Projeto de Formatura – 2025 – Press Release

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

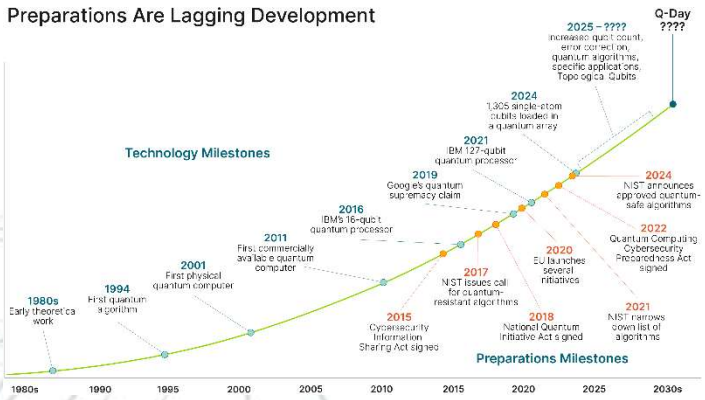
Tema:

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

Estudante da USP desenvolve processador para segurança contra ataques de computadores quânticos

São Paulo, 02 de Dezembro, 2025

Muito se fala dos perigos que a computação quântica pode trazer no futuro. Esse novo campo da computação, que se baseia em fenômenos físicos como a superposição e entrelaçamento quânticos, representa tanto um grande avanço tecnológico, mas também uma potencial ameaça para a privacidade das pessoas e a segurança dos países. O jornal Folha de São Paulo já reportou em 2023 que "A Casa Branca e o Departamento de Segurança Interna deixaram claro que, nas mãos erradas, um poderoso computador quântico poderia interromper desde comunicações seguras até os fundamentos de nosso sistema financeiro".



Na foto: cronologia da computação pós-quântica.

O problema fundamental se encontra na capacidade do um computador quântico de realizar algumas operações matemáticas de forma muito eficiente. Essas operações, como a fatoração de números primos, são fundamentais para os protocolos de segurança que protegem desde mensagens em aplicativos de celular, até dados bancários e segredos estatais. Como Marcelo Viana, Diretor-geral do Instituto de Matemática Pura e Aplicada (IMPA) no Rio de Janeiro afirmou em 2019, "quem dispuser de computadores quânticos poderá quebrar toda a criptografia atual".

Por enquanto, computadores quânticos são apenas experimentos científicos e não são estáveis o suficiente para serem uma ameaça real, mas especialistas estimam que isso pode mudar até 2030. Isso, por sua vez, disparou o campo da criptografia pós-quântica, que promove o desenvolvimento de novos protocolos resilientes contra ataques quânticos.

Nesse contexto, Francisco Mariani — um aluno da Escola Politécnica da Universidade de São Paulo (EP-USP) — desenvolveu um processador que incorpora um desses protocolos pós-quânticos. Esse tipo de processador, chamado Trusted Platform Module (TPM), já existe dentro da maioria dos desktops e laptops modernos, mas sua versão atual inclui apenas os protocolos de criptografia tradicional. O aluno modificou o TPM comum para adicionar um protocolo pós-quântico notório do momento, chamado Dilithium. Esse protocolo faz assinaturas digitais, e foi recentemente adotado pelo National Institute of Standards and Technology (NIST), uma organização governamental americana que oficializa padrões criptográficos. Além disso, essa nova versão do TPM implementa o Dilithium usando componentes físicos especializados, que aumentam tanto a velocidade do processador, quanto a proteção contra possíveis ataques.

O projeto é apenas um protótipo, mas aponta para um tópico de pesquisa em voga, que investiga como esses novos protocolos podem ser integrados de forma eficiente a sistemas computacionais que já existem. O Trusted Computing Group (TCG), que detém o padrão oficial do TPM, afirmou em Agosto que estão "trabalhando para atualizar nossas especificações em preparo para a era pós-quântica". Espera-se, com sorte, que iniciativas como esse projeto se tornem mais difundidas, antes que um computador quântico poderoso o suficiente mostre a razão para elas existirem.

Aluno: Francisco Cavalheiro Mariani

Professor Orientador: Prof. Dr. Bruno Albertini