Programa de Pós-Graduação em Ciência da Computação
Universidade Federal do ABC

orientadora: **Denise Hideko Goya**

Projeto 1: Algoritmos criptográficos pós-quânticos: teoria e prática

Descrição: Encontra-se em estágio adiantado um movimento para escolha e padronização de novos algoritmos criptográficos que sejam supostos seguros tanto em infraestruturas atuais e quanto em cenários que consideram computadores quânticos com grande capacidade de processamento. Os novos padrões criptográficos se justificam pelo fato de que vários algoritmos de chave pública usados atualmente não são seguros sob o modelo computacional quântico, a exemplo daqueles que sustentam sua segurança na dificuldade de fatoração de inteiros (como RSA) ou na dificuldade de cálculo de logaritmo discreto (como o atual padrão em assinatura digital DSA e variantes do protocolo de acordo de chaves Diffie-Hellman). Mesmo após a especificação dos novos padrões, é esperada a necessidade de adequações desses para uso em ambientes específicos como, por exemplo, de Internet das Coisas, o que demanda estudos teóricos sobre a segurança de eventuais adaptações bem como sobre implementações práticas.

Projeto 2: Desenvolvimento e validação de jogos sérios por meio do uso e avaliação do método AIMED

Descrição: O método AIMED (Agile, Integrative and Open Method for Open Educational Resources Development) é um método ágil e iterativo que integra práticas de design pedagógico, design de jogo, modelagem de simulação, engenharia de software e gerenciamento de projetos; para apoiar o desenvolvimento de recursos educacionais eficientes e eficazes (principalmente, jogos sérios). Este projeto visa estender, usar e avaliar o método AIMED no desenvolvimento de diferentes jogos sérios para educação, treinamento e avaliação. Para isso, este projeto possui três objetivos principais: (i) Expandir e avaliar o método proposto; (ii) Desenvolver e validar jogos sérios para fins educacionais, de treinamento e avaliação de desempenho humano; e (iii) Promover pesquisa, desenvolvimento e inovação tecnológica nas áreas de jogos sérios, jogos educacionais e simulações para treinamento.

Publicações e projetos relacionados: https://lirte.pesquisa.ufabc.edu.br/publicacoes/