Document details

International Journal of Interactive Mobile Technologies Open Access
Volume 13, Issue 4, 2019, Pages 117-129

[redacted] crypto functions (Article) (Open Access)

Nabeel, N.[a], Habaebi, M.H.[a], Mustapha, N.A.C.[b], Islam, M.R.[c]

[a]Department o Electrical and Computer Engineering, International Islamic University Malaysia, Malaysia
[b]Electrical and Computer Engineering Department, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM), Malaysia
[c]Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia, Malaysia

Abstract

View references (11)

We are in the era of IoT and 5G technologies. IoT has wide range of applications in Smart Home, Smart cities, Agriculture, Health etc. Due to that, the number of connected sensor devices become increased. Along with that security of these devices become a challenging issue. By the next year there would be a great increase in the number of connected sensor devices. For the power constrained devices like sensors and actuators, they requires lightweight security mechanism. There are several Lightweight (LW) energy efficient Hashing techniques are available. They are photon, quark, spongent, Lesamnta- LW etc. These all are fixed length block sized and key sized LW hashing techniques. All transformation methods used today in LW hash function only support fixed block size and key size and requires high hardware requirements too. In this paper, we compare different types of LW hash families in terms of their design and introduce the possibility of variable length hash function using Mersenne number based transform.

Author keywords

Diffusion | Energy efficiency | Lightweight hashing techniques | Mersenne number

Funding details

Funding sponsor	Funding number	Acronym
International Islamic University Malaysia	RIGS17-023-0598	IIUM

Funding text

This work is partially supported by International Islamic University Malaysia, Research Initiative Grant Scheme no. RIGS17-023-0598. It was conducted at IoT & Wireless Communication Protocols Lab, ECE/KoE/IIUM.

ISSN: 18657923
Source Type: Journal
Original language: English
DOI: 10.3991/IJIM.V13I04.10524
Document Type: Article
Publisher: International Association of Online Engineering

References (11)

View in search results format

1 Sánchez-Arias, G., González García, C., Pelayo G-Bustelo, B.C.

Midgar: Study of communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things

(2017) *Future Generation Computer Systems*, 74, pp. 444-466. Cited 13 times.
doi: 10.1016/j.future.2017.01.033

View at Publisher

2 Tareq Hammad, B., Jamil, N., Ezanee Rusli, M., Reza, M.Z.
A survey of Lightweight Cryptographic Hash Function
(2017) *Int. J. Sci. Eng. Res*, 8 (7). Cited 2 times.

3 Li, W., Liao, L., Gu, D., Ge, C., Gao, Z., Zhou, Z., Guo, Z., (...), Liu, Z.

Security analysis of the photon lightweight cryptosystem in the wireless body area network

(2018) *KSII Transactions on Internet and Information Systems*, 12 (1), pp. 476-496.
http://www.itiis.org/digital-library/manuscript/file/1913/TIIS+Vol+12,+No+1-23.pdf
doi: 10.3837/tiis.2018.01.023

View at Publisher

4 Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mennink, B., Mouha, N., Yasuda, K.

APE: Authenticated permutation-based encryption for lightweight cryptography

(2015) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8540, pp. 168-186. Cited 26 times.
http://springerlink.com/content/0302-9743/copyright/2005/
ISBN: 978-366246705-3
doi: 10.1007/978-3-662-46706-0_9

View at Publisher

5 Zhang, W., Bao, Z., Rijmen, V., Liu, M.

A new classification of 4-bit optimal s-boxes and its application to PRESENT, RECTANGLE and SPONGENT

(2015) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9054, pp. 494-515. Cited 8 times.
http://springerlink.com/content/0302-9743/copyright/2005/
ISBN: 978-366248115-8
doi: 10.1007/978-3-662-48116-5_24

View at Publisher

6 Canteaut, A., Roué, J.

Differential attacks against SPN: A thorough analysis

(2015) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9084, pp. 45-62.
http://springerlink.com/content/0302-9743/copyright/2005/
ISBN: 978-331918680-1
doi: 10.1007/978-3-319-18681-8_4

View at Publisher

7 Collard, B., Standaert, F.-X.

A statistical saturation attack against the block cipher present

(2009) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5473, pp. 195-210. Cited 61 times.
ISBN: 978-364200861-0
doi: 10.1007/978-3-642-00862-7_13

View at Publisher

8 Akhimullah, A., Hirose, S.

Lightweight hashing using lesamnta-lw compression function mode and MDP domain extension

(2016) *Proceedings - 2016 4th International Symposium on Computing and Networking, CANDAR 2016*, art. no. 7818677, pp. 590-596.
ISBN: 978-150902655-5
doi: 10.1109/CANDAR.2016.6

View at Publisher

9 Wu, W., Wu, S., Zhang, L., Zou, J., Dong, L.

LHash: A lightweight hash function

(2014) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8567, pp. 291-308. Cited 13 times.
http://springerlink.com/content/0302-9743/copyright/2005/
ISBN: 978-331912086-7
doi: 10.1007/978-3-319-12087-4_19

View at Publisher

10 Li, G., Lei, L., Zhou, W.

Radix-8 algorithm for the new Mersenne number transform

(2013) *2013 International Conference on Communications, Circuits and Systems, ICCCAS 2013*, 2, art. no. 6765305, pp. 143-146.
doi: 10.1109/ICCCAS.2013.6765305

View at Publisher

11 Rutter, N., Boussakta, S., Bystrov, A.

Assessment of the one-dimensional generalized new mersenne number transform for security systems

(2013) *IEEE Vehicular Technology Conference*, art. no. 6692461.
ISBN: 978-146736337-2
doi: 10.1109/VTCSpring.2013.6692461

View at Publisher

Nabeel, N.; Department o Electrical and Computer Engineering, International Islamic University Malaysia, Malaysia; email:13ganesh@mail.com