DOI: https://doi.org/10.5281/zenodo.14502196

LIGHTWEIGHT CRYPTOSYSTEMS FOR RESOURCE CONSTRAINED IoT DEVICES

Qozoqova To‘xtajon Qaxramon qizi
Assistant of the Department Cryptology,
TUIT named after Muhammad al-Khwarizmi
qozoqovat1516@gmail.com

ABSTRACT: *IoT is growing in popularity and prevalence because of its many uses across different industries. They gather information from the actual world and send it via networks. From tiny sensors to servers, there are numerous obstacles to overcome when implementing IoT in the real world. Since the majority of IoT devices are physically accessible in the real world and many of them have limited resources (such as electricity, memory, processing power, and even physical space), security is thought to be the biggest difficulty in IoT deployments. Since it can be difficult to secure these resource-constrained IoT devices (such as RFID tags, sensors, smart cards, etc.), we are concentrating on them in this work. It is possible to secure communication from such devices.*

Keywords: *IoT, lightweight, cryptography, sensors, RFID, smart cards.*

INTRODUCTION. The Internet of Things (IoT) is now being used in all aspects of our lives, especially in various fields such as transport, logistics, healthcare, smart infrastructure, smart cities, smart homes, smart offices, smart shopping malls, smart agriculture, etc. z remains relevant. Let’s take a look at two categories of IoT devices. In this paper, we will analyse two categories of IoT devices and the lightweight cryptographic algorithms used in them. These are consumer Internet of Things devices and Industrial Internet of Things (IIoT) devices. Figure 1 shows the categories highlighted above.

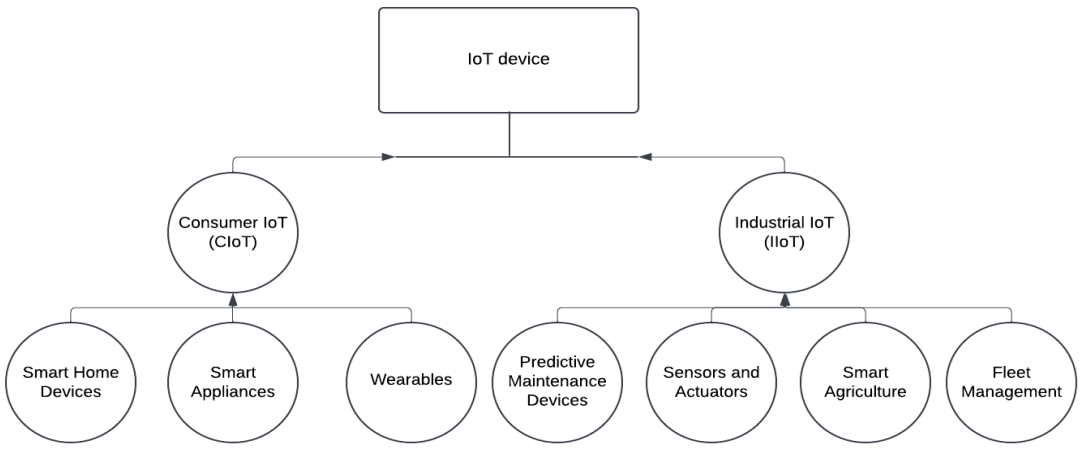

Fig. 1. Categories of IoT devices

Consumer IoT (CIoT) refers to connected devices designed for the consumer market, like smart wearables, smartphones, smart home devices, etc., that collect and share data through an internet connection. An offshoot of the Internet of Things (IoT), CIoT distinguishes itself from other IoT segments by the types of applications and or devices and technologies that power it. With fast-growing computing capabilities, Consumer IoT applications are increasingly becoming more efficient and easier to use. They use edge computing technologies to improve scalability and save power in consumer IoT devices by crunching data instantaneously while also enabling and optimizing data visualization and M2M. Large-scale implementation of CIoT devices and applications promise to revolutionize many aspects of our day-to-day life. Increased comfort, higher control, efficient tracking of loved ones/ valuables, better insights, and enhanced connections between people, systems, and the environment are some ways consumer IoT is transforming our live[10]. The industrial internet of things (IIoT) is the use of smart sensors, actuators and other devices, such as radio frequency identification tags, to enhance manufacturing and industrial processes. These devices are networked together to provide data collection, exchange and analysis. Insights gained from this process aid in more efficiency and reliability. Also known as the industrial internet, IIoT is used in many industries, including manufacturing, energy management, utilities, oil and gas.

IIoT uses the power of smart machines and real-time analytics to take advantage of the data that dumb machines have produced in industrial settings for years. The driving philosophy behind IIoT is that smart machines aren't only better than humans at capturing and analyzing data in real time, but they're also better at communicating important information that can be used to drive business decisions faster and more accurately. Connected sensors and actuators enable companies to pick up on inefficiencies and problems sooner, saving time and money while also supporting business intelligence efforts. In manufacturing specifically, IIoT has the potential to provide quality control, sustainable and green practices, supply chain traceability and overall supply chain efficiency. In an industrial setting, IIoT is key to processes such as predictive maintenance, enhanced field service, energy management and asset tracking [11]. Consumer Internet of Things (CIoT) is more focused on personal use and enhancing people's convenience, socialisation and daily activities. Business and industrial applications of the Industrial Internet of Things (IIoT) focus on operational efficiency, automation and process optimisation.

MATERIALS AND METHODS. There have been many studies of Internet of Things devices and the lightweight crypto algorithms they use. Break down a few books on the subject. One of them is lightweight cryptographic algorithms for

embedded systems. This book states, As computing technology becomes more pervasive, embedded systems are being deployed in a wide range of domains, including industrial systems, critical infrastructure, private and public spaces, and portable and wearable applications. An integral part of the functionality of these systems is the storage, access, and transmission of private, confidential, or even critical information. Thus, the confidentiality and integrity of the resources and services of these devices represent an important issue that needs to be considered in their design [1].

William Stallings' book "Cryptography and Network Security: Principles and Practice" A thorough study on protocols and methods in cryptography, including lightweight cryptography. It includes a section on resource-constrained situations, such as the Internet of Things, and discusses different encryption methods and their uses in network security. Lightweight Cryptography for Low-Latency IoT Networks by Jörg K. H. Franke, Christopher Wolf, and Achim E. Reinders. Particularly, this book concentrates on low-power cryptography strategies designed for Internet of Things devices, such as ways to lower latency and boost the effectiveness of cryptographic algorithms [2]. The authors of the book Security and Privacy in Internet of Things (IoT), Sridhar, Srinivasan, and R. R. K. Gupta, provide a thorough examination of the security and privacy issues that the quickly expanding IoT ecosystem faces. From the distinctive features of IoT devices to the changing risks and weaknesses in networked systems, the writers cover a broad spectrum of topics. It offers useful advice on how to safeguard users' privacy, secure IoT systems, and anticipate future developments in IoT security [3].

Lightweight cryptosystems for IoT devices research requires the use of a systematic and integrated methodology. In this section, the main steps and approaches used to conduct the study have been discussed. These are problem definition, selection of cryptographic algorithms, simulation and performance evaluation, prototype implementation on IoT devices, comparative analysis and evaluation.

- This methodology's initial step is to perform a thorough analysis of the body of knowledge regarding lightweight cryptography for Internet of Things devices. This aids in identifying the main obstacles and security needs for Internet of Things devices, including their constrained computing power, memory, and battery life. Important duties in this stage include review of IoT security challenges being aware of the unique security risks associated with IoT devices, such as data integrity problems, illegal access, and eavesdropping.

- Examining current cryptographic methods: examining the drawbacks of conventional cryptography techniques and how they affect IoT devices with limited resources.
- Finding Research Gaps: Identifying areas, such as high computational cost or excessive memory utilization, where current cryptography solutions fall short of the requirements of IoT devices.

The next stage is to choose cryptographic algorithms that are appropriate for Internet of Things devices when the research gaps have been determined. These algorithms must be both highly secure and sufficiently efficient to operate within the device's limitations. Several lightweight cryptography methods are examined and selected in this step according to standards like:

- Efficiency: The cryptographic algorithm should use as little memory, power, and computational overhead as possible.
- Security: The algorithm must provide a sufficient degree of protection against prevalent attacks like side-channel and brute force attacks.
- IoT suitability: The algorithms selected should be adapted to the various use cases and resource limitations of the Internet of Things.

RESULTS. Lightweight cryptosystems are necessary to provide data communication and storage security on Internet of Things devices with constrained computational, memory, and power capabilities. How security is implemented while preserving performance efficiency is largely determined by the architecture of cryptographic solutions for such devices. When implementing lightweight cryptosystems in Internet of Things networks, a number of architecture types are frequently taken into consideration. These architectures were chosen using factors including scalability, energy consumption, and computational overhead. Strong security must be offered by the selected architecture without sacrificing the device's constrained resources. It should also be versatile enough to accommodate upcoming improvements and adjustable to various network conditions. Selecting the appropriate architecture is essential since it affects how security and resource usage are balanced.

A comparative analysis of architectures for the use of lightweight crypto algorithms in Internet of Things devices is presented in (Table1). It presents the cryptographic operations and characteristics of each architecture, as well as their advantages.

Table 1. Compare architectures for using lightweight crypto algorithms in Internet of Things devices.

Architecture	Cryptographic operations	Characteristics	Advantages
Edge-Based Architecture	Local cryptographic operations on edge devices	Lightweight ciphers PRESENT, SIMON, Trivium, Key management via PUFs or ECC	Low latency. Enhanced privacy Reduced reliance on cloud systems.
Cloud-Based Architecture	Cloud handles cryptographic operations	IoT devices send raw data to cloud for processing, Lightweight algorithms for device-to-cloud communication. Centralized key management and data storage in cloud.	Offloads cryptographic tasks from IoT devices. Easier centralized key management. Scalable.
Hybrid Architecture	Combination of local and cloud cryptographic operations	Local operations for lightweight tasks Cloud handles more intensive tasks Secure transmission via TLS/DTLS.	- Reduces load on IoT devices. - Low latency for simple tasks. - Scalable and adaptable to various needs.
Peer-to-Peer (P2P) Architecture	Lightweight cryptographic protocols for direct communication (ECDH, ECDSA)	Direct communication between IoT devices. - Mutual authentication and decentralized key management	- No reliance on centralized server. - Improved privacy and low latency. - Eliminates single points of failure.
Blockchain-Based Architecture	Cryptographic ledger operations (SHA-256, ECC)	- Blockchain for transaction recording and smart contract execution. - IoT devices act as nodes in the blockchain. - PKI and cryptographic tokens for secure communication.	- Enhanced security via immutability and transparency. - Decentralized system reduces risks of failure. - Useful for supply chain, asset management, and smart contracts.

APPLICATION OF LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS IN DIFFERENT ARCHITECTURES. The following lightweight crypto algorithms are widely used in Edge-Based architecture. *PRESENT* is a lightweight block cipher, developed by the Orange Labs (France), Ruhr University Bochum (Germany) and the Technical University of Denmark in 2007. PRESENT was designed by Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. The algorithm is notable for its compact size (about 2.5 times smaller than AES). The block size is 64 bits and the key size can be 80 bit or 128 bit. The non-linear layer is based on a single 4-bit S-box which was designed with hardware optimizations in mind. *PRESENT* is intended to be used in situations where low-power consumption and high chip efficiency is desired. The International Organization for Standardization and the International Electrotechnical Commission included PRESENT in the new international standard for lightweight cryptographic methods [12].

SIMON is a lightweight encryption scheme from the Feistel-based block ciphers family where each block is divided into two halves. The cipher provides high performance on software and hardware and suitable for small IoT devices writer by Ashotosh Dhar [9]. TRIFLE is one of the round 1 candidates in the ongoing NIST Lightweight Cryptography competition, it is a AEAD scheme which uses an SPN based block cipher TRIFLE-BC as its underlying encryption algorithm. Although the design of TRIFLE-BC is heavily inspired by GIFT and PRESENT, the combination of its building blocks (operations in its round function) result in several potential weaknesses. In this study, we highlight the undesired cryptographic properties and the potential exploitation of these properties to launch attacks on TRIFLE [6].

CRAFT is a lightweight tweakable block cipher that operates on a 64-bit plaintext size, a 128-bit key size, and a 64-bit tweak size. It outputs a 64-bit ciphertext. Although quantum computing has enhanced capabilities to attack ciphers, as highlighted by Darzi et al, it is noteworthy that the probabilistic algorithm based on quantum computing, proposed by Grover et al. [8], could reduce the key space from 128-bit to 64-bit. I mentioned the results of the analysis in my article ‘Application of the CryptoSMT software tool to symmetric block encryption algorithms’ on linear and differential cryptanalysis of these two lightweight cryptographic algorithms [11]. In my article “Application of CryptoSMT software tool to symmetric block encryption algorithms” the above mentioned encryption algorithms were tested for robustness of encryption algorithms using two different cryptanalysis methods, the results are presented in (Table 2).

Table 2. Table of results

Encryption algorithms	Number of rounds	Key length (bits)	Number of weights found	Maximum weight	Minimum weight	Time spent (seconds)
Simon	8	16	18	4	2	13,63
Simon	16	16	42	6	2	1136,62
Simon liner	8	16	9	2	0	9.02
Simon liner	16	16	21	3	1	406,74
Trifle	8	128	22	3	2	252.01
Trifle	16	128	46	3	2	3133.0
Present	8	64	32	4	4	4976,78
Present	16	64	70	6	4	22555.09
Craft	8	64	52	12	2	365,96
Craft	16	64	122	10	4	10540.21
Craft liner	8	64	52	12	2	267,03
Craft liner	16	64	120	8	6	6016.19

Take this set off testing in the process of cryptanalysis to the results according to symmetric block encryption algorithms endurance in raising rounds of number and key length importance high matter is that approved. Cryptanalysis process done in raising computer strength high to be should that trust crop is done. The cryptanalysis process has proven that the right choice of method and analysis tools increases the effectiveness of the analysis. According to the results of testing the Present Block encryption algorithm proved to be reliable. The analysis time was 22555.09 seconds [10].

The importance of speed and stability of symmetric encryption algorithms in ensuring data confidentiality was determined and the requirements for stability of symmetric encryption algorithms were studied in this article. Stability to attacks of standard crypto-algorithms, corresponding to international standards, was presented and analyzed by examples. In addition, all software standards and cryptanalytical platforms have been implemented. During the cryptanalysis testing, it was confirmed that the number of rounds and key length are of great importance in enhancing the robustness of symmetric block encryption algorithms. According to test results, the Present Block encryption algorithm was reliable. The analysis time was 22555.09 seconds. It was verified that the computer power should be high when performing the cryptanalysis process, and the right choice of method and analysis tools will increase the efficiency of the analysis. Different architectures use different lightweight crypto algorithms to develop Internet of Things devices. in this section we review them. This information has been checked for statistics and analyses of possible future work.

The demand for IoT devices will further increase the demand for these devices. To prove my point, the use of IoT devices has grown 13% globally to 18.8 billion. IoT is a statistic. This is reported by Business.News in the 4 September 2024 issue. It is predicted that there will be 40 billion IoT devices by 2030. Despite ongoing challenges, including economic uncertainty, extended chipset delivery times and gradual economic recovery in China, the IoT Analytics market will continue its upward trajectory. The report predicts that the number of connected Internet of Things devices will reach 40 billion by 2030, reflecting measured but steady growth (Fig.1).

Discussion. These statistics were accompanied by figures for consumer Internet of Things devices and industrial Internet of Things devices. Security and privacy in the IIoT world are essential to preserve and protect data integrity. This security component encompasses critical aspects such as authentication, data encryption, access and key management, and the implementation of security updates and patches, among other measures to prevent cyber attacks. Some of the challenges posed by IoT cybersecurity include the diversity and heterogeneity of devices, the lack of common standards, limited computational and energy resources, and the complexity associated with effective management and monitoring.

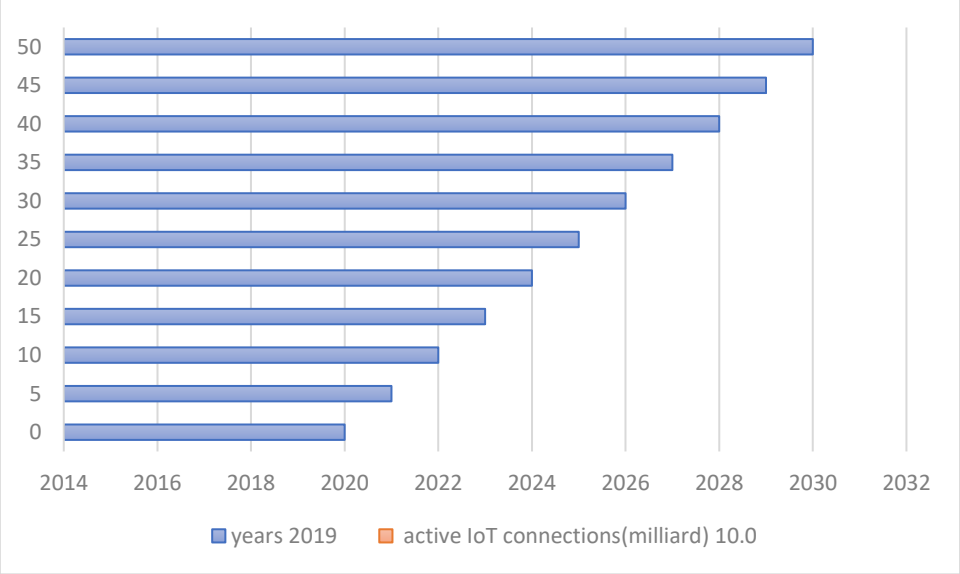

Fig. 2. Connected IoT devices

Against this backdrop, addressing the challenges becomes essential to ensure the robustness and reliability of IIoT systems. Therefore, we can anticipate that security will be one of the trends in the IoT sector in 2024, which will end up representing a significant part of global turnover in the future. Indeed, cybersecurity is no longer an optional add-on, but an imperative.

The growth of the consumer IoT market can be attributed to affordability of devices; advancements in wireless technology; and the desire to have a smart home that offers

convenience and accessibility. According to figures provided by Statista, the market is expected to reach $209.9 billion in revenue by 2024 and is expected to reach $357.8 billion by 2029. Smart speakers, home security systems, and health monitoring devices are just a few examples of the applications that have gained widespread popularity. One of the most pressing concerns surrounding consumer IoT devices is data privacy. These devices often collect and transmit vast amounts of personal data, ranging from simple usage patterns to sensitive health information. The collection, storage, and use of this data raise several privacy concerns [4].

IoT malware attacks are on the rise. According to a 2023 ThreatLabz report, there was 400% growth in IoT-targeted cyber attacks over 2022. Manufacturing has been the sector most targeted for IoT attacks, with 54.4% of reported attacks.

Table 2. Compare table of Consumer IoT and IIoT devices

Aspect	CIoT	IIoT
Market Size	$183 billion (2023, projected to grow steadily)	$238 billion (2023, with rapid growth to $1.1 trillion by 2028)
Primary applications	Smart homes, wearables, connected vehicles, health devices	Manufacturing, predictive maintenance, logistics, smart grids
Technology	Bluetooth, Wi-Fi, NFC, and RFID for easy consumer use	LPWAN, NB-IoT, advanced sensors for industrial environments
Cybersecurity	Standard protections, dependent on consumer device integrity	High standards due to critical industrial operations
Downtime tolerance	Non-critical (e.g., a smart speaker outage is inconvenient)	Minimal tolerance, as downtime can lead to safety risks and high costs
Growth drivers	Increasing adoption of smart wearables and home devices	Industry 4.0 trends like automation, AI integration, and digital twins

Governments establish IoT security standards.

To address the growing threat of cyber attacks against the rising number of IoT devices, country and regional governments are enacting legislation and programs aimed at stricter security. Earlier this year, the UK became the first country to mandate IoT cybersecurity standards, and the EU requires products sold in the EU to meet minimum standards. Additionally, the US has established a voluntary labeling program for wireless consumer IoT products.

Two cybersecurity approaches coming up. Two technology approaches, post-quantum cryptography (PQC) and zero trust security, also help address IoT security.

PQC addresses the potential risk that the rise of AI presents the ability to intelligently and quickly crack security algorithms. Zero Trust represents a security paradigm shift, whereby the security architecture focuses on securing every access request as though it originates from an open network, emphasizing the verification of every user and device. The strategy includes strong authentication mechanisms, micro-segmentation of networks, and continuous monitoring to detect and respond to threats.

Conclusion. This article has investigated the growing relevance of lightweight cryptosystems for IoT devices that have very limited resources in terms of processing power, memory, battery life, and so on. Expansion in usage of IoT applications into diverse sectors solicits the need for secure communication and protection of data. The use of lightweight cryptography provides assurance in communication since it allows IoT devices efficiency in performance while safe and secure. The research underlined the need for the existence of specialized cryptographic algorithms that focus on the specific problems surrounding IoT devices. We followed some research efforts that cover several lightweight cryptographic techniques and their applicability in various types of IoT applications. Our study also tried to find out how those algorithms can achieve an appropriate level of security against several attacks, such as the side-channel attack and the brute-force attack, by optimizing energy efficiency, memory space, and computational complexity.

I also recognized that there are other important aspects which have not been completely addressed, such as how a good level of protection could be given along with a good level of efficiency and the integration of newer cryptographic technologies that could support the fast-growing IoT framework. The results suggest that, as IoT devices are maturing, future cryptographic systems have to be designed in such a way that they can cope with the increasing vulnerability of both consumer and industrial IoT devices.

This research has underscored the significance of lightweight cryptosystems in ensuring the security and efficiency of resource-constrained IoT devices. By analyzing various cryptographic algorithms tailored to the unique needs of IoT ecosystems, we identified effective methods that balance security and resource utilization. The study revealed that lightweight cryptography, when appropriately implemented, enhances the protection of data and devices while addressing inherent vulnerabilities such as side-channel and brute-force attacks. Furthermore, the scalability of these systems supports the expanding application of IoT across both consumer and industrial domains.

References

1. William Stallings. Cryptography and Network Security: Principles and Practice. Pearson 7th (latest edition). ISBN: 978-0134444284
2. Jorg K. H. Franke, Christopher Wolf, and Achim E. Reinders. Lightweight Cryptography for Low-Latency IoT Networks. Springer 1st edition. ISBN: 978-3030605077
3. V. Sridhar, S. Srinivasan, and R. R. K. Gupta. Security and Privacy in Internet of Things (IoT). CRC Press 1st edition ISBN: 978-0367332691
4. Qusay H. Mahmoud. Internet of Things Security and Privacy. Wiley 1st edition ISBN: 978-1119257414
5. Ashutosh Dhar, Guatam Srivastava Security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK. Internet of Things 21(2023) 100677
6. T.Qozoqova, B.Shamshiyeva., Applying the CryptoSMT software tool to symmetric block encryption algorithms, Artificial Intelligence, Blockchain, Computing and Security Volume 2, p-750-754
7. Thomas Peyrin, Sumanta Sarkar, Yu Sasaki, Siang Meng Sim. A Study on TRIFLE-BC
8. Darzi S., Ahmadi K., Aghapour S., Yavuz A.A., Kermani M.M. Envisioning the future of cyber security in post-quantum era: A survey on PQ standardization, applications, challenges and opportunities 10.48550/ARXIV.2310.12037
9. Grover L.K. A fast quantum mechanical algorithm for database search Proceedings of the twenty-eighth annual ACM symposium on theory of computing STOC '96, ACM Press (1996), 10.1145/237814.237866
10. Qozoqova T.Q. Microsoft Threat Modeling Tool Dasturiy Vositasida Stride Modeli., Central asian journal of academic research. Issue -6, pp-63-70
11. Qozoqova T.Q., General concepts of cryptanalysis methods., Информатика и инженерные технологии., Том1., ст-147-150
12. Qozoqova T.Q., Teaching cryptanalysis of classic encryption methods using modern tools., «Инновации, знания, опыт – векторы образовательных треков»: Материалы международной научно-практической конференции. КНИГА I., ст-773-777
13. https://www.iotinsider.com/smart-world/consumer-iot-ensuring-security-and-privacy/
14. https://www.amantyatech.com/consumer-iot-what-it-is-prominent-use-cases
15. https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT
16. https://en.wikipedia.org/wiki/PRESENT