TELEPORTE DO SINAL QUÂNTICO DO PROTOCOLO BB84 DE DISTRIBUIÇÃO DE CHAVES CRIPTOGRÁFICAS QUÂNTICAS

Danilo Muniz da Silva Gentina[1], Roberto Baginski B. Santos
Centro Universitário da FEI
danilogentina@yahoo.com.br, rsantos@fei.edu.br

Resumo: O objetivo deste trabalho é compreender se é possível estender o alcance do sinal quântico usado no protocolo BB84 de distribuição de chaves criptográficas quânticas por meio de teleporte quântico e, em uma próxima etapa, estimar o número de operações extras necessárias.

1. Introdução

A teoria quântica da informação traz consigo o potencial para ampliar as possibilidades de armazenar, processar e transmitir informação[1]. Enquanto na computação clássica, um bit pode valer ou 0 ou 1, na computação quântica, um bit quântico (qubit) pode estar em uma superposição arbitrária dos estados distinguíveis $|0\rangle$ e $|1\rangle$. Um dos aspectos mais peculiares da teoria quântica da informação é a possibilidade de distribuir chaves criptográficas que não podem ser copiadas nem violadas, como no protocolo BB84[1,2]. A impossibilidade de copiar um estado quântico arbitrário é garantida pelo teorema *no-cloning*[1,3,4] enquanto a inviolabilidade da chave criptográfica se deve ao fato de que cada bit da chave é gerado de modo aleatório; a chave criptográfica compartilhada deve também ser usada uma única vez. O problema com os protocolos de distribuição de chaves quânticas é que os canais quânticos de comunicação têm um alcance limitado a poucas centenas de quilômetros. No caso de um sinal clássico, amplifica-se o sinal; para um sinal quântico, esta solução é inviável, pois não sendo possível copiar um sinal, não é possível amplificá-lo.

Neste trabalho, apresentaremos diversos pontos da revisão bibliográfica realizada até o momento e indicaremos os desenvolvimentos previstos para as próximas etapas, em que mostraremos como utilizar o teleporte quântico para estender o alcance dos canais quânticos de comunicação.

2. Metodologia

Até o momento, realizamos uma revisão bibliográfica de elementos da teoria quântica da informação[1]. Começamos com a noção de qubit, com o princípio da superposição, com a noção de medição do estado do qubit e com a interpretação probabilística do resultado desta medição[1]. Em seguida, estudamos o teorema *no-cloning*[1,3,4], que proíbe a cópia de estados quânticos desconhecidos e que, portanto, é vital para a segurança do protocolo de distribuição de chaves quânticas[1,2].

A distribuição de chaves quânticas é um processo pelo qual duas partes, Alice e Bob, por exemplo, podem gerar uma chave criptográfica privada usando um canal público. O protocolo BB84 de distribuição de chaves quânticas pode ser descrito da seguinte maneira[1,2]. Inicialmente, Alice gera duas sequências, a e b de bits clássicos e aleatórios. Alice codifica cada bit da sequência a como $|0\rangle$ ou $|1\rangle$ se o bit correspondente em b for 0 ou como $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ ou $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ se o bit correspondente em b for 1, isto é, a sequência a é codificada em duas bases computacionais diferentes (bases dos operadores Z e X), o que é impossível na computação clássica. Bob receb os qubits de Alice por meio de um canal quântico de comunicação e mede cada um deles na base Z ou na base X, conforme o valor do bit clássico na sequência aleatória b' que Bob gerou independentemente de Alice. Então, Alice e Bob anunciam suas sequências b e b' e descartam todos os qubits que não tenham sido codificados por Alice e medidos por Bob na mesma base. Alice seleciona aleatoriamente n dos bits restantes e informa seus valores a Bob. Se houver muita discordância entre eles, o protocolo é reiniciado. Caso a discordância seja pequena, técnicas de correção de erro permitem a produção de uma chave compartilhada de m bits. Nas próximas etapas do projeto, mostraremos como usar o teleporte quântico, que é o fenômeno pelo qual um estado quântico arbitrário pode ser comunicado entre dois pontos que estiveram ligados por um canal quântico de comunicação no passado para estender o alcance dos canais quânticos de comunicação.

3. Resultados

Como o projeto está em fase inicial, não há ainda resultados a serem relatados.

4. Conclusões

Realizamos uma revisão bibliográfica sobre as noções mais importantes da teoria quântica da informação, sobre a distribuição de chaves criptográficas quânticas, especialmente do protocolo BB84 e sobre o teleporte quântico, que deve permitir estender o alcance dos canais quânticos de comunicação para implementação no mundo real dos protocolos de distribuição de chaves quânticas.

5. Referências

[1] NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information**. Cambridge: Cambridge University Press, 2000.

[2] BENNETT, C. H.; BRASSARD, G. **Proc. IEEE Int. Conf. Comp., Syst. and Signal Proc.** v. 175, p. 8. New York: IEEE, 1984.

[3] WOOTERS, W.; ZUREK, W. **Nature** v. 299, p. 802, 1982.

[4] DIEKS, D. **Physics Letters A** v. 92, p. 271, 1982.

[1] Aluno de IC do Centro Universitário da FEI