ANÁLISE E COMPARAÇÃO DE UMA VERSÃO LEVE DO ALGORITMO CRIPTOGRÁFICO AES EM DIFERENTES FAMÍLIAS DE FPGAs

FILIPE RUTZ DOS SANTOS[1]; YURI SILVA VAZ[2]; RAFAEL IANKOWSKI SOARES[3]; JÚLIO C. B. MATTOS[4]

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

1. INTRODUÇÃO

A segurança de dados é um pilar fundamental para o funcionamento de sistemas de informação, garantindo a confidencialidade e a integridade em um mundo cada vez mais conectado (ADMASS; MUNAYE; DIRO, 2024). A transmissão de dados através da Internet representa um desafio constante que demanda proteção eficiente. Para atender essa demanda, a criptografia se estabelece como mecanismo mais eficaz, embora a sua implementação em hardware exija recursos computacionais que impactam métricas como tempo de processamento, consumo de área e *throughput* (KADHIM; ABDUL-MAJEED; ALI, 2017).

Dentre as soluções existentes, o *Advanced Encryption Standard* (AES) se destaca como um proeminente algoritmo de chave simétrica, extensivamente testado, validado e selecionado como padrão pelo NIST (VAZ; MATTOS; SOARES, 2025). Apesar de sua robustez, a implementação em hardware do AES tradicionalmente enfrenta um dilema entre a busca por uma taxa alta de transferência (*throughput*) e a necessidade de um menor consumo de área (CHENG; SU; CHAO, 2024).

A busca pelo equilíbrio entre esses dois fatores é atualmente um campo ativo de pesquisa (CHENG; SU; CHAO, 2024). Com muitos trabalhos utilizando o AES como base para otimizações, o desafio de aprimorar essa relação continua a ser um foco central na área de criptografia em hardware. Este trabalho realiza uma avaliação da arquitetura proposta por (VAZ; MATTOS; SOARES, 2025), que apresenta uma solução para este problema ao otimizar a etapa *SubBytes* do AES. A proposta, denominada aqui de *Lightweight AES* (AES-LWC), emprega uma s-box reduzida de apenas 16 elementos.

Considerando a premissa de que tal modificação arquitetural pode oferecer uma eficiência superior, o objetivo do presente estudo é, portanto, analisar o desempenho desta implementação leve em uma nova gama de plataformas de hardware, especificamente nos FPGAs das famílias Artix-7, Kintex-7 e Zynq-7000 da Xilinx, a fim de realizar uma comparação fiel com os demais trabalhos da literatura. Adicionalmente, busca-se comparar os resultados dessa implementação com os resultados dos autores Cheng, Su e Chao (2024), Diehl *et al.* (2017), Gao (2024) e Abulibdeh et al. (2023), os quais também propuseram otimizações no algoritmo AES. A análise consiste em avaliar as métricas de frequência máxima, consumo de área e, como métrica final de interesse, o *throughput*-por-área, que é a métrica utilizada para comparar as diferentes propostas entre os autores.

2. METODOLOGIA

A metodologia desse estudo foi delineada para avaliar o desempenho de uma arquitetura leve do algoritmo AES pré-existente em um novo conjunto de famílias de FPGAs. Para a nova análise, objeto deste artigo, o código-fonte em VHDL do algoritmo foi submetido ao fluxo de projeto da suíte Xilinx Vivado, versão 2018.2.

A avaliação de desempenho foi conduzida em três famílias de FPGA distintas, representando diferentes segmentos da família Xilinx, sendo elas: Artix-7 AC701, Kintex-7 KC705 e Zynq-7000. Para cada um desses alvos, o mesmo procedimento experimental foi rigorosamente aplicado.

O procedimento consistiu em extrair a frequência máxima de operação diretamente do relatório de análise de temporização gerado pela ferramenta de software. Para isso, um arquivo de restrições de projeto (XDC - *Xilinx Design Constraints*) foi utilizado para especificar o período de clock alvo. O processo foi iniciado com um período conservador de 5 nanossegundos (ns), equivalente a uma frequência de 200 MHz. A cada iteração bem-sucedida, o projeto era submetido ao fluxo completo de síntese e implementação do Vivado.

Após cada implementação, o relatório de análise estática de temporização era inspecionado. Se o projeto atendesse a todas as restrições de temporização (sem *timing violations*), o período no arquivo de restrições era sucessivamente decrementado em pequenos passos, e o processo era repetido. A iteração era interrompida no momento em que a implementação registrava falha em atender aos requisitos. O menor período de clock para o qual o projeto foi implementado era determinado, consequentemente registrado como período mínimo. Ao navegar no software capturamos a frequência de operação nesse estado desejado, além de dados de consumo de área.

3. RESULTADOS E DISCUSSÃO

Os resultados da avaliação de desempenho, consolidados na Tabela 1, demonstram a superioridade da arquitetura do AES-LWC em todas as plataformas testadas. A análise de frequência máxima evidencia um salto expressivo de performance: no dispositivo Kintex-7, o algoritmo alcançou 569,47 MHz, um valor 3,4 vezes superior à implementação de Cheng, Su e Chao (2024) e mais de 61 vezes maior que o de Diehl *et. al.* (2017) no mesmo dispositivo. Essa tendência de alta performance se manteve nos FPGAs Artix-7 e Zynq-7000, superando com vasta margem as implementações dos autores Gao (2024) e Abulibdeh *et. al.* (2023), comprovando a portabilidade e escalabilidade da otimização em diferentes tecnologias de hardware.

Também na Tabela 1, a análise de *Throughput* por Área (Mbps/LE) demonstra a magnitude da eficiência obtida. O resultado do AES-LWC de 8,04 Mbps/LE na Kintex-7 é mais de 21 vezes superior aos valores reportados por Cheng, Su e Chao (2024) e Diehl *et. al.* (2017) (0,37 Mbps/LE). De forma similar, a eficiência na Artix-7 (5,61 Mbps/LE) foi quase 5 vezes maior que a de Abulibdeh *et. al.* (2023), enquanto na Zynq-7000 (7,58 Mbps/LE) o ganho foi 3,1 vezes superior ao de Gao (2024). Esses números indicam que, para cada unidade de lógica gasta, o AES-LWC entrega uma capacidade de processamento drasticamente maior que as abordagens comparadas.

Acerca da utilização de área, detalhada na Tabela 2, a arquitetura AES-LWC também demonstra uma notável eficiência, apresentando um design significativamente mais compacto que a maioria das propostas comparadas. Na plataforma Kintex-7, o AES-LWC utilizou 907 Elementos Lógicos (LEs), uma economia de 32% em comparação com Cheng, Su e Chao (2024), enquanto na Zynq-7000, a implementação (953 LEs) se mostrou aproximadamente 31% mais econômica em área que a de Gao (2024). A discrepância é ainda maior na Artix-7, onde o AES-LWC (831 LEs) é aproximadamente 15 vezes mais compacto do que a proposta de Abulibdeh *et. al.* (2023). Este baixo e consistente consumo de recursos entre as diferentes tecnologias de FPGAs reforça o caráter leve (*lightweight*) da implementação, sendo um fator fundamental na métrica de *throughput* por área. Por fim, a proposta de Diehl *et. al.* (2017) apresentou o menor consumo de área, utilizando apenas 318 LEs, porém, em termos de *throughput* por área, o AES-LWC segue liderando com a maior vazão de dados por área consumida.

Tabela 1: Comparativo dos resultados de Frequência Máxima e *Throughput* por Área

Artigo	Frequência Máxima (MHz)			Throughput por Área (Mbps/LE)		
	DISPOSITIVOS TESTADOS			DISPOSITIVOS TESTADOS		
	Artix-7	Kintex-7	Zynq-7000	Artix-7	Kintex-7	Zynq-7000
(VAZ; MATTOS; SOARES, 2025)	364,29	569,47	564,65	5,61	8,04	7,58
(CHENG; SU; CHAO, 2024)	-	166,49	-	-	0,37	-
(DIEHL *et. al.*, 2017)	-	9,30	-	-	0,37	-
(GAO, 2024)	-	-	260,00	-	-	2,41
(ABULIBDEH *et. al.*, 2023)	12,50	-	-	1,13	-	-

Tabela 2: Comparativo dos resultados de consumo de Área

Artigo	Área (LE)		
	DISPOSITIVOS TESTADOS		
	Artix-7	Kintex-7	ZYNQ-7000
(VAZ; MATTOS; SOARES, 2025)	831	907	953
(CHENG; SU; CHAO, 2024)	-	1335	-
(DIEHL *et. al.*, 2017)	-	318	-
(GAO, 2024)	-	-	1379
(ABULIBDEH *et. al.*, 2023)	12580	-	-

4. CONCLUSÕES

Este trabalho validou com sucesso o desempenho e a portabilidade da arquitetura do AES leve (AES-LWC) em múltiplas plataformas FPGAs. Os resultados comprovaram que a otimização baseada em s-box reduzida permite que a implementação alcance frequências de operação e uma eficiência de *throughput* por área significativamente superiores às de implementações de referência na literatura.

A principal contribuição do estudo foi apresentar uma análise comparativa fiel, que, ao sintetizar a arquitetura para as mesmas plataformas de hardware utilizadas em trabalhos de referência, permitiu demonstrar de forma inequívoca a robustez e a eficácia da simplificação arquitetural. A otimização sinérgica de área e velocidade posiciona o AES-LWC como uma solução de hardware altamente competitiva para sistemas que demandam criptografia de alta velocidade com baixo consumo de recursos, abrindo caminho para futuras investigações sobre o consumo de potência e robustez contra ataques de canal lateral.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ADMASS, W. S.; MUNAYE, Y. Y.; DIRO, A. A. Cyber security: state of the art, challenges and future directions. **Cyber Security and Applications**, v. 2, 2024.

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

VAZ, Y. S.; MATTOS, J. C. B.; SOARES, R. I. High throughput-to-area AES: the role of small S-box in lightweight cryptographic design. In: **IEEE LATIN AMERICA SYMPOSIUM ON CIRCUITS AND SYSTEMS (LASCAS)**, Bento Gonçalves, 2025.

CHENG, P.-Y.; SU, Y.-C.; CHAO, P. C.-P. Novel high throughput-to-area efficiency and strong-resilience datapath of AES for lightweight implementation in IoT devices. **IEEE Internet of Things Journal**, v. 11, n. 10, p. 17678–17687, maio 2024.

DIEHL, W.; FARAHMAND, F.; YALLA, P.; KAPS, J.-P.; GAJ, K. Comparison of hardware and software implementations of selected lightweight block ciphers. In: **INTERNATIONAL CONFERENCE ON FIELD PROGRAMMABLE LOGIC AND APPLICATIONS (FPL)**, 27., 2017

GAO, R. FPGA implementation of AES algorithm for CAN FD. In: **INTERNATIONAL CONFERENCE ON ELECTRONICS, CIRCUITS AND INFORMATION ENGINEERING (ECIE)**, Hangzhou, 2024.

ABULIBDEH, E.; SALEH, H.; MOHAMMAD, B.; ALQUTAYRI, M. Computational-based advanced encryption standard (AES) accelerator. In: **INTERNATIONAL CONFERENCE ON MICROELECTRONICS (ICM)**, Abu Dhabi, 2023.