COMPUTAÇÃO QUÂNTICA E AS VULNERABILIDADES DOS ATUAIS SISTEMAS CRIPTOGRÁFICOS: RELEVÂNCIA PARA A SEGURANÇA DA INFORMAÇÃO

*SGT DANIEL **BOMFIM** NUNES*
*SGT **DERYCK** MOURA*

RESUMO

A computação quântica, uma tecnologia com potencial para transformar diversos campos da ciência, da tecnologia e consequentemente da sociedade, apresenta elevada relevância para a segurança de dados e informações. A elevada velocidade de processamento e aumento na capacidade de computação das possibilidades gera impactos na performance de diversos setores informacionais, mas também abre portas para violações de segurança. O avanço na implementação da mecânica quântica na base do funcionamento de computadores abre margem para que os alicerces da segurança cibernética, do armazenamento, manipulação e tráfego de dados sejam abalados, principalmente no que tange ao uso da criptografia. Este artigo avalia o impacto potencial da computação quântica sobre os sistemas criptográficos atuais, sua relação com tecnologias fundamentais na sociedade do séc. XXI e aponta algumas estratégias de mitigação para proteger a segurança digital na era da computação quântica.

Palavras-chave: computação quântica, criptografia, algoritmo, segurança da informação.

1 INTRODUÇÃO

A computação quântica surge como uma revolução científica e tecnológica com o potencial de transformar diversas áreas, especialmente a criptografia. Em 1994, o matemático Peter Shor apresentou um algoritmo que demonstrou como os computadores quânticos poderiam resolver problemas matemáticos complexos de forma exponencialmente mais rápida do que os computadores tradicionais. Essa descoberta revelou uma ameaça iminente aos sistemas de segurança que utilizam criptografia baseada na dificuldade de fatoração de números primos. Os sistemas criptográficos atuais, como o RSA, são amplamente utilizados para proteger informações sensíveis, confiando na dificuldade de fatorar grandes números como uma barreira intransponível para potenciais invasores. No entanto, a capacidade teórica dos computadores quânticos de quebrar esses códigos em um tempo razoável coloca em risco a segurança dos dados protegidos por essas técnicas.

Essa ameaça enfatiza a necessidade urgente de desenvolver novas formas de criptografia que possam resistir aos ataques quânticos. À medida que a computação quântica avança, a transição para algoritmos criptográficos quânticos seguros torna-se uma prioridade para garantir a proteção das informações na era pós-quântica.

2 DESENVOLVIMENTO

A exploração das propriedades da mecânica quântica, como o entrelaçamento, a interferência e a superposição de estados para realizar operações computacionais de forma mais eficiente permitiu o desenvolvimento do que se conhece por computação quântica. Em vez de bits, que são a unidade básica informacional dos computadores clássicos, os computadores quânticos utilizam qubits, que podem existir simultaneamente em múltiplos estados graças à superposição quântica. O entrelaçamento quântico também permite que qubits estejam interligados, de modo que o estado de um qubit influencia o estado de outro, mesmo que estejam separados por grandes distâncias. Essas propriedades únicas possibilitam o processamento massivo de informações simultaneamente, revolucionando a capacidade de cálculo.

Em comparação com os computadores clássicos, que processam informações de forma sequencial utilizando bits em estados de 0 ou 1, os computadores quânticos oferecem uma capacidade de processamento exponencialmente superior para certos tipos de problemas. Isso se deve ao fato de que os qubits podem representar e manipular várias

possibilidades ao mesmo tempo. Por exemplo, enquanto um computador clássico precisaria testar cada solução possível para um problema, um computador quântico pode explorar todas as soluções paralelamente, acelerando drasticamente o processo de cálculo.

Essa capacidade permite que um computador quântico execute certos algoritmos, como o de Shor, muito mais rapidamente do que qualquer computador clássico. O poder de processamento superior da computação quântica abre novas possibilidades em áreas como criptografia, simulação de sistemas físicos complexos e otimização. No entanto, também apresenta desafios únicos, como a manutenção da coerência quântica e a correção de erros quânticos, que precisam ser superados para a plena realização dessa tecnologia.

Ao citarmos a supremacia dos computadores quânticos frente aos computadores clássicos e os respectivos algoritmos de criptografia usados, é natural surgir o questionamento sobre quais fraquezas evidenciam estes problemas. No campo da criptografia assimétrica, a qual faz uso de duas chaves, uma pública e outra privada, um algoritmo amplamente utilizado é o Rivest-Shamor-Adleman (RSA). A segurança da chave criptográfica utilizada reside na dificuldade matemática da fatoração de números primos muito grandes (chaves que variam de 512 até 8192 bits). Tal entrava se dá pelo fato de que mesmo os computadores com capacidade de processamento mais robusta demorariam milhões de anos para quebrar tais chaves pelos métodos de fatoração existentes. Se levaria mais tempo do que a própria existência da humanidade para quebrar as chaves criptográficas usada no protocolo RSA, então qual a fraqueza existente? A vulnerabilidade, atualmente, não é diante dos computadores clássicos, mas sim dos eventuais computadores quânticos, pois estes fazem uso da superposição de estados para elevar exponencialmente a velocidade de processamento simultâneo de dados. Isto permite que uma tarefa que levaria milhões de anos ocorra em horas, minutos ou até mesmo segundos.

A utilização do algoritmo de Shor para exploração de vulnerabilidades dos sistemas criptográficos atuais, é um exemplo de metodologia que pode decifrar as chaves utilizadas pelo RSA, por exemplo. Para que esta aplicação logre êxito é fundamental compreender que o uso de computadores quânticos é essencial, pois a utilização do algoritmo para fatorar números primos aliada ao incremento exponencial no cômputo das probabilidades dos valores fornecidos pela superposição dos estados faz com que o tempo de cálculos dos fatores que geraram a chave mudem de um tempo exponencial para um tempo polinomial, o que significa uma robusta redução no tempo de quebra da chave.

É possível imaginar um cenário após o desenvolvimento de um computador quântico que implemente o algoritmo de Shor para fatorar números maiores que 2048 bits. Este panorama parece ser um tanto caótico, pois diversas informações confidenciais trafegadas nas redes poderiam ser violadas. Diante disto, é necessário pensar sobre como garantir a segurança dos diversos setores que fazem uso da criptografia. Os pesquisadores Charles Henry Bennett e Gilles Brassard desenvolveram, em 1984, um protocolo conhecido como BB84. A ideia era propor um sistema de distribuição de chaves baseado em alguns princípios da mecânica quântica. De modo simplificado podemos entender que a impossibilidade de medir a informação de uma partícula sem alterar seu estado e o princípio da não-clonagem impedem que os dados trafegados sejam interceptados sem detecção. Deste modo, a chave estabelecida seria segura. Certamente um atacante pode buscar acessar as máquinas envolvidas na transação para copiar a chave após ser armazenada. Depois disso ele tentaria quebrar essa sequência de bits. O detalhe é que a própria geração dos bits da chave segue um processo aleatório para o qual, em princípio, não há uma fórmula específica para reverter o processo e encontrar o valor original. Além disso, existem pesquisas de algoritmos pós-quânticos, os quais pretender ser implementados em computadores clássicos por meio de novas funções e metodologias matemáticas que proponham problemas diferentes da fatoração de números primos. O ponto crucial é elaborar um problema para o qual a complexidade seja tal que mesmo um

computador quântico não conseguiria resolvê-lo em tempo humanamente válido.

3 CONCLUSÃO

As tecnologias digitais utilizam algoritmos criptográficos em diversos setores da sociedade. Há implementações no tráfego de informações em serviços de saúde, ensino, transações financeiras por meio do protocolo HTTPS, por exemplo, o qual usa criptografia assimétrica em sua base. Este ponto, por si só, já se torna crítico pelo volume e relevância das informações pessoais compartilhados. Sistemas como criptomoedas, assinaturas digitais, acesso a servidores dentre outros para os quais a criptografia é essencial. Assim, é premente compreender que a inevitabilidade dos perigos que a computação quântica pode trazer para a segurança da informação, seja de um computador pessoal ou de uma nação, é uma realidade. Para lidar com esta realidade cada vez mais próxima é necessário investir em pesquisa, educação científica, integração entre instituições de pesquisa do Estado e empresas para pensar e desenvolver soluções no setor de tecnologias quânticas, principalmente no que concerne à criptografia quântica.

Abstract

Quantum computing, a technology with the potential to transform various fields of science, technology, and consequently society, presents significant relevance for data and information security. The high processing speed and increased computational capacity generate impacts on the performance of various informational sectors, but also open doors for security breaches. The advancement in the implementation of quantum mechanics as the foundation of computer operation raises concerns that the pillars of cybersecurity, data storage, manipulation, and traffic, could be compromised, especially in terms of cryptography. This article assesses the potential impact of quantum computing on current cryptographic systems, its relationship with fundamental technologies in 21st-century society, and suggests some mitigation strategies to protect digital security in the era of quantum computing.

Keywords: ***Quantum computing, cryptography, algorithm, information security***

4 REFERÊNCIAS

CARVALHOSA, Jonathan Correia - Aplicação de Reticulados em Criptografia. Rio de Janeiro: IME, 2012.

FREITAS, Adriana Xavier – Algoritmo de Shor e sua aplicação à fatoração de números inteiros. S.I.: UFMG, 2010.

GALVÃO, Ernesto F. O que é Computação Quântica. Vieira e Lent, 1o edição, 2007

LOPES, Bianca de Meira; LIMA, Thainá Lucciola Hipolito de. Fatoração de números com recursos da computação quântica. Projeto de Final de Curso – Instituto Militar de Engenharia, Rio de Janeiro, 2022.

OLIVEIRA, Ivan S.; SARTHOUR, Roberto S. Computação Quântica e Informação Quântica. Rio de Janeiro: CBPF, 2004.