Scopus

Documents

Windarta, S.[a] , Suryadi, S.[b] , Ramli, K.[a] , Pranggono, B.[c] , Gunawan, T.S.[d]

Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions
(2022) *IEEE Access*, 10, pp. 82272-82294.

DOI: 10.1109/ACCESS.2022.3195572

[a] Universitas Indonesia, Faculty of Engineering, Department of Electrical Engineering, Depok, 16424, Indonesia

[b] Universitas Indonesia, Faculty of Mathematics and Natural Sciences, Department of Mathematics, Depok, 16424, Indonesia

[c] Sheffield Hallam University, Department of Engineering and Mathematics, Sheffield, S1 1WB, United Kingdom

[d] International Islamic University Malaysia, Kulliyyah of Engineering, Department of Electrical and Computer Engineering, Kuala Lumpur, 50728, Malaysia

Abstract

The emergence of the Internet of Things (IoT) has enabled billions of devices that collect large amounts of data to be connected. Therefore, IoT security has fundamental requirements. One critical aspect of IoT security is data integrity. Cryptographic hash functions are cryptographic primitives that provide data integrity services. However, due to the limitations of IoT devices, existing cryptographic hash functions are not suitable for all IoT environments. As a result, researchers have proposed various lightweight cryptographic hash function algorithms. In this paper, we discuss advanced lightweight cryptographic hash functions for highly constrained devices, categorize design trends, analyze cryptographic aspects and cryptanalytic attacks, and present a comparative analysis of different hardware and software implementations. In the final section of this paper, we highlight present research challenges and suggest future research topics related to the design of lightweight cryptographic hash functions. © 2013 IEEE.

Author Keywords
Internet of Things; lightweight cryptographic hash function; lightweight cryptography; security

Index Keywords
Hash functions; Cipher, Cryptographic hash functions, Design trends, Hash function design, Light-weight cryptography, Lightweight cryptographic hash function, Security, Software algorithms; Internet of things

References

- Lueth, K.L.
(2020) *State of the IoT 2020: 12 Billion IoT Connections, Surpassing Non-IoTfor the First Time*,
[Online].

- Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., Uhsadel, L.
A survey of lightweight-cryptography implementations
(2007) *IEEE Des. Test Comput.*, 24 (6), pp. 522-533.
Dec., [Online].

- (2017) *CRYPTREC Cryptographic Technology Guideline-Lightweight Cryptography-(English Version)*,
CRYPTREC. Mar., [Online].

- Gong, G.
Securing Internet-of-Things
(2019) *Foundations and Practice of Security*, pp. 3-16.
N. Zincir-Heywood, G. Bonfante, M. Debbabi, and J. Garcia-Alfaro, Eds. Cham, Switzerland: Springer

- Zhou, L., Su, C., Yeh, K.-H.
A lightweight cryptographic protocol with certificateless signature for the Internet of Things
(2019) *ACM Trans. Embedded Comput. Syst.*, 18 (3), pp. 1-10.

Jun.

- Banerjee, S., Odelu, V., Das, A.K., Chattopadhyay, S., Rodrigues, J.J.P.C., Park, Y.
Physically secure lightweight anonymous user authentication protocol for Internet of Things using physically unclonable functions
(2019) *IEEE Access*, 7, pp. 85627-85644.

- Shin, S., Kwon, T.
A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things
(2020) *IEEE Access*, 8, pp. 67555-67571.

- Kalaria, R., Kayes, A.S.M., Rahayu, W., Pardede, E.
A secure mutual authentication approach to fog computing environment
(2021) *Comput. Secur*, 3.
Dec., [Online].

- Amiruddin, A., Ratna, A.A.P., Sari, R.F.
Systematic review of Internet of Things security
(2019) *Int. J. Commun. Netw. Inf. Secur*, 11 (2), pp. 248-255.
Aug., [Online].

- Tsai, K.-L., Leu, F.-Y., You, I., Chang, S.-W., Hu, S.-J., Park, H.
Low-power AES data encryption architecture for a LoRaWAN
(2019) *IEEE Access*, 7, pp. 146348-146357.

- Tsai, K.-L., Huang, Y.-L., Leu, F.-Y., You, I., Huang, Y.-L., Tsai, C.-H.
AES-128 based secure low power communication for LoRaWAN IoT environments
(2018) *IEEE Access*, 6, pp. 45325-45334.

- Tsai, K.-L., Leu, F.-Y., Hung, L.-L., Ko, C.-Y.
Secure session key generation method for LoRaWAN servers
(2020) *IEEE Access*, 8, pp. 54631-54640.

- Nakamoto, S.
(2008) *Bitcoin: A Peer-to-Peer Electronic Cash SysteM*,
[Online].

- Christidis, K., Devetsikiotis, M.
Blockchains and smart contracts for the Internet of Things
(2016) *IEEE Access*, 4, pp. 2292-2303.

- Novo, O.
Blockchain meets IoT: An architecture for scalable access management in IoT
(2018) *IEEE Internet Things J.*, 5 (2), pp. 1184-1195.
Apr.

- Wang, L., Shen, X., Li, J., Shao, J., Yang, Y.
Cryptographic primitives in blockchains
(2019) *J. Netw. Comput. Appl*, 127, pp. 43-58.
Feb.

- Pohrmen, F.H., Saha, G.
LightBC: A lightweight hash-based blockchain for the secured Internet of Things
(2021) *Proc. Int. Conf. Innov. Comput. Commun*, pp. 811-819.
D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, and A. Jaiswal, Eds.
Singapore: Springer

- Biryukov, A., Perrin, L.
  (2017) *State of the Art in Lightweight Symmetric Cryptography*,
  Cryptol. ePrint Arch., Univ. Luxembourg, Paper 2017/511, [Online].

- Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.
  (1997) *Handbook of Applied Cryptography, Isted*,
  Boca Raton, FL, USA.: CRC press

- Stinson, D.R.
  Some observations on the theory of cryptographic hash functions
  (2006) *Des., Codes Cryptogr*, 38 (2), pp. 259-277.
  Feb., [Online].

- Rogaway, P., Shrimpton, T.
  Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance
  (2004) *Fast Software Encryption*, pp. 371-388.
  B. Roy and W. Meier, Eds. Berlin, Germany: Springer

- Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.
  Kec-cak
  (2013) *Advances in Cryptology-EUROCRYPT 2013*, pp. 313-314.
  T. Johansson and P. Q. Nguyen, Eds. Berlin, Germany: Springer

- (2015) *Permutation-Based Hash and Extendable Output Functions*,
  Standard FIPS 202 SHA-3, NIST

- Kelsey, J., Chang, S.-J., Perlner, R.
  (2016) *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash*,
  [Online].

- Snyder, H.
  Literature review as a research methodology: An overview and guidelines
  (2019) *J. Bus. Res.*, 104, pp. 333-339.
  Nov., [Online].

- Shah, A., Engineer, M.
  A survey of lightweight cryptographic algorithms for IoT-based applications
  (2019) *Smart Innovations in Communication and Computational Sciences*, pp. 283-293.
  S. Tiwari, M. C. Trivedi, K. K. Mishra, A. K. Misra, and K. K. Kumar, Eds. Singapore: Springer

- Dhanda, S.S., Singh, B., Jindal, P.
  Lightweight cryptography: A solution to secure IoT
  (2020) *Wireless Pers. Commun.*, 112 (3), pp. 1947-1980.
  Jun.

- Rana, M., Mamun, Q., Islam, R.
  Lightweight cryptography in IoT networks: A survey
  Future Gener. Comput. Syst., 129 (2022), pp. 77-89.
  Apr., [Online].

- Thakor, V.A., Razzaque, M.A., Khandaker, M.R.
  Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities
  (2021) *IEEE Access*, 9, pp. 28177-28193.

- Kavun, E.B., Yalçin, T.
  A lightweight implementation of Keccak hash function for radio-frequency identification applications

(2010) *Proc. RFIDSec*, pp. 258-269.

- Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.
  Keccak sponge function family main document
  (2009) *Submission NIST*, 3 (30), pp. 320-337.

- Schneier, B.
  (2005) *NIST Hash Workshop Liveblogging*, 5.
  [Online].

- Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., Manifavas, C.
  A review of lightweight block ciphers
  (2017) *J. Cryptograph. Eng.*, 8 (2), pp. 141-184.

- (2012) *Information Technology-Security Techniques-Lightweight Cryptography-Part 1: General*,
  ISO/IEC 29192-1: 2012(en), ISO, [Online].

- Kerckhof, S., Durvaux, F., Hocquet, C., Bol, D., Standaert, F.-X.
  Towards green cryptography: A comparison of lightweight ciphers from the energy viewpoint
  (2012) *Proc. CHES*, pp. 390-407.

- Alizadeh, M., Hassan, W.H., Zamani, M., Karamizadeh, S., Ghazizadeh, E.
  Implementation and evaluation of lightweight encryption algorithms suitable for RFID
  (2013) *J. Next Gener. Inf. Technol.*, 4 (1), pp. 65-77.
  Feb.

- Aslan, B., Aslan, F.Y., Sakalli, M.T.
  Energy consumption analysis of lightweight cryptographic algorithms that can be used in the security of Internet of Things applications
  (2020) *Secur. Commun. Netw.*, pp. 88376711-883767115.
  Nov. 2020

- Caforio, A., Balli, F., Banik, S., Regazzoni, F.
  A deeper look at the energy consumption of lightweight block ciphers
  (2021) *Proc. Design, AutoM. Test Eur. Conf. Exhib. (DATE)*, pp. 170-175.
  Feb.

- (2018) *Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process*,
  NIST, [Online].

- Pei, C., Xiao, Y., Liang, W., Han, X.
  Trade-off of security and performance of lightweight block ciphers in industrial wireless sensor networks
  (2018) *EURASIP J. Wireless Commun. Netw.*, 2018 (1), pp. 1-18.
  Dec.

- Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B., Yoshida, H.
  A lightweight 256-bit hash function for hardware and low-end devices: Lesamnta-LW
  (2011) *Information Security and Cryptology-ICISC 2010*, pp. 151-168.
  K.-H. Rhee and D. Nyang, Eds. Berlin, Germany: Springer

- AlTawy, R., Raghvendra, R., Morgan, H., Kalikinkar, M., Gangqiang, Y., Guang, G.
  SLiSCP-light: Towards hardware optimized sponge-specific cryptographic permutations
  (2018) *ACM Trans. Embedded Comput. Syst.*, 17 (4), pp. 1-26.

- AlTawy, R., Rohit, R., He, M., Mandal, K., Yang, G., Gong, G.
  Towards a cryptographic minimal design: The sLiSCP family of permutations
  (2018) *IEEE Trans. Comput.*, 67 (9), pp. 1341-1358.
  Sep.

- Badel, S., Dagtekin, N., Nakahara, J., Ouafi, K., Reffé, N., Sepehrdad, P., Suŝil, P., Vaudenay, S.
  Armadillo: A multi-purpose cryptographic primitive dedicated to hardware
  (2010) *Cryptographic Hardware and Embedded Systems, CHES 2010*, pp. 398-412.
  S. Mangard and F.-X. Standaert, Eds. Berlin, Germany: Springer

- Bogdanov, A., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y.
  Hash functions and RFID tags: Mind the gap
  (2008) *Cryptographic Hardware and Embedded Systems-CHES 2008*, pp. 283-299.
  E. Oswald and P. Rohatgi, Eds. Berlin, Germany: Springer

- Poschmann, A.Y.
  (2009) *Lightweight Cryptography-Cryptographic engineering for a Pervasive World*, Cryptol. ePrint Arch., Ruhr Univ. Bochum, Bochum, Germany, Paper 2009/516, [Online].

- Aumasson, J.-P., Henzen, L., Meier, W., Naya-Plasencia, M.
  Quark: A lightweight hash
  (2012) *J. Cryptol.*, 26, pp. 313-339.
  May

- Berger, T.P., D'Hayer, J., Marquet, K., Minier, M., Thomas, G.
  The GLUON family: A lightweight hash function family based on FCSRs
  (2012) *Progress in Cryptology-AFRICACRYPT 2012*, pp. 306-323.
  A. Mitrokotsa and S. Vaudenay, Eds. Berlin, Germany: Springer

- Aumasson, J.-P., Bernstein, D.J.
  SipHash: A fast short-input PRF
  (2012) *Progress in Cryptology-INDOCRYPT 2012*, pp. 489-508.
  S. Galbraith and M. Nandi, Eds. Berlin, Germany: Springer

- Guo, J., Peyrin, T., Poschmann, A.
  The photon family of lightweight hash functions
  (2011) *Advances in Cryptology-CRYPTO 2011*, pp. 222-239.
  P. Rogaway, Ed. Berlin, Germany: Springer

- Choy, J., Yap, H., Khoo, K., Guo, J., Peyrin, T., Poschmann, A., Tan, C.H., Vaudenay, S.
  SPN-Hash: Improving the provable resistance against differential collision attacks
  (2012) *Progress in Cryptology-AFRICACRYPT 2012*, pp. 270-286.
  Berlin, Germany: Springer

- Al-Odat, Z.A., Al-Qtiemat, E.M., Khan, S.U.
  An efficient lightweight cryptography hash function for big data and IoT applications
  (2020) *Proc. IEEE Cloud Summit*, pp. 66-71.
  Oct.

- Bogdanov, A., Kneẑevic, M., Leander, G., Toz, D., Varici, K., Verbauwhede, I.
  Spongent: A lightweight hash function
  (2011) *Cryptographic Hardware and Embedded Systems-CHES 2011*, pp. 312-325.
  B. Preneel and T. Takagi, Eds. Berlin, Germany: Springer

- Bogdanov, A., Kneẑevic, M., Leander, G., Toz, D., Varici, K., Verbauwhede, I.
  SPONGENT: The design space of lightweight cryptographic hashing
  (2013) *IEEE Trans. Comput.*, 62 (10), pp. 2041-2053.
  Oct.

- Bernstein, D.J., Kölbl, S., Lucks, S., Massolino, P.M.C., Mendel, F., Nawaz, K., Schneider, T., Viguier, B.
  Gimli: A cross-platform permutation
  (2017) *Cryptographic Hardware and Embedded Systems-CHES 2017*, pp. 299-320.
  W. Fischer and N. Homma, Eds. Cham, Switzerland: Springer

- Bernstein, D.J., Kölbl, S., Lucks, S., Massolino, P.M.C., Mendel, F., Nawaz, K., Schneider, T., Todo, Y.
  (2019) *Gimli 20190927*,
  [Online].

- Afryansyah, D.I., Magfirawaty, M., Ramli, K.
  The development and analysis of TWISH: A lightweight-block-cipher-TWINE-based hash function
  (2018) *Proc. 13th Int. Conf. Digit. Inf. Manage. (ICDIM)*, pp. 210-215.

- AlTawy, R., Rohit, R., He, M., Mandal, K., Yang, G., Gong, G.
  SLiSCP: Simeck-based permutations for lightweight sponge cryptographic primitives
  (2018) *Selected Areas in Cryptography-SAC 2017*, pp. 129-150.
  C. Adams and J. Camenisch, Eds. Cham, Switzerland: Springer

- AlTawy, R., Rohit, R., He, M., Mandal, K., Yang, G., Gong, G.
  (2017) *SLiSCP-Light: Towards Lighter Sponge-Specific Cryptographic Permutations*,
  [Online].

- Aagaard, M., AlTawy, R., Gong, G., Mandal, K., Rohit, R.
  ACE: An authenticated encryption and hash algorithm
  Submission NIST LWC Competition,
  [Online].

- Dobraunig, C., Mendel, F., Eichlseder, M., Schläffer, M.
  (2021) *Ascon V1.2 Submission to NIST*,
  [Online].

- Zhang, W., Ding, T., Yang, B., Bao, Z., Xiang, Z., Ji, F., Zhao, X.
  (2019) *KNOT: Algorithm Specifications and Supporting Document*,
  [Online].

- Zhang, W., Ding, T., Yang, B., Bao, Z., Xiang, Z., Ji, F., Zhao, X., Zhou, C.
  (2020) *Update on Security Analysis and Implementations of KNOT*,
  [Online].

- Riou, S.
  (2019) *DryGASCON Lightweight Cryptography Standardization Process round 1 submission*,
  [Online].

- Chakraborty, B., Nandi, M.
  (2019) *ORANGE*,
  [Online].

- Bao, Z., Chakraborti, A., Datta, N., Guo, J., Nandi, M., Peyrin, T., Yasuda, K.
  (2021) *PHOTON-Beetle Authenticated Encryption and Hash Family*,
  [Online].

- Beierle, C., Biryukov, A., Santos, L.C.D., Großschädl, J., Perrin, L., Udovenko, A., Velichkov, V., Wang, Q.
  Lightweight AEAD and hashing using the sparkle permutation family
  (2020) *IACR Trans. Symmetric Cryptol.*, 2020, pp. 208-261.

Jun., [Online].

- Beierle, C., Biryukov, A., Santos, L.C.D., Großschädl, J., Moradi, A., Perrin, L., Shahmirzadi, A.R., Wang, Q.
(2021) *Schwaemm and Esch: Lightweight Authenticated Encryption and Hashing Using the Sparkle Permutation Family*,
[Online].

- Daemen, J., Massolino, P.M.C., Rotella, Y.
(2019) *The Subterranean 2.0 Cipher Suite*,
[Online].

- Daemen, J., Massolino, P.M.C., Mehrdad, A., Rotella, Y.
The subterranean 2.0 cipher suite
(2020) *IACR Trans. Symmetric Cryptol.*, 2020, pp. 262-294.
Jun., [Online].

- Daemen, J., Hoffert, S., Mella, S., Peeters, M., Assche, G.V., Keer, R.V.
(2021) *Xoodyak, a Lightweight Cryptographic Scheme*,
[Online].

- Huang, Y., Li, S., Sun, W., Dai, X., Zhu, W.
HVH: A lightweight hash function based on dual pseudo-random transformation
(2021) *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, pp. 492-505.
G. Wang, B. Chen, W. Li, R. Di Pietro, X. Yan, and H. Han, Eds. Cham, Switzerland: Springer

- Hanouti, I.E., Fadili, H.E., Hraoui, S., Jarjar, A.
A lightweight hash function for cryptographic and pseudo-cryptographic applications
(2022) *WITS 2020*, pp. 495-505.
S. Bennani, Y. Lakhrissi, G. Khaissidi, A. Mansouri, and Y. Khamlichi, Eds. Singapore: Springer

- Wu, W., Wu, S., Zhang, L., Zou, J., Dong, L.
(2013) *LHASH: A Lightweight Hash Function (Full Version)*,
Cryptol. ePrint Arch., Paper 2013/867, [Online].

- Wu, W., Wu, S., Zhang, L., Zou, J., Dong, L.
LHash: A lightweight hash function
(2014) *Information Security and Cryptology (Lecture Notes in Computer Science)*, 8567, pp. 291-308.
D. Lin, S. Xu, and M. Yung, Eds. Cham, Switzerland: Springer

- Bussi, K., Dey, D., Kumar, M., Dass, B.K.
(2016) *Neeva: A Lightweight Hash Function*,
Cryptol. ePrint Arch., New Delhi, India, Paper 2016/042, [Online].

- Hanin, C., Echandouri, B., Omary, F., Bernoussi, S.E.
L-CAHASH: A novel lightweight hash function based on cellular automata for RFID
(2017) *Ubiquitous Networking*, pp. 287-298.
E. Sabir, A. G. Armada, M. Ghogho, and M. Debbah, Eds. Cham, Switzerland: Springer

- Mukundan, P.M., Manayankath, S., Srinivasan, C., Sethumadhavan, M.
Hash-one: A lightweight cryptographic hash function
(2016) *IET Inf. Secur.*, 10 (5), pp. 225-231.
Sep.

- Sadak, A., Echandouri, B., Ezzahra, F., Hanin, C., Omary, F.
  LCAHASH-1.1: A new design of the LCAHASH system for IoT
  (2019) *Int. J. Adv. Comput. Sci. Appl.*, 10 (11), pp. 1-5.

- Zhang, X., Xu, Q., Li, X., Wang, C.
  A lightweight hash function based on cellular automata for mobile network
  (2019) *Proc. 15th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, pp. 247-252.
  Dec.

- Nabeel, N., Habaebi, M.H., Islam, M.D.R.
  Security analysis of LNMNT-lightweight crypto hash function for IoT
  (2021) *IEEE Access*, 9, pp. 165754-165765.

- Nabeel, N., Habaebi, M.H., Rafiqul Islam, M.
  LNMNT-new Mersenne number based lightweight crypto hash function for IoT
  (2021) *Proc. 8th Int. Conf. Comput. Commun. Eng. (ICCCE)*, pp. 68-71.
  Jun.

- Merkle, R.C.
  One way hash functions and DES
  (1990) *Advances in Cryptology-CRYPTO'89 Proceedings*, pp. 428-446.
  G. Brassard, Ed. New York, NY, USA: Springer

- Damgård, I.B.
  A design principle for hash functions
  (1989) *Advances in Cryptology-CRYPTO'89 Proceedings (Lecture Notes in Computer Science)*, 435, pp. 416-427.
  New York, NY, USA: Springer, [Online].

- Duong, T., Rizzo, J.
  (2009) *Flickr's API Signature Forgery Vulnerability*,
  [Online].

- Al-Odat, Z., Khan, S.
  Constructions and attacks on hash functions
  (2019) *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, pp. 139-144.
  Los Alamitos, CA, USA: IEEE Computer Society, Dec., [Online].

- Brachtl, B.O., Coppersmith, D., Hyden, M.M., Matyas, S.M., Jr., Meyer, C.H., Oseas, J., Pilpel, S., Schilling, M.
  (1990) *Data Authentication Using Modification Detection Codes Based On A Public One Way Encryption Function*,
  U.S. Patent, Mar. 13

- (1977) *Data Encryption Standard Standard FIPS PUB 46*, pp. 42-46.
  Federal Information Processing Standards Publication, NBS

- Preneel, B.
  Davies-Meyer hash function
  (2005) *Encyclopedia of Cryptography and Security*, pp. 136-136.
  H. C. A. van Tilborg, Ed. Boston, MA, USA: Springer

- Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.
  (2007) *Sponge Functions*,
  [Online].

- Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.
  (2011) *The Keccak reference*, pp. 1-14.
  [Online].

- Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.
  On the indif-ferentiability of the sponge construction
  (2008) *Advances in Cryptology-EUROCRYPT 2008*, pp. 181-197.
  N. Smart, Ed. Berlin, Germany: Springer

- Li, Y., Ge, G., Xia, D.
  Chaotic hash function based on the dynamic S-box with variable parameters
  (2016) *Nonlinear Dyn.*, 84 (4), pp. 2387-2402.

- Alawida, M., Samsudin, A., Alajarmeh, N., Teh, J.S., Ahmad, M., Alshoura, W.H.
  A novel hash function based on a chaotic sponge and DNA sequence
  (2021) *IEEE Access*, 9, pp. 17882-17897.

- Teh, J.S., Tan, K., Alawida, M.
  A chaos-based keyed hash function based on fixed point representation
  (2019) *Cluster Comput.*, 22 (2), pp. 649-660.

- Abdoun, N., Assad, S.E., Hoang, T.M., Deforges, O., Assaf, R., Khalil, M.
  Designing two secure keyed hash functions based on sponge construction and the chaotic neural network
  (2020) *Entropy*, 22 (9), p. 1012.
  Sep., [Online].

- Teh, J.S., Alawida, M., Ho, J.J.
  Unkeyed hash function based on chaotic sponge construction and fixed-point arithmetic
  (2020) *Nonlinear Dyn.*, 100 (1), pp. 713-729.
  Mar.

- Hirose, S.
  Some plausible constructions of double-block-length hash functions
  (2006) *Fast Software Encryption*, pp. 210-225.
  M. Robshaw, Ed. Berlin, Germany: Springer

- Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.
  TWINE: A lightweight block cipher for multiple platforms
  (2013) *Selected Areas in Cryptography*, pp. 339-354.
  L. R. Knudsen and H. Wu, Eds. Berlin, Germany: Springer

- Doganaksoy, A., Ege, B., Koçak, O., Sulak, F.
  (2010) *Cryptographic Randomness Testing of Block Ciphers And Hash Functions*,
  Cryptol. ePrint Arch., Paper 2010/564, [Online].

- Hell, M., Johansson, T.
  Breaking the F-FCSR-H stream cipher in realtime
  (2008) *Advances in Cryptology-ASIACRYPT 2008*, pp. 557-569.
  J. Pieprzyk, Ed. Berlin, Germany: Springer

- De Cannière, C., Dunkelman, O., Kneẑevic, M.
  KATAN and KTANTAN-A family of small and efficient hardware-oriented block ciphers
  (2009) *Cryptographic Hardware and Embedded Systems-CHES 2009*, pp. 272-288.
  C. Clavier and K. Gaj, Eds. Berlin, Germany: Springer

- Berger, F.A.T., Lauradoux, C.
  (2008) *F-FCSR (Phase 3 Profile 2)*,
  [Online].

- Arnault, F., Berger, T.P., Lauradoux, C., Minier, M.
  (2007) *X-FCSR: A New Software Oriented Stream Cipher Based Upon FCSRS*,
  [Online].

- Wu, H.
  (2011) *The Hash Function JH*,
  [Online].

- (2001) *Announcing the Advanced Encryption Standard (AES)*,
  NIST, [Online].

- Aumasson, J.-P., Meier, W., Phan, R., Henzen, L.
  (2014) *The Hash Function BLAKE*,
  Berlin Germany: Springer

- Ferguson, N.
  The skein hash function family
  (2010) *Argument*, 30 (4), p. 79.
  [Online].

- Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.
  The Simeck family of lightweight block ciphers
  (2015) *Cryptographic Hardware and Embedded Systems-CHES 2015*, pp. 307-329.
  T. Güneysu and H. Handschuh, Eds. Berlin, Germany: Springer

- Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.
  (2015) *The Simeck Family of Lightweight Block Ciphers*,
  Cryptol. ePrint Arch., Waterloo, ON, Canada, Paper 2015/612, [Online].

- Bernstein, D.J.
  (2019) *CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness*,
  Feb., [Online].

- Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.
  (2014) *Rectangle: A Bit-Slice Lightweight Block Cipher Suitable For Multiple Platforms*,
  Cryptol. ePrint Arch., Paper 2014/084, [Online].

- Zhang, W.T., Bao, Z.Z., Lin, D.D., Rijmen, V., Yang, B., Verbauwhede, I.
  RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms
  (2015) *Sci. China Inf. Sci.*, 58 (12), pp. 1-15.
  Dec.

- Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.
  Ascon v1.2
  (2016) *Submission CAESAR Competition*,
  [Online].

- Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.
  Duplexing the sponge: Single-pass authenticated encryption and other applications
  (2012) *Selected Areas in Cryptography*, pp. 320-337.
  A. Miri and S. Vaudenay, Eds. Berlin, Germany: Springer

- (2007) *Federal Register: Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family*,
  NIST, [Online].

- Chakraborti, A., Datta, N., Nandi, M., Yasuda, K.
  Beetle family of lightweight and secure authenticated encryption ciphers
  (2018) *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, 2018 (2), pp. 218-241.

May, [Online].

- Claesen, L., Daemen, J., Genoe, M., Peeters, G.
Subterranean: A 600 Mbit/sec cryptographic VLSI chip
(1993) *Proc. IEEE Int. Conf. Com-put. Design (ICCD)*, pp. 610-613.
Oct.

- Daemen, J., Hoffert, S., Van Assche, G., Van Keer, R.
The design of Xoodoo and Xoofff
(2018) *IACR Trans. Symmetric Cryptol.*, 2018 (4), pp. 1-38.
Dec., [Online].

- Daemen, J., Hoffert, S., Peeters, M., Assche, G.V., Keer, R.V.
Xoodoo cookbook
(2018) *Cryptol. ePrint Arch*,
Nijmegen, The Netherlands, Tech. Rep. 2018/767, [Online].

- Xuejun, D., Yuhua, H., Lu, C., Lu, T., Fei, S.
VH: A lightweight block cipher based on dual pseudo-random transformation
(2015) *Proc. Int. Conf. Cloud Comput. Secur.*, pp. 3-13.

- Marsaglia, G.
(2016) *The Marsaglia Random Number CDROM Including the Diehard Battery of Tests of Randomness*,
Jan., [Online].

- Biham, E., Shamir, A.
(1993) *Differential Cryptanalysis of the Data Encryption Standard*,
Berlin Germany: Springer-Verlag

- Biham, E., Shamir, A.
Differential cryptanalysis of the full 16-round DES
(1993) *Advances in Cryptology-CRYPTO'92*, pp. 487-496.
E. F. Brickell, Ed. Berlin, Germany: Springer

- Biham, E., Shamir, A.
Differential cryptanalysis of DES-like cryp-tosystems
(1990) *Proc. Adv. Cryptol. (CRYPTO)*, 537, pp. 2-21.
A. J. Menezes and S. A. Vanstone, Eds. Berlin, Germany: Springer

- Biham, E.
New types of cryptanalytic attacks using related keys
(1994) *J. Cryptol.*, 7 (4), pp. 229-246.
Dec.

- Wiener, M.J.
The full cost of cryptanalytic attacks
(2004) *J. Cryptol.*, 17 (2), pp. 105-124.
Mar.

- Bagheri, N., Ghaedi, N., Sanadhya, S.K.
Differential fault analysis of SHA-3
(2015) *Proc. INDOCRYPT*, pp. 253-269.

- Altawy, R., Youssef, A.M.
Differential fault analysis of Streebog
(2015) *Proc. ISPEC*, pp. 35-49.

- Safkhani, M., Arghavani, M.A.
  A survey of cube, differential fault analysis attacks and linear structures on Keccak hash function (SHA-3)
  (2017) *Biannual J. Monadi Cyberspace Secur.*, 5 (2), pp. 3-14.
  [Online].

- Luo, P., Fei, Y., Zhang, L., Ding, A.A.
  Differential fault analysis of SHA-3 under relaxed fault models
  (2017) *J. Hardw. Syst. Secur.*, 1 (2), pp. 156-172.
  Jun.

- Matsui, M.
  Linear cryptanalysis method for DES cipher
  (1994) *Advances in Cryptology-EUROCRYPT'93*, pp. 386-397.
  T. Helleseth, Ed. Berlin, Germany: Springer

- Matsui, M.
  The first experimental cryptanalysis of the data encryption standard
  (1994) *Advances in Cryptology-CRYPTO'94*, pp. 1-11.
  Y. G. Desmedt, Ed. Berlin, Germany: Springer

- Daemen, J., Knudsen, L., Rijmen, V.
  The block cipher SQUARE
  (1997) *Proc. Int. Workshop Fast Softw. Encryption (Lecture Notes in Computer Science)*, 1267, pp. 149-165.

- Lucks, S.
  Attacking seven rounds of Rijndael under 192-bit and 256-bit keys
  (2000) *Proc. 3rd AES Candidate Conf*, pp. 215-229.
  New York, NY, USA, Apr., [Online].

- Knudsen, L., Wagner, D.
  Integral cryptanalysis
  (2002) *Fast Software Encryption*, pp. 112-127.
  J. Daemen and V. Rijmen, Eds. Berlin, Germany: Springer

- Matsui, M.
  New block encryption algorithm MISTY
  (1997) *Fast Software Encryption*, pp. 54-68.
  E. Biham, Ed. Berlin, Germany: Springer

- (2016) *Information Technology-Security Techniques-Lightweight Cryptography-Part 5: Hash-Functions*,
  Standard ISO/IEC 29192-5: 2016(en), [Online].

- Kaps, J.-P., Diehl, W., Tempelmeier, M., Farahmand, F., Homsirikamol, E., Gaj, K.
  (2019) *A Comprehensive Framework For Fair And Efficient Benchmarking Of Hardware Implementations Of Lightweight Cryptography*,
  Cryptol. ePrint Arch., Paper 2019/1273, [Online].

- Al-Shatari, M.O.A., Hussin, F.A., Aziz, A.A., Witjaksono, G., Tran, X.-T.
  FPGA-based lightweight hardware architecture of the PHOTON hash function for IoT edge devices
  (2020) *IEEE Access*, 8, pp. 207610-207618.

- (2020) *Benchmarking of Lightweight Cryptographic Algorithms on Microcontrollers*,
  NIST, [Online].

- Renner, S., Pozzobon, E., Mottok, J.
  (2021) *LWC Benchmark*,
  [Online].

- Beierle, C., Biryukov, A., Santos, L.C.D., Großschädl, J., Perrin, L., Udovenko, A., Velichkov, V., Wang, Q.
  Alzette: A 64-bit ARX-box
  (2020) *Advances in Cryptology-CRYPTO 2020*, pp. 419-448.
  D. Micciancio and T. Ristenpart, Eds. Cham, Switzerland: Springer

- Moldovyan, A.A., Moldovyan, N.A.
  A cipher based on data-dependent permutations
  (2002) *J. Cryptol.*, 15 (1), pp. 61-72.
  Mar.

- Naya-Plasencia, M., Peyrin, T.
  Practical cryptanalysis of ARMADILLO2
  (2012) *Fast Software Encryption*, pp. 146-162.
  A. Canteaut, Ed. Berlin, Germany: Springer

- Abdelraheem, M.A., Blondeau, C., Naya-Plasencia, M., Videau, M., Zenner, E.
  Cryptanalysis of ARMADILLO2
  (2011) *Advances in Cryptology-ASIACRYPT 2011*, pp. 308-326.
  D. H. Lee and X. Wang, Eds. Berlin, Germany: Springer

- Koyama, T., Sasaki, Y., Kunihiro, N.
  Multi-differential cryptanalysis on reduced DM-PRESENT-80: Collisions and other differential properties
  (2012) *Proc. ICISC*, pp. 352-367.

- Blondeau, C., Peyrin, T., Wang, L.
  (2015) *Known-Key Distinguisher On Full Present*,
  Cryptol. ePrint Arch., Paper 2015/575, [Online].

- Sasaki, Y., Aoki, K.
  Improved integral analysis on tweaked Lesamnta
  (2011) *Proc. ICISC*, pp. 1-17.

- Shiba, R., Sakamoto, K., Liu, F., Minematsu, K., Isobe, T.
  Integral and impossible-differential attacks on the reduced-round Lesamnta-LW-BC
  (2022) *IET Inf. Secur.*, 16 (2), pp. 75-85.
  Mar.

- Zhang, K., Guan, J., Fei, X.
  Improved conditional differential crypt-analysis
  (2015) *Secur. Commun. Netw.*, 8 (9), pp. 1801-1811.
  Jun.

- Yang, J., Liu, M., Lin, D., Wang, W.
  Symbolic-like computation and conditional differential cryptanalysis of quark
  (2018) *Proc. IWSEC*, pp. 244-261.

- Lu, C.-Y., Lin, Y.-W., Jen, S.-M., Yang, J.-F.
  Cryptanalysis on PHOTON hash function using cube attack
  (2012) *Proc. Int. Conf. Inf. Secur. Intell. Control*, pp. 278-281.
  Aug.

- Walter, M.
  (2012) *Algebraic Methods in Analyzing Lightweight Cryptographic Symmetric Primitives*,
  Technische Universitat Darmstadt, Darmstadt, Germany, [Online].

- Abdelraheem, M.A.
Estimating the probabilities of low-weight differential and linear approximations on present-like ciphers
(2013) *Information Security and Cryptology-ICISC 2012*, pp. 368-382.
T. Kwon, M.-K. Lee, and D. Kwon, Eds. Berlin, Germany: Springer

- Fan, S., Duan, M.
Improved zero-sum distinguisher for SPONGENT-88
(2015) *Proc. Int. Conf. Electromech. Control Technol. Transp. Dordrecht, The Netherlands: Atlantis Press*, pp. 582-587.
Nov.

- Sun, L., Wang, W., Wang, M.
(2016) *MILP-Aided Bit-Based Division Property For Primitives With Non-Bit-Permutation Linear Layers*,
Cryptol. ePrint Arch., Paper 2016/811, [Online].

- Perrin, L., Khovratovich, D.
Collision spectrum, entropy loss, T-sponges, and cryptanalysis of GLUON-64
(2015) *Fast Software Encryption*, pp. 82-103.
C. Cid and C. Rechberger, Eds. Berlin, Germany: Springer

- Dobraunig, C., Mendel, F., Schläffer, M.
Differential cryptanalysis of SipHash
(2014) *Selected Areas in Cryptography-SAC 2014*, pp. 165-182.
A. Joux and A. Youssef, Eds. Cham, Switzerland: Springer

- Xin, W., Liu, Y., Sun, B., Li, C.
Improved cryptanalysis on SipHash
(2019) *Cryptology and Network Security*, pp. 61-79.
Y. Mu, R. H. Deng, and X. Huang, Eds. Cham, Switzerland: Springer

- Susanti, B.H., Bayhaqi, M.R.R., Ardyani, M.W.
Correcting block attack on the 32-bit reduced NEEVA
(2020) *Proc. 1st Int. Conf. Inf. Technol., Adv. Mech. Electr. Eng. (ICITAMEE)*, pp. 85-90.
Oct.

- Gutiérrez, A.F., Leurent, G., Naya-Plasencia, M., Perrin, L., Schrotten-Loher, A., Sibleyras, F.
(2020) *Internal symmetries and linear properties: Full-permutation distinguishers and improved collisions on Gimli*,
Cryptol. ePrint Arch., Inria, France, Paper 2020/744, [Online].

- Gutiérrez, A.F., Leurent, G., Naya-Plasencia, M., Perrin, L., Schrot-Tenloher, A., Sibleyras, F.
New results on Gimli: Full-permutation distinguishers and improved collisions
(2020) *Advances in Cryptology-ASIACRYPT 2020*, pp. 33-63.
S. Moriai and H. Wang, Eds. Cham, Switzerland: Springer

- Liu, F., Isobe, T., Meier, W.
(2020) *Preimages and Collisions For Up to 5-Round Gimli-Hash Using Divide-And-Conquer Methods*,
Cryptol. ePrint Arch., Shanghai, China, Tech. Rep. 2019/1080, [Online].

- Liu, F., Isobe, T., Meier, W.
Exploiting weak diffusion of Gimli: Improved distinguishers and preimage attacks
(2021) *IACR Trans. Symmetric Cryptol.*, 2021 (1), pp. 185-216.
Mar., [Online].

- Liu, F., Isobe, T., Meier, W.
  (2019) *Exploiting weak diffusion of Gimli: Improved distinguishers and preimage attacks*,
  Cryptol. ePrint Arch., Shanghai, China, Paper 2020/561, [Online].

- Liu, F., Isobe, T., Meier, W.
  Automatic verification of differential characteristics: Application to reduced Gimli
  (2020) *Advances in Cryptology-CRYPTO 2020*, pp. 219-248.
  D. Micciancio and T. Ristenpart, Eds. Cham, Switzerland: Springer

- Liu, Y., Sasaki, Y., Song, L., Wang, G.
  Cryptanalysis of reduced sLiSCP permutation in sponge-hash and duplex-AE modes
  (2019) *Selected Areas in Cryptography-SAC 2018*, pp. 92-114.
  C. Cid and M. J. Jacobson, Jr., Eds. Cham, Switzerland: Springer

- Kraleva, L., Posteuca, R., Rijmen, V.
  Cryptanalysis of the permutation based algorithm SpoC
  (2020) *Progress in Cryptology-INDOCRYPT 2020*, pp. 273-293.
  K. Bhargavan, E. Oswald, and M. Prabhakaran, Eds. Cham, Switzerland: Springer

- Liu, J., Liu, G., Qu, L.
  A new automatic tool searching for impossible differential of NIST candidate ACE
  (2020) *Mathematics*, 8 (9), p. 1576.
  Sep.

- Zong, R., Dong, X., Wang, X.
  (2019) *Collision attacks on round-reduced Gimli-Hash/Ascon-Xof/Ascon-Hash*,
  Cryptol. ePrint Arch., Shanghai, China, Paper 2019/1115, [Online].

- Tezcan, C.
  Analysis of Ascon, DryGASCON, and Shamash permutations
  (2020) *Int. J. Inf. Secur. Sci.*, 9 (3), pp. 172-187.

- Ramezanpour, K., Abdulgadir, A., Diehl, W., Kaps, J.-P., Ampadu, P.
  (2020) *Active and Passive Side-Channel Key Recovery Attacks on Ascon*,
  [Online].

- Zhang, W., Ding, T., Zhou, C., Ji, F.
  (2020) *Security Analysis of KNOT-AEAD and KNOT-Hash*,
  [Online].

- Tezcan, C.
  (2020) *Analysis of Ascon, DryGASCON, and Shamash permutations*,
  Cryptol. ePrint Arch., Ankara, Turkey, Paper 2020/1458, [Online].

- Liang, H., Mesnager, S., Wang, M.
  Cryptanalysis of the AEAD and hash algorithm DryGASCON
  (2022) *Cryptogr. Commun.*, 14 (3), pp. 597-625.
  May

Correspondence Address
Ramli K.; Universitas Indonesia, Indonesia; email: kalamullah.ramli@ui.ac.id

Publisher: Institute of Electrical and Electronics Engineers Inc.

ISSN: 21693536
Language of Original Document: English
Abbreviated Source Title: IEEE Access
2-s2.0-85135766413
Document Type: Article
Publication Stage: Final
Source: Scopus