Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Um estudo passo a passo do Algoritmo de Shor

Luciano Alves Vieira [1]
CCT - Universidade Federal do Cariri
Clarice Dias de Albuquerque [2]
CCT - Universidade Federal do Cariri

1 Introdução

Classicamente, o uso da criptografia está relacionado à proteção de informação militar, governamental ou empresarial. Contudo, após a invenção do computador e o crescente uso da Internet para executar várias tarefas financeiras, a criptografia passou a ter importância para qualquer usuário da Internet.

O método criptográfico pode ser de chave privada ou de chave pública. Até a década de 70, todos os métodos criptográficos eram de chave privada, onde a chave compartilhada pelo remetente e o destinatário deve ser comunicada via um canal confiável. A partir do momento em que as redes de computadores começaram a se tornar comuns, surgiu a necessidade de um novo método criptográfico, o de chave pública, onde é necessário um par de chaves, uma pública para encriptar a mensagem, que é do conhecimento de todos, e uma privada, mantida em segredo e usada para decriptar a mensagem. Para garantir a segurança desse método, o cálculo do valor da chave privada a partir do valor conhecido da chave pública é baseado em problemas matemáticos difíceis de serem resolvidos computacionalmente.

A primeira técnica de chave pública é a RSA inventada em 1977, e ainda é um dos métodos mais utilizados, [1]. Nesta técnica, o cálculo do valor da chave privada a partir da chave pública é equivalente ao problema de fatorar um número inteiro muito grande. Tal problema não pode ser resolvido em tempo polinomial por um computador clássico.

Contudo, em 1994, Peter Shor descreveu um algoritmo baseado em propriedades da mecânica quântica que resolvia o problema de fatoração de um número N em tempo polinomial, [2]. Esse trabalho impulsionou enormemente a pesquisa em computação e criptografia quântica, [3].

No algoritmo de Shor o problema de fatorar um número N composto é reduzido ao cálculo da ordem de um número menor do que N, escolhido aleatoriamente, [4]. Para fazer esse cálculo, o algoritmo baseia-se especialmente nas características do paralelismo quântico e na Transformada de Fourier Quântica Discreta.

[1] luciano.alves.vieira@gmail.com
[2] clarice.albuquerque@ufca.edu.br

O presente trabalho tem como objetivo estudar o algoritmo de Shor e descrever passo a passo o circuito quântico para achar a ordem de um inteiro positivo x módulo N, calculando o estado após cada porta. Para isso, tomou-se o exemplo $N = 15$.

2 O Algoritmo de Shor para $N = 15$

Tomando $N = 15$, inicialmente calculamos o valor $n = \lceil \log_2^{15} \rceil$, neste caso $n = 4$. O próximo passo é escolher x coprimo com 15 e de modo que $1 < x < 15$, escolhemos $x = 2$. O objetivo do algoritmo de Shor é determinar a ordem de x, ou seja, o menor inteiro r tal que $2^r \equiv 1 \; mod \; 15$, donde $r = 4$. Como $r = 2^2$, então podemos usar $t = n = 4$. Assim teremos 4 qubits no primeiro registrador e 4 qubits no segundo registrador.

O computador quântico é inicializado no estado $|\psi_0\rangle = |0000\rangle|0000\rangle$. Em seguida, são aplicadas as portas de Hadamard nos primeiros 4 qubits deixando o primeiro registrador em uma superposição de estados da base computacional com amplitude $\frac{1}{\sqrt{2^4}}$. Depois é aplicado V_x que é um operador linear unitário dado por $V_x(|j\rangle|k\rangle) = |j\rangle|k + x^j\rangle$, onde $|j\rangle$ e $|k\rangle$ são os estados do primeiro e do segundo registrador. V_x age simultaneamente em todos os termos e gera todas as potências de x ao mesmo tempo. É feita uma medida no segundo registrador, gerando um dos números $\{1, 2, 4, 8\}$ com igual probabilidade. O próximo passo é aplicar a Transformada de Fourier Inversa $DFT^{-1} = DFT^\dagger$ no primeiro registrador. Neste momento existem várias etapas que são calculadas uma a uma. O resultado após a $DFT^\dagger$ é $\frac{1}{2}[|0000\rangle - |0001\rangle + i|0010\rangle - i|0011\rangle]|2\rangle$, os estados são equiprováveis com probabilidade $\frac{1}{4}$. É feita uma medida no primeiro registrador. Supondo, sem perda de generalidade, que o resultado seja $|0011\rangle = |3\rangle$, como $2^n = 16$, resolvemos por frações contínuas $\frac{3}{16}$ e obtemos r.

Agradecimentos

Este trabalho teve o suporte do CNPq através do projeto 425224/2016-3 e da UFCA.

Referências

[1] A. C. Faleiros. *Criptografia*. vol. 52 das Notas em Matemática Aplicada. Sociedade Brasileira de Matemática Aplicada e Computacional (SBMAC), São Carlos, 2011.

[2] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124, 1994.

[3] M. A. Nilsen and I. L. Chuang. *Computação Quântica e Informação Quântica*. Bookman, 2003.

[4] R. Portugal, C. C. Lavor, L. M. Carvalho e N. Maculan. *Uma Introdução à Computação Quântica*. vol. 8 das Notas em Matemática Aplicada. Sociedade Brasileira de Matemática Aplicada e Computacional (SBMAC), São Carlos, 2004.