FORMULÁRIO DE REGISTRO DO PROJETO DE TCC

UNIVERSIDADE FEDERAL DE ITAJUBÁ

Instituto de Matemática e Computação

Colegiado do Curso de Ciência da Computação

Do (a) aluno (a): Gustavo Gimenez Teixeira

Ao (À) Coordenador (a) de TCC: Profa. Dra.Vanessa Cristina Oliveira de Souza

Encaminho o meu projeto de Trabalho de Conclusão de Curso, com as seguintes descrições:

Aluno (a):	**Gustavo Gimenez Teixeira**
Matrícula:	**2021006467**
Orientador (a):	**Otávio de Souza Martins Gomes**
Co-orientador(a): (não obrigatório)	**Bruno Guazzelli Batista**
Título:	**Criptografia Pós-Quântica para IoT: Implementação e Avaliação de Algoritmos em Dispositivos Embarcados**
Palavras-chave	PQC, IoT, Segurança, Dispositivos Embarcados, Kyber.
Introdução/ Justificativa/ Relevância do tema	Com a evolução da computação quântica, diversos algoritmos criptográficos amplamente utilizados atualmente, como RSA e ECC, se tornarão vulneráveis. Isso representa um grande risco para dispositivos IoT, que já possuem restrições computacionais e de consumo energético. A Criptografia Pós-Quântica (PQC) surge como uma solução para garantir segurança a longo prazo. No entanto, sua implementação em dispositivos embarcados traz desafios, como o alto custo computacional e o impacto na latência e no consumo de energia. Este trabalho visa analisar a viabilidade da PQC em dispositivos IoT de baixo consumo, investigando o desempenho, a segurança e as otimizações necessárias para sua implementação prática.
Objetivos	O objetivo principal deste projeto é avaliar a implementação de algoritmos de Criptografia Pós-Quântica em dispositivos IoT embarcados, medindo o impacto no consumo de energia, tempo de execução e segurança. Especificamente, pretende-se: 1. Selecionar e implementar algoritmos PQC recomendados pelo NIST (como Kyber, Dilithium ou Falcon) em dispositivos embarcados. 2. Analisar o desempenho desses algoritmos em comparação com soluções clássicas (ECC/RSA). 3. Investigar otimizações para reduzir o impacto da PQC em consumo energético e latência, incluindo: ○ Uso de co-processadores criptográficos (TPMs, Secure Elements). ○ Modelos híbridos combinando ECC + PQC. 4. Testar a aplicação da PQC em protocolos IoT seguros, como TLS 1.3 em MQTT/CoAP. 5. Propor recomendações para uso eficiente da PQC em cenários IoT reais.
Bibliografia básica	DONG, Cheng; QIAN, Yi; KAZMI, Aqeel; et al. Post-Quantum Cryptography for Internet of Things: A Survey on Performance. *arXiv preprint*, arXiv:2401.17538, 2024. Disponível em: https://arxiv.org/abs/2401.17538 NIST. "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)." 2024. BERNSTEIN, Daniel J.; BUCHMANN, Johannes; DÜLL, Martin. Post-Quantum Cryptography. Springer, 2009.
Descrição Resumida da Metodologia	A metodologia consistirá em experimentos e análises para avaliar a implementação de algoritmos PQC (Post-Quantum Cryptography) em dispositivos IoT, com foco em SBCs (Single Board Computers), como Raspberry Pi, ESP32 e STM32, integrados a

	protocolos de comunicação IoT. Serão exploradas técnicas avançadas para otimização de desempenho, eficiência energética e segurança, incluindo: 1. Seleção e Implementação: ○ Escolha de algoritmos PQC recomendados pelo NIST para integração em dispositivos IoT. ○ Testes em SBCs, como Raspberry Pi, ESP32 e STM32, com foco na compatibilidade com protocolos IoT (MQTT, CoAP, TLS 1.3). 2. Avaliação de Desempenho e Eficiência: ○ Comparação entre algoritmos PQC e clássicos em termos de tempo de execução, uso de recursos (CPU/RAM) e consumo de energia. ○ Utilização de ferramentas como Wireshark para monitoramento de tráfego e medidores de energia para análise da eficiência computacional. 3. Otimização e Segurança: ○ Exploração de técnicas de aceleração por hardware (TPMs, Secure Elements) para melhorar o desempenho dos algoritmos PQC. ○ Implementação de modelos híbridos (ECC + PQC) para reduzir o impacto da criptografia pós-quântica em dispositivos com recursos limitados. ○ Análise de segurança e resistência contra ataques em cenários reais de aplicação IoT.
Resultados esperados:	1. Avaliação quantitativa do impacto da PQC em dispositivos IoT em termos de latência, consumo energético e uso de recursos. 2. Demonstração da viabilidade (ou não) de algoritmos PQC em SBCs e microcontroladores embarcados. 3. Exploração de otimizações para melhorar o desempenho e reduzir custos computacionais da PQC, incluindo redução do tamanho de chave/cifra. 4. Direcionamento para futuras implementações de PQC em IoT, com recomendações práticas para adoção segura.
Cronograma de atividades:	1. Revisão bibliográfica e estudo teórico: ● Estudo dos algoritmos PQC recomendados pelo NIST (Kyber, Dilithium, Falcon). ● Pesquisa sobre dispositivos IoT e SBCs (Raspberry Pi, ESP32, STM32). ● Estudo dos protocolos IoT (MQTT, CoAP, TLS 1.3). 2. Configuração do ambiente de desenvolvimento: ● Preparação dos dispositivos selecionados para testes. ● Integração dos protocolos IoT com os dispositivos. 3. Implementação inicial: ● Primeira implementação dos algoritmos PQC nos dispositivos embarcados. 4. Testes preliminares: ● Comparação inicial entre algoritmos PQC e clássicos (ECC/RSA) em termos de tempo de execução, uso de recursos e consumo energético. ● Análise de tráfego com ferramentas como Wireshark. 5. Preparação do TFG Parcial: ● Redação da primeira versão do trabalho, incluindo metodologia e resultados preliminares. 6. Entrega do TCC Parcial: ● Submissão do TCC Parcial ao orientador até 04/07/2025. 7. Avaliação do TCC Parcial pelo orientador: ● Período para o orientador avaliar e fornecer feedback sobre o TFG Parcial. 8. Refinamento das implementações: ● Exploração de técnicas de otimização, como uso de co-processadores criptográficos (TPMs, Secure Elements). ● Implementação de modelos híbridos (ECC + PQC). 9. Testes de otimização: ● Avaliação de impacto no consumo energético e latência. ● Análise de segurança contra ataques em cenários IoT reais. 10. Análise comparativa final:

	● Consolidação dos dados de desempenho, consumo energético e segurança. 11. Redação do TCC Final: ● Início da redação da versão final do trabalho, incluindo resultados finais e discussões. 12. Revisão e ajustes: ● Revisão do TCC com base no feedback do orientador. ● Finalização dos testes e análises pendentes. 13. Finalização do TCC: ● Conclusão da redação do TCC, incluindo conclusões e recomendações. ● Preparação da apresentação final. 14. Entrega do TCC Final: ● Submissão do TCC Final para defesa até 10 dias antes da data de defesa (data limite: 15/12). 15. Preparação para defesa: ● Revisão final do documento e ensaios para a apresentação. 16. Defesa do TCC: ● Apresentação do trabalho para a banca examinadora.

Atv.	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
1	X	X								
2			X							
3			X							
4				X						
5				X						
6					X					
7					X					
8					X	X				
9					X	X				
10							X			
11							X			
12								X		
13									X	X
14										X
15										X
16										X