Pratikbhai Patel, 2019, 7:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

VLSI Architecture for Advanced Cryptographic Hardware in Global Data Security

Pratikbhai Patel
Gujarat technology university A.D patel institute of technology, Electronic and communication engineering

Abstract- The fast paced growth of the international digital infrastructure has also heightened the need to have safe and high-performance cryptographic frameworks that are able to safeguard sensitive data in large scale data centres and distributed computing setting. Cryptographic processors implemented in hardware via application of Very Large Scale Integration (VLSI) technology can be highly beneficial in encryption speed, energy consumption, and system security as opposed to encryption methods in software. The study explores the design and analysis of VLSI architecture of putting into practice Application-Specific Integrated Circuit (ASIC) cryptographic hardware with the use of AES-256 encryption algorithm. The paper analyzes hardware architectural designs applied in AES-256 processors and discusses the important performance metrics such as the throughput of encryption process, the power usage, the silicon area, and resilience to security. The comparison of ASIC and FPGA cryptography platforms is also analyzed to find the best hardware platforms to use in high-performance encryption systems. Supportively, the study considers hardware security risks such as side-channel attacks, and hardware Trojans that are capable of weakening cryptographic processors used in the international computing infrastructure. The results underscore the relevance of energy-efficient hardware architectures and built-in security countermeasures in the development of secure cryptographic processors that can support the current data centre activities. The paper finds that optimised ASIC- based AES-256 architectures present a trade-off solution in the need to address a strong encryption security and efficient power consumption in the large-scale digital system.

Keywords: Cryptographic Processors, Very Large Scale Integration (VLSI), Application-Specific Integrated Circuit (ASIC), Field Programmable Gate Array (FPGA), AES-256 Encryption, Hardware Security, Data Encryption.

I. INTRODUCTION

Global Cybersecurity Landscape

The worldwide digital infrastructure has augmented data centre tasks on delicate information that elevates cybersecurity issues which need enhanced cryptography. The current cloud systems are performing billions of encrypted transactions on a daily basis, which require high standards of financial, governmental, and organisational data security [6]. With the convergence of computing systems, processor, memory and network communications attacks become more difficult to detect [7]. Vulnerabilities at the hardware level pose a threat because an attacker can overcome software protection with ease owing to the physical design of computing devices [4]. The increasing networks of the digital communication demand the high performance encryption systems that can effectively process massive encrypted data. Cryptography helps secure important information on systems and other infrastructure of the international communication systems [3]. Large-scale computing demands encryption engines of high speed, which are able to secure communication without compromising on performance [9]. Existing computing architectures require cryptographic hardware to be secure and performant.

Importance of Hardware Security in Data Centres

Cloud services, financial transaction platforms, and big enterprise computers are supported by data centres. These amenities handle large amounts of sensitive information, and thus are exposed to cyberattacks to steal information or disrupt services [7]. Encryption based on software in the operating

system or application level is computationally intensive and can be attacked [6]. Cryptography on hardware is more secure because semiconductor circuits are not encrypted with software. Encryption keys and processing are safeguarded using cryptographic processors, which are dedicated [2]. Encryption hardware devices are quicker than software since special circuitry permits parallel cryptographic transformations [9]. Encryption software requires massive amounts of computer power therefore massive data centres require power efficiency. Good circuits layout of cryptography uses less energy [1]. Cryptography processors Hardware cryptography devices enhance the security and efficiency of a data centre.

Role of VLSI in Cryptographic Hardware

VLSI technology includes the capacity of millions-transistor integrated circuits to perform complicated computing functions on small semiconductors. VLSI architectures allow a quick cryptographic computer with the aid of encryption methods [2]. VLSI hardware circuits have cryptographic elements, which enhance faster encryption and security when compared with software [1]. VLSI cryptographic processors hardware modules are used to carry out substitution, permutation and arithmetic transformations of existing encryption algorithms. These modules enhance the speed of cryptography processors through encrypting in parallel [9]. Side-channel attack and tampering prevention can be instantly added to the VLSI chips by designers [4]. The semiconductors enhance the performance and resilience of New VLSI security architectures. ICs are 3D, which enhances density and discourages reverse engineering [4]. These developments show that VLSI designs are relevant in safe and effective cryptographic devices in the contemporary digital systems.

AES-256 as the Global Encryption Standard

The AES symmetric encryption is used to secure computer systems and digital communications across the globe. Routine conversion of AES data blocks of 128 bits will be used to make cryptographic security [2]. The 256 bit size of AES-256 key with fourteen encryption cycles, is immune to brute force attacks due to its very large key space [3]. Because of its high-quality cryptography and effective hardware implementation, AES-256 finds application in secure communication systems, financial transaction systems, and cloud computing systems. Structured hardware circuit chips perform SubBytes, ShiftRows, MixColumns, and AddRoundKey effectively [9]. These features render AES suitable with high-performance VLSI cryptographic processors. Hardware AES is sub-optimal to software in that specialized circuits can be used to parallelise encryption and to cut down on the number of computations. CPUs that support AES hardware accelerators enhance large-scale encryption speed and efficiency in power [10].

Problem Statement

Despite AES-256 having good cryptography, semiconductor design is challenging due to power usage, complexity of the circuit, and system performance. Encryption of hardware demands a lot of mathematical modifications that may overload the computers [1]. Global data centres are inefficient in hardware utilization which is both energy-wasting and inefficient. The security and hardware should be balanced. The cost of making encryption circuit topologies is more complex in silicon area and chip manufacturing [2]. Hardware designers require secure and power-efficient semiconductor designs. Avoid physical attacks that indirectly examine the behaviour of hardware to obtain the encryption keys. Attacks on side-channels can expose sensitive cryptographic data through their analysis using differential power [7]. These issues demand special VLSI designs of safe, efficient, and durable cryptography.

Research Objectives

- To examine VLSI architecture of VLSI-based cryptographic processors in current computers.
- To test the design features of AES-256 encryption algorithm hardware implementation based on ASIC.
- To investigate the trade-offs in the energy used in cryptographic processors, hardware complexity, and the speed of the encryption process.

- To determine architectural mechanisms that enhance security resilience to hardware based attack in VLSI cryptographic design.

II. LITERATURE REVIEW

Evolution of Hardware Cryptography

Communication hardware encryption has been replaced by cryptographic processors over computers. Initial hardware encryption systems based on safe communication circuits were based on symmetric algorithms such as DES [2]. These devices enhanced encryption and, although limited in terms of algorithm and intensive in hardware, they enhanced encryption. Semiconductor technology can be used to implement a wide range of encryption algorithms in processors with flexible cryptographic architecture. Hardware encryption engines are configured hardware modules that allow flexible modification of algorithms on behalf of system requirements [10]. These architectures increase the processing power and versatility of modern computers. Lightweight cryptography hardware that operates in limited resources such as IoT and distributed computing systems is required. Lightweight encryption cuts hardware complexity and power consumption [3]. The results emphasize the importance of hardware encrypted digital security.

AES-256 Cryptographic Algorithm Architecture

A 2,000 times replacement and permutation of 128-bit data blocks generate the cryptographic dispersion and confounding [2]. There are four important metamorphoses that increase the security of encryption at every stage of the cycle. SubBytes encryption is provided with non-linear substitution by S-boxes. ShiftRows scrambles encryption state matrix bytes to transmit data in between algorithm components. MixColumns dispenses input data among encryption by multiplying the values of matrices in a finite field [9]. AddRoundKey incorporates round-specific key encryption. It has a hierarchical structure that encourages software implementation since some arithmetic circuits and look-up tables can implement AES operations. AES software implementations are slower than hardware since expert circuits can execute multiple encryptions [9].

ASIC Design for Cryptographic Processors

Application-Specific Integrated Circuits (ASICs) are one of the most efficient cryptographic processing platforms that execute the encryption algorithms on a set of hardware circuits. ASIC encryption devices do not increase software encryption overhead, and they are faster than CPUs [9]. ASIC encryption is speeded up using parallel processing units, pipelined encryption engines, and loop-unrolled architectures. Cryptographic processors based on architectural ideas are able to provide large-scale computing communication networks with high throughput [10].

VLSI Implementation Techniques

Iterative looping, loop unrolling and pipelining allow flexible symmetric-key crypto engines to trade off throughput, silicon area and power [2]. In reconfigurable and ASIC-oriented cryptographic solutions, architectural choice has a strong effect on the resource usage and performance and thus is a significant optimisation parameter in cryptographic VLSI design [9]. An in-depth analysis of flexible cryptographic designs revealed that reuse of Datapath, modular round-based and reconfigurable control logic of many symmetric algorithms within a single engine can enhance design complexity and switching activity [10].

A case study of stimulating VLSI design revealed that embedded and networked security policies are energy wasteful and therefore cryptographic devices should be designed to minimise switching activity and maximise security circuitry integration density within limited chip areas [1]. 3D design of security integration research proposed that VLSI design can utilise 3D IC technology to minimise reverse engineering and IP pirating as well as maximised security circuitry integration density on compact chip designs [4]. VLSI-relevant [5] devices are new hardware-level security and non-CMOS cryptographic primitives' devices. The cryptographic engines need VLSI memory encryption systems at memory controllers and data paths to encrypt plaintext data on external buses and physical memory interfaces [6].

Hardware Security Threats

Hardware Trojan can compromise cryptographic systems by leaking secrets or altering functionality during design or manufacturing [7]. Attackers who physically access global computing chips are able to reverse engineer IP and pirate it [4]. Our adversary can infer power or timing behaviour in high-frequency and throughput encryption engines using cryptographic hardware side-channel leakage [7]. The patterns of memory accesses or accessed memory interfaces may spill out plaintext data and cryptographic keys without encryption of end-to-end memory hierarchy [6]. Less cryptography is utilized in constrained devices and compromised endpoints have access to infrastructure [3]. The security of hardware is required since safety- critical implications of embedded cryptography security failures exist, as reported by a medical and developing device security study [8].

Research Gap

The design issue of choosing an AES-256 ASIC architecture to optimise power, area, throughput, and hardware attack resilience is not addressed by flexible symmetric-key crypto engine architecture surveys when constrained by the global data-centre deployment constraints [2]. Implementations of flexible cryptography are not architecture- and platform-neutral, but comparative studies have not associated AES-256 design choices with energy-per-bit in comparable evaluation environments [9]. A single optimisation model of contemporary threat models does not have rapid and effective physical-layer responses [10]. Loose designs enhance the agility in algorithms. The extreme-low-power hardware security research is dominated by energy-driven design and novel technologies, but the high-throughput infrastructure encryption on the basis of AES-256 ASICs is unavailable yet [1].

III. METHODOLOGY

Research Design

VLSI AES-256 cryptographic processor hardware architectural assessment on global data security. Studies of ASIC-based hardware architecture research are due to the fact that they are faster and consume not as much energy compared to software encryption [9]. The performance of cryptographic hardware implementation in the literature is quantitatively measured.

VLSI Design Framework

VLSI cryptographic processors implement semiconductor circuitry encryption techniques using numerous phases. Encryption that is implemented on hardware is computational [2]. In this case, data flow and functionality of the digital circuit encryption are created. Interconnect encryption hardware designed in RTL. The RTL encryption requirements are substitution modules, APUs, and key expansion circuits [9]. Improve the processing speed and make circuits easier. Hardware synthesis then produces semiconductor device gate-level digital circuits after RTL descriptions to VLSI design. Hardware synthesis makes logic digital at transistor level [4]. Conduct performance and power analysis to ascertain the hardware design requirements.

AES-256 ASIC Architecture Design

This architecture of cryptographic processors relies on AES-256 ASIC. AES-256 uses 128-bit keys to encrypt blocks of 128 bits in 14 transformation cycles [3]. Algorithms are modified with hardware. SubBytes nonlinear replacement makes use of AES S-box lookups. The technique of dispersion is spread through ShiftRows rearranging the encryption state matrix bytes. The encryption and decryption multiply the values of the finite field matrices to spread the input data [9]. The major expansion modules produce encryption keys, round- specific addition key round keys, based on secret keys. Implementations of AES on ASICs use pipeline topology due to the capability to execute numerous encryption rounds on the data blocks. Pipelined systems optimise the hardware and encryption [10].

Hardware Performance Metrics

Computing and hardware efficiency is used to measure cryptographic hardware efficiency. Encryption pace is megabits or gigabits [9]. ASIC high-throughput encryption processors can be used in secure communication infrastructure. Cryptography involves a lot of digital circuit switching, and thus power consumption is an issue. The switching power of encrypting is dynamic due to

the transistor switching, but the currents in the semiconductor leakages are inert [1]. Big data computing requires the reduction of power. Cryptographic processor silicon is measured in hardware area. Minimisation of hardware enhances production and multiplies numerous chip encryption engines [2]. In this way, designers compromise between complexity of hardware and performance.

Evaluation Parameters

The VLSI cryptography designs are considered to be efficient and secure with many performance measures.

Table 1
Evaluation Parameters

Parameter	Description
Throughput	Amount of data encrypted per second
Power Consumption	Electrical energy required for encryption
Silicon Area	Physical hardware size required for implementation
Latency	Time required to complete encryption process
Security Resilience	Resistance to hardware-based attacks

IV. ANALYSIS

AES-256 Hardware Architecture Analysis

AES-256 hardware designs are often built on iterative or loop-unrolled or pipelined designs which compute the encryption throughput and circuit complexity of integrated cryptographic processors. AES-256 processes 128-bit data blocks with a 256-bit key, and does 14 rounds of encryption and encryption (repeated substitution and permutation), which is to be effectively implemented on hardware data paths in ASIC-based security processors. The architectures of hardware systems needed to support secure communication infrastructure, should therefore scale the Datapath width and the pipeline depth to support the continuous encryption processes at large scale computing systems. The application of secure hardware modules is gaining popularity in a variety of IoT and distributed computing systems where billions of connected devices create encrypted traffic of communication which needs to be decrypted by centralised infrastructure systems [11]. Cryptographic accelerators on hardware can be implemented on a server or a networking device and run encryption rounds in parallel, greatly enhancing the encryption throughput of any cryptographic cipher implementation over software-based implementation. Optimisation of architecture is thus aimed at minimising latency and maximising throughput by having parallel Datapath structures that enable parallel implementation of cryptographic transformations. More sophisticated arithmetic architectures such as residue number system (RNS) computing have also been considered as a way to do cryptographic processing since they can be used to parallel perform arithmetic operations and hence reduce carry propagation delays and other enhance computational efficiency in digital signal and security processors [16]. Through these architectures, it is shown that design methods in arithmetic may have a substantial impact on encryption speed when applied in VLSI cryptographic processors.

Power Consumption Analysis

Power consumption is a key design factor in cryptographic hardware development in large-scale computing infrastructure since encryption engines must be active in all periods of time when transmitting and storing of secure data is taking place. Hardware encryption engines should thus minimise the switching activity and maximise the use of circuit to ensure energy efficiency at the high-performance computing infrastructure. According to the research on edge computing, IoT and distributed computing settings tend to need energy-efficient hardware accelerators since devices must have power and thermal limits and operate under strict data integrity workloads [18]. The split of energy consumed by cryptographic hardware is usually between dynamic and static leakage.

The dynamic energy is due to switching transistors and the leakage power is due to the nature of semiconductor devices. Dynamic power consumption is of particular significance to reduce since encryption algorithms have repeated computational processes which enhance switching activities in digital circuits. The hardware design methods like: pipelining and Datapath optimisation

can be used to optimise energy use per encryption operation and also achieve high processing throughput. Encryption processors are then considered by hardware designers in terms of energy per encrypted bit, which is a metric that quantifies the efficiency of cryptographic hardware implementation to turn electrical energy into secure computing output.

ASIC vs FPGA Cryptographic Implementations

The cryptographic hardware may be adopted either in Application-Specific Integrated Circuits (ASICs) or in Field Programmable Gate Arrays (FPGAs), both having various benefits based on performance, flexibility, and security. ASIC designs are generally optimised to perform certain cryptographic algorithms and can be much more performant as well as use less energy than reconfigurable FPGA architectures. FPGA is flexible in design Since encryption architectures can be updated after deployment, researchers and engineers can explore alternative cryptographic algorithms and hardware implementations.

Side-Channel Attack Resistance

Cryptographic devices can be attacked physically to exploit information leakage that they generate when performing encryption. Side-channel attacks examine such indirect data as power usage, timing, or electromagnetic radiation to deduce secret cryptographic keys that are being used in an encryption process. Trusted ICs have been cited as one of the biggest problems of contemporary semiconductor systems by hardware security research due to the ability to disrupt the security of cryptographic processing units installed in sensitive infrastructure by illicit alterations or subterranean hardware layouts [17]. Hardware Trojan attacks are also a serious threat since an attacker can destroy built-in circuitry with malicious circuitry as they will leak secret data or modify cryptographic functions without detection.

The testing and verification methods are thus needed to identify malicious alterations in the hardware systems during design and manufacturing phases. There have been logic testing methods that have been suggested to detect malicious behaviour in integrated circuits through an Examination of circuit outputs and identification of deviant logic patterns that might signify hardware Trojans existence [12].

V. DISCUSSION

Security vs Power Consumption Trade-off

Cryptographic hardware design needs to balance between the level of security and hardware efficiency since more secure encryption algorithms and security designs tend to raise the computational load and energy usage. Encryption systems made with extra security protocols like side- channel countermeasures can raise hardware system complexity and switching rates. More sophisticated cryptographic methods like homomorphic encryption permit calculating on encrypted data without decryption, but these methods cause serious computational overhead that adds complexity to hardware and energy consumption [13]. The implication of this is that when hardware designers are designing cryptographic processors to work in large-scale computing contexts, they need to consider trade-offs related to security functionality and performance efficiency.

Implications for Global Data Security Infrastructure

Hardened cryptographic devices are critical to safeguarding the world digital infrastructure since encryption engines fortify communication technologies employed in the financial sector, health care networks, and other vital government infrastructure. Architectures of distributed computing that need to support billions of interconnected devices must have high-performance cryptographic processors that can continuously process encrypted data. The application research related to the IoT has proved that efficient data transmission may be used to secure sensitive data produced by devices connected in a network and used to monitor sensitive systems and promote industrial automation [14]. Cryptographic devices hence offer a critical security base of modern-day digital infrastructure.

Limitations of Current VLSI Cryptographic Designs

Although there have been major developments in the design of cryptographic hardware, multiple drawbacks are found in the present VLSI designs that are deployed in secure computing system. Hardware security systems typically add complexity to the circuitry which adds chip area and production costs, which can make large scale implementation in cost-sensitive applications difficult. The other weakness is the fact that it is hard to check the hardware security properties during the manufacturing experience of semiconductors. Researchers in the field of hardware security emphasize that it is still a major difficulty to detect malicious non-conformance of the integrated circuits due to the existence of millions of transistors and elaborate circuit designs in modern chips [17].

Future Hardware Security Directions

Future studies on the cryptographic hardware design work are likely to centre on the incorporation of new security primitives that will offer enhanced defence against developing cyber threats. Physical unclonable functions (PUFs) have been suggested as hardware security primitives, which can be used to produce unique cryptography keys which are generated due to natural physical differences in semiconductor devices [15]. Such technologies are used to facilitate secure authentication of devices and generation of keys that are tamper-resistant to reinforce the basic security architecture of cryptographic hardware systems.

VI. CONCLUSION AND RECOMMENDATIONS

Key Findings

This paper examined how VLSI architectures have been used to execute AES-256 cryptographic processors that are intended to secure digital infrastructure around the world. The discussion revealed that hardware-based encryption processors can develop computational efficiency and resistance to security at a greater level than software-based encryption systems. The paper further determined that design decisions made during architectural design play a major role in determining the encryption throughput, energy use and the hardware security resilience of modern cryptographic processors.

Practical Recommendations

This research can be used to make several recommendations to enhance the cryptography hardware in global computing infrastructure. ASIC-based AES-256 encryption processors should be installed in data centres to offer high throughput secure data processing. Semiconductor manufacturers need to incorporate hardware security testing methods to ensure that hardware Trojan and malicious circuit modification are detected. Architectures of cryptography hardware must have measures against side-channel attacks of sensitive encryption keys. The VLSI design methods that consume less energy should be given priority to lower the power use in the large-scale encryption systems.

Future Research

Future studies must examine sophisticated hardware security solutions, which have the potential of enhancing the cryptographic processor resiliency to new cyber threats. Future research avenues entail physical unclonable functionality to be used to authenticate devices, designing low power cryptography architectures to operate in distributed computing contexts, and new semiconductor technologies that can implement secure hardware platforms.

REFERENCE

1. J.-S. Yuan, J. Lin, Q. Alasad, and S. Taheri, "Ultra-Low-Power Design and Hardware Security Using Emerging Technologies for Internet of Things," Electronics, vol. 6, no. 3, p. 67, Sep. 2017, doi: https://doi.org/10.3390/electronics6030067.
2. L. Bossuet, M. Grand, L. Gaspar, V. Fischer, and G. Gogniat, "Architectures of flexible symmetric key crypto engines—a survey," ACM Computing Surveys, vol. 45, no. 4, pp. 1–32, Aug. 2013, doi: https://doi.org/10.1145/2501654.2501655.
3. I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptography for Internet of

Insecure Things: A Survey," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2019, doi: https://doi.org/10.1109/ccwc.2019.8666557.

4. P. Gu et al., "Leveraging 3D Technologies for Hardware Security," Proceedings of the 26th edition on Great Lakes Symposium on VLSI, May 2016, doi: https://doi.org/10.1145/2902961.2903512.
5. A. P. James, "An overview of memristive cryptography," The European Physical Journal Special Topics, vol. 228, no. 10, pp. 2301–2312, Oct 2019, doi: https://doi.org/10.1140/epjst/e2019- 900044-x.
6. M. Henson and S. Taylor, "Memory encryption," ACM Computing Surveys, vol. 46, no. 4, pp. 1–26, Apr. 2014, doi: https://doi.org/10.1145/2566673.
7. S. Sidhu, B. J. Mohd, and T. Hayajneh, "Hardware Security in IoT Devices with Emphasis on Hardware Trojans," Journal of Sensor and Actuator Networks, vol. 8, no. 3, p. 42, Aug. 2019, doi: https://doi.org/10.3390/jsan8030042.
8. M. M. Kermani, Reza Azarderakhsh, and Mehdi Mirakhorli, "Multidisciplinary Approaches and Challenges in Integrating Emerging Medical Devices Security Research and Education," RIT Digital Institutional Repository, 2016. https://repository.rit.edu/other/859/ (accessed Mar. 04, 2026).
9. M. Rashid, M. Imran, and A. R. Jafri, "Comparative analysis of flexible cryptographic implementations," 2016 11th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), pp. 1–6, Jun. 2016, doi: https://doi.org/10.1109/recosoc.2016.7533901.
10. M. Rashid, M. Imran, A. R. Jafri, and T. F. Al-Somani, "Flexible Architectures for Cryptographic Algorithms — A Systematic Literature Review," Journal of Circuits, Systems and Computers, vol. 28, no. 03, p. 1930003, Feb. 2019, doi: https://doi.org/10.1142/s0218126619300034.
11. D. V. Jose and A. Vijyalakshmi, "An Overview of Security in Internet of Things," Procedia Computer Science, vol. 143, pp. 744–748, 2018, doi: https://doi.org/10.1016/j.procs.2018.10.439.
12. S. Dupuis, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, "Protection Against Hardware Trojans With Logic Testing: Proposed Solutions and Challenges Ahead," IEEE Design & Test, vol. 35, no. 2, pp. 73–90, Apr. 2018, doi: https://doi.org/10.1109/mdat.2017.2766170.
13. A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes," ACM Computing Surveys, vol. 51, no. 4, pp. 1–35, Sep. 2018, doi: https://doi.org/10.1145/3214303.
14. H. Djelouat, A. Amira, and F. Bensaali, "Compressive Sensing-Based IoT Applications: A Review," Journal of Sensor and Actuator Networks, vol. 7, no. 4, p. 45, Oct. 2018, doi: https://doi.org/10.3390/jsan7040045.
15. J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, "A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs," Journal of Computer Science and Technology, vol. 29, no. 4, pp. 664–678, Jul. 2014, doi: https://doi.org/10.1007/s11390-014-1458-1.
16. W. Kenneth Jenkins, M. A. Soderstrand, and C. Radhakrishnan, "Historical Patterns of Emerging Residue Number System Technologies During the Evolution of Computer Engineering and Digital Signal Processing," IEEE International Symposium on Circuits and Systems (ISCAS), Jan. 2018, doi: https://doi.org/10.1109/iscas.2018.8351066.
17. Yongqiang Lv, Q. Zhou, Y. Cai, and G. Qu, "Trusted Integrated Circuits: The Problem and Challenges," Journal of computer science and technology, vol. 29, no. 5, pp. 918–928, Sep. 2014, doi: https://doi.org/10.1007/s11390-014-1479-9.
18. M. Capra, R. Peloso, G. Masera, M. R. Roch, and M. Martina, "Edge Computing: A Survey On the Hardware Requirements in the Internet of Things World," Future Internet, vol. 11, no. 4, p. 100, Apr. 2019, doi: https://doi.org/10.3390/fi11040100.
19. N. Anagnostopoulos, S. Katzenbeisser, J. Chandy, and F. Tehranipoor, "An Overview of DRAM-Based Security Primitives," Cryptography, vol. 2, no. 2, p. 7, Mar. 2018, doi: https://doi.org/10.3390/cryptography2020007.

20. G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of Security and Privacy for the Internet of Medical Things (IoMT)," 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Distributed Computing in Sensor Systems (DCOSS), 2019 15th International Conference on, pp. 457–464, May 2019, doi: https://doi.org/10.1109/DCOSS.2019.00091.