ID da Contribuição: **29** Tipos: **Trabalho consolidado ou em conclusão**

Aceleração de operações NTT em processadores RISC-V para criptografia pós-quântica

quinta-feira, 4 de dezembro de 2025 10:44 (12 minutos)

Este trabalho apresenta a extensão de um núcleo RISC-V com um conjunto de instruções dedicado à aritmética modular para acelerar operações NTT e sua inversa (INTT). Os resultados obtidos em uma implementação em FPGA apresentam aumento de desempenho em 2, 84, vezes para a NTT e em 3, 80 vezes para a INTT.

Autor: Sr. PEIXOTO ALVES, Pedro (Universidade Estadual de Campinas)

Co-autor: AMARAL HENRIQUES, Marco (Universidade Estadual de Campinas)

Apresentador: Sr. PEIXOTO ALVES, Pedro (Universidade Estadual de Campinas)

Classificação da Sessão: Sessões orais