ALGORITMOS CRIPTOGRÁFICOS LEVES PARA A INTERNET DAS COISAS: UMA ANÁLISE MULTIMÉTRICA

YURI SILVA VAZ[1]; RAFAEL IANKOWSKI SOARES[2]; JÚLIO C. B. MATTOS[3]

[1]*Universidade Federal de Pelotas – ysvaz@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br*
[3]*Universidade Federal de Pelotas – julius@inf.ufpel.edu.br*

1. INTRODUÇÃO

A Internet das Coisas, do inglês *Internet of Things* (IoT), refere-se a dispositivos físicos que possuem sensores, *software* e conectividade com a Internet de forma integrada, permitindo-lhes coletar e compartilhar dados (IBM, 2023). Com uma projeção de 40 bilhões de dispositivos conectados até 2030, a segurança e a privacidade se tornam preocupações centrais, visto que muitos destes dispositivos são vulneráveis a ataques (SINHA, 2024).

A criptografia é uma solução eficaz para proteção dos dados que trafegam pela Internet. Contudo, algoritmos clássicos de criptografia são computacionalmente custosos, impactando em desempenho e consumo energético, o que é muito indesejado em aplicações IoT, nas quais são usualmente implementadas em dispositivos com recursos computacionais limitados (KADHIM; ABDUL-MAJEED; ALI, 2017). Para atender a esta demanda, surgiu a criptografia leve, do inglês *lightweight cryptography* (LWC), na qual busca reduzir a complexidade computacional dos algoritmos, propondo soluções mais leves, que consumam menos memória e também energia, porém, não abrindo mão de níveis aceitáveis de segurança (ORANGE, 2022).

Este trabalho realiza uma análise comparativa e abrangente dos algoritmos criptográficos simétricos leves ASCON, AES-LWC, PRESENT, SHADOW, SLIM e XTEA. Utiliza-se o algoritmo AES como referência, por ser um padrão amplamente validado e aprovado. Estes algoritmos foram selecionados por estarem entre os mais citados em estudos recentes envolvendo criptografia leve, juntamente com o AES e sua variante leve, o AES-LWC, descrito em Vaz, Mattos e Soares (2023). A avaliação considera métricas de desempenho (tempo de execução, consumo de memória e consumo energético) e segurança (efeito avalanche, balanceamento de bits e testes do NIST), executando os algoritmos nas plataformas ESP32 e Raspberry Pi Pico.

Os resultados trazidos por este trabalho não somente preenchem as lacunas deixadas por outros estudos comparativos, como também trazem três algoritmos (AES-LWC, SHADOW e SLIM) ainda não avaliados conjuntamente nesse contexto.

2. METODOLOGIA

Os experimentos foram conduzidos em duas plataformas populares para o desenvolvimento de aplicações IoT: ESP32 e Raspberry Pi Pico. A ESP32 possui um processador dual-core Xtensa de até 240 MHz, 520 KB de memória RAM e 4MB de memória flash, enquanto a Raspberry Pi Pico possui um processador ARM Cortex-M0+ de até 133 MHz, 264 KB de memória RAM e 2MB de memória flash.

A análise de consumo energético foi realizada com o auxílio da Power Profiler Kit II (PPK2), uma ferramenta de alta precisão para monitoramento de corrente elétrica. Cada algoritmo foi executado 100 vezes em sequência em cada

plataforma, com a PPK2 amostrando a corrente elétrica a uma taxa de 100.000 amostras por segundo.

Para calcular o consumo total de energia, cada amostra de corrente elétrica do arquivo CSV foi multiplicada pela tensão de alimentação (3,3 V) para obter a potência instantânea. Esses valores foram então multiplicados pelo intervalo de amostragem (10 µs) para calcular a energia instantânea. A energia total foi obtida somando-se todos os valores resultantes.

3. RESULTADOS E DISCUSSÃO

Os resultados aqui apresentados foram descritos em Vaz, Mattos e Soares (2025). Inicialmente, os tempos de execução dos algoritmos foram medidos em ambas as plataformas. Para isso, foi utilizada a função *micros()* da IDE do Arduino de modo a registrar o tempo decorrido durante a execução das funções de encriptação. Cada algoritmo foi executado 100 vezes, em sequência, e então foi calculada a média do tempo. A entrada utilizada foi uma *string* gerada aleatoriamente do tamanho de um bloco (16 bytes). A Tabela 1 apresenta os resultados obtidos.

Tabela 1 - Tempos de Execução de Cada Algoritmo em Ambas Plataformas

Algoritmo	ESP32 (µs)	Raspberry Pi Pico (µs)
XTEA	32	28
ASCON	124	181
SLIM	157	152
AES-LWC	411	422
SHADOW	892	866
AES	1519	1802
PRESENT	2360	2306

Conforme a Tabela 1, os algoritmos AES, AES-LWC e ASCON apresentam tempos de execução ligeiramente inferiores na ESP32, enquanto os algoritmos PRESENT, SHADOW, SLIM e XTEA têm desempenho superior na Raspberry Pi Pico — embora, na maior parte dos casos, as diferenças sejam pequenas (com picos de até 283 µs no AES). Notavelmente, o PRESENT, mesmo sendo um algoritmo projetado para ser LWC, é mais lento que o AES em software devido às suas permutações bit-a-bit e às 31 rodadas, o que também resulta em maior consumo de energia, prejudicando aplicações IoT.

Já em termos de consumo de memória, a IDE do Arduino foi utilizada para verificar os *sketchs*, a qual exibe ao final da verificação o consumo de memória de programa (espaço para o código-fonte) e de memória dinâmica (utilizada para variáveis durante a execução). Estes dados são referentes apenas a parte de encriptação dos algoritmos e estão sendo apresentados na Figura 1.

Como mostra a Figura 1, o XTEA é o algoritmo que consome menos memória, enquanto o ASCON, que foi desenvolvido para ser um LWC, apresenta o maior uso de memória de programa, superando até o AES. Isso se deve à sua estrutura esponja com estado interno de 320 bits e funções de permutação complexas, o que pode torná-lo inadequado para dispositivos IoT com fortes restrições de memória.

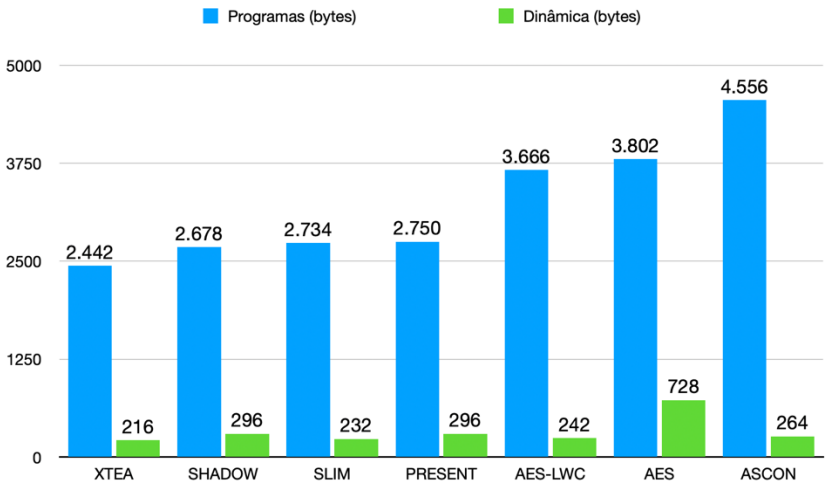

Figura 1 - Consumo de Memória de Programas e Dinâmica de Cada Algoritmo

Os valores totais de energia dissipada são apresentados no gráfico da Figura 2, calculados a partir das amostras de corrente elétrica coletadas com a PPK2.

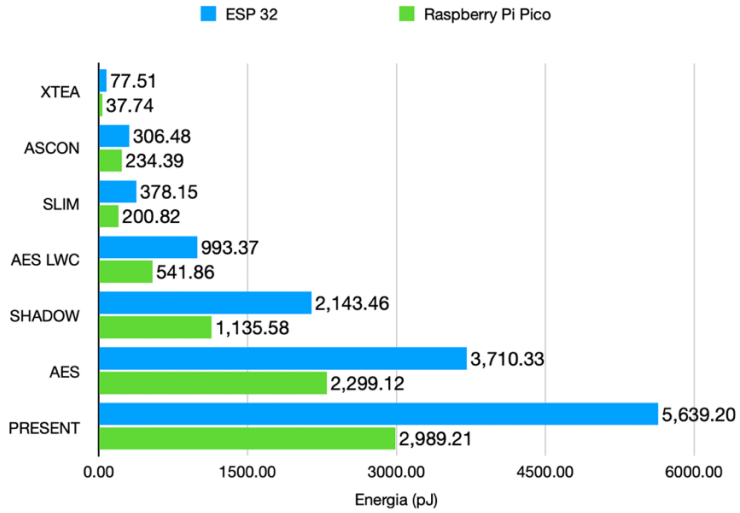

Figura 2 - Energia Total Consumida (em picojoules) por Cada Algoritmo Criptográfico em Ambas Plataformas

O gráfico da Figura 2 mostra que a dissipação total de energia está fortemente relacionada ao tempo de execução. Comparando com a Tabela 1, nota-se que os algoritmos AES, AES-LWC e ASCON foram mais rápidos na ESP32, enquanto os algoritmos PRESENT, SHADOW, SLIM e XTEA tiveram melhor desempenho na Raspberry Pi Pico. Ainda assim, todos os algoritmos consumiram menos energia na Raspberry Pi Pico, com variações distintas: o ASCON gastou 23,52 % a mais no ESP32, enquanto o XTEA teve um aumento de 51,31 %.

Já em termos de segurança, os algoritmos foram submetidos a três diferentes testes: efeito avalanche, balanceamento de bits e NIST.

A Figura 3 apresenta os valores de efeito avalanche e o balanceamento de bits obtidos. Como é possível verificar, os algoritmos apresentaram uma distribuição muito semelhante de 0's e 1's em seus *ciphertexts*. No entanto, em relação ao efeito avalanche, ASCON e SLIM exibiram valores significativamente abaixo de 50%, com médias observadas de aproximadamente 12% e 20%, respectivamente.

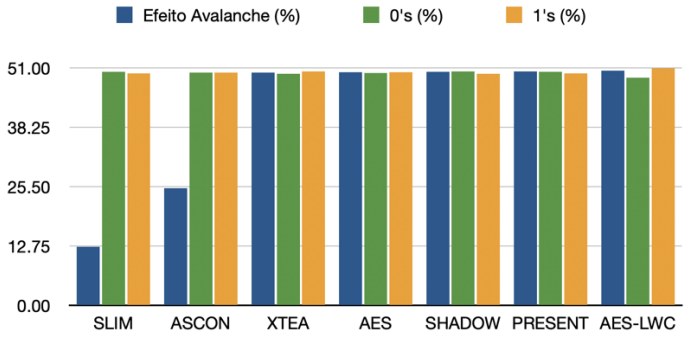

Figura 3 - Valores de Efeito Avalanche e Distribuição de 0s e 1s no Ciphertext

4. CONCLUSÕES

Este trabalho apresentou uma análise comparativa abrangente de sete algoritmos criptográficos, incorporando métricas de desempenho, consumo energético e segurança, realizando os testes em duas plataformas amplamente utilizadas. A principal contribuição é a proposta de uma abordagem multimétrica que, além de avaliar eficiência e consumo energético, inclui testes estatísticos e critérios de segurança. A inclusão de algoritmos pouco explorados em estudos comparativos, como SLIM, SHADOW e AES-LWC, reforça a originalidade da análise, ampliando o repertório de alternativas viáveis para aplicações em dispositivos com restrições computacionais.

5. REFERÊNCIAS BIBLIOGRÁFICAS

IBM. **What is the Internet of Things (IoT)?**. IBM Webpage, 12 mai. 2023. Acessado em 05 ago. 2025. Online. Disponível em: https://www.ibm.com/think/topics/internet-of-things

SINHA, S. **State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally.** IoT Analytics, 03 set. 2024. Acessado em 05 ago. 2025. Online. Disponível em: https://iot-analytics.com/number-connected-iot-devices/

KADHIM, F. A.; ABDUL-MAJEED, G. H.; ALI, R. S. Enhancement CAST block algorithm to encrypt big data. *In:* **2017 ANNUAL CONFERENCE ON NEW TRENDS IN INFORMATION & COMMUNICATIONS TECHNOLOGY APPLICATIONS (NTICT)**, Bagdah, Iraque, 2017

ORANGE. **Lightweight cryptography for strong security of the Internet of Things**. Hello Future Homepage, 06 dez. 2022. Acessado em 05 ago. 2025. Online. Disponível em: https://hellofuture.orange.com/en/lightweight-cryptography-for-strong-security-of-the-internet-of-things/

VAZ, Y. S.; MATTOS, J. C. B.; SOARES, R. I. Improving an Ultra Lightweight AES for IoT Applications. *In:* **2023 IEEE 9th WORLD FORUM ON INTERNET OF THINGS (WF-IoT),** Aveiro, 2023.

VAZ, Y. S.; MATTOS, J. C. B.; SOARES, R. I. Lightweight Cryptography for the Internet of Things: A Multi-Metric Experimental Assessment. *In:* **2025 Brazilian Symposium on Computing Systems Engineeting (SBESC),** Campinas, 2025 (enviado para avaliação).