杂凑密码与分组密码安全性分析

华中科技大学，Huazhong University of Science and Technology

2022 年 10 月 27 日

1 SM3 密码杂凑算法安全性分析

表 1: SM3 密码杂凑算法和其他杂凑标准的最好分析结果

算法	攻击类型)	步（轮）数	百分比/%	文献
SM3	碰撞攻击	20	31	[1]
	原像攻击	30	47	[2, 3]
	区分器攻击	37	58	[4]
SHA-1	碰撞攻击	80	100	[5–7]
	原像攻击	80	100	[8]
RIPEMD-128	碰撞攻击	40	62.5	[9]
	原像攻击	36	56.25	[10]
	区分器攻击	64	100	[11]
RIPEMD-160	原像攻击	34	53.12	[12]
	区分器攻击	51	79.68	[13]
SHA-256	碰撞攻击	31	48.4	[14]
	原像攻击	45	70.3	[15]
	区分器攻击	47	73.4	[16]
Whirlpool	碰撞攻击	8	80	[17]
	原像攻击	6	60	[17]
	区分器攻击	10	100	[18]
Stribog	碰撞攻击	7.5	62.5	[19]
	原像攻击	6	50	[20]

2 SM4 分组密码算法安全性分析

表 2: SM4 分组密码算法的最好分析结果

攻击方法	攻击轮数)	时间复杂度	数据复杂度	存储复杂度	文献
差分攻击	23	$2^{126.7}$	2^{118}	$2^{120.7}$	[21]
线性攻击	23	2^{122}	$2^{126.54}$	$2^{120.7}$	[22]
多维线性攻击	23	$2^{122.7}$	$2^{122.6}$	$2^{120.6}$	[22]
不可能差分攻击	17	2^{132}	2^{117}	2^{-}	[23]
零相关线性攻击	14	$2^{120.7}$	$2^{123.5}$	2^{73}	[24]
积分攻击	14	$2^{96.5}$	2^{32}	2^{-}	[25]
矩形攻击	18	$2^{96.5}$	2^{32}	2^{-}	[26]

References

[1] Florian Mendel, Tomislav Nad, and Martin Schläffer. Finding collisions for round-reduced sm3. In *Cryptographers' Track at the RSA Conference*, pages 174–188. Springer, 2013.

[2] Jian Zou, Wenling Wu, Shuang Wu, Bozhan Su, and Le Dong. Preimage attacks on step-reduced sm3 hash function. In *International Conference on Information Security and Cryptology*, pages 375–390. Springer, 2011.

[3] Gaoli Wang and Yanzhao Shen. Preimage and pseudo-collision attacks on step-reduced sm3 hash function. *Information Processing Letters*, 113(8):301–306, 2013.

[4] Dongxia Bai, Hongbo Yu, Gaoli Wang, and Xiaoyun Wang. Improved boomerang attacks on round-reduced sm3 and keyed permutation of blake-256. *IET Information Security*, 9(3):167–178, 2015.

[5] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full sha-1. In *Annual international cryptology conference*, pages 17–36. Springer, 2005.

[6] Xiaoyun Wang, Andrew C Yao, and Frances Yao. Cryptanalysis on sha-1. In *Cryptographic Hash Workshop hosted by NIST*, 2005.

[7] Marc Stevens. New collision attacks on sha-1 based on optimal joint local-collision analysis. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 245–261. Springer, 2013.

[8] Thomas Espitau, Pierre-Alain Fouque, and Pierre Karpman. Higher-order differential meet-in-the-middle preimage attacks on sha-1 and blake. In *Annual Cryptology Conference*, pages 683–701. Springer, 2015.

[9] Gaoli Wang. Practical collision attack on 40-step ripemd-128. In *Cryptographers' Track at the RSA Conference*, pages 444–460. Springer, 2014.

[10] Lei Wang, Yu Sasaki, Wataru Komatsubara, Kazuo Ohta, and Kazuo Sakiyama. (second) preimage attacks on step-reduced ripemd/ripemd-128 with a new local-collision approach. In *Cryptographers' Track at the RSA Conference*, pages 197–212. Springer, 2011.

[11] Franck Landelle and Thomas Peyrin. Cryptanalysis of full ripemd-128. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 228–244. Springer, 2013.

[12] Gaoli Wang and Yanzhao Shen. (pseudo-) preimage attacks on step-reduced has-160 and ripemd-160. In *International Conference on Information Security*, pages 90–103. Springer, 2014.

[13] Yu Sasaki and Lei Wang. Distinguishers beyond three rounds of the ripemd-128/-160 compression functions. In *International Conference on Applied Cryptography and Network Security*, pages 275–292. Springer, 2012.

[14] Florian Mendel, Tomislav Nad, and Martin Schläffer. Improving local collisions: new attacks on reduced sha-256. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 262–278. Springer, 2013.

[15] Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva. Bicliques for preimages: attacks on skein-512 and the sha-2 family. In *International Workshop on Fast Software Encryption*, pages 244–263. Springer, 2012.

[16] Alex Biryukov, Mario Lamberger, Florian Mendel, and Ivica Nikolić. Second-order differential collisions for reduced sha-256. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 270–287. Springer, 2011.

[17] Yu Sasaki, Lei Wang, Shuang Wu, and Wenling Wu. Investigating fundamental security requirements on whirlpool: improved preimage and collision attacks. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 562–579. Springer, 2012.

[18] Mario Lamberger, Florian Mendel, Martin Schläffer, Christian Rechberger, and Vincent Rijmen. The rebound attack and subspace distinguishers: Application to whirlpool. *Journal of Cryptology*, 28(2):257–296, 2015.

[19] Bingke Ma, Bao Li, Ronglin Hao, and Xiaoqian Li. Improved cryptanalysis on reduced-round gost and whirlpool hash function. In *International Conference on Applied Cryptography and Network Security*, pages 289–307. Springer, 2014.

[20] Riham AlTawy and Amr M Youssef. Preimage attacks on reduced-round stribog. In *International Conference on Cryptology in Africa*, pages 109–125. Springer, 2014.

[21] Bo-Zhan Su, Wen-Ling Wu, and Wen-Tao Zhang. Security of the sms4 block cipher against differential cryptanalysis. *Journal of Computer Science and Technology*, 26(1):130–138, 2011.

[22] Ming-Jie Liu and Jia-Zhe Chen. Improved linear attacks on the chinese block cipher standard. *Journal of Computer Science and Technology*, 29(6):1123–1133, 2014.

[23] Gaoli Wang. Improved impossible differential cryptanalysis on sms4. In *2010 International Conference on Communications and Intelligence Information Security*, pages 105–108, 2010. doi: 10.1109/ICCIIS.2010.26.

[24] 马猛, 赵亚群, 刘庆聪, and 刘凤梅. Sms4 算法的多维零相关线性分析. 密码学报, (5):458–466, 2015.

[25] 钟名富, 胡予濮, and 陈杰. 分组加密算法 sms4 的 14 轮 square 攻击. 西安电子科技大学学报, 35(1): 105–109, 2008.

[26] 薛萍. 对分组密码算法 sms4 的矩形攻击. Master's thesis, 山东大学, 2012.