IMPLEMENTAÇÃO FPGA DE UM MAPA CAÓTICO DE ESPAÇO DISCRETO

JOÃO INÁCIO MOREIRA BEZERRA[1]; ALEXANDRE MOLTER;[2]
VINÍCIUS VALDUGA DE ALMEIDA CAMARGO[2]
RAFAEL IANKOWSKI SOARES[2]
[1]*Universidade Federal de Pelotas – jimbezerra@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – alexandre.molter@ufpel.com.br*
[2]*Universidade Federal de Pelotas – vvacamargo@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br*

1. INTRODUÇÃO

Em decorrência dos avanços tecnológicos, o uso de dispositivos de Internet das Coisas (IoT) vem crescendo de forma exponencial, com aplicações no setor de compras, jogos e aplicações militares (SHAFIQUE, 2020). Como estes dispositivos estão conectados à Internet, um canal público não seguro, os dados transmitidos por estes dispositivos estão passíveis de ataques por partes não autorizadas. Isto aumenta significativamente a importância da criptografia, que é a definida como a ciência que estuda técnicas de proteção destes arquivos.

O processo responsável por proteger dados de ataques por partes não autorizadas é denominado cifragem. Em um dispositivo IoT, o bloco responsável pela cifragem dos dados corresponde a uma fração de uma aplicação, de forma que seu custo em termos de área e também de consumo de potência não pode ser excedente. Levando em conta que imagens correspondem a 70% dos arquivos transmitidos pelos dispositivos IoT(ARAB, 2019), o bloco responsável pela cifragem dos arquivos em um dispositivo IoT deve ser otimizado para a cifragem de imagens, enquanto o AES (*Advanced Encryption Standard*), que é o algoritmo de criptografia simétrica mais utilizado é otimizado para a cifragem de textos (CHAI et al., 2019), arquivos dos quais as imagens destoam pelas seguintes razões.

- alta correlação entre *pixels* adjacentes;
- alto consumo de potência;
- tamanho dos arquivos.

A Teoria do Caos apresenta propriedades semelhantes à criptografia, tais quais à sensibilidade às condições iniciais, ergodicidade, dinâmicas determinísticas e a possibilidade de obtenção de comportamento matemático complexo com implementações de baixo custo computacional, e em virtude disso, atrai atenção significativa por parte de pesquisadores (CHAI et al., 2019; TEH, 2019; LAMBIC, 2020). Contudo, os mapas ou sistemas caóticos usados para propor cifradores são definidos em um espaço contínuo, trabalhando com valores decimais, o que requer o uso da arquitetura de ponto flutuante, que possui um alto custo computacional se comparada à arquitetura de ponto fixo. Outros dois problemas relativos ao trabalho com sistemas caóticos no espaço contínuo são o efeito transiente e a degradação dinâmica. O efeito transiente significa dois mapas caóticos com condições inicialmente próximas precisam de aproximadamente 100 iterações para começarem a divergir, o que aumenta o consumo de tempo da aplicação. A degradação dinâmica, por sua vez, decorre do fato que as máquinas nas quais os sistemas são implementados possuem arquitetura discreta, requerendo que os sistemas caóticos definidos no espaço contínuo sejam transformados em valores discretos. Como essa transformação é aproximada, em um alto número de iterações que é requerido para cifrar uma

imagem, as dinâmicas caóticas do sistema são enfraquecidas, e assim transformações são necessárias para lidar com este problema, o que aumentam os custos de área e de potência da aplicação (MOREIRA BEZERRA, 2023).

Se o mapa caótico for implementado no espaço discreto, nem o efeito transiente nem a degradação dinâmica se fazem presentes. Em virtude disso, este trabalho apresenta os resultados da implementação de um mapa caótico de espaço discreto em *Field-Programmable Gate Array* (FPGA), mostrando que o mapa de espaço discreto pode ser operado a uma frequência máxima maior, ocupando menor área e consumindo menos potência que sistemas caóticos de espaço contínuo.

2. METODOLOGIA

A definição do mapa de tempo discreto, considerando a implementação de 32 *bits,* foi proposta por Lambic(2020) e é dada pela Equação (1) que segue.

$$f(x_n) = x_{n+1} = (z << (z\%32))|(z >> (32 - z\%32)), \qquad (1)$$

$$z = (2^{-16}x_n + 1) \times (x_n\%2^{16} + 1) + 1.$$

Nesta definição, x_n é a variável do sistema, e não há variável de controle. Embora com a ausência do parâmetro de controle, um estudo por exaustão das condições iniciais mostrou que o mapa não apresenta pontos fixos, assim apresentando comportamento caótico independente da condição inicial.

A tecnologia escolhida para a implementação do mapa caótico é um FPGA, que é um dispositivo bastante usado na literatura em virtude de sua reprogramabilidade e custos inferiores aos Circuitos Integrados de Aplicações Específicas (ASIC). A implementação de *32 bits* do mapa é realizada em virtude de ser a quantidade de *bits* para qual o bloco Multiplica-Acumula do FPGA modelo Cyclone X 10CX105YF672E5G consegue operar em uma maior frequência máxima. Buscando reduzir o consumo de potência, o mapa caótico também foi implementado no FPGA *low-power* Spartan 7 xc7s75fgga676-1Q.

3. RESULTADOS E DISCUSSÃO

Na Tabela 1 que segue, o mapa caótico de espaço discreto definido pela Equação (1) tem sua implementação em FPGA comparada com outros sistemas caóticos, definidos em espaço contínuo, na literatura considerando os seguintes fatores:

- Área *(look-up tables* e registradores);
- Frequência máxima.
- Consumo de potência.

Trabalho	Dispositivo	*Look-up tables*	Registradores	Frequência máxima (MHz)
Este	Cyclone X	166	192	474
Este	Spartan 7	200	233	250
Caplingis(2021)	Cyclone V	785	633	76

Tuna(2019)	Virtex 6	1924	2243	463
Hagras (2020)	Spartan 6	294	948	393

Tabela 1: Comparação de área e de frequência máxima da implementação FPGA do mapa caótico de espaço discreto com sistemas caóticos de espaço contínuo.

Os trabalhos acima foram escolhidos pelas seguintes razões:

- Caplingis (2022): semelhança de dispositivo FPGA.
- Tuna (2019): maior frequência máxima encontrada na literatura.
- Hagras (2020): menor área e menor consumo de potência encontrados na literatura.

A Tabela mostra que o uso do mapa caótico definido no espaço discreto reduz significativamente a área ocupada pelo mapa caótico se comparada à implementação dos sistemas caóticos de espaço contínuo. Isso se dá em virtude do mapa de espaço discreto não necessitar lidar com degradação dinâmica, efeito transiente, nem com a necessidade de usos de métodos numéricos como o Runge-Kutta de quarta ordem para obter a solução numérica. Outra vantagem do uso do mapa caótico de espaço discreto é a baixa latência, sendo que apenas seis ciclos de relógio são necessários para gerar um novo valor caótico, quantidade que é aproximadamente um sexto da necessária em Tuna(2019), que é de 47. Dessa forma, embora a frequência máxima de operação de ambos os sistemas seja aproximada, o nosso trabalho consegue gerar valores caóticos seis vezes mais rápido. O gargalo da arquitetura do mapa caótico é dado pela multiplicação entre inteiros, que limita a frequência máxima de operação da arquitetura à 474 MHz no FPGA Cyclone X. O FPGA Spartan 6 não possui um bloco interno específico para a operação de multiplicação, assim diminuindo a frequência máxima que a implementação do mapa pode alcançar.

O consumo de potência da implementação do mapa caótico é de 63 *milliwatts* (mW) na Cyclone X e de 10 mW na Spartan 7. A menor métrica encontrada na literatura para sistemas no espaço contínuo foi de 117 mW em Hagras (2020), de forma que o uso da arquitetura de espaço discreto reduz o consumo de potência em 46% no FPGA Cyclone X e em 91% no FPGA Spartan 7. Nesse contexto, se o objetivo de uma aplicação for o baixo consumo de potência, o FPGA Spartan 7 deve ser usado, assim como se o objetivo for um desempenho superior com consumo de potência sob controle, o FPGA Cyclone X deve ser utilizado.

Consequentemente à redução de área e do consumo de potência no bloco de geração das sequências caóticas, a área ocupada pelo bloco correspondente ao cifrador na aplicação também é reduzida, assim como o consumo de potência. O consumo baixo de potência tanto no FPGA Cyclone X como no FPGA Spartan 7 mostra que o baixo custo e o alto desempenho do mapa caótico de espaço discreto é independente do dispositivo.

4. CONCLUSÕES

Neste trabalho, a implementação FPGA de um mapa caótico de espaço discreto foi discutida, mostrando que o uso da arquitetura no espaço discreto reduz a área ocupada pelo mapa, além do consumo de potência, enquanto uma frequência máxima superior aos sistemas caóticos de espaço contínuo é obtida.

Essas métricas foram observadas em dois FPGAs de fabricantes diferentes, verificando que os resultados são independentes do dispositivo, e o uso de mapas caóticos de espaço discreto pode preencher a lacuna presente na literatura com caos, que são os altos custos associados à arquiteturas de ponto flutuante.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ARAB, Alireza; ROSTAMI, Mohammad Javad; GHAVAMI, Behnam. An image encryption method based on chaos system and AES algorithm. **The Journal of Supercomputing**, v. 75, p. 6663-6682, 2019.

CAPLIGINS, Filips et al. FPGA Implementation and study of synchronization of modified Chua's circuit-based chaotic oscillator for high-speed secure communications. In: **2020 IEEE 8th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)**. IEEE, 2021. p. 1-6.

CHAI, Xiuli; FU, Xianglong; GAN, Zhihua; LU, Yang; CHEN, Yiran. A color image cryptosystem based on dynamic DNA encryption and chaos. **Signal Processing**, v. 155, p. 44-62, 2019.

HAGRAS, Esam AA; SABER, Mohamed. Low power and high-speed FPGA implementation for 4D memristor chaotic system for image encryption. **Multimedia Tools and Applications**, v. 79, n. 31-32, p. 23203-23222, 2020.

LAMBIĆ, Dragan. A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. **Nonlinear Dynamics**, v. 100, n. 1, p. 699-711, 2020.

BEZERRA, João Inácio Moreira et al. A novel simultaneous permutation–diffusion image encryption scheme based on a discrete space map. **Chaos, Solitons & Fractals,** v. 168, p. 113160, 2023.

PREISHUBER, Mario et al. Depreciating motivation and empirical security analysis of chaos-based image and video encryption. **IEEE Transactions on Information Forensics and Security**, v. 13, n. 9, p. 2137-2150, 2018.

SHAFIQUE, Kinza et al. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. **Ieee Access**, v. 8, p. 23022-23040, 2020.

TUNA, Murat et al. High speed FPGA-based chaotic oscillator design. **Microprocessors and Microsystems**, v. 66, p. 72-80, 2019.