul, Korea, pp: 286-303.

Sasaki, Y., L. Wang and K. Aoki, 2009. Preimage attacks on 41-step SHA-256 and 46-step SHA-512. http://eprint.iacr.org/2009/479.pdf

Sasaki, Y., Y. Li, L. Wang, K. Sakiyama and K. Ohta, 2010. Non-full-active super-sbox analysis: Applications to ECHO and Grostl. Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security, December 5-9, 2010, Singapore, pp: 38-55.

Schlaffer, M., 2011. Updated differential analysis of Grostl. http://groestl.info/groestl-analysis.pdf

Schneier, B., 2009. Schneier on security: A blog covering security and security technology. http://www.schneier.com/

Su, B., W. Wu, S. Wu and L. Dong, 2010a. Near-collisions on the reduced-round compression functions of Skein and BLAKE. Proceedings of the 9th International Conference on Cryptology and Network Security, December 12-14, 2010, Kuala Lumpur, Malaysia, pp: 124-139.

Su, B., W. Wu, S. Wu and L. Dong, 2010b. Near-collisions on the reduced-round compression functions of skein and BLAKE. http://eprint.iacr.org/2010/355.pdf

Turan, M.S. and E. Uyan, 2010. Practical near-collisions for reduced round Blake, Fugue, Hamsi and JH. http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010/documents/papers/TURAN_Paper_Erdener.pdf

Vidali, J., P. Nose and E. Pasalic, 2010. Collisions for variants of the BLAKE hash function. Inf. Process. Lett., 110: 585-590.

Wang, L., K. Ohta and K. Sakiyama, 2009. Free-start preimages of step-reduced Blake compression function. The University of Electro-Communications, Japan. http://asiacrypt2009.cipher.risk.tsukuba.ac.jp/rump/slides/11.pdf

Wu, H., 2009. The complexity of Mendel and Thomsen's preimage attack on JH-512. http://ehash.iaik.tugraz.at/uploads/6/6f/Jh_mt_complexity.pdf

Xie, T. and D. Feng, 2009. How to find weak input differences for MD5 collision attacks. Cryptotology ePrint Archive: Report 2009/223. http://eprint.iacr.org/2009/223