Інженерія, виробництво, транспорт, будівництво, природничі науки, математика, статистика

DOI: 10.61718/att8.01
UDC 004.056.55

Cherniavskyi Bohdan Vadymovych
Oles Honchar Dnipro National University
ORCID: 0009-0006-3933-1423
Scientific supervisor: Chernetchenko Dmytro Volodymyrovych, Associate Professor,
Oles Honchar Dnipro National University

CRYPTOGRAPHIC ALGHORITMS FOR IOT AND FULL-SIZE PROCESSORS

This thesis analyzes cryptographic algorithms for IoT devices and full-size processors, considering resource constraints, performance, and security. It recommends suitable algorithms for each platform and discusses future trends like post-quantum cryptography and lightweight cryptography advancements. *Keywords: Cryptography, IoT, Full-size Processors, Lightweight Cryptography, AES, ECC, ChaCha20, RSA, SHA-256, SHA-512, 3DES, Ascon, Post-Quantum Cryptography, Security, Performance.*

The increasing reliance on interconnected devices, spanning from resource-constrained Internet of Things (IoT) devices to high-performance full-size processors, necessitates robust security measures. Cryptography provides the essential tools for ensuring data confidentiality, integrity, and authenticity across these diverse platforms [1]. However, the stark contrast in computational capabilities between IoT devices and full-size processors presents unique challenges for cryptographic algorithm implementation. This thesis analyzes cryptographic algorithms for their suitability across both IoT devices and full-size processors, considering performance based on benchmark data and security strengths, to recommend appropriate cryptographic solutions for each platform.

Cryptography secures data through confidentiality, integrity, and authentication. Symmetric cryptography uses a single secret key for encryption and decryption and is generally faster. Examples include Advanced Encryption Standard (AES), ChaCha20, and Triple DES (3DES) [1]. Asymmetric cryptography uses a public key for encryption and a private key for decryption, simplifying key management. RSA is a prominent asymmetric algorithm, as is Elliptic Curve Cryptography (ECC) [2]. Cryptographic hash functions like SHA-256 and SHA-512 generate fixed-size data digests for integrity verification [3].

IoT devices face unique cryptographic challenges due to resource constraints. Limited processing power and memory hinder the use of computationally intensive algorithms. Energy efficiency is crucial for battery-powered devices. The diverse nature of IoT devices and the lack of universal security standards complicate security implementation [4]. Managing numerous devices and deploying updates are also significant challenges. These limitations necessitate lightweight cryptography tailored for constrained platforms.

Benchmark data is crucial for evaluating cryptographic algorithm suitability across platforms. Key metrics include execution time and memory usage. Performance varies significantly among algorithms and platforms. Hardware acceleration, like for AES on modern processors, improves performance [5]. Lightweight algorithms may perform better on resource-constrained devices like Raspberry Pi [6].

Security strengths and weaknesses are paramount in algorithm selection. AES is a secure and efficient standard with strong resistance to brute-force attacks [1]. Bcrypt is strong for password hashing due to its computational cost. ChaCha20 is a fast and secure stream cipher, efficient in software. ECC offers strong security with smaller key sizes [2]. HMAC provides robust message authentication and integrity [1]. RSA is slower and more resource-intensive. SHA-256 and SHA-512 are secure hashing algorithms [3]. 3DES is a legacy algorithm with security limitations [1].

Academic literature and industry standards guide cryptographic algorithm selection. For IoT devices, lightweight cryptography is essential. NIST selected Ascon as the lightweight cryptography standard for IoT [7]. Lower-power sensors can use simpler symmetric algorithms like PRESENT or SPECK [8]. Edge devices can use lightweight AES or ChaCha20. ECC is suitable for asymmetric operations on IoT devices [2]. For full-size processors, AES-256 is recommended for bulk encryption due to its security and hardware acceleration [1]. ChaCha20 is a good software alternative. Bcrypt is recommended for password hashing. RSA and ECC are suitable for asymmetric encryption, with ECC generally offering better performance.

Recommended Algorithms:

Low-Power IoT:

- *Data Encryption:* Lightweight AES, ChaCha20, Ascon
- *Authentication/Integrity:* HMAC-SHA-256, Lightweight MAC, ECC

Edge IoT:

- *Data Encryption:* AES-128/256, ChaCha20
- *Authentication/Integrity:* HMAC-SHA-256/512, ECC

Full-Size Processor:

- *Bulk Data Encryption:* AES-256, ChaCha20
- *Password Hashing:* bcrypt, Argon2, scrypt
- *Asymmetric Encryption/Key Exchange:* RSA (≥ 2048-bit), ECC (≥ 256-bit)
- *Data Integrity/Authentication:* HMAC-SHA-256/512

Post-quantum cryptography (PQC) is a significant trend due to the threat of quantum computers breaking current public-key cryptosystems. NIST is standardizing quantum-resistant algorithms [9]. Lightweight cryptography continues to advance, optimizing algorithms for resource-constrained devices. Hardware-based cryptographic accelerators are increasingly integrated into processors [6].

Selecting appropriate cryptographic algorithms for IoT devices and full-size processors requires careful consideration of platform capabilities and security requirements. Lightweight algorithms are crucial for resource-constrained IoT devices, while full-size processors can leverage more computationally intensive algorithms and hardware acceleration. The emergence of post-quantum computing necessitates a transition to quantum-resistant cryptography. Continuous evaluation and adaptation of cryptographic strategies are essential for maintaining security across diverse computing platforms.

Sources.

1. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. Pearson Education, 2017.
2. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer, 2004.
3. National Institute of Standards and Technology (NIST). Secure Hash Standard (SHS). FIPS PUB 180-4, 2015.
4. Abomhara M., Koien G. M. "Security and privacy in the Internet of Things: Current status and open issues." International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014.
5. McLaughlin S. et al. "The Energy Cost of Security in Embedded Systems." IEEE Transactions on Computers, 2012.
6. Kaur H., Kaur R. "Performance Evaluation of Lightweight Cryptographic Algorithms on Raspberry Pi." International Journal of Computer Applications, 2018.
7. National Institute of Standards and Technology (NIST). "NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices", 2023.
8. Bogdanov A. et al. "PRESENT: An Ultra-Lightweight Block Cipher." CHES 2007: Cryptographic Hardware and Embedded Systems, 2007.
9. Chen L. et al. "Report on Post-Quantum Cryptography." NISTIR 8105, 2016.

УДК 621.65

Яременко Андрій Леонідович
Поліський національний університет
Науковий керівник: Савченко Василь Миколайович, кандидат технічних наук, доцент,
Поліський національний університет

УДОСКОНАЛЕННЯ КОНСТРУКЦІЇ ЛОПАТЕЙ РОБОЧОГО КОЛЕСА ВІДЦЕНТРОВОГО НАСОСА ДЛЯ ЗМЕНШЕННЯ КАВІТАЦІЇ

У тезах розглянуто можливість покращення гідравлічних характеристик відцентрового насоса за рахунок впровадження біонічного дизайну лопатей. Аналіз показує, що застосування синусоїдальної форми переднього краю дозволяє зменшити інтенсивність кавітації, покращити напір і підвищити ефективність роботи насоса. Ключові слова: кавітація, відцентровий насос, біонічний дизайн, лопаті, напір.

У сучасних системах зрошення відцентрові насоси відіграють ключову роль у забезпеченні водопостачання. Однією з основних проблем, що знижує їх ефективність, є кавітація – руйнівне явище, яке виникає при падінні тиску нижче рівня насичення. Це призводить до утворення парових бульбашок, які спричиняють ерозійний знос лопатей та зменшення терміну служби обладнання.

У кваліфікаційній роботі було запропоновано вдосконалити конструкцію лопатей робочого колеса шляхом застосування біонічного підходу: впровадження синусоїдального переднього краю, аналогічного