15º Congresso de Inovação, Ciência e Tecnologia do IFSP - 2024

COMPUTAÇÃO QUÂNTICA: O FUTURO DA SEGURANÇA CIBERNÉTICA OU O FIM DA CRIPTOGRAFIA CLÁSSICA?

Guilherme Gomes Zunta Camacho[1], Ronaldo Rossetti Dearo[2], Vinicius Tiago de Santana[3], Diego Ribeiro Bastos[4], Wendel Marcos dos Santos[5]

[1] Graduando em Sistemas da Informação, IFSP, Campus São Paulo, g.zunta@aluno.ifsp.edu.br
[2] Graduando em Sistemas da Informação, IFSP, Campus São Paulo, ronaldo.dearo@aluno.ifsp.edu.br
[3] Graduando em Sistemas da Informação, IFSP, Campus São Paulo, v.tiago@aluno.ifsp.edu.br
[4] Graduando em Sistemas da Informação, IFSP, Campus São Paulo, bastos.diego@aluno.ifsp.edu.br
[5] Professor, IFSP, Campus São Paulo, wendel.santos@ifsp.edu.br

Área de conhecimento (Tabela CNPq): 1.03.03.04-9 Sistemas de Informação

RESUMO: Este trabalho tem como objetivo demonstrar como a computação quântica pode tornar vulneráveis as técnicas criptográficas utilizadas atualmente. Para isso, apresenta-se uma análise histórica da evolução dos computadores quânticos e suas principais diferenças em relação aos computadores clássicos. O estudo aborda, de forma concisa, a importância da criptografia na proteção de dados, comparando os tipos de criptografias clássicas com as soluções emergentes de criptografia quântica resistente. Além disso, são discutidas as limitações tecnológicas que ainda impedem os computadores quânticos de quebrar os sistemas criptográficos existentes, mas que indicam a necessidade de adaptação diante do avanço rápido dessa tecnologia. Por fim, o trabalho destaca as pesquisas em andamento voltadas para a criação de novas soluções que reforcem a segurança tanto na criptografia clássica quanto na quântica resistente.

PALAVRAS-CHAVE: criptografia quântico-resistente; computador quântico; segurança de dados; criptografia clássica; computador clássico; algoritmo quântico

QUANTUM COMPUTING: THE FUTURE OF CYBERSECURITY OR THE END OF CLASSICAL CRYPTOGRAPHY?

ABSTRACT: This paper aims to demonstrate how quantum computing could render current cryptographic techniques vulnerable. To this end, it provides a historical analysis of the evolution of quantum computers and their key differences from classical computers. The study concisely addresses the importance of cryptography in data protection, comparing classical cryptographic methods with emerging quantum-resistant solutions. Additionally, the technological limitations that currently prevent quantum computers from breaking existing cryptographic systems are discussed, highlighting the need to adapt for the rapid advancement of this technology. Finally, the paper emphasizes ongoing research focused on developing new solutions to strengthen security in both classical and quantum-resistant cryptography.

KEYWORDS: quantum-resistant cryptography; quantum computer; data security; classical cryptography; classical computer; quantum algorithm.

INTRODUÇÃO

A computação quântica, proposta inicialmente por Deutsch (1985), baseia-se em princípios fundamentais da mecânica quântica, como os explorados por Feynman (1982), que investigou a simulação de sistemas físicos, e Benioff (1982), que propôs um modelo de máquina de Turing quântica. Essas ideias estabeleceram as bases teóricas para o desenvolvimento da computação quântica. O trabalho de Shor (1994), ao demonstrar a eficiência dos computadores quânticos na fatoração de números, trouxe grande atenção à área. Diferente dos computadores clássicos, que operam com bits (0 ou 1), os computadores quânticos utilizam *qubits*, que permitem maior paralelismo e eficiência (Jose et al., 2013).

A criptografia clássica, como RSA (*Rivest-Shamir-Adleman*) e ECC (*Elliptic Curve Cryptography*), evoluiu para proteger dados, mas os algoritmos assimétricos são vulneráveis à computação quântica, que pode quebrar essas chaves mais rapidamente (Mavroeidis et al., 2018). Já a criptografia simétrica, como o AES (*Advanced Encryption Standard*), é mais resistente e pode ser reforçada com chaves maiores (Mavroeidis et al., 2018). O algoritmo de Shor (1994) compromete a segurança de sistemas criptográficos baseados em fatoração, como o RSA, enquanto o algoritmo de Grover (1996) acelera buscas, reduzindo o tempo necessário para quebrar criptografias simétricas, como o AES, que pode ser reforçado com chaves maiores.

A criptografia quântica, com técnicas como a distribuição de chaves quânticas (*QKD - Quantum Key Distribution*), oferece maior segurança, sublinhando a necessidade de desenvolver criptografias quântico-resistentes para mitigar ameaças futuras. Este trabalho discute essas vulnerabilidades e explora alternativas para garantir a segurança dos dados no cenário quântico.

MATERIAL E MÉTODOS

A pesquisa foi baseada na coleta de informações a partir de dados secundários obtidos de diversas fontes, como livros, artigos, teses e dissertações. Essas fontes foram selecionadas com o objetivo de investigar o estado atual das pesquisas em computação quântica:

a) Análise das Diferenças entre Computações Quântica e Clássica

A primeira etapa concentrou-se na comparação entre a computação quântica e a computação clássica, identificando algoritmos como SHA (*Secure Hash Algorithm*), ECDSA (*Elliptic Curve Digital Signature Algorithm*), ECDH (*Elliptic Curve Diffie-Hellman*), DSA (*Digital Signature Algorithm*) e RNG (*Random Number Generator*) com o foco em identificar como as propriedades únicas dos computadores quânticos, como sua alta eficiência no processamento de operações complexas, podem comprometer a segurança de dados criptografados por algoritmos clássicos.

b) Estágios de Desenvolvimento da Computação Quântica

Nesta etapa, foram examinados os principais avanços no desenvolvimento da computação quântica, abordando componentes e materiais utilizados, bem como os desafios técnicos na construção e manutenção desses sistemas em comparação com os computadores clássicos. Além disso, foram analisados estudos sobre os investimentos realizados e as potenciais aplicações dessa tecnologia na resolução de problemas complexos, tais como a técnica QRNG (*Quantum Random Number Generation*).

c) O Funcionamento da Criptografia Quântica

A investigação também abrangeu o funcionamento da criptografia quântica, explorando seus níveis superiores de segurança em comparação com a criptografia clássica e destacando as vulnerabilidades associadas às novas técnicas de decifragem desenvolvidas com o avanço da computação quântica.

d) A Criptografia Quântico-Resistente

Outra etapa da pesquisa focou-se no estudo da criptografia quântico-resistente, que surgiu em resposta aos desafios impostos pela computação quântica. Analisou-se o desenvolvimento de novas soluções que buscam proteger dados diante das técnicas quânticas de decifragem, além dos esforços para mitigar vulnerabilidades tanto em criptografias clássicas quanto nas novas criptografias quânticas.

e) Estado da Arte do Desenvolvimento de Criptografias Baseadas na Teoria Quântica

Por fim, foram analisados textos que fornecem um panorama das criptografias clássicas que ainda resistem aos ataques quânticos, tanto em sistemas assimétricos quanto simétricos. Além disso, foi avaliado o estágio atual de desenvolvimento de criptografias baseadas na teoria quântica, observando as tendências e os desafios enfrentados nessa área.

RESULTADOS E DISCUSSÃO

Após a pesquisa descrita na seção anterior, apresentam-se os resultados das pesquisas em computação quântica e suas principais diferenças em relação à computação clássica (Quadro 1). Os resultados indicam que a computação quântica, com sua alta eficiência no processamento e execução de operações complexas, apresenta uma ameaça potencial à segurança de dados protegidos por criptografias clássicas, que dependem dessas operações para manter sua robustez (Mavroeidis et al., 2018; Fernandez-Carames, 2020).

QUADRO 1. Principais diferenças entre o computador clássico e o quântico.

Atributo	Computador Clássico	Computador Quântico
Tipo de representação de dados	Bits (0 e 1)	Qubits (0, 1 e superposição)
Tipo de processamento	Bit a bit	Paralelismo quântico (operações complexas)
Estágio de Desenvolvimento	Tecnologia conhecida, componentes acessíveis	Tecnologia em desenvolvimento, componentes caros
Estabilidade	Estáveis em temperatura ambiente	Instáveis em temperatura ambiente (requer criogenia) Vulnerabilidade a múltiplas interferências externas
Algoritmos de criptografia / descriptografia relevantes	RSA, AES, SHA, ECDSA, ECDH e DSA RNG Força bruta e interceptação	QKD QRNG Algoritmo de Shor e Grover

Fonte: Os Autores

Apesar das limitações no desenvolvimento da computação quântica, principalmente devido à instabilidade dos componentes e materiais, há um crescente investimento nessa tecnologia, visando sua aplicação para resolver problemas complexos de forma mais eficiente (Mavroeidis et al., 2018; Jose et al., 2013). Em termos de segurança, a criptografia quântica, que utiliza os princípios da mecânica quântica para criptografar e descriptografar dados, promete maior segurança em comparação à criptografia clássica. No entanto, também introduz novas vulnerabilidades, como técnicas avançadas de decifragem.

Os resultados indicam que, em cenários futuros, as criptografias clássica e quântica provavelmente coexistirão, sendo usadas conforme a necessidade. Enquanto a descriptografia clássica utiliza métodos como a força bruta e a interceptação, a descriptografia quântica recorre aos algoritmos de Shor e Grover, que exploram o paralelismo quântico para quebrar chaves com mais eficiência (Portugal et al., 2012; Vedral, 2006).

Além disso, a criptografia quântico-resistente surgiu em resposta ao avanço da computação quântica, com o objetivo de proteger dados importantes contra novas técnicas de decifragem quântica. Pesquisadores como Mavroeidis *et al.* (2018) e Mattsson *et al.* (2021), identificaram vulnerabilidades em algoritmos criptográficos assimétricos baseados em fatoração de inteiros primos, como o **RSA** (*Rivest-Shamir-Adleman*)e o **DSA** *(Digital Signature Algorithm*), que são suscetíveis ao **algoritmo de Shor**. Por outro lado, os algoritmos simétricos, como AES e SHA, são menos vulneráveis e podem ser ajustados para resistir a ataques quânticos, como mostrado no Quadro 2. (Mavroeidis et al., 2018; Mattsson et al., 2021).

QUADRO 2. Impacto da computação quântica nos esquemas de criptografia.

Algoritmo Criptográfico	Tipo	Propósito	Impacto da Computação Quântica
AES-256, SHA-256, SHA-3	Chave simétrica	Criptografia, Funções de Hash	Seguro
RSA, ECDSA, ECDH	Chave pública	Assinaturas, troca de chave	Não é mais seguro
DSA (campo finito)	Chave pública	Assinaturas, troca de chave	Não é mais seguro

Fonte: Os Autores

Embora a criptografia quântica pura seja promissora, ela ainda enfrenta desafios. O consenso atual é de que essa tecnologia está em estágio prematuro e requer mais avanços antes de ser aplicada em larga escala. Além disso, o uso de técnicas híbridas, combinando sistemas clássicos e quânticos, também é visto como uma alternativa, embora ainda com muitas questões a serem resolvidas (Mattsson et al., 2021).

CONCLUSÕES

Este estudo demonstrou que a computação quântica representa uma ameaça significativa para as técnicas criptográficas atuais, especialmente aquelas baseadas em algoritmos clássicos que dependem de operações matemáticas complexas. Embora a aplicação imediata da computação quântica ainda enfrente limitações técnicas, o potencial de "quebrar" algoritmos amplamente utilizados já é suficiente para gerar preocupação na comunidade científica, incentivando o investimento em soluções preventivas.

Além disso, observou-se que a busca por novas soluções de criptografia, incluindo aquelas quântico-resistentes, está em pleno desenvolvimento, refletindo o esforço global para antecipar e mitigar futuras vulnerabilidades. A criptografia quântica, baseada em princípios da mecânica quântica, representa uma dessas alternativas promissoras, embora ainda enfrente desafios técnicos que precisam ser superados antes de uma aplicação em larga escala.

Portanto, a computação quântica se configura tanto como o futuro da segurança cibernética quanto como um potencial "fim" para a criptografia clássica, que precisará ser gradualmente substituída por métodos mais robustos e quântico-resistentes para garantir a proteção dos dados. Em vista disso, torna-se essencial continuar investindo em pesquisas que abordem não apenas as fragilidades da criptografia clássica, mas também as possíveis vulnerabilidades dos métodos emergentes, de forma a assegurar uma infraestrutura segura para o cenário tecnológico futuro.

CONTRIBUIÇÕES DOS AUTORES

Guilherme Gomes Zunta Camacho e Ronaldo Rossetti Dearo contribuíram com a conceituação e curadoria da coleta bibliográfica de dados. Vinicius Tiago de Santana e Diego Ribeiro Bastos foram responsáveis pela metodologia e condução da análise teórica. Guilherme Gomes Zunta Camacho e Ronaldo Rossetti Dearo colaboraram na redação e preparação do manuscrito original. Wendel Marcos dos Santos orientou o trabalho e foi responsável pela submissão. Todos os autores contribuíram com a redação, revisão e aprovaram a versão final do manuscrito submetido.

AGRADECIMENTOS

Os autores agradecem ao Instituto Federal de São Paulo (IFSP) pela oportunidade e suporte oferecidos durante a realização desta pesquisa, desenvolvida no âmbito da disciplina Metodologia de Pesquisa Científica, do curso Bacharelado em Sistemas da Informação (Campus São Paulo). Agradecemos também aos colegas de classe pelo apoio e troca de conhecimentos.

REFERÊNCIAS

BENIOFF, P. Quantum Mechanical Models of Turing Machines That Dissipate No Energy. **Physical Review Letters**, v. 48, n. 23, p. 1581–1585, 7 jun. 1982.

DEUTSCH, D. Quantum theory, the Church–Turing principle and the universal quantum computer. **Proceedings Of The Royal Society Of London. A. Mathematical And Physical Sciences**, [S.L.], v. 400, n. 1818, p. 97-117, 8 jul. 1985. The Royal Society. http://dx.doi.org/10.1098/rspa.1985.0070.

FERNANDEZ-CARAMES, T. M. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. **IEEE Internet of Things Journal**, v. 7, n. 7, p. 6457–6480, jul. 2020.

FEYNMAN, R P. Simulating physics with computers. **International Journal Of Theoretical Physics,** v. 21, n. 6-7, p. 467-488, jun. 1982. Springer Science and Business Media LLC. http://dx.doi.org/10.1007/bf02650179..

MATTSSON, J. P; SMEETS, B; THORMARKER, Quantum-Resistant Cryptography. **Arxiv**, 2021. ArXiv. http://dx.doi.org/10.48550/ARXIV.2112.00399.

MAVROEIDIS, V; VISHI, K; ZYCH, M. D.; JØSANG, A. The Impact of Quantum Computing on Present Cryptography. **Arxiv**, [S.L.], p. 1-12, 2018. ArXiv. http://dx.doi.org/10.48550/ARXIV.1804.00200.

PORTUGAL, R. et al. Uma introdução à computação quântica. São Carlos: SBMAC, 2012.

SHOR, P. W. **Algorithms for quantum computation: discrete logarithms and factoring**. Proceedings 35th Annual Symposium on Foundations of Computer Science. **Anais**... Em: 35TH ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE. Santa Fe, NM, USA: IEEE Comput. Soc. Press, 1994. Disponível em: <http://ieeexplore.ieee.org/document/365700/>. Acesso em: 30 jul. 2024

VEDRAL, V. Introduction to quantum information science. New York: Oxford University Press, 2006.