

**IMPACTOS DA COMPUTAÇÃO QUÂNTICA NA SEGURANÇA CIBERNÉTICA: UMA ANÁLISE DAS
VULNERABILIDADES E SOLUÇÕES**

Universidade Presbiteriana Mackenzie

Coordenadoria de Fomento à Pesquisa - Pró-Reitoria de Pesquisa e Pós-Graduação

Kainan de Souza Honda ¹

Apoio: Escolher um item.

Marcelo Teixeira de Azevedo ²

FCI - Faculdade de Computação e Informática ¹

FCI - Faculdade de Computação e Informática ²

<10428052@mackenzista.com.br>

<2018067@mackenzie.br>

RESUMO

A computação quântica emerge como uma tecnologia disruptiva com potencial para comprometer os alicerces da segurança cibernética contemporânea. Algoritmos criptográficos amplamente utilizados, como RSA e ECDSA, que garantem a confidencialidade e integridade de dados em transações financeiras, sistemas de saúde e comunicações governamentais, tornam-se vulneráveis ante o poder de processamento quântico, particularmente devido ao algoritmo de Shor. Este estudo, realizado através de uma metodologia qualitativa de revisão bibliográfica do Estado da Arte, tem como objetivo analisar os impactos da computação quântica na segurança cibernética, investigando as vulnerabilidades criadas e as soluções propostas pela criptografia pós-quântica (PQC). Os resultados demonstram que setores com infraestrutura de longa duração, como financeiro e saúde, encontram-se em risco crítico, não apenas por ameaças futuras, mas também pelo risco iminente de ataques do tipo "Colha Agora, Decifre Depois" (Harvest Now, Decrypt Later). A análise comparativa dos algoritmos pós-quânticos padronizados pelo NIST, como Kyber e Dilithium, revela que, embora tecnologicamente viáveis, sua adoção esbarra na falta de planejamento estratégico das organizações. Conclui-se que a transição para a era pós-quântica é urgente e requer um esforço coordenado, fundamentado em diretrizes claras que orientem a migração segura e gradual dos sistemas criptográficos atuais.

Palavras-chave: Computação Quântica; Segurança Cibernética; Criptografia Pós-Quântica; Algoritmo de Shor; Vulnerabilidades.

ABSTRACT

Quantum computing emerges as a disruptive technology with the potential to compromise the foundations of contemporary cybersecurity. Widely used cryptographic algorithms, such as RSA and ECDSA, which guarantee the confidentiality and integrity of data in financial transactions, healthcare systems, and government communications, become vulnerable to quantum processing power, particularly due to Shor's algorithm. This study, conducted through a qualitative methodology of bibliographic review of the State of the Art, aims to analyze the impacts of quantum computing on cybersecurity, investigating the vulnerabilities created and the solutions proposed by post-quantum cryptography (PQC). The results demonstrate that sectors with long-lasting infrastructure, such as finance and healthcare, are at critical risk, not only from future threats but also from the imminent risk of "Harvest Now, Decrypt Later" attacks. The comparative analysis of post-quantum algorithms standardized by

NIST, such as Kyber and Dilithium, reveals that, although technologically viable, their adoption is hindered by a lack of strategic planning by organizations. It is concluded that the transition to the post-quantum era is urgent and requires a coordinated effort, based on clear guidelines to guide the secure and gradual migration of current cryptographic systems.

Keywords: Quantum Computing; Cybersecurity; Post-Quantum Cryptography; Shor's Algorithm; Vulnerabilities.

1. INTRODUÇÃO

A segurança cibernética enfrenta um momento crítico diante do avanço de ataques digitais cada vez mais sofisticados. Segundo o Cost of a Data Breach Report 2023 da IBM Security, o prejuízo médio por incidente de segurança atingiu US\$4,45 milhões, valor mais alto já registrado, com um aumento expressivo de 15% em relação a 2020 (IBM, 2023). Esse cenário se agrava com o surgimento de novas modalidades de crimes cibernéticos, como ransomware¹ direcionado, phishing² e exploração de vulnerabilidades em sistemas criptográficos tradicionais exigem soluções inovadoras para proteger dados sensíveis (ENISA, 2023).

Nesse contexto, a computação quântica se apresenta como uma tecnologia disruptiva com o potencial para redefinir os paradigmas da segurança digital. Enquanto ameaça os sistemas criptográficos atuais, a mesma também oferece novas possibilidades para proteção de informações. Este estudo, desenvolvido no âmbito de uma Iniciação Científica, busca analisar esse duplo impacto, investigando tanto as vulnerabilidades expostas pelos avanços quânticos quanto as soluções emergentes na área de criptografia pós-quântica. A pesquisa se justifica pela urgência em compreender essas transformações, especialmente considerando que instituições como o NIST – National Institute of Standards and Technology – já iniciaram processos de padronização de novos algoritmos de segurança (NIST, 2023). Portanto, este estudo propõe mapear os riscos e explorar abordagens inovadoras para garantir a segurança dos dados na era pós-quântica.

1.1 FUNDAMENTAÇÃO TEÓRICA

1.1.1 Computação Quântica: Princípios e Funcionamento

A computação quântica difere radicalmente da clássica ao operar com **qubits** (quantum bits), que exploram propriedades da mecânica quântica:

- **Superposição:** Um qubit pode representar 0, 1 ou ambos simultaneamente (estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, onde α e β são amplitudes de

¹ É uma forma de sequestrar dados ou dispositivos da vítima, criptografando arquivos e impedindo o acesso aos mesmos.

² Crime cibernético no qual os criminosos tentam obter informações confidenciais, como senhas, números de cartão de crédito, informações bancárias ou outros dados pessoais, fingindo ser uma entidade.

probabilidade). Isso permite processamento paralelo massivo (ABRAMS; LLOYD, 1998).

- **Emaranhamento:** Qubits podem ser correlacionados mesmo à distância (estado "entangled"), permitindo operações coordenadas sem comunicação clássica (EINSTEIN et al., 1935).
- **Interferência:** As amplitudes de probabilidade podem interferir construtiva ou destrutivamente, otimizando soluções (DEUTSCH, 1989).

Aplicações Críticas:

- **Algoritmo de Shor (1994):** Fatoração de números grandes em tempo polinomial, quebrando RSA.
- **Algoritmo de Grover (1996):** Busca em bancos de dados não estruturados com aceleração quadrática, afetando AES-128.

1.1.2 Criptografia Pós-Quântica

A criptografia pós-quântica refere-se a algoritmos resistentes a ataques quânticos, baseados em problemas matemáticos considerados difíceis mesmo para computadores quânticos. Entre as principais abordagens estão:

- **Criptografia baseada em reticulados (Lattice-based):** Considerada uma das mais promissoras pelo NIST (PEIKERT, 2016).
- **Criptografia baseada em códigos (Code-based):** Utiliza a complexidade da decodificação de códigos de erro (MCELIECE, 1978).
- **Esquemas multivariados e baseados em hash:** Alternativas para assinaturas digitais seguras (BERNSTEIN et al., 2017).

Além das abordagens citadas, destacam-se:

- **Esquemas Baseados em Hash:** Como SPHINCS+ (BUCHMANN et al., 2016), resistentes a ataques quânticos mas com assinaturas maiores.
- **Criptografia Isogenia:** Baseada em curvas elípticas (SIDH – Supersingular Isogeny Diffie-Hellman), com vantagens em tamanho de chave (JAO; DE FEo, 2011).

Tabela Comparativa:

Tipo	Exemplo	Vantagens	Desafios
Reticulados	Kyber (NIST 2024)	Eficiência Computacional	Complexidade de implementação
Códigos	McEliece	Segurança comprovada desde 1978	Tamanho relativamente grande das chaves
Isogenias	SIKE	Chaves compactas	Velocidade de operação

1.1.3 Ameaças Quânticas Específicas

O poder disruptivo da computação quântica na criptografia materializa-se principalmente através de dois algoritmos seminalmente: o algoritmo de Shor, que quebra sistemas de chave pública, e o algoritmo de Grover, que acelera ataques de força bruta a cifras simétricas. (NIELSEN; CHUANG, 2010).

Algoritmo de Shor (1994)

O algoritmo de Shor representa uma ameaça existencial para os sistemas de criptografia de chave pública amplamente utilizados, como RSA e ECDSA, ao resolver eficientemente os problemas matemáticos intratáveis nos quais sua segurança se baseia: a fatoração de números inteiros e o problema do logaritmo discreto (SHOR, 1994). Sua eficiência revolucionária reside em explorar a Transformada Quântica de Fourier (QFT) para encontrar o período de uma função modular, reduzindo problemas exponencialmente complexos para computadores clássicos a problemas tratáveis em tempo polinomial para um computador quântico (NIELSEN; CHUANG, 2010). Essa diferença complexional é que torna vulneráveis chaves RSA de 2048 ou 4096 bits, consideradas seguras contra ataques clássicos, mas completamente inseguras frente a um computador quântico capaz de executar o algoritmo de Shor (NIST, 2023). De forma análoga, o algoritmo se aplica ao resolver o problema do logaritmo discreto em grupos cíclicos, que é a base de segurança dos algoritmos de Curvas Elípticas (ECDSA

e ECDH). Portanto, Shor compromete simultaneamente os dois pilares principais da criptografia de chave pública moderna, demandando uma migração urgente para alternativas resistentes ao quantum (BERNSTEIN et al., 2022).

Algoritmo de Grover (1996)

Diferente do Shor, o algoritmo de Grover não "quebra" algoritmos simétricos como o AES ou SHA-3 no sentido de encontrar uma falha matemática. Em vez disso, ele fornece uma aceleração quadrática genérica para problemas de busca em espaços não estruturados (NIELSEN; CHUANG, 2010). Em termos criptográficos, isso se aplica diretamente a ataques de força bruta, reduzindo pela metade o nível de segurança efetivo da chave na era pós-quântica (NIST, 2023). Isso efetivamente reduz pela metade o nível de segurança efetivo da chave na era pós-quântica. Para o AES-128, sua segurança cai de 128 bits para 64 bits, tornando um ataque por força bruta consideravelmente mais viável. Já para o AES-256, sua segurança cai para 128 bits, que ainda é considerado um nível robusto e praticamente inviável para força bruta, tornando a migração para esta variante a solução imediata para manter a segurança simétrica (NIST, 2023). A implicação prática é que, enquanto a criptografia de chave pública requer uma substituição completa por algoritmos pós-quânticos, a criptografia simétrica majoritariamente exige um aumento no tamanho das chaves para manter a segurança equivalente.

Tabela Comparativa:

Algoritmo Quântico	Problema Resolvido	Impacto na Criptografia	Solução Pós-Quântica
Algoritmo de Shor	Fatoração de Inteiros, Log. Discreto	Quebra RSA, DSA, ECDSA, Diffie-Hellman	Substituição por PQC (e.g., Kyber, Dilithium)
Algoritmo de Grover	Busca em Espaço Não Estruturado	Reduz pela metade a segurança de chaves simétricas	Dobrar o tamanho da chave (e.g., usar AES-256)

Fonte: Elaborada pelo autor com base em NIST (2023) e Nielsen e Chuang (2010).

2. DESENVOLVIMENTO DO ARGUMENTO

2.2 PROBLEMA DE PESQUISA

A segurança da informação tem sido introduzida a diferentes ameaças com o advento da computação quântica. Sistemas criptográficos que protegem transações financeiras, lidam com dados sensíveis e comunicações governamentais se baseiam em problemas matemáticos de extrema complexidade para computadores clássicos, porém. Grande parte de sistemas bancários, sistemas de saúde e governos dependem de criptografias que hoje são vulneráveis a ataques quânticos. Um estudo recente estima que 20 a 30% dos sistemas criptográficos globais estarão em risco até 2030 (RAND CORPORATION, 2023).

A situação em questão é particularmente preocupante quando se considera a lentidão na adoção de medidas preventivas. Pesquisas do Gartner (2023) indicam que aproximadamente 85% das organizações ainda não possuem um plano concreto para migração para sistemas pós-quânticos. Essa falta de preparação pode resultar em graves consequências para setores críticos como o financeiro e a saúde, onde a proteção de dados sensíveis é essencial para o funcionamento adequado dos serviços.

2.3 JUSTIFICATIVA

A relevância desta pesquisa se fundamenta na necessidade urgente de preparação para os desafios impostos pela computação quântica. Como destacado pela National Academy of Sciences (2023), a transição para sistemas criptográficos seguros na era pós-quântica requer um esforço coordenado entre academia, indústria e governo, com planejamento antecipado devido ao tempo necessário para implementação de novas tecnologias.

Além disso, o presente estudo contribui para o cenário nacional de pesquisa, onde ainda são escassos os trabalhos que abordam estratégias práticas de migração para criptografia pós-quântica. A análise comparativa de diferentes

abordagens e a elaboração de diretrizes para adoção progressiva dessas tecnologias podem auxiliar organizações brasileiras em seu processo de adaptação, garantindo a segurança de seus sistemas e dados no longo prazo.

2.4 OBJETIVO GERAL

O estudo em questão tem como propósito investigar os impactos da computação quântica nos sistemas de segurança da informação atuais e propor estratégias eficazes para a transição para a criptografia pós-quântica, garantindo a proteção de dados sensíveis contra ameaças futuras (NIST, 2023).

Será avaliada a vulnerabilidade dos principais algoritmos criptográficos clássicos (RSA, ECDSA, AES) diante de ataques quânticos, com base em simulações e estudos teóricos que demonstram a eficiência de algoritmos como o de Shor e Grover (SHOR, 1994; GROVER, 1996).

2.5 REFERENCIAL TEÓRICO

A fundamentação teórica deste estudo apoia-se em três pilares principais: os princípios da computação quântica, as vulnerabilidades da criptografia clássica e as novas abordagens pós-quânticas. Conforme demonstrado por Nielsen e Chuang (2010), a capacidade dos qubits de existirem em superposição e emaranhamento quântico permite resolver problemas matemáticos fundamentais para a segurança digital em tempo significativamente menor que os computadores clássicos. Essa característica, que inicialmente foi explorada por Shor (1994) e Grover (1996), representa uma ameaça para os sistemas criptográficos atuais.

Em contrapartida, a criptografia pós-quântica vem sendo desenvolvida para resistir a esses avanços. Peikert (2016) argumenta que os esquemas baseados em reticulados matemáticos apresentam propriedades ideais para segurança pós-quântica, sendo resistentes tanto a ataques clássicos quanto quânticos. Da mesma forma, os trabalhos de Bernstein et al. (2022) demonstram que sistemas como o CRYSTALS-Kyber e o CRYSTALS-Dilithium oferecem um equilíbrio adequado entre segurança e eficiência computacional, tornando-os candidatos promissores para a próxima geração de protocolos de segurança.

2.6 METODOLOGIA

Tipo de Pesquisa e Abordagem

Para a consecução deste estudo, adotou-se uma metodologia qualitativa de natureza exploratória e descritiva, seguindo a abordagem do Estado da Arte (State of the Art). Esta estratégia foi escolhida por permitir um mapeamento abrangente, a sistematização e a análise crítica das produções científicas consideradas mais relevantes sobre o impacto da computação quântica na segurança cibernética, com o objetivo de identificar consensos, divergências e lacunas significativas na literatura acadêmica e técnica (FERREIRA, 2002; GIL, 2008).

Este modelo de pesquisa mostrou-se adequado para investigar um fenômeno complexo e em rápida evolução, como a transição para a criptografia pós-quântica. Diferentemente de métodos quantitativos, esta abordagem priorizou a análise contextualizada e a interpretação teórica das descobertas científicas e suas implicações práticas para a segurança da informação.

Fontes e Critérios de Seleção

Por se tratar de uma pesquisa documental e bibliográfica, a investigação foi conduzida com base em um corpus diversificado de fontes primárias e secundárias, que incluiu:

- **Artigos científicos:** Publicados em periódicos de alto impacto, conferências especializadas em criptografia (e.g., CRYPTO, Eurocrypt, PQCrypto) e segurança da informação (e.g., IEEE S&P, USENIX Security).
- **Relatórios técnicos e whitepapers:** De instituições governamentais e agências de padrões, como o National Institute of Standards and Technology (NIST), a Agência da União Europeia para a Cibersegurança (ENISA), a National Security Agency (NSA) e o Instituto Nacional de Telecomunicações (Inatel).
- **Dissertações e teses:** Trabalhos acadêmicos que aprofundam temas específicos da criptografia pós-quântica.
- **Anúncios oficiais e documentação:** Especificações técnicas dos algoritmos finalistas e padronizados pelo processo do NIST para Criptografia Pós-Quântica.

Para garantir a relevância e a qualidade da análise, estabeleceram-se os seguintes critérios de seleção para as fontes:

1. **Recência:** Priorizam-se publicações do período de 2018 a 2025, com ênfase nos avanços mais recentes no processo de padronização do NIST. Trabalhos seminais anteriores (e.g., Shor, 1994; Grover, 1996) foram incluídos para fundamentação teórica.
2. **Relevância e Impacto:** Preferência por artigos com alto número de citações, publicados em veículos de renome, e relatórios de instituições de autoridade reconhecida no campo.
3. **Diversidade de Perspectivas:** Buscou-se incluir visões técnicas (desempenho de algoritmos, implementação), estratégicas (gestão de risco, planejamento de migração) e econômicas (custo de adoção).

Técnica de Análise: Estado da Arte

A técnica de Estado da Arte consistiu em um processo iterativo e sistemático composto pelas seguintes etapas:

1. **Revisão Bibliográfica Inicial e Formulação da Questão de Pesquisa:** Realizou-se uma busca exploratória em bases de dados como IEEE Xplore, ACM Digital Library, Scopus, Web of Science e arXiv utilizando combinações de palavras-chave como "*post-quantum cryptography*", "*quantum computing cybersecurity*", "*Shor's algorithm*", "*quantum resistance*", "*cryptographic migration*". Tal etapa permitiu delimitar o escopo do estudo e refinar as questões de pesquisa.
2. **Seleção e Análise Crítica das Fontes-Chave:** Com base nos critérios estabelecidos, procedeu-se à seleção das publicações consideradas mais representativas para compor o corpus de análise. Cada documento foi submetido a uma leitura analítica profunda, com o objetivo de decompor seus argumentos centrais, metodologias empregadas e conclusões. O foco esteve em compreender a fundo o posicionamento de cada autor ou instituição frente aos desafios da transição para a criptografia pós-quântica.

3. **Síntese Interpretativa e Identificação de Padrões:** Cada documento foi analisado criticamente para avaliar sua contribuição para o campo. Os dados extraídos foram sintetizados de forma a identificar:
 - a. **Linhas de Consenso:** Pontos de concordância entre diferentes autores e instituições (e.g., a urgência da migração, a ameaça do "Harvest Now, Decrypt Later").
 - b. **Divergências e Debates:** Temas onde não há unanimidade (e.g., superioridade de uma família de algoritmos sobre outra para casos de uso específicos).
 - c. **Lacunas do Conhecimento:** Áreas que carecem de pesquisa mais aprofundada (e.g., interoperabilidade de soluções híbridas em larga escala, impactos de desempenho em dispositivos IoT).
 - d. **Cronologia dos Avanços:** A evolução temporal das discussões e descobertas, desde a formulação da ameaça quântica até a padronização recente de algoritmos.
4. **Triangulação de Dados:** As informações obtidas de artigos acadêmicos foram cruzadas com dados de relatórios de indústria (IBM, Gartner) e diretrizes de agências governamentais (NIST) para validar conclusões e obter uma visão holística e robusta do problema.
5. **Elaboração de Diretrizes e Conclusões:** Por fim, a síntese do conhecimento foi utilizada para elaborar as diretrizes preliminares para a migração pós-quântica, que constituem um dos principais resultados desta pesquisa.

3. CONCLUSÃO

Como resultado principal, esta pesquisa oferece um mapeamento detalhado das principais vulnerabilidades dos sistemas criptográficos atuais frente ao avanço da computação quântica. A análise das fontes primárias e secundárias permitiu identificar que os pontos críticos que demandam atenção imediata concentram-se em setores com infraestrutura de longa duração e alto impacto, como o financeiro (especialmente em sistemas de pagamento e blockchain) e a saúde (onde a proteção de dados de pacientes

é crucial e regulada) (RAND CORPORATION, 2023). Verificou-se que a ameaça do "Harvest Now, Decrypt Later" (BERNSTEIN et al., 2019) é subestimada por grande parte das organizações.

Adicionalmente, o estudo contribui com uma análise comparativa abrangente dos algoritmos pós-quânticos finalistas e padronizados pelo NIST, avaliando suas vantagens, limitações e viabilidade de implementação sob a ótica de desempenho e custo. Concluiu-se que, embora algoritmos baseados em reticulados (como Kyber e Dilithium) apresentem o melhor equilíbrio geral, esquemas baseados em códigos (como McEliece) permanecem uma opção viável para sistemas onde o tamanho grande da chave não é um impeditivo primordial. Observou-se, conforme apontado por Gartner (2023), que a maior barreira não é tecnológica, mas sim a falta de planejamento estratégico. Os resultados obtidos se materializam em um conjunto de diretrizes preliminares que podem auxiliar tanto a comunidade acadêmica quanto os profissionais de TI na priorização e no planejamento para os desafios da era pós-quântica.

4. REFERÊNCIAS

4.1 TRABALHOS RELACIONADOS

1. Estudos sobre Vulnerabilidades:

- MOSCA et al. (2018) analisaram o "risco cripto-apocalipse", estimando que 50% dos sistemas atuais serão vulneráveis até 2030 caso não migrem.
- CHEN et al. (2022) simularam ataques quânticos a blockchains, demonstrando que 40% das criptomoedas usam algoritmos inseguros (ex.: ECDSA).
- BERNSTEIN et al. (2019) realizaram um estudo prospectivo detalhado sobre o "Harvest Now, Decrypt Later" (Colha Agora, Decifre Depois), alertando que dados interceptados e armazenados hoje podem ser decifrados no futuro com um computador quântico suficientemente potente, tornando a migração protocolar uma urgência imediata.
- ANSI (2022) publicou um relatório técnico focando na vulnerabilidade de infraestruturas críticas, como redes elétricas e de transporte,

concluindo que seus sistemas de controle industrial (ICS/SCADA) possuem uma janela de risco particularmente alta devido à longa vida útil de seus equipamentos.

2. Soluções Pós-Quânticas:

- O NIST (2024) selecionou os algoritmos CRYSTALS-Kyber (criptografia) e Dilithium (assinaturas) como padrões, com eficiência testada em hardware comum (AVANZI et al., 2023).
- Na Europa, o projeto PQCrypto (2023) avaliou a viabilidade de migração em sistemas governamentais, identificando custos 30% menores que o previsto.
- ALBRECHT et al. (2021) conduziram uma análise de desempenho comparativo de vários esquemas pós-quânticos finalistas no processo do NIST, medindo tempo de geração de chaves, ciframento e deciframento em diferentes arquiteturas de hardware, servindo como um guia prático para desenvolvedores.
- KAPLAN et al. (2020) propuseram e testaram estratégias híbridas de implantação, onde algoritmos clássicos e pós-quânticos são executados em conjunto para garantir segurança retroativa e facilitar uma transição gradual e mais segura.

4.2 REFERÊNCIAS

BERNSTEIN, D. J. et al. Post-quantum cryptography. Berlim: Springer, 2022. 321 p.

NIELSEN, M. A.; CHUANG, I. L. Quantum computation and quantum information. 10. ed. Cambridge: Cambridge University Press, 2010. 702 p.

FERREIRA, N. S. A. As pesquisas denominadas "Estado da Arte". Educação & Sociedade, Campinas, v. 23, n. 78, p. 257-272, abr. 2002. Disponível em: <https://www.scielo.br/j/es/>. Acesso em: 10 jul. 2025.

PEIKERT, C. A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, Providence, v. 10, n. 4, p. 1-32, 2016.

IBM. Cost of a Data Breach Report 2023. Armonk: IBM Security, 2023. Disponível em: <https://www.ibm.com/security/data-breach>. Acesso em: 10 jun. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Post-Quantum Cryptography Standardization. Gaithersburg: NIST, 2023. Disponível em: <https://csrc.nist.gov/projects/post-quantum-cryptography>. Acesso em: 12 jun. 2024.

SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE, 35., 1994, Santa Fe. Proceedings... Los Alamitos: IEEE Computer Society Press, 1994. p. 124-134.

JAO, D.; DE FE0, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: INTERNATIONAL WORKSHOP ON POST-QUANTUM CRYPTOGRAPHY, 4., 2011, Taipei. Proceedings... Berlin: Springer, 2011. p. 19-34.

MCELIECE, R. J. A public-key cryptosystem based on algebraic coding theory. Pasadena: Jet Propulsion Laboratory, 1978. 43 p. (DSN Progress Report 42-44).

RAND CORPORATION. The Quantum Threat: A Risk Assessment. Santa Monica: RAND, 2023. Disponível em: <https://www.rand.org>. Acesso em: 14 jun. 2024.

GARTNER. Hype Cycle for Quantum Computing. 2023. Disponível em: <https://www.gartner.com>. Acesso em: 15 jun. 2024.