ID da Contribuição: **31** Tipos: **Trabalho em estágio inicial**

Estudo sobre aplicação de protocolos de criptografia híbridos (pré e pós-quânticos) em ambientes restritos

sexta-feira, 5 de dezembro de 2025 16:03 (1 minuto)

Com o avanço no desenvolvimento de computadores quânticos, surge uma grande preocupação a respeito de algoritmos quânticos que potencialmente quebrarão os esquemas criptográficos atuais.
Em virtude disso, foram urgentemente desenvolvidos algoritmos criptográficos para serem teoricamente seguros contra ataques utilizando computadores quânticos.
Contudo, esses algoritmos demandam maiores recursos computacionais e de memória, em consequência, são mais difíceis de implementar em ambientes restritos como dispositivos do tipo IoT (Internet of Things).
Esta pesquisa possui como objetivo ultrapassar as barreiras impostas pelo custo computacional e de armazenamento desses algoritmos e implementá-los em dispositivos com memória limitada.

Autores: PENIDO, Fernando; AMARAL HENRIQUES, Marco (DCA/FEEC)

Apresentador: PENIDO, Fernando

Classificação da Sessão: Sessão de Pôsteres