Título: Computação Multipartidária Segura com Assistência Quântica
Nome: Manuel Maria Trigueiros Sampaio Batalha dos Santos
Doutoramento em: Segurança da Informação
Orientador: Paulo Alexandre Carreira Mateus
Co-Orientador: Armando Humberto Moreira Nolasco Pinto

Resumo

A criptografia quântica explora as propriedades da física quântica para robustecer os métodos criptográficos para além das abordagens clássicas. A distribuição quântica de chaves (QKD) tem sido um foco importante, mas os avanços em primitivas de dois participantes, como a transferência quântica oblívia (QOT), também oferecem desenvolvimentos para a computação segura quântica. Esta tese começa por apresentar uma revisão da literatura sobre QOT, abrangendo protocolos propostos, requisitos de segurança, resultados de impossibilidade e examinando condições para a segurança da QOT.

A transferência oblívia (OT) desempenha um papel crucial na computação segura multipartidária (SMC), prometendo avanços na análise de dados e privacidade na computação. A tese avalia a complexidade da OT quântica em comparação com dois protocolos OT clássicos, lançando luz sobre benefícios e limitações potenciais para a segurança e eficiência da SMC.

Expandindo a análise teórica da transferência oblívia quântica e clássica, a tese integra ambas num sistema de computação segura multipartidária para análise de genoma. Usando protocolos criptográficos quânticos, o sistema proposto melhora a privacidade do calculo de uma árvore filogenética a partir de sequências privadas de genoma. Três protocolos criptográficos quânticos são integrados para fortalecer a segurança contra ataques quânticos. Incluímos uma análise de complexidade, uma prova de segurança e detalhes da implementação. A avaliação do sistema quântico em comparação com uma solução exclusivamente clássica mostra tempos de execução semelhantes, com a abordagem quântica introduzindo um aumento de tempo devido ao sistema de gestão de chaves oblívias.

A tese apresenta o primeiro protocolo quântico para avaliação linear oblívia, uma forma generalizada de transferência oblívia. Nesse cenário, as dua partes, Alice e Bob, calculam colaborativamente uma função linear sem revelar as suas entradas. Enquanto os métodos clássicos dependem da transferência oblívia, a tese propõe um novo protocolo quântico independente da transferência quântica oblívia. O protocolo utiliza estados quânticos de alta

dimensão para calcular a função linear em corpos de Galois, estendendo-se de configurações semi-honestas para desonestas usando uma estratégia de compromisso e abertura. A segurança é rigorosamente comprovada no contexto da composabilidade universal quântica, e o protocolo é generalizado para avaliação linear oblívia de vetores, melhorando a eficiência.

Palavras-chave: criptografia quântica, transferência oblívia quântica, avaliação linear oblívia quântica, computação multipartidária segura, segurança UC.