TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Lightweight Cryptography over Constrained IoT Devices: Securities the Smallest Machines.

The latest generation of highly-efficient cryptography is enabling the protection of even the smallest IoT devices without consuming their few power, memory, or processing resources.

By **Fizah Iman** | University of Agriculture, Faisalabad | Published: June, 2026
Imanfizah28@email.com | Position: Student

Introduction

The surrounding world is turning into the world of smart devices. Be it a wearable device that counts our physical activity, or a high tech system in the home, in the industry, or in the farm, there are now an increasing number of connected devices than ever. Although all these devices simplify our lives, they may lead us to face severe threats due to cyberattacks.

The problem with IOT devices are that they are limited inresources. That is, such devices do not have enough computing capabilities to support complex cryptographic algorithms. As such, it renders lots of IoT systems vulnerable to any attack.

This is where lightweight cryptography can come to the rescue. That is, it provides encryption methods to devices that have limited computing abilities.

The use of IoT devices is increasing in Pakistan.

> ***""Security is not a choice; every device big or small needs protection in today's highly interconnected world."***

Technology Overview

Explain The lightweight cryptography concept is defined as cryptographic schemes that are designed to be able to run on machines with low computational capabilities. Such schemes are differentiated with the traditional encryption schemes in terms of fewer memory requirements, less power consumption, and high execution time.

The Ineffectiveness of the Traditional Approaches:

Some traditional encryption methods include AES and RSA that have the benefit of offering an adequate level of security. But they are challenging to apply in the IoT since:

- They require large processing speeds.
- They consume much battery capacity
- They have higher memory requirements

As an example, the simple temperature sensor in smart farming will not be capable of using such techniques without undermining its productivity.

Why Special Lightweight Cryptography?

Lightweight cryptography has the following characteristics:

- Lower power usage
- Reduced memory needs
- Higher execution speed
- Sufficient security

The aim of such algorithms is to achieve a trade-off between security and efficiency.

Lightweight Cryptography Methods:

1. Block Ciphers:

   They cipher data in blocks. The lightweight block ciphers that are popularly employed include PRESENT and LED.

2. Stream Ciphers:

   They work on bits of data in a sequence. They are comparatively quicker and can be used in real-time applications.

3. Hash Functions:

   They are used in guaranteeing the integrity and authentication of the data. Less computation is required of hash functions.

4. Authenticated Encryption:

   It involves the concurrent use of encryption and authentication.

5. Lightweight Cryptography Applications:

6. Smart Homes:

   Secure data transfer in devices such as smart locks and cameras

7. Healthcare:

   Wearable technologies data security.

8. Agriculture:

   Integrity of data in sensors used to measure soil quality and weather conditions.

9. Industry IoT:

   Factory automation systems Smart irrigation and remote health monitoring are two applications of lightweight cryptography in Pakistan.

But, lightweight cryptography is not solely about conserving computing power, but rather optimization of the algorithms themselves down to the bottom. Algorithms written in a manner that they can execute what they are meant to execute without numerous logical operations, access to memory and clock operations. As a result, such algorithms are well-suited to embedded systems and microcontrollers that are utilized in IoT applications.

The other major aspect of lightweight cryptography is that it can be used effectively in a vast variety of hardware designs. The processors based on low-energy consumption such as ARM Cortex-M families are used in most IoT applications. The use of traditional cryptographic algorithms might lead to a delay in the execution of the tasks by the processor and hence inefficiency to the whole system. Special purpose optimization was made in lightweight algorithms.

Figure 1: Example of lightweight cryptography protecting interconnected IoT devices within smart city infrastructures., Credit: Adapted from online resources

Key Findings & Impact

- Increased Efficiency:

  Recent studies show that savings of up to 50 percent in energy usage can be made by use of lightweight cryptography. This is important in the functioning of battery-operated IoT devices.

- Security Enhancements:

  Although lightweight, such cryptographic systems provide good protection against:

- Security breaches:

  Hacking,Tampering So, even low-budgets devices will work with enough security.

- Scalability:

  A thousand or more connected devices can be part of an IoT network in certain instances. Lightweight cryptography also allows the development of scalable networks that are capable of communicating effectively between the devices.

- Cost Efficiency:

The manufacturing cost will be significantly lower with the lower hardware requirements. This is very important to Pakistan as it is a developing nation.

The contribution to the Pakistani Technology Industry is:

Lightweight cryptography will have the following advantages to Pakistan:

Startups: The development of low-cost safe IoT devices.

- Agricultural Industry: Securing IoT devices within the smart agriculture industry.
- Healthcare: Data that is transferred to remote servers is protected.
- Smart Cities: Traffic management, surveillance, and other IoT-based technologies security.

Security will be among the components of the digital transformation in Pakistan as it shifts its path towards digital transformation.

What's Next?

However, despite the benefits offered by lightweight cryptography, there are some issues that should be resolved.

Standardization:

Global organizations have made efforts to standardize lightweight algorithms.

- Efficiency vs. Security:

There should be a good balance between the performance of the algorithms and security. Overly lightweight algorithms can easily be attacked.

- Knowledge and Deployment:

Cryptography lightweight: not every IoT developer knows how to use security protocols, and therefore requires training on implementing lightweight cryptography.

Future Prospects:

- Combining lightweight algorithms with artificial intelligence
- Implementing lightweight cryptography on 5G-based IoT.
- Lightweight cryptography of smart infrastructural projects.

When used correctly, Pakistan can use these technologies to develop its digital ecosystem

About the Author

I am Fizah Iman currently pursuing the degree of Bachelor of Computer Science. I can be reached at imanfizah8@gmail.com

Keywords: Cryptography, Cyber Security, Embedded Systems;

References

[1] SIMON and SPECK: Light Block Ciphers. IEEE.

[2] Lightweight Cryptography Lightweight Cryptographic Engineering in the Pervasive World.

[3] Mahmood, K. et al. (2022). IoT Security Issues