Título: Computação Multipartidária Segura com Assistência Quântica

Resumo alargado em Português

A criptografia quântica é o campo da criptografia que explora as propriedades quânticas da matéria. Geralmente, visa desenvolver primitivas fora do alcance da criptografia clássica e melhorar as implementações clássicas existentes. Embora grande parte do trabalho neste campo se foque na distribuição de chaves quânticas (*quantum key distribution*, QKD), também têm existido desenvolvimentos cruciais para a compreensão e desenvolvimento de outras primitivas criptográficas, como a transferência oblívia quântica (*quantum oblivious transfer*, QOT). Pode-se mostrar a semelhança entre a estrutura de aplicação das primitivas QKD e QOT. Assim como os protocolos QKD permitem comunicação com segurança quântica, os protocolos QOT permitem computação com segurança quântica. No entanto, as condições sobre as quais o QOT é totalmente seguro têm sido sujeitas a um intenso estudo.

Embora os protocolos clássicos de OT dependam de primitivas criptográficas assimétricas, que são conhecidas por serem vulneráveis a ataques quânticos ou terem segurança baseada em conjecturas, vários trabalhos usaram as leis da física para provar a segurança do OT quântico baseados em adversários maliciosos com acesso a computadores quânticos. Nesta tese, começamos por fazer um levantamento do trabalho desenvolvido em torno do conceito de OT dentro da criptografia quântica teórica. A nossa análise é centrada no uso the chaves oblívias e concentramo-nos em alguns protocolos propostos e nos seus requisitos de segurança. Analisamos o perigo posto por técnicas quânticas de hacking e apresentamos uma avaliação de medidas práticas e teóricas de modo a mitigar esses ataques. Por último, também revisitamos os resultados de impossibilidade desta primitiva e discutimos vários modelos quânticos de segurança sobe os quais é possível provar a segurança do QOT.

A aplicação mais famosa do OT está no domínio da computação multipartidária segura (*secure multiparty computation*, SMC). Esta tecnologia tem o potencial de ser disruptiva nas áreas de análise e computação de dados. Esta permite que vários participantes calculem uma certa função, preservando a privacidade dos seus dados. No entanto, a maior parte da segurança e eficiência do protocolos SMC dependem da segurança e eficiência do OT. Por esta razão, fazemos uma comparação detalhada entre a complexidade da QOT baseada em chaves oblívias e dois dos protocolos OT clássicos mais rápidos (ALSZ15 and KOS15). O protocol QOT utilizado para a comparação com a abordagem clássica resulta de uma optimização por nós proposta da versão BBCS. Ambos os tipos de protocolos podem ser divididos em duas fases: pré-computação e transferência. A fase de pré-computação é independente das contribuições dos participantes e é utilizada para gerar os recursos necessários na fase de transferência, que tem em consideração as contribuições dos participantes. Notavelmente, a fase de transferência do OT quântico envolve apenas comunicação clássica, tor-

nando possível e justo compará-la com a fase de transferência dos protocolos clássicos. Concluímos que ambos os protocolos clássicos (ALSZ15 and KOS15) têm uma complexidade de computação e comunicação superiores à versão optimizada de QOT.

À luz das preocupações com a privacidade dos indivíduos e das regulamentações legais, é crucial manusear e estudar dados genômicos usando técnicas altamente seguras de preservação da privacidade. Seguindo a comparação teórica entre OT quântico e clássico, integramos e comparamos ambas as abordagens dentro de um sistema SMC baseado na análise de sequências genéticas. Em resumo, propomos um sistema SMC auxiliado por protocolos criptográficos quânticos com o objectivo de calcular uma árvore filogenética a partir de um conjunto de sequências genéticas privadas. Este sistema melhora significativamente a privacidade e a segurança da computação graças a três protocolos criptográficos quânticos que fornecem segurança aprimorada contra ataques de computadores quânticos. Este sistema adapta vários métodos baseados em distância (Unweighted Pair Group Method with Arithmetic Mean (UPGMA), Neighbour-Joining (NJ), Fitch-Margoliash (FM)) num ambiente privado onde as sequências de cada participante não são divulgadas aos demais membros presentes no protocolo. Em vez de usar uma implementação genérica de SMC para árvores filogenéticas, desenvolvemos um protocolo privado especializado que melhora a eficiência para este caso de uso específico. Avaliamos teoricamente as garantias de desempenho e privacidade do sistema através de uma análise de complexidade e prova de segurança, e fornecemos uma extensa explicação dos detalhes de implementação e protocolos criptográficos. Implementamos este sistema com base na implementação Libscapi do protocolo de Yao, na biblioteca PHYLIP e em chaves simuladas de dois sistemas quânticos: distribuição de chaves oblívias quânticas e distribuição de chaves quânticas. Comparamos esta implementação com uma solução somente clássica e concluímos que ambas as abordagens apresentam tempos de execução semelhantes. A única diferença entre os dois sistemas é a sobrecarga de tempo tomada pelo sistema de gestão de chaves oblívias da abordagem quântica.

Finalmente, apresentamos o primeiro protocolo quântico de avaliação linear oblívia (*oblivious linear evaluation*, OLE). O OLE é uma generalização do OT, em que dois participantes calculam de forma oblívia uma função linear, $f(x) = ax + b$. Ou seja, cada participante fornece os seus dados de forma privada, a fim de calcular o resultado $f(x)$ que se torna conhecido por apenas um deles. Do ponto de vista estrutural e de segurança, o OLE é fundamental para protocolos SMC baseados em circuitos aritméticos. No caso clássico, sabe-se que o OLE pode ser gerado com base no OT, e as contrapartes quânticas desses protocolos podem, em princípio, ser construídas como extensões directas baseadas em QOT. Aqui, apresentamos o primeiro, protocolo quântico OLE que não depende de QOT. Começamos apresentando um protocolo semi-honesto e depois estendemo-lo para o cenário desonesto através de uma estratégia *commit-and-open*. O nosso protocolo usa estados quânticos para calcular a função linear, $f(x)$, em corpos de Galois de dimensão prima, $GF(d)$, ou dimensão de potência prima, $GF(d^M)$. Estas construções utilizam a existência de um conjunto

completo de *mutually unbiased bases* em espaços de Hilbert de dimensão de potência prima e o seu comportamento linear sobre os operadores de Heisenberg-Weyl. Também generalizamos o nosso protocolo para obter uma versão vectorial do OLE, onde são geradas várias instâncias de OLE, tornando o protocolo mais eficiente. Provamos que os protocolos têm segurança estática no âmbito da composição universal quântica. Para tal, utilizamos o conceito de *min-entropy* quântica como forma de descrever a quantidade de informação que um agente malicioso Bob tem em relação aos estados quânticos de um agente honesto Alice. A prova de segurança no âmbito da composição universal quântica requer a realização de duas propriedades: indistinguibilidade entre um mundo ideal, onde consta a definição de segurança, e um mundo real, onde é executado o protocolo; a extracção dos *inputs* do agente malicioso. A indistinguibilidade é obtida através da quantificação da *min-entropy* quântica e a extracção dos *inputs* através do acesso à funcionalidade de comprometimento no caso de um Bob malicioso e através do ataque ao protocolo semi-honesto no caso de uma Alice maliciosa.

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