SEMINÁRIO DE INICIAÇÃO CIENTÍFICA E TECNOLÓGICA DO IFG

ESTUDO E ANÁLISE DAS TÉCNICAS CRIPTOGRÁFICAS ATUAIS PARA UMA PROPOSTA DE CRIPTOGRAFIA

TIBURCIO, Wagner Ezequiel Gonçalves

Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Inhumas, Bacharelado em Engenharia de Software.

FURLAN, Pablo Vandré Jacob

Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Inhumas, Departamento de Áreas Acadêmicas.

A criptografia de chave pública empregada atualmente em serviços digitais baseia-se, em grande parte, na dificuldade computacional da fatoração de inteiros, no caso do RSA, e do logaritmo discreto em curvas elípticas, no caso da ECC. O avanço da computação quântica, especialmente pela existência do algoritmo de Shor, torna necessária a compreensão das limitações desses métodos e das alternativas pós-quânticas em processo de adoção. Este trabalho teve como objetivo estudar os fundamentos matemáticos das principais técnicas criptográficas de chave pública, analisar vulnerabilidades de projeto e implementação e, a partir desse levantamento, delimitar uma proposta de criptografia viável no escopo de uma iniciação científica. A metodologia foi organizada de forma cumulativa, iniciando pela revisão de aritmética modular, função totiente de Euler, Teorema de Euler, algoritmo de Euclides estendido e aritmética de curvas elípticas sobre corpos finitos. Os resultados teóricos foram acompanhados por exemplos numéricos resolvidos manualmente e por implementações didáticas em Python, posteriormente comparadas com bibliotecas de referência. Também foram estudados ataques contra RSA, ECC e implementações

pós-quânticas, além dos fundamentos de reticulados, do problema Learning With Errors e dos padrões ML-KEM e ML-DSA. A etapa aplicada concentrou-se na combinação entre criptografia pós-quântica e esteganografia adaptativa em imagens, considerando métodos de embutimento, esteganálise e capacidade do portador. Entre os resultados, as implementações didáticas reproduziram os valores obtidos pelas bibliotecas de referência, e a análise dos artefatos pós-quânticos evidenciou o aumento expressivo do volume de dados em relação aos esquemas clássicos. Para uma imagem de 512 por 512 pixels, o conjunto formado pela chave pública e pelo texto cifrado do ML-KEM-768 exige aproximadamente 0,069 bit por pixel, enquanto uma assinatura ML-DSA-65 exige cerca de 0,101 bit por pixel, valor superior à referência de 0,1 adotada no estudo. Com base nesses resultados, a proposta foi delimitada como uma composição de primitivas já padronizadas, utilizando ML-KEM-768 para encapsulamento de chave, AES-256 para cifragem dos dados e embutimento adaptativo em imagens, em vez da criação de uma nova primitiva criptográfica. Conclui-se que o trabalho consolidou a base matemática necessária e estabeleceu uma proposta tecnicamente delimitada, porém os resultados permanecem teóricos e exploratórios, pois ainda não foram realizados experimentos de embutimento e detecção. A continuidade deverá avaliar experimentalmente a proposta frente a detectores e protocolos padronizados de esteganálise.

Palavras-chave

Criptografia; criptografia pós-quântica; RSA; curvas elípticas; esteganografia.

Agradecimentos

O presente trabalho foi realizado com apoio do Instituto Federal de Educação, Ciência e Tecnologia de Goiás.