ARQUITETURAS APROXIMADAS DE NTT/INTT POR MEIO DE UM PROJETO ORIENTADO PELO FALSAX

RODRIGO LOPES[1]; LEONARDO ANTONIETTI[2]; MORGANA DA ROSA[3]; EDUARDO DA COSTA[4]; RAFAEL SOARES[5]

[1,2,5]Universidade Federal de Pelotas – rmdlopes@inf.ufpel.edu.br; leonardo.antonietti@inf.ufpel.edu.br; rafael.soares@inf.ufpel.edu.br.
[3,4]Universidade Católica de Pelotas - morganamacedoazevedodarosa@gmail.com; ecosta.dacosta@gmail.com.

1. INTRODUÇÃO

A *Number Theoretical Transform* (NTT) e sua inversa (INTT) surgiram como ferramentas matemáticas indispensáveis para a aceleração da multiplicação polinomial em sistemas de criptografia *lattice-based*, particularmente no contexto da criptografia pós-quântica e em aplicações de criptografia de imagens. No entanto, apesar de sua eficiência algorítmica, as implementações em hardware da NTT e da INTT são frequentemente limitadas por suas elevadas demandas de energia e pelas características de área em silício, fatores críticos para ambientes com recursos restritos, como sistemas de IoT e sistemas embarcados. Para lidar com essa limitação, diversos estudos têm explorado o uso de arquiteturas de geometria constante (Barros, 2025) e de técnicas de multiplicadores de entrada única para simplificar a arquitetura da NTT e INTT, juntamente com a integração de padrões otimizados de acesso à memória para garantir uma execução livre de conflitos (Liu, 2024).
Avanços mais recentes têm se concentrado em aprimorar a eficiência energética por meio de estratégias de computação aproximada, em especial pela adoção de unidades aritméticas aproximadas nas arquiteturas de NTT/INTT. Quando utilizados de forma criteriosa, os somadores aproximados oferecem reduções significativas no consumo de energia e de área ao relaxar a exigência de exatidão no cálculo, em aplicações tolerantes a erros, como no processamento de imagens (da Rosa, 2022).

2. METODOLOGIA

Os projetos tradicionais de NTT/INTT empregam unidades aritméticas precisas que, embora garantam a exatidão numérica, resultam em maior consumo de energia e área em silício, uma limitação crítica em cenários embarcados e restritos em energia. Por isto, foi proposta a exploração de 16 arquiteturas de somadores aproximados já consolidadas no fluxo computacional da NTT e da INTT a fim de superar essas limitações. Esses somadores, implementados no nível *butterfly* das etapas da transformada, substituem as operações exatas de adição nos segmentos menos significantes do caminho de dados. Cada uma das 16 arquiteturas de somadores aproximados, que variam desde estratégias de baixa complexidade, como truncamento e *COPY*, até esquemas logicamente intensivos, como HOERAA, MHEAA e AxPPA. Esta avaliação foi feita via FALSAx, o qual fornece modelagem sistemática de acurácia e custo em hardware utilizando aprendizado de máquina supervisionado. O FALSAx possibilita a estimativa de métricas de energia, área e acurácia com base em parâmetros de projeto (por exemplo, largura de palavra W, nível de aproximação K) e correlaciona esses resultados com métricas de qualidade específicas da aplicação, tais como correlação cruzada

normalizada (NC), índice de similaridade estrutural (SSIM) e erro quadrático médio (MSE).

O fluxo de implementação integra os somadores aproximados dentro da arquitetura *butterfly* da NTT/INTT de 8 pontos. Os *twiddle factors* foram preservados em sua forma aproximada (por exemplo, $W_8^0 = W_8^1 = W_8^2 = W_8^3 = 1$), e os somadores aproximados foram seletivamente introduzidos em posições demonstradas como capazes de proporcionar compromissos significativos sem degradar de forma relevante a qualidade da reconstrução. Essa abordagem complementa avanços recentes em redução modular por meio da técnica AxRLL-16, que combina um detector de primeiro '1' (*Leading-One Detector – LOD*) e um codificador radix-16 para aproximação logarítmica rápida, reduzindo a sobrecarga computacional das unidades aritméticas modulares. Além disso, nosso arranjo experimental adota o esquema NTT de geometria constante a fim de manter um padrão de acesso à memória livre de conflitos e um fluxo computacional consistente em todas as etapas. Isso possibilita a integração dos somadores aproximados de maneira transparente, sem introduzir contenção de memória ou paralisações no pipeline, o que é essencial para garantir baixo consumo de área e energia.

3. RESULTADOS E DISCUSSÃO

As Figuras 1 e 2 abaixo ilustram o comportamento de quatro métricas-chave de qualidade e precisão em diferentes níveis de aproximação: correlação cruzada normalizada (NCC), erro quadrático médio (RMSE), erro absoluto médio (MAE) e taxa de erro de bits (BER). Esses resultados foram obtidos a partir de simulações dos processos de criptografia baseados em NTT e de descriptografia baseados em INTT, utilizando 100 imagens hospedeiras do banco de imagens público disponível em Kaggle (2022). Foi integrado cada configuração de somadores aproximados nas etapas da *butterfly* nos caminhos de dados da NTT e da INTT, comparando a precisão da imagem reconstruída com a implementação de referência (exata). No processo de criptografia (Figura 3), o NCC mantém-se consistentemente acima de 0,6968 para a maioria dos somadores aproximados até K = 2, com uma degradação gradual observada para TRUNC, COPY e LOA conforme o nível de aproximação aumenta. RMSE e MAE apresentam crescimento linear com K, indicando uma propagação controlada do erro. Notavelmente, AxPPA, HERLOA e M-HERLOA preservam a precisão de forma mais eficaz, com BER permanecendo abaixo de 100 para $K \leq 3$ na maioria dos casos.

Os resultados da descriptografia (Figura 4) seguem uma tendência semelhante, embora com degradação de precisão mais acentuada além de K = 6, especialmente para TRUNC e COPY. A métrica NCC apresenta uma queda brusca para alguns somadores aproximados em níveis elevados de aproximação, confirmando que a aproximação agressiva dos bits menos significativos afeta mais significativamente a reversibilidade do processo INTT. Ainda assim, AxPPA, HEAA e SETA mantêm uma precisão robusta mesmo para níveis moderados de aproximação, evidenciando sua adequação para tarefas seguras de reconstrução de imagens.

A Figura 3 ilustra os resultados de qualidade visual dos processos de criptografia e descriptografia utilizando as etapas NTT e INTT, respectivamente, para os 16 somadores em diferentes níveis de aproximação K = {1, 2, ..., 8}. Cada coluna representa um somador aproximado específico, enquanto cada linha exibe a saída visual para um dado valor de K. As visualizações fornecem uma análise qualitativa de como os níveis de aproximação afetam a ofuscação da criptografia e a fidelidade

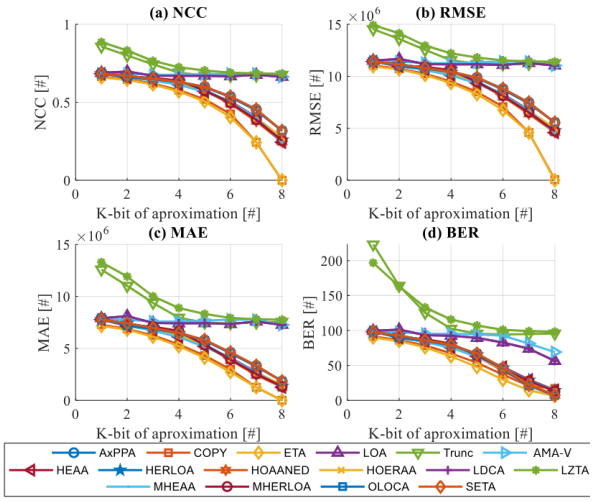

Fig. 1

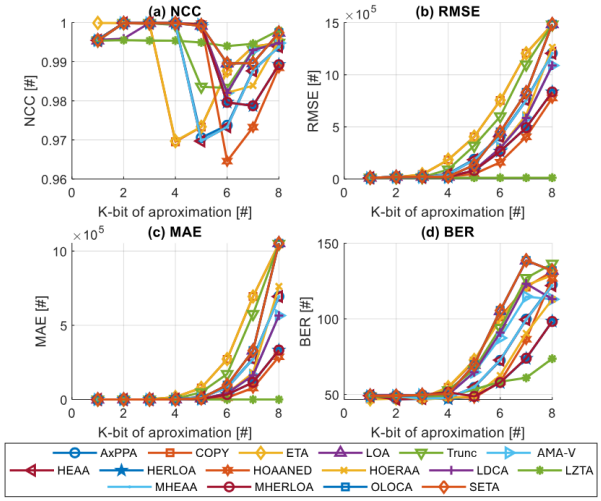

Fig. 2

da reconstrução da imagem. A Figura 3, que apresenta as imagens criptografadas produzidas pela etapa NTT, evidencia que a maioria dos somadores mantém um forte efeito de ofuscação visual até K = 4, destruindo efetivamente o conteúdo reconhecível da imagem. À medida que K ultrapassa esse limite, especialmente em arquiteturas mais simples como TRUNC e COPY, surgem artefatos, indicando aleatoriedade insuficiente na saída criptografada. Por outro lado, arquiteturas mais resilientes como AxPPA, HERLOA e M-HERLOA sustentam altos níveis de degradação visual mesmo em K = 7, reforçando sua eficácia em aplicações críticas para segurança, mostrando as imagens descriptografadas correspondentes, obtidas após a aplicação da INTT. Para níveis baixos de aproximação (K ≤ 4), a maioria dos somadores aproximados restaura com sucesso a imagem original com degradação perceptual mínima. Configurações como AxPPA, HEAA e MHERLOA preservam detalhes de bordas e contraste em todos os níveis de aproximação, inclusive em K = 5. No entanto, para valores mais altos de K (especialmente K = 7 e K = 8), distorções visíveis tornam-se mais pronunciadas em somadores como COPY, TRUNC e LZTA, levando a perdas estruturais severas ou corrupção completa da imagem reconstruída. Essas avaliações visuais confirmam as tendências observadas nas métricas quantitativas de precisão. Somadores como AxPPA e MHERLOA demonstram um equilíbrio favorável entre a agressividade da aproximação e a qualidade perceptual, possibilitando seu uso em sistemas de criptografia de imagens energeticamente eficientes, nos quais a fidelidade visual permanece prioritária. Em contraste, somadores mais simples podem ser limitados a configurações com valores mais baixos de K para evitar perdas inaceitáveis na precisão da descriptografia.

4. CONCLUSÕES

As arquiteturas aproximadas de NTT e INTT propostas, desenvolvidas para baixo consumo de energia e utilização compacta de área, demonstram resultados significativos em comparação com as arquiteturas exatas de última geração em que alcança um NCC de 0,5995 na arquitetura NTT. Por outro lado, a arquitetura INTT apresenta resultados ainda melhores, com projetos que atingem de forma semelhante à arquitetura NTT, mas alcançando um NCC de 0,99. Esses resultados evidenciam melhorias expressivas nas arquiteturas NTT/INTT, com degradação mínima ou imperceptível de precisão. Este trabalho representa um avanço notável

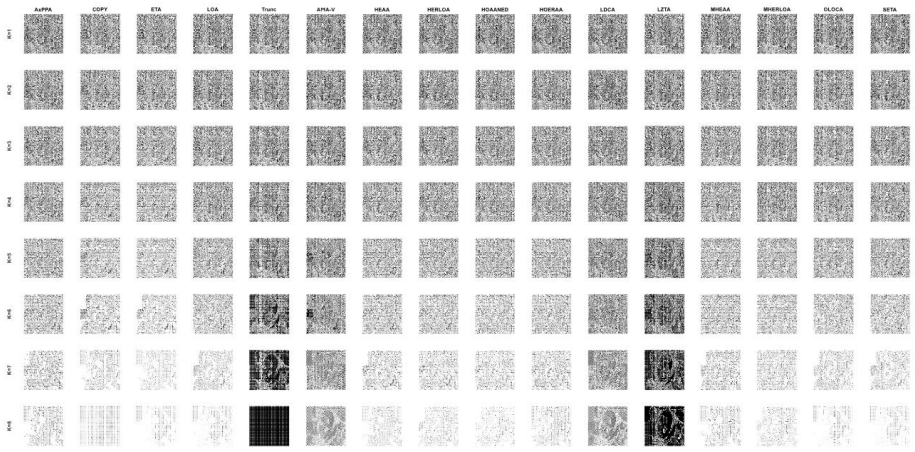

Fig.3

Fig.4

nos esquemas de aproximação explorados nas arquiteturas NTT/INTT, marcando um progresso no desmistificar do uso de técnicas aproximadas em projetos de segurança. Este trabalho como próximos passos vai implementar esta arquitetura em ferramentas de síntese e comparar com outras implementações da literatura para descobrir quanto de área e energia foi possível salvar.

5. REFERÊNCIAS BIBLIOGRÁFICAS

Kaggle, “256 x 256 iWildCam 2021 - Starter Notebook,” acessado em novembro de 2022. [Online]. Disponível em: https://www.kaggle.com/competitions/iwildcam2021-fgvc8

Barros, E. Low-Energy NTT and INTT Architectures for Image Encryption and Decryption, **ISCAS**, Londres, p.1-5, 2025

Da Rosa, M. AxPPA: Approximate parallel prefix adders, **IEEE Transactions on Very Large Scale Integration (VLSI) Systems**, vol. 31, n. 1, pp. 17–28, 2022.

Liu, S-H. An Area-Efficient, Conflict-Free, and Configurable Architecture for Accelerating NTT/INTT**, IEEE Transactions on Very Large Scale Integration (VLSI) Systems**, vol. 32, n. 3, pp. 519–531, 2024.