UDC 004.056

PROSPECTS OF USING LIGHTWEIGHT CRYPTOGRAPHY IN IoT DEVICES

Gasimov V.A., Zahidova G.A., Zeynalli-Huseynzada L.R
Baku Engineering University, Baku, Azerbaijan

Abstract. The expansion of the IoT ecosystem necessitates a fundamental shift in securing cyber-physical systems. While security is paramount where sensors and actuators operate, resource constraints-limited memory, low throughput, and energy reserves-often make standard protocols like AES-128 technically prohibitive. This paper analyzes the transition toward Lightweight Cryptography (LWC), exploring architectural trade-offs between security margins and hardware efficiency. By evaluating optimized algorithms such as ASCON and PRESENT, the study examines their performance in constrained environments. Acknowledging current limitations, this research identifies future development paths to enhance both the performance and defensive capabilities of IoT systems.
Keywords: Lightweight cryptography; Internet of Things (IoT) security; cryptography; Advanced Standard Encryption (AES); ASCON; PRESENT; cyber-physical systems; block cipher

Introduction

With computing becoming more prevalent in people's life, they are increasingly defined by a plethora of smart gadgets or devices, Internet of Things (IoT) is one of them. Things that can communicate and interact with one another via wired or wireless transmission are referred to as IoT. These devices are time-related in that they convey information based on real-time data acquired from sensors that connect with users through a network, allowing them to take action based on their needs. IoT is a network of networked devices as shown on figure that communicate information and data in real time. The three vital main components of IoT architecture are perception layer, network layer and application layer. The physical layer, where devices such as RFID tags, sensors, and cameras assist in collecting data from the environment. The network layer, which acts as the heart of IoT as it consists of both hardware and software components and transmits information collected by the physical layer. The application layer, which serves as a link between the user and the IoT device. The devices are used in a variety of industries as:

Smart Residential Environments: In the realm of home automation, the interconnection of diverse smart devices allows for centralized management of

domestic infrastructure. Users can remotely orchestrate lighting systems, climate control, and energy consumption through mobile interfaces, achieving a seamless balance between convenience and resource efficiency.

Next-Generation Healthcare: The healthcare sector has witnessed a paradigm shift through the deployment of IoT-enabled medical sensors. By facilitating continuous, real-time physiological monitoring, these devices transmit critical patient data directly to clinical practitioners. This instantaneous feedback loop ensures that life-saving interventions can be initiated immediately upon the detection of anomalous vital signs, significantly reducing mortality rates.

Enhanced Surveillance and Public Safety: Security frameworks have been substantially fortified by networked monitoring systems. The synergy between high-definition cameras and motion sensors enables the precise tracking of assets and individuals across vast distances. This synchronized data stream, accessible via handheld devices, provides an unprecedented level of situational awareness for both private and public safety sectors.

Environmental Monitoring and Disaster Mitigation: IoT technology plays a pivotal role in catastrophe management by providing early warning systems for natural disasters. Through a distributed network of environmental sensors, vast amounts of geological and atmospheric data are analyzed to predict seismic activities or extreme weather patterns. These predictive analytics are essential for disaster preparedness, effectively minimizing human casualties and infrastructural damage.

The proliferation of Internet of Things (IoT) devices has introduced a critical challenge: the secure management of highly sensitive data, often collected autonomously without direct human intervention. In these hyper-connected environments, ensuring data integrity and preventing unauthorized access is paramount. However, the architectural reality of most IoT nodes-characterized by minimal computational throughput, restricted memory, and finite battery reserves-creates a significant barrier to traditional security implementation. These "resource-constrained" devices cannot effectively support conventional cryptographic suites such as AES, DES, or RC6, as their high-power consumption and area overhead are incompatible with the scalable and dynamic nature of IoT networks.

Furthermore, the complexity of encryption key management adds another layer of vulnerability; inadequate protocols can jeopardize the entire security framework of a lightweight system. To bridge this gap, modern scientific discourse has pivoted toward Lightweight Cryptography (LWC). These optimized algorithms are specifically engineered to strike a delicate balance between robust security margins and hardware efficiency. By mitigating the computational burden of encryption, LWC solutions offer a sustainable pathway to safeguarding privacy without compromising device performance.

This paper evaluates recent advancements in this field, comparing various block ciphers and assessing the adaptability of the Advanced Encryption Standard (AES) within the specialized constraints of the IoT domain.

Design Constraints and Security Requirements in IoT

The development of cryptographic solutions for the IoT landscape is primarily dictated by the rigorous constraints of the hardware. These devices, characterized by their compact physical dimensions, possess minimal memory (RAM/ROM) and limited computational power, yet they often require real-time responsiveness. Traditional security protocols frequently fail to meet these specific needs, leading to the emergence of Lightweight Cryptography (LWC). A qualified LWC algorithm must satisfy four fundamental security pillars: confidentiality (ensuring data is only accessible to authorized parties), integrity (preventing unauthorized alterations), authentication (verifying the identity of the communicating entities), and non-repudiation (ensuring that a transaction cannot be denied by the sender).

From an algorithmic perspective, both hardware and software efficiency are critical. In software, the focus is on reducing temporal complexity and optimizing memory footprints. In hardware, the emphasis shifts to minimizing power consumption and reducing latency – the delay between input and output –which is vital for time-sensitive IoT applications.

While both symmetric and asymmetric encryption models exist within the LWC framework, symmetric key algorithms are generally preferred for IoT designs. Asymmetric cryptography, although offering robust security, is often too computationally intensive and complex for resource-constrained nodes. In contrast, symmetric encryption provides a high-speed, low-latency alternative with significantly lower demands on storage and processing bandwidth.

Within symmetric cryptography, block ciphers have gained more traction than stream ciphers over the last decade. Their popularity stems from their versatility and the symmetry between encryption and decryption processes, which allows for the reuse of hardware components. Furthermore, block ciphers exhibit superior error propagation and diffusion characteristics, making them easier to implement in both hardware and software with minimal resource overhead. The efficacy of these ciphers is typically determined by four factors: the number of rounds, block size, key length, and the underlying architectural structure.

The internal design of a block cipher usually relies on several core mechanisms to ensure security:

Substitution-box (S-box): This component performs non-linear transformations (typically on 4-bit blocks). While S-boxes increase processing time, a higher number of active S-boxes significantly strengthens the cipher's resistance to cryptanalysis.

Permutation-box (P-box): This layer shuffles the bits to redistribute information across the block, providing the necessary bit-level diffusion.

Substitution-Permutation Network (SPN): Utilized by modern standards like AES, the SPN structure alternates between substitution and permutation layers in each round to achieve "confusion and diffusion" – the two hallmarks of secure encryption.

Iterative Rounds: Encryption is achieved through multiple rounds of these operations, with each round utilizing a unique sub-key derived from the master key.

Feistel Network**:** An alternative structure that divides the data into two halves, applying transformations to only one half per round before swapping them. This design simplifies the decryption process, as the same internal function can be used for both directions.

Efficiency and Attack Resistance in LWC Design

The primary objective in developing cryptographic solutions for resource-constrained hardware is to minimize the overhead across memory, silicon area, and power consumption. Optimization strategies often focus on balancing high performance with robust security. For instance, recent methodologies suggest using masking techniques – such as generating "fake keys" to hide secret keys from substitution layers – to enhance security, though this may increase the power area.

Additionally, researchers have explored methods to mitigate attack complexity by manipulating the number of iterations through related-key approaches. Specifically, in the context of AES-192, studies on reduced-round attacks indicate that the strategic placement of rounds – before rather than after the point where "impossible conditions" (cryptanalytic vulnerabilities) arise – can significantly influence the cipher's resistance to attacks. These structural refinements are essential for maintaining cryptographic strength without exceeding the strict limitations of IoT devices.

The PRESENT algorithm is a widely recognized block cipher in the LWC domain, characterized by its 64-bit block size and 80-bit key length. Research indicates that this cipher provides a robust security margin while remaining exceptionally hardware-friendly. Furthermore, implementations on FPGA (Field Programmable Gate Array) demonstrate that algorithms like Blowfish can achieve high-speed execution with minimal latency. By leveraging Hardware Description Languages (HDL) for integrated circuit design, these approaches minimize encryption time and significantly maximize system throughput, making them ideal for high-performance IoT applications.

The ASCON Cipher and the NIST LWC Standard

A significant milestone in the field of lightweight cryptography is the emergence of the ASCON family of algorithms. Designed to provide both Authenticated Encryption with Associated Data (AEAD) and hashing

capabilities, ASCON was officially selected by the National Institute of Standards and Technology (NIST) as the new standard for lightweight cryptography in 2023. This selection was primarily driven by its exceptional performance in resource-constrained environments where traditional standards like AES-GCM are inefficient.

ASCON is based on a sponge-based construction, utilizing a 320-bit permutation that balances security and throughput. It is specifically engineered to be resilient against side-channel attacks, which is a critical requirement for IoT devices deployed in physically accessible or hostile environments. The algorithm's flexibility – supporting 128-bit keys and offering various variants like ASCON-128 and ASCON-128a – allows developers to optimize for either minimum area overhead or maximum speed. By integrating ASCON into the IoT ecosystem, developers can achieve high-level data confidentiality and integrity with significantly lower power consumption and a smaller hardware footprint compared to conventional cryptographic suites.

Conclusion

The pervasive integration of IoT devices into critical sectors such as healthcare, surveillance, and disaster management underscore the urgent need for robust yet efficient security frameworks. As this research has demonstrated, traditional cryptographic standards often fail to meet the stringent power and memory requirements of resource-constrained IoT nodes. The transition toward Lightweight Cryptography (LWC) represents the most viable pathway to bridging the gap between high-level security and hardware efficiency.

Through the analysis of optimized algorithms like PRESENT and the NIST-standardized ASCON, it is evident that symmetric block ciphers and sponge-based constructions offer superior performance in constrained environments. While the adaptation of established standards like AES remains a challenge due to their inherent complexity, architectural optimizations such as S-box refining and hardware-efficient implementations provide promising results. Ultimately, the future of IoT security lies in the continued development of algorithms that provide resilience against both mathematical cryptanalysis and physical side-channel attacks. By adopting these lightweight solutions, the IoT ecosystem can achieve a sustainable balance between operational throughput and the non-negotiable requirement of data privacy.

References

1. Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M. J., Seurin Y., Vikkelsoe C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. International Workshop on Cryptographic Hardware and Embedded Systems. Springer. 4727, 450–466.

2. Dobraunig C., Eichlseder M., Mendel F., Schläffer M. (2021). Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology. Springer. 34 (3), 1–42.

3. Menezes A. J., Van Oorschot P. C., Vanstone S. A. (2018). Handbook of Applied Cryptography. CRC Press. 5th Edition, 191–220.

4. Daemen J., Rijmen V. (2002). The Design of Rijndael: AES – The Advanced Encryption Standard. Information Security and Cryptography. Springer. 1, 31–55.

5. Hatzivasilis G., Fysarakis K., Papaefstathiou I., Papadakis C. (2018). A Review of Lightweight Block Ciphers. Journal of Cybersecurity and Information Management. Elsevier. 2 (1), 15–32.

6. NIST. (2023). NIST Selects 'Ascon' Algorithms for Lightweight Cryptography. National Institute of Standards and Technology. NIST News (Special Publication), 800–175.

7. Rolfes C., Poschmann A., Paar C. (2008). Ultra-Lightweight Implementations for Smart Devices – Is PRESENT Enough? International Conference on Smart Card Research and Advanced Applications. Springer. 5189, 247–262.

8. Guo J., Peyrin T., Poschmann A., Robshaw M. (2011). The PHOTON Family of Lightweight Hash Functions. International Cryptology Conference. Springer. 6841, 222–239.

Information about the authors

Gasimov V.A., Professor, Dean of the Faculty of Information and Computer Technologies, Baku Engineering University, vaqasimov@beu.edu.az.

Zahidova G.A., Lecturer of Cybersecurity and Computer Engineering Department, Baku Engineering University, guabdullayeva@beu.edu.az.

Zeynalli-Huseynzada L.R., Lecturer of Cybersecurity and Computer Engineering Department, Baku Engineering University, lzeynalli@beu.edu.az.