# Projeto de Formatura – 2025

## PCS - Departamento de Engenharia de Computação e Sistemas Digitais

### Engenharia de Computação

Tema:

## Project Petalite: a proposal for a post-quantum Trusted Platform Module

## Contexto

É esperado que na próxima década, computadores quânticos consigam quebrar os esquemas criptográficos que são o alicerce de toda segurança computacional. Dessa forma, esquemas de **criptografia pós-quântica** vem sendo desenvolvidos para sanar esse problema. Uma das soluções mais relevantes é a suite CRYSTALS, que inclui o esquema de assinatura **Dilithium**.

Assim, criptoprocessadores como o **Trusted Platform Module (TPM)** vão precisar ser atualizados para incluir esses algoritmos. Tanto por motivos de latência, quanto de segurança, é vantajoso que esses algoritmos sejam **acelerados em hardware**.

## Objetivo e Metodologia

**Desenvolver um TPM que seja capaz de executar todas as operações do Dilithium, e que essas sejam aceleradas em hardware.** Isso requer:

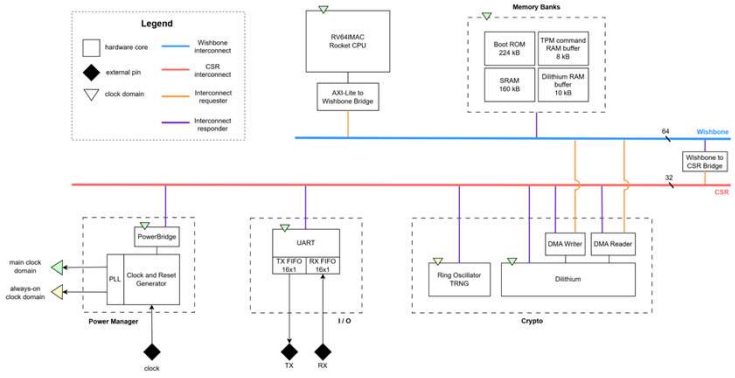
1. Validar um acelerador em hardware do algoritmo Dilithium, seja ele novo ou pré-existente.
2. Expandir a especificação oficial do TPM para contemplar esse algoritmo.
3. Implementar o TPM como um **SoC**, e integrar o acelerador do Dilithium a essa plataforma.
4. Desenvolver um firmware baremetal para ser excecutado na CPU do SoC, que realize todas as funcionalidades de um TPM.

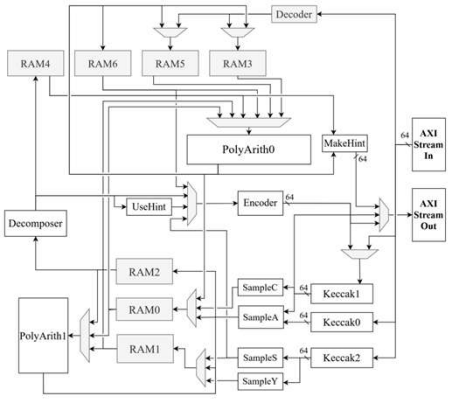
## Solução

**Novos comandos TPM** foram criados, e outros foram refatorados, para contemplarem a execução do Dilithium.

Um **SoC com uma CPU RISC-V** foi desenvolvido, e um **design RTL** pré-existente do Dilithium foi integrado a esse.

Implementação de referência do TPM foi revisada para executar como um **firmware baremetal**, com **drivers** para os cores do SoC, como uma **UART** para I/O, um **TRNG** baseado em **Ring Oscillators,** e o próprio **Dilithium**.




## Resultados

O TPM foi validado por uma suite de testes que usa os novos comandos desenvolvidos. **Todos os testes realizados foram bem-sucedidos.**

Além disso, comparado a um TPM que implementasse o Dilithium em software, obteve-se um **speedup de até 122 vezes** para esses comandos.

| Implementation | TPM 2.0 command sequence | | |
|---|---|---|---|
| | CreatePrimary | HashSign | HashVerify |
| Reference software | 14,738,219 | 107,385,854 | 11,891,749 |
| Hardware accelerated | 5,679,331 | 880,151 | 1,118,290 |
| Speedup (%) | **259.5%** | **12,200.8%** | **1,063.4%** |

## Conclusão e Contribuições

**Esse projeto atingiu todas as principais metas estabelecidas** ao início, criando assim um TPM completamente funcional, e ainda capaz de executar um inédito esquema de assinatura pós-quântico.

**A principal contribuição** desse projeto foi a demonstração técnica de como integrar algoritmos pós-quânticos à especificação do TPM; um tópico de pesquisa que a própria TCG está conduzindo no momento.

Uma segunda contribuição foi a utilização de aceleradores em hardware do Dilithium, que geralmente são desenvolvidos apenas como provas de conceito, em um projeto com aplicações no mundo real.

Contudo, há inúmeras melhorias que podem ser feitas ao projeto, seja incluindo aceleradores para outros esquemas (tradicionais ou pós-quânticos), ou usando um protocolo de I/O mais comum para um TPM (SPI, I2C).


Aluno: Francisco Cavalheiro Mariani

Professor Orientador: Prof. Dr. Bruno Albertini