iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.84007

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

FPGA Implementation and Analysis of Cryptographic Hash Functions for Blockchain Systems

Ms. P. R. Lawhale[1], Dr. S. N. Kale[2]
[1]*PhD Scholar,PG Department of Applied Electronics,SGBAU,Amravati*
[2]*Professor, PG Department of Applied Electronics, SGBAU, Amravati*

Abstract: ***Due to the rapid developments in the wireless communications area and personal communications systems, providing information security has become a more and more important subject. This security concept becomes a more complicated subject when next-generation system requirements and real-time computation speed are considered. Most of the data transmitted over the communication channel are highly confidential so it needs more security. But this confidential data are easily stolen by hackers and it affects the users' privacy. Nowadays, so many cryptographic algorithms have been established to protect the original information of the users. Cryptographic hash functions are used to protect information integrity and authenticity in a wide range of applications. Hash Function (HF) security is the most important primitive which used for data authentication and data integrity. The reconfigurable cryptography integrated with chip which used for cryptography. Hashing algorithm is used to generate the random number which also used as a key value for cryptography.***

In our propose work, we will construct the lightweight blockchain architecture based on FPGA, mainly we have to consider the performance of the hash function. Also, we will conduct an analysis of lightweight hash for blockchain, and propose a new lightweight hash-based blockchain architecture that can change the hash algorithm used for mining. We will investigate high speed and low-area hardware architectures. The hardware is described in VHDL/Verilog and simulate, verify on Altera/Xilinx FPGAs using Quartus II/Xilinx ISE software. The circuit realized through the FPGA is tested as a prototype on FPGA Development Board/Kit. However, in results, the analysis in perspective of cryptographic performance will be done by area, throughput, latency and power consumption.

Keywords: FPGA, Lightweight Cryptography, Blockchain, Hash Function, Power Consumption, SHA-256, Secure Architecture.

I. INTRODUCTION

Nowadays, in wireless communication, the Internet-of-Things (IoT) is the backbone for a variety of smart application domains, including smart cities, smart healthcare, smart transportation and many sectors. The Internet of Everything (IoE) is a concept that has the IoT integrated as one of the components of its architecture and environment. People, Data and Processes are the other three components in an IoE environment. Data collection is one of the crucial elements of IoE. The amount of data collected in the IoE environment increases daily. The devices used for such applications are low performance, low power consumption devices which cannot provide high computational power to the architecture. In such scenarios, introducing an "Edge Layer" will aid the entire network of devices by reducing the computing load. In some use cases, near real-time processing can also be achieved with the help of an edge datacenter. Blockchain technology can be used to remove the requirement of a central entity from IoT architectures. A decentralized public ledger is used in the blockchain for organizing the data and executing the transactions. Every node connected to the network has a copy of the ledger . This helps in maintaining consistency and security. A blockchain is cryptographically anchored and tamper-proof and is a collection of different transactions that occurred among the participants in the network. The data blocks are connected with the hash value of each previous block, and the ledger, including all of the information about the transactions, which is stored in each node in the distributed network. The distributed ledger is updated by making a consensus using defined consensus protocol such as Proof of Work (PoW), Proof of Stake (PoS), Proof of Property (PoP) , it helps entire sharing of the same data blocks for all nodes of the network. The idea goes far beyond the usual Internet devices such as computers, tablets or smart phones and a large part of these devices will use wireless network technologies. Almost all of these applications need to be protected by effective security mechanisms, because many will have an influence of the privacy or the safety of people. Many more such modern applications of networking technology exist and a lot of them are in need of tailored security solutions.

©IJRASET: All Rights are Reserved

In the current day of the Internet of Things (IoT) and embedded processor and internet connections are getting integrated seamlessly into our everyday life. Access of the information or control over the smart devices by unsavory people would lead to undesirable consequences. Hence, safeguarding one's privacy and security is paramount. Cryptographic algorithms are employed to address these issues.

There are three types of cryptographic algorithms: Message Encryption, Message Authentication Code (MAC) and Hash functions. To provide data integrity, any message could be simply encrypted. But the heavy mathematical functions involved utilize bulk of the CPU resources thus incurring large overheads. To reduce this load, certain applications use a lightweight procedure called a oneway hash or simply hash functions. Unlike Message Encryption and MAC, hash functions have no key. A hash function accepts a variable-size message M as input and produces a fixed-size output, referred to as a hash code H(M). The hash code is also referred to as a Message Digest or Hash Value. Typical application of Hash function includes Universal Unique Identifiers (UUID/GUID), Password tables, Random Number Generators and many more. But they finds their major application in Digital Signatures.

Traditional cryptographic algorithms may not be applicable for low end IoT devices as they have limited memory and computational power along with serious power and energy constraints. The branch of cryptography which addresses the security and privacy issues of these devices is called LightWeight Cryptography (LWC). Traditional cryptographic algorithms were made for data processing on a computer. Initially these algorithms were tailored for lightweight cryptographic applications. But this tailoring degraded the performance of the algorithms either in terms of security or speed or both. Therefore, new cryptographic algorithms such as Present, Hight, XTEA etc. are a few to name were designed exclusively for lightweight cryptographic applications. In general, LWC algorithms must have the attributes, Small internal state, lower area consumption, short processing time, lower energy consumption, short outputs, lower communication cost, allow serialization, lower power consumption, same primitives and same security level as traditional Some of these attributes are complimentary which can be seen in Figure 1.1. For example: Making the algorithm more serialized would reduce area and power consumption at the cost of energy and throughput. Hence, depending on the application and target device, optimization criteria and limitations are determined. In general, corner 1 in Figure 1.1 is the ideal place for lightweight applications. The other two corners 2 and 3 are for high security and low latency applications respectively. In general, corner 1 in Figure 1.1 is the ideal place for lightweight applications. The other two corners 2 and 3 are for high security and low latency applications respectively.

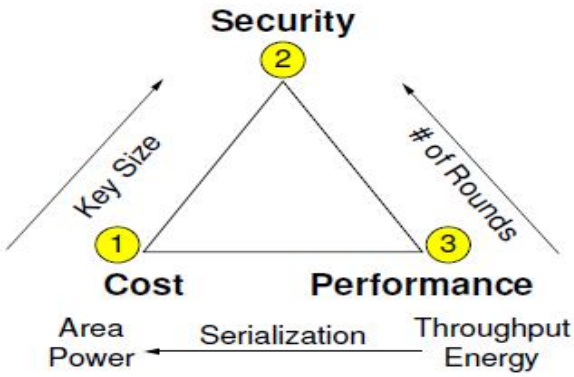


Figure 1.1: Relation of various performance parameters on algorithmic parameter

Based on the target platform, LWC algorithms can be broadly classified into two categories as software oriented and hardware algorithms. Software algorithms are implemented on a microprocessor or a microcontroller. The second category is hardware oriented algorithms which are mainly targeted for ASICs and FPGAs. Lightweight devices such as RFID tags, wireless sensor nodes and smart cards are increasingly common in applications of our daily life. These smart lightweight devices might manipulate sensitive data and thus usually require some security. Classical cryptographic algorithms are not very suitable for this type of applications, especially for very constrained environments. The main focus of lightweight cryptography research has been on the trade-offs between cost, security and performance in terms of speed, area and computational power. These primitives can be implemented either in software or in hardware platforms such as Field-Programmable Gate Array (FPGA) and Application Specific Integrated Circuit (ASIC). Compared to ASICs, FPGAs offer additional advantages in terms of time-to-market, reconfigurability and cost.

II. MOTIVATION

In the Internet of Things (IoT) vision, conventional devices become smart and autonomous. This vision is turning into a reality thanks to advances in technology, but there are still challenges to address, particularly in the security domain e.g., data reliability. Taking into account the predicted evolution of the IoT in the coming years, it is necessary to provide confidence in this huge incoming information source. Blockchain has emerged as a key technology that will transform the way in which we share information. Building trust in distributed environments without the need for authorities is a technological advance that has the potential to change many industries, the IoT among them. Disruptive technologies such as big data and cloud computing have been leveraged by IoT to overcome its limitations since its conception, and we think blockchain will be one of the next ones. Especially in IoT, most of the connected devices are small, ubiquitous, and running on battery but aimed to work for a long period of the time remotely and securely. This motivates to develop a Lightweight Blockchain which is a modified blockchain with a simplified algorithm without sacrificing data security. This type of blockchain is suitable for applications that need data reliability but limited computational resources like the Internet of Things (IoT) and Autonomous Driving. Lightweight blockchain-enabled trust evaluation mechanism in a wireless sensor network for secured data transactions between nodes.

A. Review of Literature

Vijayakumar Peroumal *et al* [1] presents a combination of RSA and SHA together to create a block on an FPGA, which when combined with other blocks establishes an encrypted Blockchain, which overcomes limitations of traditional methods of securing data using cryptographic algorithms. Synthesis and implementation of the encrypted block have been compared and analyzed on Virtex-4, Virtex-5, and Spartan-6 FPGA boards. Based on the resource requirement like the slice registers.Sa'ed Abed et.al.[2] present a literature review on the common hash functions used in blockchain-based applications. Evaluated and tested the common lightweight hash functions (SPONGENT, PHOTON, and QUARK) on FPGA platforms to determine which is most suitable for blockchain-IoT devices. Assessed lightweight hash functions in terms of area, power, energy, security, and throughput. The results show tradeoffs between these hash functions. Kwangki Ryoo et.al. [3] study implements a System-on-Chip (SoC) based lightweight cryptographic core that consists of two encryption protocols, four authentication protocols, and a key generation/exchange protocol for ultra-low-cost devices. The hardware architectures use the concept of resource sharing to minimize the hardware area. HAN Songshen et.al. [4] studies the authentication mechanism from the user equipment to the external data network in 5G and proposed an authentication protocol prototype that conforms to the Third Generation Partnership Program (3GPP) standard. The operation of the proposed authentication scheme is mainly based on the Hash function, which is more efficient than the traditional authentication scheme. It provides flexible and high-quality authentication services for IoT devices cluster in the 5G environment combining the advantages of Hash-based signature technology and 5G architecture. Florian Unterstein et.al. [5] propose a comprehensive concept that uses an alternative and side-channel protected cryptographic engine within the FPGA logic instead of the built-in one for the crucial task of bitstream decryption.. The lack of accessible secret key storage poses a significant challenge and requires the use of a physical unclonable function (PUF) to generate a device intrinsic secret within the FPGA logic. D. Kundi's et. al. [6] work undertakes AE$HA-3, a unified hardware implementation of AES+SHA-3, both of which are NIST standards for data confidentiality and integrity, respectively. Jinhua Fu et.al. [8] proposes a new scheme to optimize the blockchain hashing algorithm based on PRCA (Proactive Reconfigurable Computing Architecture). In order to improve the calculation performance of hashing function, the paper realizes the pipeline hashing algorithm and optimizes the efficiency of communication facilities and network data transmission by combining blockchains with mimic computers. Meanwhile, to ensure the security of data information, this paper chooses lightweight hashing algorithm to do multiple hashing and transforms the hash algorithm structure as well. The experimental results show that the scheme given in the paper not only improves the security of blockchains but also improves the efficiency of data processing. Byoungjin Seok et.al.[9] in this paper, the analysis in perspective of cryptographic performance (area, throughput, and power consumption) has not been considered sufficiently, or only focused on the architecture of the blockchain network. Therefore, in this paper, we analyze the considerations of lightweight blockchain for IoT. Also, we conduct an analysis of lightweight hash for blockchain, and propose a new lightweight hash-based blockchain architecture that can change the hash algorithm used for mining adjust to network traffic.. F. Assad et. al. [11] presented an optimal implementation of the Keccak hash function, which is one of more than fifty candidates accepted by NIST for the SHA-3 hash function competition. This implementation intended to reducing circuit complexity, and increasing performance hardware implementations of this cryptographic hash function. The proposed design is coded in VHDL and implemented on Virtex 5 FPGA.

Rastoceanu Florin et. al. [12] propose a solution for securing IoT systems using blockchain technology, implemented on a FPGA based architecture. possible to implement this architecture in FPGAs.

The results presented are useful in choosing the family and type of FPGAs, as they provide information about the number of SHA256 cores that can be implemented, the output in Gbit/sec and the power consumption. Yuliya Tanasyuk et. al. [16] analyzed the usage of FPGA technology for cellular automata implementation. The universal way of cellular automata rule parameterization and the approach of parameterized implementation of one-dimensional cellular automata are proposed. The way of hardware implementation of cryptographic hash functions using cellular automata is discussed. The software and hardware versions of cellular automata were developed. The comparison of performance and resource estimation for both implementations is done. The FPGA-based case-study is developed. Carlos Andres Lara-Nino et. al. [17] presents hardware realizations of two lightweight hash function families on FPGA: SPONGENT and LHash. The assessment provided for both cryptographic primitives is in terms of area, performance, and energy consumption, when implemented in LUT-4 and LUT-6 FPGA technology for equivalent security levels. To the best of our knowledge, they reports the most compact SPONGENT FPGA implementation and the first FPGA implementation of LHash. Shamsiah binti Suhaili et. al. [18] developed and designed a new SHA family in order to fulfil the cryptographic algorithm performance requirement. Thus, SHA-256 design and SHA-256 unfolding design based on reconfigurable hardware have been successfully completed using Verilog code. These designs were simulated and verified using ModelSim.

III.PROPOSED WORK

A. Scope for the Proposed Work:

Blockchain technology is one of the exploding technologies around the world which has the potential to be introduced as a solution to various issues in different environments and day-to-day applications, such as the IoT. The blockchain uses cryptographic hashing functions for security aspects, and this also helps in achieving an append-only approach to the data, where once it gets added to the blockchain, it can neither be edited not deleted. The blockchain, along with its advantages, also faces some challenges which need solving before it can be integrated into any environment.

1) Some of the challenges are scalability, high computational requirements, high power consumption, and security and privacy. For example, if an IoT environment is considered, almost all these properties, such as, power consumption, computational requirements and security and privacy are bottlenecks for the integration of blockchain.

2) Mining in the blockchain in some consensus algorithms requires very high computational power and dedicated hardware. The main selection criteria for a good cryptographic hash function after security is performance in software and hardware.

3) For hardware implementations the two major platforms are Application Specific Integrated Circuit (ASICs) and Field Programmable Gate Arrays (FPGAs). When considering hardware implementations, apart from speed the scalability of the algorithm also plays an important role. Reconfigurability at run time, design re-usability, low non recurring engineering costs and faster time to market make the FPGA preferable at certain times.

4) With the development of low power and low cost FPGAs, implementing applications that use cryptographic hash functions (along with some other component) especially for resource constrained environments like battery powered hand held devices, on FPGAs thus seems a logical choice.

B. Scope of Research

Most of the implementations that were reported so far [2], [6] were on based on high speed implementations on FPGAs. To be an all-round candidate, it is thus important that the Hash algorithms perform well on resource constrained environments. The goal is to implement them as small as possible, but it is also important to take the throughput into consideration while designing. With respect to the basic architectures of the algorithms that can be built in a straightforward fashion, the reduction in the datapath for compact implementations may sometimes lead to unrealistic clock cycles or complex controller logic. This is due to interdependencies among intermediate values in forthcoming functions. This leads to unrealistic processing time and low throughput. Thus the best compact implementation would be the one that offers optimum trade off between speed and area. There are many use cases for blockchain but there are also many challenges. Various challenges of blockchain technology which either prevent its application or make it computationally and energy demanding. There are also the issues of attacks on the blockchain where fake blocks can be generated. Blockchain major issues are lack of scalability, high energy consumption, high latency, lack of privacy, fake block generation.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

IV. METHODOLOGY

The Proposed approach for FPGA based Lightweight blockchain algorithm for lightweight Hash mentioned below.

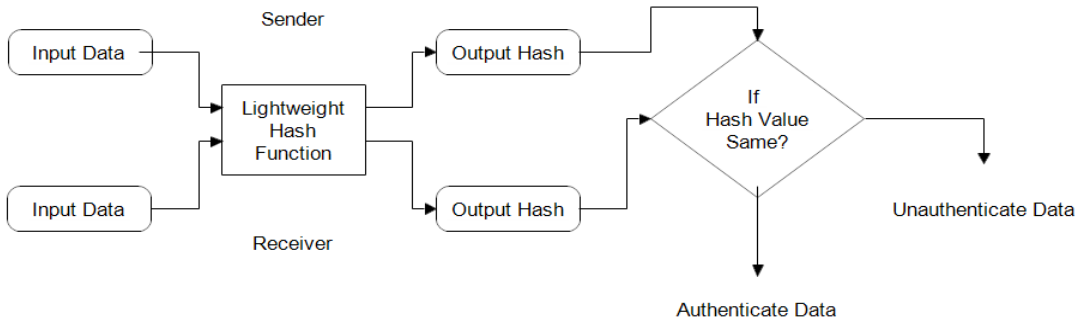


Fig 1.2 : Principle block diagram of hash function

Hash Function is mainly one way function. If sender want to send some message or data then it calculates its Hash value based lightweight hash function. Then sender want to verify it, it will send data again its hash has been calculated by has function. Later if both hash value are equal then data will authenticate of receiver otherwise its discarded. Proposed design flow is as first define the specification of lightweight hash function based FPGA for Blockchain implementation, introduce the pipelining and area optimization concept to improve the existing architecture of cryptographic system and describe the behavior of proposed system in Hardware descriptive language then simulate and verify the operation of architecture. If behavior is successfully verified then analyze and synthesis the proposed architecture on FPGA device platform based on Altera or Xilinx Vendor Platform and analyze the architecture parameters for system performance parameters like area, propagation delay, frequency and power consumption.

V. CONCLUSION

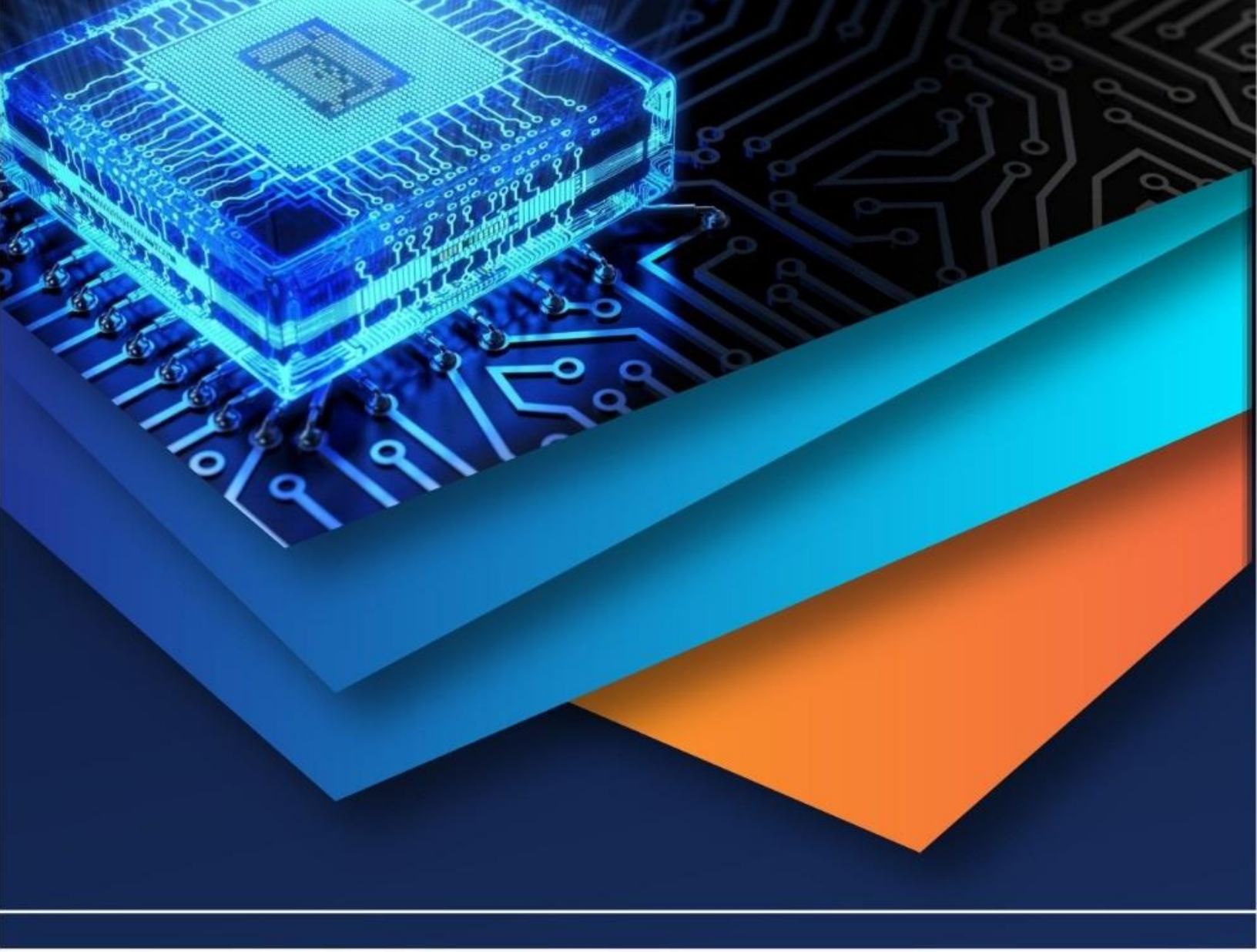
The Internet of Things has spread widely due to resource constraints, the widespread deployment of small devices, and their wireless communication with the Internet and one another. Lightweight cryptography is used to address this issue in light of resource constraints and security requirements. In this article, a lightweight cryptographic hash function supporting IoT and big data applications was introduced. The bit permutation, linear transformation, and S-Box paradigms are used in the proposed study. The outcomes demonstrate notable gains in terms of performance, memory, and power use. We have designed our system to meet the broad needs of lightweight cryptography protocols while adhering to traditional hash standard security specifications. In order to accommodate a range of IoT applications, the suggested architecture will thereafter be evaluated on diverse hardware and platforms.

REFERENCES

[1] Vijayakumar Peroumal et al ," FPGA Implementation of Secure Block Creation Algorithm for Blockchain Technology", The Electrochemical Society *ECS Trans.* Volume 107, Number 1, 2022
[2] Sa'ed Abed, Reem Jaffal, Bassam J. Mohd & Mohammad Al-Shayeji,"An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices"Springer, June 2021,DOI : 10.1007/s10586-021-03324-1
[3] Gookyi DAN, Ryoo K. "A Lightweight System-On-Chip Based Cryptographic Core for Low-Cost Devices". Sensors (Basel). 2022 Apr 14;22(8):3004. doi: 10.3390/s22083004. PMID: 35458989; PMCID: PMC9030163]
[4] Songshen HAN, Kaiyong XU, Zhiqiang ZHU, Songhui GUO, Haidong LIU and Zuohui LI, "Hash-Based Signature for Flexibility Authentication of IoT Devices", Wuhan Univ. J. Nat. Sci., 27 1 (2022) 1-10, DOI: 10.1051/wujns/2022271001
[5] Unterstein, F., Jacob, N., Hanley, N. et al. "SCA secure and updatable crypto engines for FPGA SoC bitstream decryption: extended version." J Cryptogr Eng 11, 257–272 (2021). https://doi.org/10.1007/s13389-020-00247-2
[6] D. Kundi, A. Khalid, A. Aziz, C. Wang, M. O'Neill and W. Liu, "Resource-Shared Crypto-Coprocessor of AES Enc/Dec With SHA-3," in IEEE Transactions on Circuits and Systems I: Regular Papers, doi: 10.1109/TCSI.2020.2997916.
[7] J. Tetu, L. Trudeau, M. Van Beirendonck, A. Balatsoukas-Stimming and P. Giard, "A Standalone FPGA-Based Miner for Lyra2REv2 Cryptocurrencies," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 67, no. 4, pp. 1194-1206, April 2020, doi: 10.1109/TCSI.2020.2970923.
[8] Jinhua Fu ,Sihai Qiao, Yongzhong Huang, Xueming Si, Bin Li and Chao Yuan, "A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA" Volume 2020 ,doi.org/10.1155/2020/8876317
[9] Byoungjin Seok, Jinseong Park, Jong Hyuk Park "A Lightweight Hash-Based Blockchain Architecture for Industrial IoT" Applied Sciences 9(18):3740, September 2019, DOI:10.3390/app9183740
[10] F.Assad, F. Elotmani, M. Fettach and A. Tragha, "An optimal hardware implementation of the KECCAK hash function on virtex-5 FPGA," 2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS), Casablanca, Morocco, 2019, pp. 1-5, doi: 10.1109/SysCoBIoTS48768.2019.9028028

[11] R.Florin and R. Ionut, "FPGA based architecture for securing IoT with blockchain," 2019 International Conference on Speech Technology and Human-Computer Dialogue (SpeD), Timisoara, Romania, 2019, pp. 1-8, doi: 10.1109/SPED.2019.8906595.
[12] D.Kim, S. Lee and K. Shin, "A Hardware Implementation of SHA3 Hash Processor using Cortex-M0," 2019 International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, 2019, pp.1-4, doi: 10.23919/ELINFOCOM.2019.8706419.
[13] I.Korotkyi and S. Sachov, "Hardware Accelerators for IOTA Cryptocurrency," 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2019, pp. 832-837, doi: 10.1109/ELNANO.2019.8783449.
[14] Y.Luo, S. Han, J. Liu, Z. Liang and S. Yang, "Hash Hardware Generator Based on Mutual Perturbed Logistic Map," 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 2019, pp. 353-358, doi:10.1109/HPCC/SmartCity/DSS.2019.00061.
[15] D.K.N. and R. Bhakthavatchalu, "Parameterizable FPGA Implementation of SHA-256 using Blockchain Concept," 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0370-0374, doi: 10.1109/ICCSP.2019.8698069.
[16] C. A. Lara-Nino, M. Morales-Sandoval and A. Diaz-Perez, "Small lightweight hash functions in FPGA," 2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS), Puerto Vallarta, 2018, pp. 1-4, doi:10.1109/LASCAS.2018.8399948.
[17] Y. Yang, D. He, N. Kumar and S. Zeadally, "Compact Hardware Implementation of a SHA-3 Core for Wireless Body Sensor Networks," in IEEE Access, vol. 6, pp. 40128-40136, 2018, doi: 10.1109/ACCESS.2018.2855408.
[18] S. binti Suhaili and T. Watanabe, "Design of high-throughput SHA-256 hash function based on FPGA," 2017 6th International Conference on Electrical Engineering and Informatics (ICEEI), Langkawi, 2017, pp. 1-6, doi:10.1109/ICEEI.2017.8312449.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)