POLI TÉCNICO GUARDA

PROPOSTA
DE PLANO DE TRABALHO

Cursos de Mestrado (2.º ciclo)

(não aplicável aos Cursos de Mestrado Habilitadores à Docência)

MODELO

EA.034.05

1. ESTUDANTE

Nome completo: Vagner Monteiro Vaz de Almeida Bom Jesus

Escola: ☐ ESECD ☐ ESS ☒ ESTG ☐ ESTH **N.º de estudante:** 1701172

Curso: CIBERSEGURANÇA Telm.: +351933077024

2. PROPOSTA

☒ Projeto Aplicado / Projeto de Investigação ☐ Relatório de Atividade Profissional ☐ Dissertação

☐ Estágio Profissionalizante/Estágio de Natureza Profissional ☐ Estágio com Relatório Final (Enfermagem)

Criptografia Pós-Quântica em Aplicações Móveis

3. RESUMO DO TRABALHO A DESENVOLVER (área / tema)

O trabalho a desenvolver é uma pesquisa aplicada na área de Cibersegurança em articulação com a Computação Móvel.

Com o crescimento da complexidade e criticidade das infraestruturas digitais tem vindo a exigir novos métodos de proteção capazes de mitigar proativamente as vulnerabilidades de segurança decorrentes da evolução tecnológica. Tradicionalmente, a proteção das transações dos ecossistemas e infraestruturas de informação e comunicalção (e.g. em homebanking) depende de mecanismos criptográficos clássicos, o que as torna vulneráveis à ameaça iminente de ataques com recurso a tecnologias quânticas.

Neste contexto, o presente projeto propõe investigar e explorar as potencialidades de sistemas emergentes de Criptografia Pós-Quântica (PQC) como mecanismo potenciador de proteção de longo prazo para as aplicações móveis, mesmo em ambiente clássico. A viabilidade desta investigação decorre da natureza fisico-matemática transversal da PQC, que ao contrário da criptografia quântica per se não requer a utilização de equipamento especificamente quântico.

A hipótese de trabalho baseia-se na observação de que alterações no paradigma da computação como o surgimento de ataques alavancados por tecnologias quânticas exigem que o sistema de segurança do modelo homebanking se adapte e implemente um protocolo quântico resistente (quantum-resistant protocol). O projeto tem como objetivo desenvolver um sistema de segurança adaptável, recorrendo a técnicas de criptografia Pós-Quântica e Avaliação de Risco para validação, implementadas em dispositivos de computação móvel clássica.

4. OBJETIVOS PREVISTOS

Analisar as vulnerabilidades de segurança das aplicações móveis como homebanking em relação a ataques oriundos de agentes munidos de tecnologias quânticas.

Investigar e selecionar protocolos e algoritmos de Criptografia Pós-Quântica (PQC) mais adequados para o ambiente restrito de plataformas móveis.

Propor e implementar um protótipo de um protocolo PQC selecionado num caso de estudo simulado de "homebanking" em ambiente móvel clássico.

Realizar uma Avaliação de Risco comparativa do sistema com criptografia clássica vs. munido de PQC, quantificando o impacto da transição na segurança "Avaliação Antes e Depois da implementação da solução Pós-Quântica".

Avaliar a viabilidade prática dos algoritmos PQC em plataformas móveis clássicas.

5. METODOLOGIA A UTILIZAR

A metodologia proposta vem combinar a investigação teórica, desenvolvimento prático e avaliação quantitativa, seguindo as etapas do quadro:

Fundamentos Teórico-Metodológicos: Revisão crítica da literatura sobre Segurança Quântica, identificação de ameaças quânticas e definição do caso de estudo de "Homebanking". Elaboração da Avaliação de Risco Pré-PQC.

Desenvolvimento Científico em Criptografia Pós-Quântica: Estudo e seleção dos algoritmos PQC, otimização teórica para o ambiente móvel, e definição da Avaliação de Risco Pós-PQC.

Implementação Técnico-Científica: Desenvolvimento de um protótipo de aplicativo móvel (prova de conceito em ambiente de software clássico) para o caso de estudo. Codificação e integração do protocolo PQC selecionado.

Análise e Discussão dos Resultados: Testes de desempenho no dispositivo móvel. Medição e avaliação de métricas (latência, throughput, tamanho das chaves/assinaturas). Validação dos resultados da Análise de Risco. Conclusões e perspetivas.

Documentação: Apresentação e discussão de resultados de forma clara e estruturada na dissertação e demais produção académico-científica relevante.

6. TRABALHO A DESENVOLVER (com indicação das aprendizagens a efetuar e possíveis dificuldades)

Preveem-se as seguintes tarefas:

1. Revisão do Estado da Arte e Enquadramento Científico - Revisão sobre vulnerabilidade e sistemas, criptografia quântica (QKD) vs. Pós-Quântica (PQC), e a Avaliação de Risco (Clássico).

2. Desenvolvimento Científico - Seleção, estudo e otimização do protocolo PQC (quantum-resistant protocol) para dispositivos móveis.

3. Implementação Técnico-Científica - Desenvolvimento do aplicativo móvel (protótipo) e implementação do protocolo quântico no módulo de comunicação.

4. Análise e Discussão - Análise do impacto e Validação dos resultados; fiabilidade do PQC em plataforma móvel.

5. Escrita da Dissertação - Redação do relatório técnico e científico, Preparação de artigo para apresentação em conferência ou workshop académico.

7. REFERÊNCIAS BIBLIOGRÁFICAS

Perdigão, Rui A.P. (2024): From Quantum Information to Post-Quantum Security. DOI: 10.46337/uc.241019.
C. Cohen-Tannoudji, B. Diu, F. Laloë (2020): Quantum Mechanics, Volume I: Basic Concepts, Tools, and Applications (2nd Edition).Wiley.
M. Nielsen, I. Chuang (2010): Quantum Computation and Quantum Information. Cambridge Univ. Press.
D.J. Bernstein, J. Buchmann and E. Dahmen (2009): Post-Quantum Cryptography. Springer Berlin.
S. Barnett (2009): Quantum Information (Vol. 16). Oxford University Press.
P. Kaye, R. Laflamme, and M. Mosca (2007): An Introduction to Quantum Computing. Oxford Univ. Press.
J. Watrous (2018): The Theory of Quantum Information. Cambridge Univ. Press.
A. Yu. Kitaev, A. H. Shen and M. N. Vyalyi (2002): Classical and Quantum Computation (Graduate Studies in Mathematics)

POLI TÉCNICO GUARDA

PROPOSTA DE PLANO DE TRABALHO

Cursos de Mestrado (2.º ciclo)

(não aplicável aos Cursos de Mestrado Habilitadores à Docência)

MODELO

EA.034.05

8. CRONOGRAMA

Início: 2025/10/01

1.ª etapa: Fundamentos Teórico-Metodológicos em Tecnologias de Informação e Segurança Quântica e Pós-(

2.ª etapa: Desenvolvimento Científico em Criptografia Pós-Quântica.

3.ª etapa: Implementação Técnico-Científica – Aplicativo Móvel Pós-Quântico.

4.ª etapa: Análise, Validação e Discussão dos Resultados, e Conclusão da Dissertação

Previsão de conclusão: _____ **Previsão de apresentação / defesa:** _____

9. DOCENTE ORIENTADOR E DOCENTE(S) COORIENTADOR(ES)

(preencher o n.º de campos necessários)

1) Nome: Rui Alexandre Pita Perdigão

Categoria profissional: Professor Coordenador Grau académico: Doutor

[X] Interno(a) ao IPG - N.º mecanográfico: 1305

[ ] Externo(a) ao IPG - Instituição de ensino / Fac. / Dep.: _____

Data: 2025/10/26 O(A) Docente: Assinado por: **Rui Alexandre Pita Perdigão**
Num. de Identificação: 10984953
Data: 2025.10.26 13:07:13 +0000
(assinatura)

2) Nome: _____

Categoria profissional: Assistente Grau académico: Doutor

[ ] Interno(a) ao IPG - N.º mecanográfico: _____

[ ] Externo(a) ao IPG - Instituição de ensino / Fac. / Dep.: _____

Data: _____ O(A) Docente: _____
(assinatura)

3) Nome: _____

Categoria profissional: Assistente Grau académico: Doutor

[ ] Interno(a) ao IPG - N.º mecanográfico: _____

[ ] Externo(a) ao IPG - Instituição de ensino / Fac. / Dep.: _____

Data: _____ O(A) Docente: _____
(assinatura)

10. DOCUMENTOS EM ANEXO (aplicável APENAS aos cursos de mestrado da *Escola Superior de Saúde*)

[ ] **Estado de arte - Projeto Aplicado / Projeto de Investigação / Dissertação** (não ultrapassar 5 páginas)
Apresentação do problema de investigação e importância para a melhoria do conhecimento.
Descrição do que está referenciado sobre o tema e considerado relevante para a compreensão do projeto a desenvolver.

[ ] **Registo Biográfico de Tutor/Supervisor** (MODELO GRH.019)

[ ] ***Curriculum vitae*** **do(a) docente orientador(a) e docente(s) coorientador(es), caso externo(s) ao IPG**

[ ] Outro: _____

11. CONSELHO TÉCNICO-CIENTÍFICO

Apreciado em reunião realizada em: _____ (D D M M A A A A) **Decisão:** [ ] Favorável [ ] Desfavorável

Fundamentação: _____

O(A) Presidente do Conselho Técnico-Científico: _____
(assinatura)

Após apreciação do Conselho Técnico-Científico, deverá ser comunicada a decisão ao(à) requerente e enviada cópia ao(à) Coordenador(a) do Mestrado.