Scopus

Documents

Khan, B.U.I.[a] , Olanrewaju, R.F.[a] , Morshidi, M.A.[a] , Mir, R.N.[b] , Kiah, M.L.B.M.[c] , Khan, A.M.[d]

EVOLUTION AND ANALYSIS OF SECURED HASH ALGORITHM (SHA) FAMILY

(2022) *Malaysian Journal of Computer Science*, 35 (3), pp. 179-200.

DOI: 10.22452/mjcs.vol35no3.1

[a] Department of ECE, KOE, International Islamic University Malaysia (IIUM), Kuala Lumpur, 50728, Malaysia
[b] Department of Computer Science and Engineering, National Institute of Technology (NIT), Srinagar, 190006, India
[c] Department of Computer System & Technology, Universiti Malaya (UM), Kuala Lumpur, 50603, Malaysia
[d] ALEM Solutions and Technologies, Aspen Commercial Tower, Dubai, 11562, United Arab Emirates

Abstract

With the rapid advancement of technologies and proliferation of intelligent devices, connecting to the internet challenges have grown manifold, such as ensuring communication security and keeping user credentials secret. Data integrity and user privacy have become crucial concerns in any ecosystem of advanced and interconnected communications. Cryptographic hash functions have been extensively employed to ensure data integrity in insecure environments. Hash functions are also combined with digital signatures to offer identity verification mechanisms and non-repudiation services. The federal organization National Institute of Standards and Technology (NIST) established the SHA to provide security and optimal performance over some time. The most well-known hashing standards are SHA-1, SHA-2, and SHA-3. This paper discusses the background of hashing, followed by elaborating on the evolution of the SHA family. The main goal is to present a comparative analysis of these hashing standards and focus on their security strength, performance and limitations against common attacks. The complete assessment was carried out using statistical analysis, performance analysis and extensive fault analysis over a defined test environment. The study outcome showcases the issues of SHA-1 besides exploring the security benefits of all the dominant variants of SHA-2 and SHA-3. The study also concludes that SHA-3 is the best option to mitigate novice intruders while allowing better performance cost-effectively. © 2022. All Rights Reserved.

Author Keywords

Cryptographic Hashing; Fault Analysis; Message Digest; Secured Hash Algorithms; Statistical Analysis

References

- Wang, T., Bhuiyan, M., Wang, G., Qi, L., Wu, J., Hayajneh, T.
  Preserving Balance Between Privacy and Data Integrity in Edge-Assisted Internet of Things
  (2020) *IEEE Internet of Things Journal*, 7 (4), pp. 2679-2689.
  [1]

- Chen, D., Bovornkeeratiroj, P., Irwin, D., Shenoy, P.
  Private Memoirs of IoT Devices: Safeguarding User Privacy in the IoT Era
  (2018) *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1327-1336.
  [2] in Vienna, Austria

- Solangi, Z. A., Solangi, Y. A., Chandio, S., Aziz, M. bt. S. Abd., bin Hamzah, M. S., Shah, A.
  The Future of Data Privacy and Security Concerns in Internet of Things
  (2018) *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, pp. 1-4.
  [3] in Bangkok, Thailand

- Ochôa, I., Calbusch, L., Viecelli, K., de Paz, J., Leithardt, V., Zeferino, C.
  Privacy in the Internet of Things: A Study to Protect User's Data in LPR Systems Using Blockchain
  (2019) *2019 17th International Conference on Privacy, Security and Trust (PST)*, pp. 1-5.
  [4] in Fredericton, NB, Canada

- Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., Balusamy, B.
  Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques
  (2020) *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50 (1), pp. 73-80.
  [5]

- Al Hamid, H., Rahman, S., Hossain, M., Almogren, A., Alamri, A.
  A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography
  (2017) *IEEE Access*, 5, pp. 22313-22328.
  [6]

- Sharma, N., Parveen Sultana, H., Singh, R., Patil, S.
  Secure Hash Authentication in IoT based Applications
  (2019) *Procedia Computer Science*, 165, pp. 328-335.
  [7]

- Suhail, S., Hussain, R., Khan, A., Hong, C. S.
  On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions
  (2021) *IEEE Internet of Things Journal*, 8 (1), pp. 1-17.
  [8]

- Saravanan, K., Senthilkumar, A.
  Theoretical Survey on Secure Hash Functions and Issues
  (2013) *International Journal of Engineering Research & Technology (IJERT)*, 2 (10), pp. 1150-1153.
  [9]

- Jurcut, A., Niculcea, T., Ranaweera, P., Le-Khac, N.
  Security Considerations for Internet of Things: A Survey
  (2020) *SN Computer Science*, 1 (4), pp. 1-19.
  [10]

- Huang, H., Huang, Q., Xiao, F., Wang, W., Li, Q., Dai, T.
  An Improved Broadcast Authentication Protocol for Wireless Sensor Networks Based on the Self-Reinitializable Hash Chains
  (2020) *Security and Communication Networks*, 2020, pp. 1-17.
  [11]

- Stevens, M., Bursztein, E., Karpman, P., Albertini, A., Markov, Y.
  The First Collision for Full SHA-1
  (2017) *Annual International Cryptology Conference*, pp. 570-596.
  [12] in Santa Barbara, USA

- Martino, R., Cilardo, A.
  SHA2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey
  (2020) *IEEE Access*, 8, pp. 28415-28436.
  [13]

- Mohammed Ali, A., Kadhim Farhan, A.
  A Novel Improvement with an Effective Expansion to Enhance the MD5 Hash Function for Verification of a Secure E-Document
  (2020) *IEEE Access*, 8, p. 8029080304.
  [14]

- Liu, H., Kadir, A., Liu, J.
  Keyed Hash Function Using Hyper Chaotic System with Time-Varying Parameters Perturbation

(2019) *IEEE Access*, 7, pp. 37211-37219.
[15]

- Rathor, M., Sengupta, A.
IP Core Steganography Using Switch Based Key-Driven Hash-Chaining and Encoding for Securing DSP Kernels Used in CE Systems
(2020) *IEEE Transactions on Consumer Electronics*, 66 (3), pp. 251-260.
[16]

- Ouyang, J., Zhang, X., Wen, X.
Robust Hashing Based on Quaternion Gyrator Transform for Image Authentication
(2020) *IEEE Access*, 8, pp. 220585-220594.
[17]

- Zhou, Y., Yang, B., Xia, Z., Mu, Y., Wang, T.
Anonymous and Updatable Identity-Based Hash Proof System
(2019) *IEEE Systems Journal*, 13 (3), pp. 2818-2829.
[18]

- Nassr, D. I.
Secure Hash Algorithm-2 formed on DNA
(2019) *Journal of the Egyptian Mathematical Society*, (24), pp. 1-20.
[19] Articl

- Lee, Y., Rathore, S., Park, J. H., Park, J. H.
A Blockchain-Based Smart Home Gateway Architecture for Preventing Data Forgery
(2020) *Human-centric Computing and Information Science*, 10 (1), p. 114.
[20]

- Rezazadeh Baee, M. A., Simpson, L., Boyen, X., Foo, E., Pieprzyk, J.
Authentication Strategies in Vehicular Communications: A Taxonomy and Framework
(2021) *EURASIP Journal on Wireless Communication and Networking*, 2021 (1), pp. 1-50.
[21]

- Martino, R., Cilardo, A.
SHA2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey
(2020) *IEEE Access*, 8, pp. 28415-28436.
[22]

- Salem, I. E., Salman, A. M., Mijwil, M. M.
A Survey: Cryptographic Hash Functions for Digital Stamping
(2019) *Journal of Southwest Jiaotong University*, 54 (6), pp. 1-11.
[23]

- Mo, Jianhua, Xiao, Xiawen, Tao, Meixia, Zhou, Nanrun
Hash Function Mapping Design Utilizing Probability Distribution for Preimage Resistance
(2012) *2012 IEEE Global Communications Conference (GLOBECOM)*, pp. 862-867.
[24] in Anaheim, CA

- Preneel, B.
Second Preimage Resistance
(2005) *Encyclopedia of Cryptography and Security*,
[25] Boston, MA, Springer

- Maetouq, A., Daud, S. M.
HMNT: Hash Function Based on New Mersenne Number Transform
(2020) *IEEE Access*, 8, pp. 80395-80407.

[26]

- Jing, W., Zhang, D., Song, H.
  An Application of Ternary Hash Retrieval Method for Remote Sensing Images in Panoramic Video
  (2020) *IEEE Access*, 8, pp. 140822-140830.
  [27]

- Cui, H., Zhu, L., Li, J., Yang, Y., Nie, L.
  Scalable Deep Hashing for Large-Scale Social Image Retrieval
  (2020) *IEEE Transactions on Image Processing*, 29, pp. 1271-1284.
  [28]

- Zheng, Y., Cao, Y., Chang, C. H.
  UDhashing: Physical Unclonable Function-Based User-Device Hash for Endpoint Authentication
  (2019) *IEEE Transactions on Industrial Electronics*, 66 (12), p. 95599570.
  [29]

- Biswas, A., Majumdar, A., Nath, S., Dutta, A., Baishnab, K. L.
  LRBC: A Lightweight Block Cipher Design for Resource Constrained IoT Devices
  (2020) *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-15.
  [30]

- Chanal, P., Kakkasageri, M.
  Security and Privacy in IoT: A Survey
  (2020) *Wireless Personal Communications*, 115 (2), pp. 1667-1693.
  [31]

- Molina, E., Jacob, E.
  Software-Defined Networking in Cyber-Physical System: A Survey
  (2018) *Computers & Electrical Engineering*, 66, pp. 407-419.
  [32]

- Graja, I., Kallel, S., Guermouche, N., Cheikhrouhou, S., Hadj Kacem, A.
  A Comprehensive Survey on Modeling of Cyber - Physical Systems
  (2018) *Concurrency and Computation: Practice and Experience*, 32 (5), pp. 1-18.
  [33]

- Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Yaacob, M.
  Offline OTP Based Solution for Secure Internet Banking Access
  (2018) *2018 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*, pp. 167-172.
  [34] in Langkawi, Malaysia

- Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Mir, R. N., Najeeb, A.
  A Critical Insight into the Effectiveness of Research Methods Evolved to Secure IoT Ecosystem
  (2019) *International Journal of Information and Computer Security*, 11 (45), pp. 332-354.
  [35]

- Jin, C.
  (2019) *Cryptographic Solutions for Cyber-Physical System Security*,
  [36] Doctoral Dissertation, University of Connecticut, Storrs

- Tawalbeh, A., Tawalbeh, H.
  Lightweight Crypto and Security
  (2017) *Security and Privacy in Cyber-Physical Systems*, pp. 243-261.
  [37] John Wiley & Sons

- Sabaliauskaite, G., Mathur, A.
  Aligning Cyber-Physical System Safety and Security
  (2021) *Complex System Design & Management*, pp. 41-53.
  [38] Cham, Springer

- Wang, J., Zhang, T., Song, J., Sebe, N., Shen, H.
  A Survey on Learning to Hash
  (2018) *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40 (4), pp. 769-790.
  [39]

- Ebrahim, M., Khan, S., Khalid, U. B.
  Symmetric Algorithm Survey: A Comparative Analysis
  (2013) *International Journal of Computer Applications*, 61 (20), pp. 12-19.
  [40]

- Moayed, M. J., Ghani, A. A. A., Mahmod, R.
  A Survey on Cryptography Algorithms in Security of Voting System Approaches
  (2008) *2008 International Conference on Computational Sciences and its Applications*, pp. 190-200.
  [41] in Perugia, Italy

- Lee, D.
  Hash Function Vulnerability Index and Hash Chain Attacks
  (2007) *2007 3rd IEEE Workshop on Secure Network Protocols*, pp. 1-6.
  [42] in Beijing, China

- Breitinger, F., Baier, H.
  Properties of a Similarity Preserving Hash Function and Their Realization in SDhash
  (2012) *2012 Information Security for South Africa*, pp. 1-8.
  [43] in Johannesberg, South Africa

- El Moumni, S., Fettach, M., Tragha, A.
  High Throughput Implementation of SHA3 Hash Algorithm on Field Programmable Gate Array (FPGA)
  (2019) *Microelectronics Journal*, 93, pp. 1-8.
  [44]

- Choi, H., Seo, S.
  Fast Implementation of SHA-3 in GPU Environment
  (2021) *IEEE Access*, 9, pp. 144574-144586.
  [45]

- Rahaman, S., Meng, N., Yao, D.
  Tutorial: Principles and Practices of Secure Crypto Coding in Java
  (2018) *2018 IEEE Cybersecurity Development (SecDev)*, pp. 122-123.
  [46] in Cambridge, MA

- Baksi, A., Bhasin, S., Breier, J., Jap, D., Saha, D.
  Fault Attacks in Symmetric Key Cryptosystems
  (2020) *IACR Cryptology ePrint Archive*, pp. 1-24.
  [47]

- Gundaram, P. K., Naidu Tentu, A., Muppalaneni, N. B.
  Performance of Various SMT Solvers in Cryptanalysis
  (2021) *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pp. 298-303.
  [48] in Greater Noida, India

Correspondence Address
Khan B.U.I.; Department of ECE, Malaysia; email: burhan.iium@gmail.com

Publisher: Faculty of Computer Science and Information Technology

ISSN: 01279084
Language of Original Document: English
Abbreviated Source Title: Malays. J. Comput. Sci.
2-s2.0-85135511083
Document Type: Article
Publication Stage: Final
Source: Scopus