ID da Contribuição: **34** Tipos: **Trabalho consolidado ou em conclusão**

Implementação e análise do produto de polinômios baseados na Transformada de Teoria dos Números(NTT) em FPGA

sexta-feira, 5 de dezembro de 2025 14:34 (12 minutos)

A ascensão da computação quântica ameaça a infraestrutura de segurança da informação atual, tornando a migração para a Criptografia Pós-Quântica (PQC) uma necessidade urgente. Os principais algoritmos PQC padronizados até o momento são baseados em reticulados e dependem intensamente da multiplicação de polinômios de grande porte, sendo essa a operação de gargalo computacional. Nesse contexto, a implementação da Transformada de Teoria dos Números(NTT) é utilizada como ferramenta essencial para acelerar operações. Entretanto, implementações puramente em software dessa operação em CPUs de propósito geral sofrem com alta latência, limitando sua aplicação em ambiente de computação de alto-desempenho e em dispositivos computacionalmente limitados. Este trabalho apresenta o projeto, implementação e análise de um sistema hardware-software para a aceleração da NTT em FPGA. A arquitetura proposta divide-se entre uma aplicação em C, executada na CPU, e uma unidade de processamento NTT dedicada em hardware (FPGA). A comunicação entre os domínios é estabelecida via barramento PCI Express (PCIe), utilizando Acesso Direto à Memória (DMA) para a transferência de dados dos polinômios e E/S Programada (PIO) para o envio de comandos de controle (início/fim) do processamento dos dados. A comparação dos resultados experimentais com diferentes implementações em software valida a arquitetura como uma solução viável e de alto desempenho. Desta forma, o trabalho contribui para a viabilização de sistemas criptográficos seguros e eficientes para a era pós-quântica.

Autor: SILVA, Ronald

Co-autor: AMARAL HENRIQUES, Marco

Apresentador: SILVA, Ronald

Classificação da Sessão: Sessões orais