A AMEAÇA DA QUEBRA DE CRIPTOGRAFIA POR MEIO DA COMPUTAÇÃO QUÂNTICA: um estudo de caso no setor financeiro empresarial

Matheus Vilela Diniz Maia[1]*

Prof. Esp. Rafael Hungaro Cabral[2]*

RESUMO

Este trabalho aborda a ameaça da quebra de criptografia por meio da computação quântica e seu impacto na segurança da informação no contexto empresarial. A justificativa para essa abordagem se deve ao avanço tecnológico da computação quântica, que pode comprometer a segurança da informação e colocar em risco dados confidenciais, como informações financeiras, estratégias de negócios e informações pessoais de clientes. O objetivo deste trabalho é discutir as possíveis soluções e estratégias de segurança da informação utilizadas para lidar com a ameaça da quebra de criptografia em uma empresa do setor financeiro. A metodologia empregada será o estudo de caso. O estudo evidenciou que a computação quântica e suas ameaças são negligenciadas pela empresa estudada, mostrando que a segurança da informação deve ser uma preocupação crítica para empresas e organizações. Portanto, é fundamental que as empresas invistam em medidas de segurança da informação robustas e atualizadas, além de ficarem atentas às tendências tecnológicas e às vulnerabilidades que possam afetar seus sistemas de segurança.

Palavras-chave: criptografia; computação quântica; segurança da informação; quebra de criptografia; estudo de caso.

[1]*Aluno de Sistemas de Informação - UNIS. matheus.maia@unis.edu.br.

[2]*Prof. Esp. Rafael Hungaro Cabral. Graduado em Ciência da Computação pelo Centro Universitário do Sul de Minas (2015). Especialista em Engenharia de Sistemas de Informação pelo Centro Federal de Educação Tecnológica de Minas Gerais (2018). Atualmente é professor titular do Centro Universitário do Sul de Minas e analista de processos acadêmicos do Centro Universitário do Sul de Minas.

1 INTRODUÇÃO

A criptografia emerge como pilar fundamental para a segurança da informação no contexto empresarial, assegurando a integridade e confidencialidade de dados cruciais. Contudo, a evolução da computação quântica pode potencialmente comprometer tal segurança. O risco de comprometimento da criptografia via computação quântica constitui uma inquietação crescente para o tecido empresarial, o qual deve compreender integralmente as ramificações desta ameaça.

Diversos domínios, desde comunicações online até a salvaguarda de informações médicas e financeiras, empregam criptografia. Givens (2013) destaca a centralidade da criptografia na era contemporânea, com inovações contínuas em resposta a desafios emergentes. Curran (2018) ressalta que, embora a computação quântica ainda esteja em maturação, avança a passos largos, solidificando-se como uma ameaça iminente.

Até a presente data, não se tem registro de comprometimentos criptográficos via computação quântica, contudo, outras modalidades de invasões são frequentemente registradas, sendo muitas vezes mantidas em sigilo pelas entidades afetadas, para mitigação de danos reputacionais (Mosca, 2018). A mesma fonte também reforça a perspectiva de que a ameaça quântica é palpável a médio prazo, tornando a proteção de dados um imperativo.

A potencial vulnerabilidade dos sistemas criptográficos diante da computação quântica é reconhecida por especialistas, como Gueron (2018). Para contrapor essa ameaça emergente, Aranha et al. (2021) sugerem a criptografia pós-quântica como uma possível solução. Contudo, Peikert (2018) lembra que muitos obstáculos ainda precisam ser superados antes de sua ampla adoção.

A grande maioria dos sistemas de proteção de dados corporativos se apoia em criptografia de chave pública, como a criptografia de chave pública e a criptografia de curva elíptica, que apresentam robustez diante de ataques tradicionais. Porém, a vulnerabilidade frente à computação quântica é real e coloca em xeque a segurança de dados cruciais.

Assim, este artigo postula que a ascensão da computação quântica representa uma revolução para a segurança da informação empresarial. Surge, portanto, a necessidade de desenvolver e adotar novos algoritmos criptográficos resistentes a tais avanços.

No âmbito deste estudo, foram estabelecidos cinco objetivos específicos com o propósito de analisar as implicações da computação quântica na segurança da criptografia empresarial. Os objetivos delineados incluem a investigação das limitações da criptografia atual em face da computação quântica, a identificação das informações empresariais mais suscetíveis a ataques quânticos e suas consequências para as organizações, a análise das técnicas de criptografia quântica disponíveis e sua aplicabilidade no contexto empresarial, a proposição de estratégias que as empresas podem adotar para salvaguardar suas informações contra potenciais quebras de criptografia por meio da computação quântica, e a avaliação das implicações financeiras e operacionais associadas à adoção de novas técnicas de criptografia no ambiente empresarial.

Para tal, foi realizado um estudo de caso em uma empresa do setor financeiro para avaliar as estratégias de segurança da informação utilizadas para lidar com a ameaça da quebra de criptografia em geral e a possível quebra por meio da computação quântica. Nesse contexto, serão discutidas as implicações dessa ameaça para as empresas e as medidas que podem ser tomadas para reduzir este impacto, permitindo que as organizações se preparem adequadamente para os desafios que virão.

2 A CRIPTOGRAFIA

Criptografia é a arte e ciência de codificar informações para garantir que apenas o destinatário pretendido possa decodificar e entender. Ela serve como uma das principais ferramentas para a segurança da informação, protegendo dados de acessos não autorizados ou alterações maliciosas. A criptografia é fundamental em diversas aplicações modernas, como comércio eletrônico, comunicações seguras e autenticação de identidade. Além de garantir a confidencialidade, a criptografia também pode prover autenticidade, integridade e não repúdio às mensagens.

2.1 Histórico

A criptografia é uma técnica antiga que remonta a pelo menos 4.000 anos atrás, quando os antigos egípcios usavam hieróglifos para criptografar mensagens. Desde então, muitas civilizações têm usado técnicas de criptografia para proteger a privacidade e

segurança de suas comunicações, como os gregos, romanos, chineses e árabes. (Simon, 2000).

Entre os pioneiros da criptografia moderna, destaca-se Kerckhoffs, que desenvolveu o "princípio de Kerckhoffs", um conjunto de regras para projetar sistemas de criptografia seguros. Como afirmado por Stinson (2019), o princípio de Kerckhoffs diz que um sistema criptográfico deve ser seguro, mesmo que tudo sobre o sistema, exceto a chave, seja conhecido pelos atacantes.

Durante a Primeira Guerra Mundial, a criptografia foi utilizada de forma intensa pelas forças militares. Nesse período, um dos mais conhecidos sistemas de criptografia foi o cifrador ADFGX, que foi usado pelo exército alemão para proteger suas mensagens. De acordo com Kahn (1996), o cifrador ADFGX foi quebrado pelos franceses, que conseguiram decifrar as mensagens criptografadas e obter informações estratégicas importantes.

Já na Segunda Guerra Mundial, a criptografia tornou-se um campo de batalha crucial, com destaque para o trabalho de decodificação realizado pela equipe de criptografia britânica em Bletchley Park. Segundo Kahn (1996), a equipe liderada por Alan Turing foi capaz de decifrar as mensagens criptografadas do código Enigma usado pelos nazistas, o que contribuiu para o sucesso dos Aliados na guerra.

2.2 Tipos de criptografia

Shor (1994) revelou que desafios previamente inabordáveis pelos computadores tradicionais, tal qual a fatoração por números primos (base criptografia moderna), poderiam ser solucionados pelos computadores quânticos.

De acordo com Singh (2000), alguns dos principais tipos de criptografia incluem:

- Criptografia de Substituição: Um tipo de criptografia em que cada letra ou símbolo da mensagem original é substituído por outro símbolo, conforme uma tabela predefinida. A Cifra de César é um exemplo de criptografia de substituição simples.
- Criptografia de Transposição: Um tipo de criptografia em que as letras ou símbolos da mensagem original são reorganizados de acordo com uma ordem específica. A cifra de coluna é um exemplo de criptografia de transposição.

- Criptografia de Chave Simétrica: Um método criptográfico em que uma única chave é usada tanto para cifrar quanto para decifrar a mensagem. A criptografia DES e AES são exemplos de algoritmos de chave simétrica.
- Criptografia de Chave Pública: Um método criptográfico que envolve um par de chaves, uma pública e outra privada, para realizar a criptografia e descriptografia de mensagens. RSA (Rivest-Shamir-Adleman) e Diffie-Hellman são exemplos de algoritmos de criptografia de chave pública.
- Criptografía de Curva Elíptica (CEC): Um tipo de criptografía de chave pública que usa curvas elípticas em vez de números inteiros para gerar chaves. É uma forma mais segura de criptografia de chave pública em comparação com a criptografia RSA.
- Criptografia Quântica: Um método de criptografia que se baseia nas características da mecânica quântica para assegurar a proteção das mensagens. É tida como uma das técnicas mais confiáveis de codificação.

Esses são apenas alguns exemplos de tipos de criptografia, e existem muitos outros algoritmos e abordagens disponíveis. A escolha do método de criptografia mais adequado para uma determinada aplicação depende dos requisitos de segurança, desempenho e compatibilidade com outras tecnologias.

2.3 Princípios do funcionamento de um computador quântico

Os computadores quânticos representam um avanço significativo na capacidade de processamento de informações, explorando os princípios da mecânica quântica para realizar cálculos complexos de forma mais eficiente do que os computadores clássicos tradicionais. Enquanto os computadores clássicos usam bits para representar informações como 0s e 1s, os computadores quânticos usam qubits, que podem estar em estados superpostos, permitindo um processamento paralelo massivamente escalável (Feynman, 1982).

O funcionamento de um computador quântico baseia-se em alguns princípios fundamentais:

- Superposição: Diferentemente dos bits clássicos, que podem ser apenas 0 ou 1, os qubits podem estar em uma superposição desses estados. Isso significa que um qubit pode existir em uma combinação linear de 0 e 1 ao mesmo tempo, permitindo que um

computador quântico realize várias operações simultaneamente (Nielsen & Chuang, 2010).

- Emaranhamento: Os qubits podem estar interconectados, o que implica que a condição de um qubit está intimamente relacionada à condição do outro, independentemente da distância que os separa. Isso possibilita a correlação instantânea das informações entre qubits, o que pode ser explorado para realizar operações complexas (Einstein et al., 1935).
- Portas Quânticas: Assim como os circuitos lógicos em computadores clássicos, os computadores quânticos usam portas quânticas para realizar operações sobre os qubits. Essas portas quânticas manipulam os estados de superposição e emaranhamento dos qubits para executar cálculos (Nielsen & Chuang, 2010).
- Medição Quântica: Ao medir um qubit, seu estado de superposição colapsa em um estado clássico definido, ou seja, 0 ou 1. A medição é uma parte crítica do processo, pois é o momento em que os resultados quânticos são convertidos em resultados clássicos compreensíveis (Nielsen & Chuang, 2010).
- Decoerência: Um desafio significativo em computação quântica é a decoerência, que resulta da interação dos qubits com o ambiente. O ambiente pode causar a perda de informações quânticas, levando a erros nos cálculos. Portanto, técnicas de correção de erros quânticos são essenciais para manter a integridade dos resultados (Preskill, 1998).

Em Suma, um computador quântico aproveita os princípios da superposição e emaranhamento para executar cálculos complexos de maneira paralela e eficiente. Tal abordagem promete revolucionar a computação em várias áreas, como criptografia, otimização, simulações moleculares e inteligência artificial, mas também apresenta desafios técnicos consideráveis que estão sendo abordados por pesquisadores em todo o mundo.

2.4 A quebra da criptografia tradicional pelo computador quântico

A emergente computação quântica, como destacado por Stinson e Paterson (2018), possui a capacidade intrínseca de comprometer grande parte dos sistemas criptográficos hoje vigentes. Tal potencial decorre da habilidade dos computadores quânticos de efetuarem

operações em simultaneidade, desvendando algoritmos criptográficos em tempos exponencialmente mais curtos comparados aos computadores convencionais.

O avanço em pesquisas como a da IBM, ressaltado por Schneier (2020), exemplifica um progresso significativo na trajetória da computação quântica, possibilitando a execução de operações de alta complexidade em prazos muito mais reduzidos. Isso inaugura horizontes promissores, sobretudo para campos como a criptografia e inteligência artificial.

Conforme Dodt (2021), a emergência da computação quântica introduz alterações significativas no campo da computação, especialmente quando se considera o Algoritmo de Shor. Este algoritmo, fundamentado na mecânica quântica, facilita a decomposição de números em seus componentes primários (números primos), tarefa que é notavelmente desafiadora para computadores convencionais, particularmente com números de grande magnitude. Esta inovação é de suma importância, pois muitos algoritmos de criptografia assimétrica, como o RSA, baseiam-se na premissa de que a fatoração de grandes números inteiros é uma tarefa computacionalmente desafiadora.

Não apenas sistemas criptográficos, mas também sistemas de autenticação encontram-se vulneráveis perante a computação quântica, conforme indicam Ekert e Renner (2014). Setores específicos, como o financeiro, poderão sentir ainda mais intensamente as repercussões da computação quântica na segurança da informação, conforme delineado por Gisin e Thew (2007). A essência de muitos sistemas adotados nesse segmento é sustentada por algoritmos criptográficos, fundamentais para assegurar a integridade das transações financeiras.

Aranha et al. (2021) realçam que, diante deste cenário, a transição para a criptografia pós-quântica emerge como uma alternativa viável. Ao lado dela, protocolos quânticos, destacados por Scarani e Kurtsiefer (2020), apresentam-se como soluções possíveis, baseando-se nas características peculiares da física quântica.

O NIST (2021) enfatiza o iminente advento da era quântica e os desafios que ela representa para a segurança da informação. Nessa conjuntura, torna-se vital que empresas aproximem laços com instituições acadêmicas e centros de pesquisa, conforme sugere Stebila (2020), visando acesso contínuo às inovações e novas perspectivas sobre computação quântica.

Schaffner et al. (2019) também sublinham a imperatividade da capacitação contínua dos profissionais de segurança da informação. Esse investimento no capital humano é crucial para garantir a preparação adequada das empresas frente aos desafios emergentes.

Em síntese, o perigo que a computação quântica representa para a criptografia não é restrito apenas ao mundo corporativo, mas se estende a governos e à sociedade global. A colaboração entre diversos stakeholders torna-se, assim, uma estratégia indispensável para priorizar e fortalecer a segurança da informação.

3 MATERIAL E MÉTODOS

Para atingir esse objetivo do presente artigo, foi utilizada a metodologia de estudo de caso. Nesta seção, apresentam-se os materiais e métodos empregados no desenvolvimento da pesquisa. O objetivo do estudo foi avaliar as estratégias de segurança da informação empregadas pela organização para enfrentar a ameaça potencial da quebra de criptografia, incluindo a que poderia surgir devido à computação quântica.

Foi escolhida para o estudo uma empresa atuante no ramo financeiro de médio porte, localizada em Curitiba - PR, que oferece uma plataforma unificada de pagamentos para outras empresas. A escolha dessa empresa baseou-se em sua relevância no mercado e na disponibilidade de informações necessárias para análise. Por questões de confidencialidade, o nome da empresa nem de seus participantes será revelado neste estudo.

O estudo foi realizado em uma instituição financeira que lida com informações confidenciais e sensíveis de seus clientes e transações. O foco foi examinar as estratégias de segurança da informação implementadas pela empresa para proteger seus dados contra possíveis ameaças à criptografia, incluindo os impactos potenciais da computação quântica.

3.1 Metodologia

A metodologia empregada abrangeu as seguintes etapas:

3.1.1 Coleta de Dados

Para compreender as estratégias de segurança da informação adotadas pela empresa, foram utilizadas diversas abordagens de coleta de dados:

Formulário: Foi disponibilizado um formulário eletrônico (APÊNDICE A) contendo perguntas relacionadas às estratégias de segurança da informação da organização. O formulário foi distribuído entre os funcionários da área de tecnologia da informação para coletar perspectivas adicionais.

Análise Documental: Políticas de segurança da informação, relatórios de incidentes de segurança e outros documentos foram analisados para compreender as abordagens existentes em relação à proteção de dados sensíveis.

3.1.2 Análise de Dados

Os dados coletados foram submetidos a uma análise mista, combinando abordagens quantitativas e qualitativas. As respostas das entrevistas e do formulário foram codificadas para identificar padrões e tendências, enquanto a análise documental ajudou a contextualizar as práticas de segurança em vigor.

3.1.3 Pesquisas Bibliográficas

Foram realizadas pesquisas bibliográficas em fontes diversas, como livros, artigos científicos, periódicos e documentos técnicos. Essas pesquisas visam a obtenção de conhecimentos aprofundados sobre técnicas de criptografia, computação quântica e segurança da informação, embasando a análise do estudo de caso.

4 RESULTADO E DISCUSSÃO

Com a realização do estudo de campo e análise detalhada dos dados coletados junto aos 7 profissionais da área de tecnologia da informação da empresa em estudo, chegou-se a conclusões pertinentes sobre a atual postura e consciência da organização em relação à ameaça emergente da computação quântica e suas implicações na segurança da informação.

A pesquisa revelou que 57,1% dos profissionais avaliam a eficácia das estratégias de criptografia atualmente implementadas como boas e 42,9% como regulares. O estudo também revelou que cerca de 28,6% dos profissionais não estavam cientes das implicações da computação quântica na quebra de criptografia convencional e 71,4% não acreditam que a empresa esteja preparada para os desafios da quebra da criptografia convencional pela computação quântica. Essa lacuna de conhecimento sugere uma necessidade imediata de

educação e treinamento direcionados.

Outro indicador merecedor de uma análise é a consciência e familiaridade dos profissionais com as políticas específicas da empresa para responder a possíveis violações de segurança. Enquanto 71,4% dos respondentes afirmaram conhecer e estar cientes de tais políticas, uma parcela considerável de 14,3% confirmou a existência das políticas, mas não as conhece, e outro igual percentual de 14,3% nem mesmo sabe se tais políticas existem. Isso evidencia uma possível lacuna na comunicação e treinamento interno, fundamental para responder adequadamente a incidentes de segurança. A importância da atualização constante das estratégias de segurança foi amplamente reconhecida como um pilar fundamental para o sucesso e resiliência da empresa.

A organização emprega uma abordagem multifacetada para garantir a proteção dos dados. A criptografia de dados, tanto em repouso quanto em trânsito, é central para a estratégia, assegurando a proteção integral das informações financeiras e dos dados dos clientes. Além disso, a criptografia de chave pública é utilizada para autenticação, enquanto a criptografia de ponta a ponta é aplicada em todas as comunicações com os clientes. A organização também se beneficia do uso de VPNs criptografadas para comunicações interescritórios e da aplicação de criptografia robusta em seus sistemas e servidores. Esta abordagem integrada, que combina técnicas como criptografia simétrica, assimétrica (RSA) e de curva elíptica, visa garantir que os dados sejam inacessíveis e ininteligíveis para partes não autorizadas.

Embora a empresa utilize padrões de criptografia reconhecidos e respeitados, como a criptografia de chave pública e a de curva elíptica, a discussão sobre a implementação de técnicas de criptografia resistente à computação quântica ainda é incipiente. É alarmante notar que todos os profissionais relevantes no estudo expressaram preocupações sobre a robustez das estratégias de criptografia atuais diante dos avanços da computação quântica.

No que tange à autenticação e controle de acesso, a empresa demonstra uma abordagem assertiva. Os protocolos adotados, como Autenticação Multifatorial (MFA), Listas de Controle de Acesso (ACLs), Gestão de Identidade e Acesso (IAM), e Criptografia em VPNs, evidenciam um compromisso com a proteção de dados e informações vitais. As ameaças percebidas também variaram de ataques sofisticados, como Ransomware e Ataques DDoS, até preocupações mais simples, como compartilhamento de senhas entre colegas.

Diante dos resultados, fica evidente que, enquanto a empresa adota medidas consistentes de segurança da informação, ainda há lacunas significativas em sua preparação para enfrentar as ameaças da computação quântica. A ameaça da quebra de criptografia por computação quântica é real e iminente, e as empresas precisam reconhecer e se preparar para esse desafio.

Além disso, a pesquisa também evidenciou oportunidades. A adoção precoce de técnicas de criptografia pós-quântica pode não apenas proteger a empresa contra futuras ameaças, mas também posicionar a organização como líder em segurança da informação, proporcionando vantagem competitiva no mercado.

5 CONSIDERAÇÕES FINAIS

Ao longo deste estudo, a potencial ameaça representada pela quebra de criptografia através da computação quântica no setor empresarial foi abordada de forma aprofundada. Os avanços da computação quântica, embora promissores em diversos campos da ciência e tecnologia, trazem consigo desafios significativos no âmbito da segurança da informação.

A criptografia, historicamente, tem sido a linha de defesa primária para assegurar a confidencialidade, integridade e autenticidade das informações. Entretanto, como evidenciado, os métodos criptográficos convencionais, como o RSA e o CEC, que são considerados atualmente seguros contra-ataques clássicos, estão em risco potencial diante da capacidade computacional quântica.

O estudo de caso da empresa no setor financeiro revelou uma certa negligência em relação às ameaças potenciais apresentadas pela computação quântica. Esta conclusão reforça a necessidade urgente de uma maior conscientização sobre a importância da preparação para um futuro em que a computação quântica pode ser uma realidade acessível.

Dada a iminência desta revolução tecnológica, a implementação de soluções de criptografia pós-quântica se torna imperativa. Essas soluções, projetadas especificamente para resistir a ataques quânticos, devem ser consideradas por empresas que desejam garantir a segurança de suas informações a longo prazo.

Além disso, é crucial que as empresas não apenas invistam em tecnologia, mas também em formação e conscientização. O capital humano, por meio da capacitação e do

conhecimento das ameaças emergentes, é um componente essencial para fortalecer as estratégias de segurança da informação.

Em resumo, a computação quântica, apesar de seus benefícios, apresenta desafios que necessitam ser enfrentados com seriedade e proatividade pelas organizações. A segurança da informação não deve ser vista apenas como uma necessidade técnica, mas como uma estratégia integrada que envolve tecnologia, processos e pessoas.

O futuro da criptografia está em constante evolução e, assim como a tecnologia avança, as ameaças também se adaptam. Portanto, é de extrema importância que as empresas estejam sempre um passo à frente, antecipando riscos e preparando-se para um cenário em que a segurança da informação é mais crítica do que nunca.

THE THREAT OF CRYPTOGRAPHY BREAKING THROUGH QUANTUM COMPUTING: a case study in the financial business sector

ABSTRACT

This work addresses the threat of cryptography breaking through quantum computing and its impact on information security in the business context. The justification for this approach is due to the technological advancement of quantum computing, which can compromise information security and put confidential data at risk, such as financial information, business strategies and personal customer information. The objective of this paper is to discuss the possible solutions and information security strategies used to deal with the threat of cryptography breach in a financial sector company. The methodology used will be the case study. The study showed that quantum computing and its threats are neglected by the studied company, showing that information security must be a critical concern for companies and organizations. Therefore, it is essential that companies invest in robust and up-to-date information security measures, in addition to being aware of technological trends and vulnerabilities that may affect their security systems.

Keywords: cryptography; quantum computing; information security; encryption breaking; case study.

APÊNDICE A: Formulário Eletrônico de Perguntas

As seguintes perguntas foram utilizadas durante as entrevistas semiestruturadas realizadas com profissionais de tecnologia da informação da empresa:

1. Como a empresa aborda a proteção de dados confidenciais e sensíveis dos clientes?
2. Quais são as estratégias de criptografia atualmente empregadas pela organização?
3. A equipe de segurança da informação está ciente das ameaças potenciais da computação quântica à criptografia convencional?
4. Como a organização acompanha e se adapta às mudanças tecnológicas que podem afetar a segurança da informação?
5. Quais práticas de segurança da informação você considera cruciais para proteger os dados da empresa?
6. Como você avalia a eficácia das estratégias de criptografia atualmente implementadas?
7. Você já participou de treinamentos ou workshops relacionados à conscientização sobre segurança da informação?
8. Na sua opinião, quais são as principais ameaças à segurança da informação que a organização enfrenta?
9. Você está ciente das implicações da computação quântica na quebra de criptografia convencional?
10. Quais medidas de controle de acesso são aplicadas em sua área de atuação para garantir a confidencialidade dos dados?
11. A empresa possui políticas específicas para responder a possíveis violações de segurança? Você conhece essas políticas?
12. Como você percebe a importância da atualização constante das estratégias de segurança diante das mudanças tecnológicas?
13. Quais sugestões você teria para aprimorar as medidas de segurança da informação da organização?
14. A empresa considera a adoção de técnicas de criptografia pós-quântica em suas estratégias de segurança?

REFERÊNCIAS

BERNSTEIN, D. J. (2017). **Post-quantum cryptography. Nature, 549(7671), 188-190.**

BERNSTEIN, D., EKERT, A., & ZEILINGER, A. (2021). **The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation. Springer.**

CHEN, L., LUO, M., ZHANG, J., & ZHAO, Y. (2019). **Towards Post-quantum Cryptography on Lightweight Devices: A Survey. Journal of Computer Science and Technology, 34(1), 9-26.**

CURRAN, K. (2018). **The Quantum Computing Apocalypse Is Imminent. Forbes.**

DOT, CLÁUDIO. (2021). **Computação Quântica e seus efeitos na criptografia.** Disponível em: https://www.securityreport.com.br/computacao-quantica-e-seus-efeitos-na-criptografia/.Acesso em:12.set.2023

EINSTEIN, A., PODOLSKY, B., & ROSEN, N. (1935). **Can Quantum-Mechanical Description of Physical Reality be Considered Complete? Physical Review, 47(10), 777-780.**

FEYNMAN, R. P. (1982). **Simulating Physics with Computers. International Journal of Theoretical Physics, 21(6/7), 467-488.**

GIVENS, **John R. The ABCs of Encryption: Cryptography Demystified. Apress, 2013.**

GROVER, L. K. (1996). **A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 212-219.**

GUERON, S. (2018). **Post-quantum cryptography: A brief introduction. NIST.**

KAHN, David. **The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner, 1996.**

MOSCA, M. (2018). **Quantum Computing and Cryptography. In K. D. Kammeyer & K. M. Martin (Eds.), Cybersecurity: A practical guide to the law of cybersecurity (pp. 77-94). Edward Elgar Publishing.**

National Institute of Standards and Technology (NIST). (2021). **Post-Quantum Cryptography. Recuperado de Post-Quantum Cryptography | NIST.**

NIELSEN, M.A. and CHUANG, I.L. (2000). **Quantum Computation and Quantum Information. Cambridge University Press.**

NIELSEN, M. A., & CHUANG, I. L. (2010). **Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press.**

PEIKERT, C. (2018). **A Decade of Lattice Cryptography. In S. Maitra & S. Sarkar (Eds.), Progress in Cryptology – INDOCRYPT 2018 (pp. 27-53). Springer. Executable Counterexamples in Software Model Checking | SpringerLink.**

PRESKILL, J. (1998). **Quantum Computation: Lecture Notes (Caltech).**

SCHAFFNER, C., TERZAKIS, G., & VAUDENAY, S. (2019). **Quantum-safe cryptography: from theory to practice. Springer International Publishing.**

SCHNEIER, B. (2015). **Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.**

SCHNEIER, B. (2020). **IBM's Quantum Computer May Not Change the World, But It Matters Anyway. Disponível em: https://newsroom.ibm.com/2020-01-16-The-Qua-n-tum-Computing-Era-Is-Here-Why-It-Matters-And-How-It-May-Change-Our-World.**

SHOR, P. W. (1994). **Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124-134.**

SINGH, Simon (2000). **The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Nova York: Anchor, 2000.**

STINSON, Douglas R. **Cryptography: Theory and Practice. CRC Press, 2019.**

STEBILA, D. (2020). **Quantum-Safe Cryptography: Understanding, Adapting, and Deploying New Security Solutions. O'Reilly Media, Inc.**

U.S. Department of Commerce. (2019). **Information Security and Privacy Advisory Board. Report on Post-Quantum Cryptography.**

WANG, J., Wu, X., & Li, C. (2020). **A survey of post-quantum cryptography. Journal of Information Security and Applications, 50, 102454.**

WIESNER, S. (1983). **Conjugate Coding. SIGACT News, 15(1), 78-88.**

YAO, A. C. (1979). **Some complexity questions related to distributive computing. Proceedings of the eleventh annual ACM symposium on Theory of computing, 209-213.**

ZALKA, C. (1998). **Grover's quantum searching algorithm is optimal. Physical review A, 60(4), 2746.**

ZHANG, F., & ZHANG, Y. (2020). **Survey on Cryptography in the Quantum Computing Era. IEEE Access, 8, 152853-152873.**