ECC1296

LIGHTWEIGHT CRYPTOGRAPHY FOR IOT SECURITY

Privacy and Security in IoT (CO2)

In today's connected world, security is not an option – it's a necessity. Let's safeguard the digital age together.

HARISH PRANAV S

927624BEC066

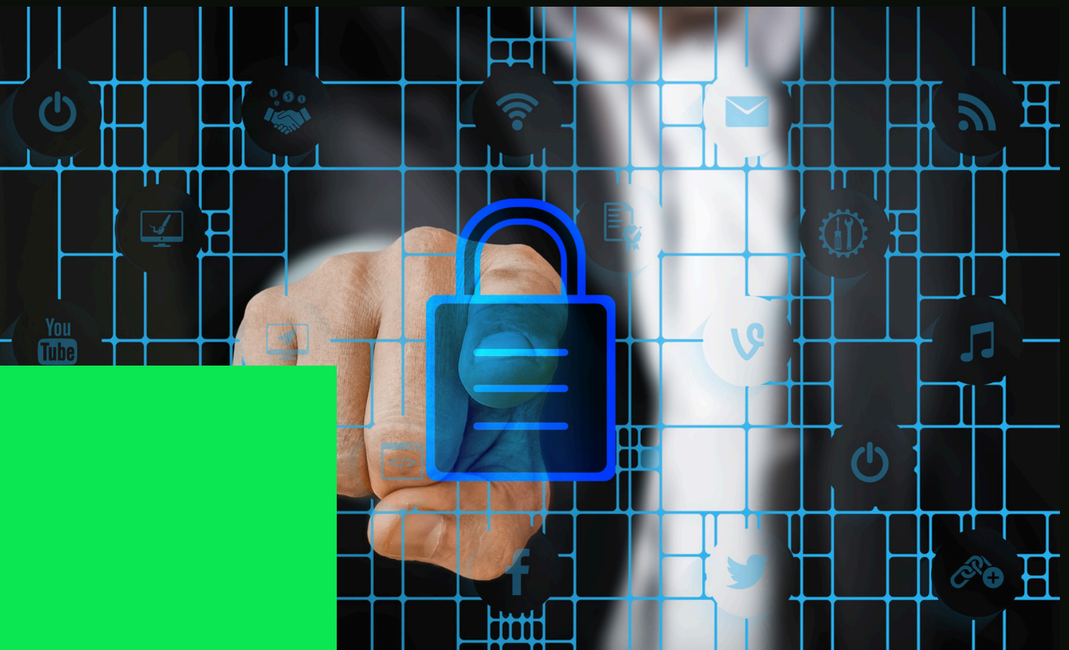
ECC1296

INTRODUCTION

The Internet of Things (IoT) refers to a network of interconnected devices such as sensors, smart appliances, and wearable systems that continuously collect and exchange data. As IoT systems increasingly interact with the physical world, ensuring **security and privacy** becomes a critical requirement rather than an optional feature.

ECC1296

WHY IOT DEVICES ARE VULNERABLE?



•IoT devices are typically designed to be **low-cost, compact, and energy-efficient**. Due to these constraints, they operate with:

- Limited processing power
- Restricted memory capacity
- Low battery availability

•These factors make IoT systems more vulnerable to security attacks.

ECC1296

ROLE OF CRYPTOGRAPHY IN IOT

•Cryptography forms the backbone of IoT security by ensuring:

- Confidentiality of data
- Integrity of transmitted information
- Authentication of devices

•Without cryptographic protection, IoT communication channels can be easily exploited.

ECC1296

LIMITATIONS OF TRADITIONAL CRYPTOGRAPHY

Conventional cryptographic algorithms such as RSA and standard AES were designed for powerful computing systems. When implemented in IoT devices, they result in **high computational overhead**, increased energy consumption, and reduced device lifespan.

ECC1296

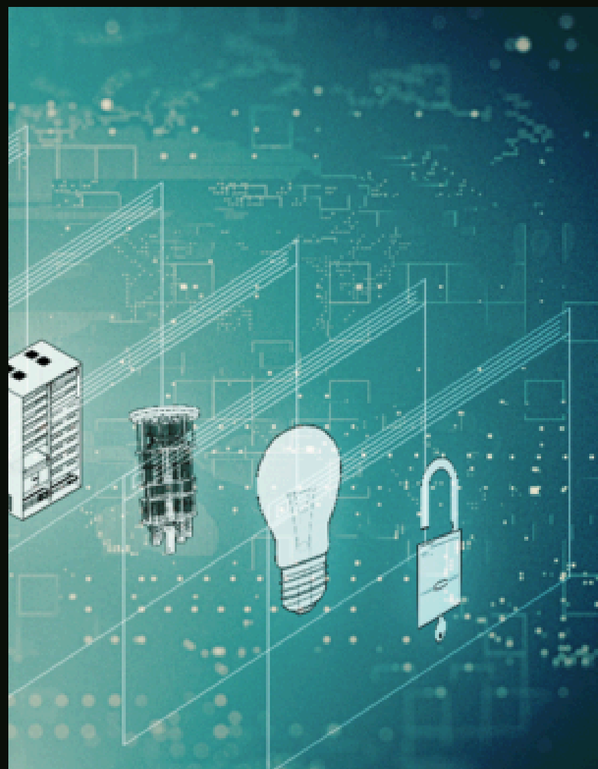
NEED FOR LIGHTWEIGHT CRYPTOGRAPHY

To address the limitations of traditional cryptographic techniques, **lightweight cryptography** has been introduced. It aims to provide adequate security while operating efficiently within constrained IoT environments

ECC1296

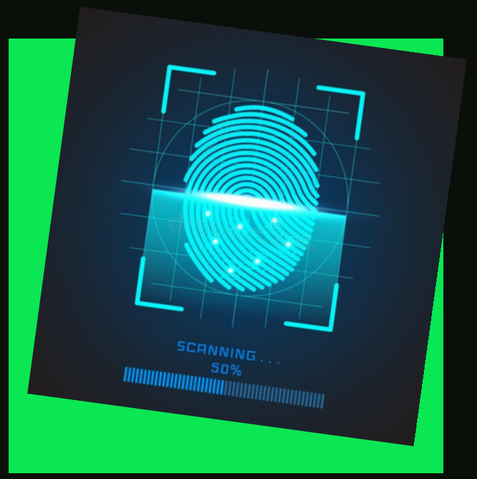
WHAT IS LIGHTWEIGHT CRYPTOGRAPHY?

Lightweight cryptography focuses on achieving **optimal security-performance balance**. It uses simplified mathematical operations, reduced key sizes, and efficient execution models suitable for resource-constrained devices.



ECC1296

COMPONENTS OF LIGHTWEIGHT CRYPTOGRAPHY



•Lightweight cryptographic systems typically include:

- Lightweight encryption algorithms
- Lightweight hash functions
- Efficient authentication mechanisms

•These components work together to ensure secure communication.

ECC1296

KEY MANAGEMENT IN IOT

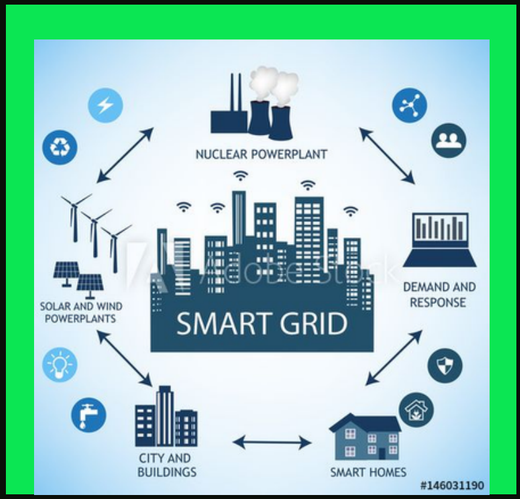
• Effective key management is crucial for IoT security. Even the strongest cryptographic algorithm can fail if keys are poorly managed.

•Common approaches include:

- Pre-shared keys
- Dynamic key generation
- Secure key storage mechanisms

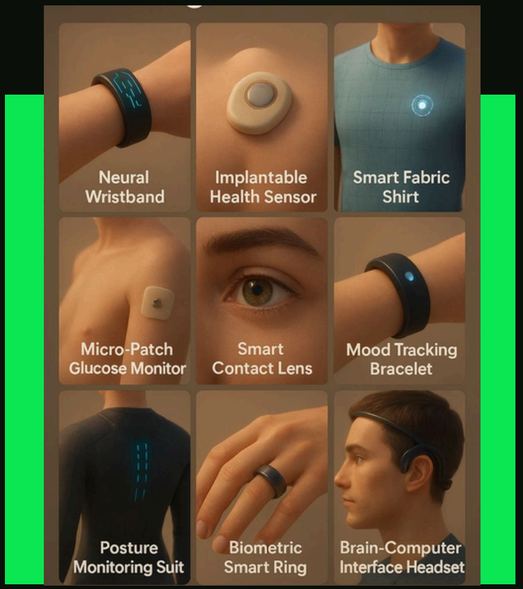
ECC1296

REAL-WORLD APPLICATIONS



Smart Grids

IoT systems



Wearable & healthcare

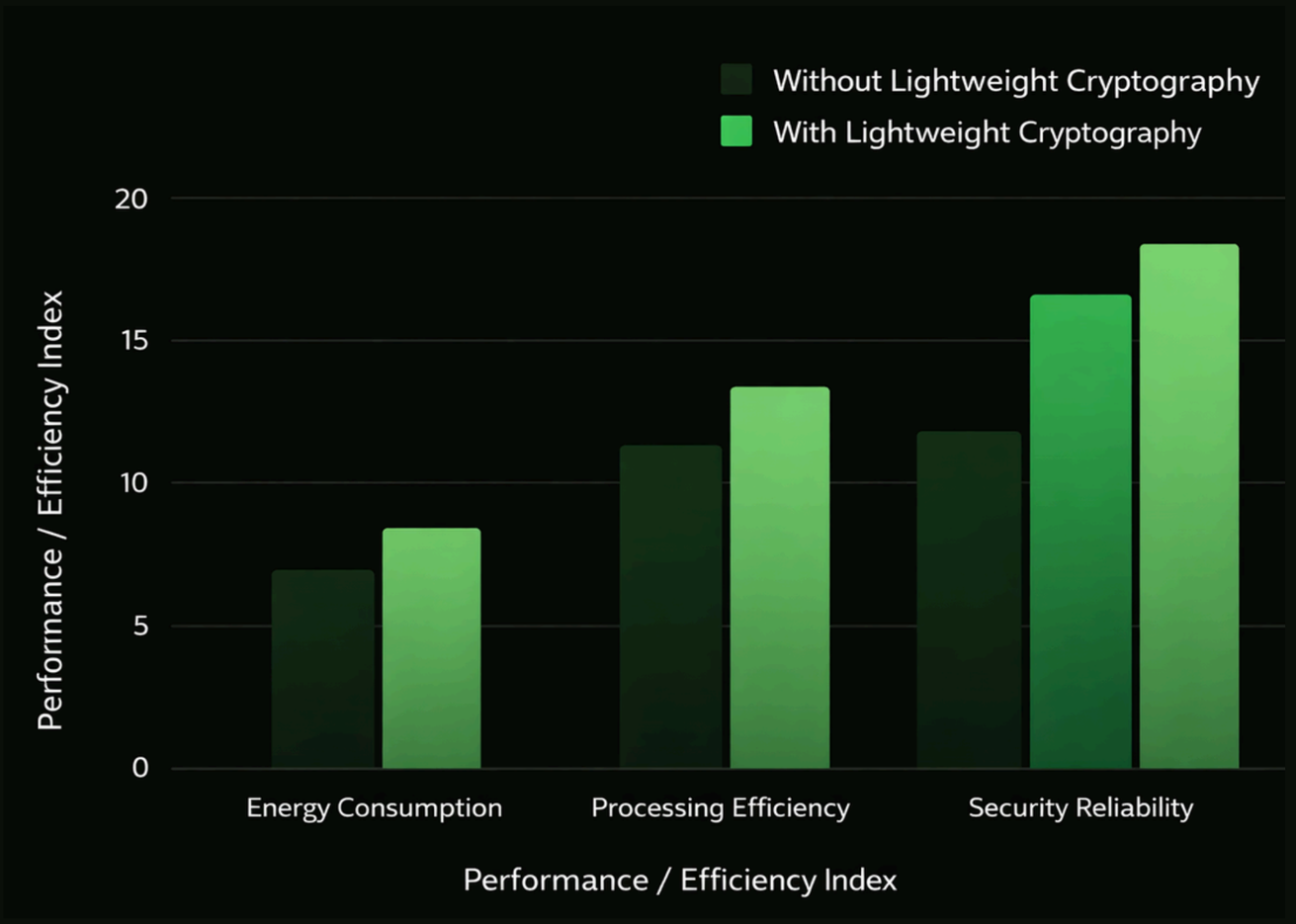
quantum computing

ECC1296

CHALLENGES AND FUTURESCOPE

Despite its advantages, lightweight cryptography faces challenges such as standardization, scalability, and resistance to advanced attacks.

Future research focuses on combining lightweight cryptography with **AI-assisted security** and hardware-based protection.



ECC1296

CONCLUSION

Lightweight cryptography is essential for securing modern IoT systems. It is not about achieving maximum theoretical security, but about designing **efficient and practical security solutions** that fit IoT constraints

ECC1296

CASE STUDY

Smart Healthcare Wearables secured using Lightweight Cryptography

Result: Secure patient data transmission, reduced power consumption, and extended device lifetime through efficient cryptographic design.

ECC1296

BEST PRACTICES FOR INDIVIDUALS

Strong Passwords

Two-factor Auth

Avoid Suspicious Link

ECC1296

THANK YOU!

91+ 7845693765

harishpranavs259@gmail.com

@Cryptographysite

Lightweight_Cryptography.com