A EVOLUÇÃO DA COMPUTAÇÃO QUÂNTICA: IMPACTO NA CRIPTOGRAFIA RSA E A SEGURANÇA NACIONAL

Breno Augusto R. Campos[1], Eduardo C. Rosa[2],

Data de aprovação: 06/07/2024
Data de submissão: 27/07/2024

RESUMO

A chegada da computação quântica representa um novo paradigma para a segurança da informação. Algoritmos criptográficos amplamente utilizados, como o RSA, enfrentam a perspectiva de se tornarem vulneráveis à poderosa capacidade de computação quântica. Este artigo explora o impacto potencial da computação quântica na criptografia de redes, com foco na quebra do algoritmo RSA. É investigada a evolução histórica da quantidade de publicações sobre computação quântica, destacando-se sua importância na proteção da confidencialidade, integridade e autenticidade das comunicações digitais. Além disso, são examinados os avanços recentes na área, incluindo o desenvolvimento de soluções pós-quânticas, constantes investimentos por vários países e os impactos geopolíticos. Conclui-se que este estudo identificou contínuos avanços na área, evidenciados pela publicação de quase 1500 artigos de alto impacto anualmente. Além disso, os significativos investimentos iniciados por volta de 2015 reforçam a relevância e a crescente atividade no campo.

Palavras-chave: computação quântica; RSA; geopolítica.

ABSTRACT

The arrival of quantum computing represents a new paradigm for information security. Widely used cryptographic algorithms such as RSA face the prospect of becoming vulnerable to the powerful capabilities of quantum computing. This article explores the potential impact of quantum computing on network cryptography, focusing on breaking the RSA algorithm. The historical evolution of the number of publications on quantum computing is investigated, highlighting its importance in protecting the confidentiality, integrity and authenticity of digital communications. In addition, recent advances in the area are examined, including the development of post-quantum solutions, constant investments by several countries and geopolitical impacts. It is concluded that this study identified continuous advances in the area, evidenced

[1] Graduando em Sistemas de Informação no Instituto Federal de Ciência, Tecnologia e Educação Goiano - Campus Avançado Catalão. E-mail: breno.campos@estudante.ifgoiano.edu.br

[2] Doutorando em Ciência da Computação pela Universidade Federal de Uberlândia (UFU), Mestre em Engenharia Elétrica pela FEELT/UFU com foco em Telecomunicações e Redes Móveis de Quarta Geração e Professor no IFGoiano de Catalão. E-mail: eduardo.rosa@ifgoiano.edu.br

by the publication of almost 1500 high-impact articles annually. Furthermore, the significant investments started around 2015 reinforce the relevance and growing activity in the field.

Palavras-chave estrangeira: *quantum computation; RSA; geopolitics*.

1 INTRODUÇÃO

A criptografia, ferramenta essencial para proteger dados sensíveis e garantir a privacidade das comunicações, desempenha um papel crucial na segurança das informações. O algoritmo RSA (*Rivest-Shamir-Adleman*), um dos mais amplamente utilizados na criptografia moderna, tem sido fundamental para proteger transações online, comunicações governamentais e outras aplicações críticas conforme Kurose e Ross (2013) e Zhou e Tang (2011). No entanto, essa é uma área que exige contínua evolução e essa necessidade se amplificou ainda mais com a computação quântica.

A computação quântica, com seu potencial para revolucionar a computação, emerge como uma das tecnologias mais disruptivas do século XXI. Esse novo paradigma computacional, ainda em desenvolvimento, promete solucionar problemas complexos que a computação clássica levaria trilhões de anos, com impacto direto em diversas áreas, incluindo a segurança da informação. No cerne dessa revolução, encontra-se a ameaça à criptografia moderna, no qual este estudo trata especificamente o algoritmo RSA.

O impacto da computação quântica na segurança da informação é profundo e está transformando o cenário geopolítico mundial. Países como China e Estados Unidos, líderes nessa corrida tecnológica, investem maciçamente em pesquisa e desenvolvimento, buscando vantagem estratégica em termos de segurança e inteligência. Essa disputa global por supremacia tecnológica reconfigura as relações de poder no ciberespaço e coloca em xeque a segurança de dados sensíveis em escala global.

Este artigo, por meio de uma revisão bibliográfica, investiga a crescente preocupação com a quebra do algoritmo RSA pela computação quântica, ao analisar a evolução das pesquisas nesse campo. O estudo busca entender se a crescente quantidade de pesquisas em computação quântica e criptoanálise quântica representa uma ameaça real à segurança nacional, especialmente no que diz respeito à criptografia de dados sensíveis, já que o RSA é um pilar importante para a criptografia mundial como descrito por Zhou e Tang (2011).

A análise de publicações científicas revela um aumento significativo de pesquisas nesse campo nos últimos anos, demonstrando a crescente preocupação com a vulnerabilidade do RSA e a necessidade de desenvolver soluções de criptografia pós-quântica (PQC) que sejam resilientes aos ataques de computadores quânticos. O artigo explora os desafios e oportunidades que essa transição representa para a segurança global, além disso aborda a importância da cooperação internacional para garantir a segurança de um mundo cada vez mais dependente de tecnologias digitais.

Diante do exposto, este trabalho está estruturado da seguinte forma: na sessão 2, será tratado o referencial teórico para embasar a discussão. Na sessão 3, será descrito os matérias e métodos utilizados para alcançar os resultados da revisão. Já na sessão 4, estão apresentados os resultados e discussões seguido da sessão 5 com as considerações finais.

2 DESENVOLVIMENTO

Nesta sessão, será definido o referencial teórico, onde os principais tópicos como computação quântica, o algoritmo RSA, e a computação quântica na segurança nacional.

2.1 REFERENCIAL TEÓRICO

2.1.1 Computação Quântica

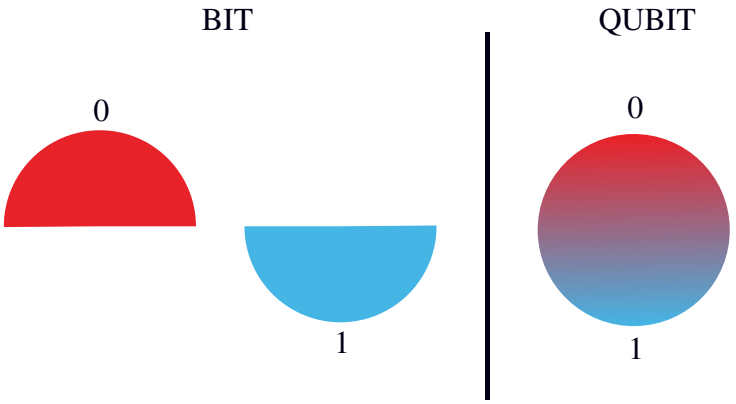
A computação quântica, uma área vasta e complexa da ciência da computação, ainda não atingiu um estágio de aplicabilidade prática plenamente desenvolvida para o contexto da realidade. Atualmente, as tecnologias quânticas estão em um estágio inicial de desenvolvimento, com desafios significativos de implementação em larga escala. Contudo, quando essa capacidade se tornar prática, espera-se que seja especialmente adequada para resolver classes específicas de problemas complexos que desafiam os limites da computação clássica (GRUMBLING; HOROWITZ, 2019).

Há uma diferença basal nas categorias de máquinas, sendo que um computador clássico utiliza de valores binários para funcionar e princípios da física clássica, onde 0 representa ausência de energia e 1 representa a presença. Porém, a computação quântica utiliza de princípios da física quântica para existir. É importante ressaltar que a computação quântica não é concebida como um substituto direto para os recursos computacionais de uso geral. Em vez disso, ela representa uma abordagem complementar e altamente especializada, capaz de lidar de forma eficiente com tarefas e demandas computacionais específicas que estão além do alcance dos computadores convencionais. Essa distinção destaca a perspectiva de coexistência e colaboração entre os paradigmas clássico e quântico, cada um desempenha papéis distintos e complementares no avanço da computação e da tecnologia assim como afirmado por Grumbling e Horowitz (2019) e Galvão (2007).

Ao longo do desenvolvimento da história, no decorrer do século XX, alguns físicos começaram a notar comportamentos anormais em experimentos que envolviam objetos muito pequenos. Essas observações geraram muitas dúvidas. Cientistas como Thomas Young, Erwin Schrödinger e Werner Heisenberg, entre outros, começaram a desenvolver uma lógica para representar o comportamento dos elementos subatômicos Galvão (2007).

Em meados de 1935, Erwin Schrödinger formulou a conhecida teoria do gato de Schrödinger. Em suma, essa teoria descreve uma analogia que envolve um gato e uma caixa com veneno, onde Schrödinger então propõe que o gato logicamente está vivo e morto ao mesmo tempo, dessa forma, foi definido o conceito de sobreposição. Esse conceito aplicado em sua

Figura 1 — Comparação bit com qubit em estado de sobreposição.



Fonte: Produzido pelo autor.

teoria indica que não é possível afirmar se o gato está vivo ou morto, até que a caixa seja aberta e o estado de saúde verificado (SCHRÖDINGER, 1935).

Assim, ao se aplica alguns desses conceitos da física quântica, matemáticos e físicos se juntaram para construir um paralelo à máquina de Turing, conhecido como a Máquina de Turing Quântica, onde foi criado também o conceito de *qubits* (GALVÃO, 2007).

Qubit é um *bit* quântico, que possui o estado de sobreposição com visto na Figura 1, portanto ele pode estar em 0 e 1 ao mesmo tempo e somente quando avaliado, definirá seu valor 0 ou 1, e não voltará novamente ao estado de sobreposição. A partir das características do *quibit*, pode-se então construir uma memória quântica, essa nova modalidade supera um computador clássico na medida que se possa definir um novo modelo de memória onde ela poderia representar elementos com 2^n comparado com um computador clássico que seria representado por N. Por exemplo, se há um computador quântico com 2 *qubits*, então ele seria equivalente a 4 bits em um computador clássico (GALVÃO, 2007).

Além disso, em 1994, Peter Shor, um matemático estadunidense, desenvolveu o algoritmo de Shor que revolucionou a computação e a visão mundial sobre criptografia e criptoanálise. Esse algoritmo consegue descrever logicamente como fatorar grandes números inteiros semiprimos - um de dois números primos - em um computador quântico em tempo polinomial. Essa descoberta provocou uma grande movimentação mundial em como o mundo observava a criptografia com fatores primos, como utilizado no RSA (GALVÃO, 2007).

Para que a computação quântica possa atingir seu potencial máximo e ser plenamente integrada no cenário tecnológico, são necessários avanços significativos em áreas como tolerância a erros, escalabilidade e capacidade de manipulação de *qubits*. Além disso, é essencial o desenvolvimento de algoritmos quânticos otimizados e a adaptação de infraestruturas computacionais para suportar as demandas únicas e complexas desse novo paradigma tecnológico. Assim, embora a computação quântica prometa revolucionar a forma como lidamos com problemas computacionais desafiadores, sua implementação prática e efetiva dependerá de avanços contínuos e de uma abordagem cuidadosa e estratégica no seu desenvolvimento e adoção

(GRUMBLING; HOROWITZ, 2019).

2.1.2 O Algoritmo RSA

O algoritmo RSA (*Rivest-Shamir-Adleman*), desenvolvido por Ron Rivest, Adi Shamir e Leonard Adleman na década de 1970, é um dos mais amplamente utilizados na criptografia moderna. Baseado no conceito de chave pública e chave privada, o RSA é fundamental para garantir a segurança das comunicações digitais, onde ele é empregado em uma variedade de aplicações, desde transações financeiras online até assinaturas digitais. Sua segurança reside na dificuldade computacional de fatorar grandes números semiprimos, o que torna impraticável para adversários decifrar mensagens criptografadas sem possuir a chave privada correspondente com os recursos computacionais atuais (KUROSE; ROSS, 2013).

Por meio do RSA é possível atender os três critérios descritos por Kurose e Ross (2013):

- Confidencialidade, assegura que a mensagem seja acessível apenas ao destinatário;
- Integridade, para garantir a intocabilidade do conteúdo durante o envio; e
- Autenticação, um meio seguro de confirmar a identidade do emissor.

Para ficar mais claro pode-se observar um cálculo adaptado do exemplo de Kurose e Ross (2013) de como o algoritmo RSA pode ser quebrado envolve a fatoração de números semiprimos pequenos. Imagine dois números primos relativamente pequenos, por exemplo, p = 5 e q = 7. A multiplicação desses números resulta em n, que é o produto dos dois números primos e é usado como parte da chave pública.

$$n = p \times q = 5 \times 7 = 35$$

Em seguida, calculamos a função totiente de Euler de n, que para dois números primos é simplesmente $(p-1) \times (q-1)$. Portanto:

$$\phi(n) = (5-1) \times (7-1) = 4 \times 6 = 24$$

A seguir, escolhe-se um expoente de criptografia pública, comumente denotado como e. Para este exemplo, vamos escolher $e = 5$. O par de chaves público e privado é então definido como $(n, e) = (35, 5)$.

Agora, o desafio para um atacante é calcular a chave privada, que requer a determinação de um número d tal que $(d \times e) \mod \phi(n) = 1$. Para este exemplo, precisamos encontrar d tal que $(d \times 5) \mod 24 = 1$. Após algum cálculo, descobrimos que $d = 5$, que é a chave privada.

Neste exemplo, a quebra do RSA envolve fatorar n em seus fatores primos p e q, permite assim o cálculo da chave privada. No entanto, atualmente o RSA é calculado com 2048 *bits*, porém para valores similares a este, levaria cerca de 300 trilhões de anos quando se utiliza a computação clássica (WOOD, 2022).

Porém, ao introduzir o conceito de computação quântica, o prazo estabelecido seria extremamente menor, na ordem de segundos. Segundo definido por Chen *et al.*, (2016) no NIST *(National Institute of Standards and Technology)* em 2030, o RSA 2048 já pode estar em risco, recomendado ainda que sejam utilizados os de 3072 ou 4096 (FERRAIOLO; REGENSCHEID, 2023).

A evolução da computação quântica traz consigo um cenário revolucionário na segurança cibernética, especialmente no que diz respeito à quebra de algoritmos criptográficos convencionais. Um marco significativo nesse avanço é a capacidade prevista de um computador quântico com mais de 400 *qubits* em quebrar o algoritmo RSA em questão de segundos (YAN *et al.*, 2022). Essa perspectiva lança uma nova luz sobre a segurança das comunicações digitais e tem implicações profundas não apenas no mundo da tecnologia, mas também na geopolítica global.

Ao longo das últimas décadas, o algoritmo RSA tem sido um pilar fundamental da segurança na Internet (ZHOU; TANG, 2011). Por exemplo, a criptografia de chave pública comumente utilizada no fluxo HTTPs (*Hyper Text Transfer Protocol Secure*) é utilizado em 99% do tempo de navegação no navegador *Google Chrome*, segundo a própria Google LLC (2024) em seu relatório de transparência. Desta forma, o RSA fornece um método robusto para a criptografia de dados sensíveis. No entanto, com a chegada iminente da capacidade computacional quântica para quebrar esse algoritmo como demonstrado por Yan *et al.* (2022), surgem desafios sem precedentes que afetam não apenas empresas e organizações, mas também governos e políticas internacionais.

A rapidez com que um computador quântico pode comprometer a segurança de sistemas criptográficos tradicionais tem implicações profundas na proteção de dados sensíveis, como informações financeiras, segredos comerciais e comunicações governamentais. Isso levanta questões sobre a necessidade urgente de desenvolver e adotar sistemas de criptografia pós-quântica que sejam resistentes aos avanços da computação quântica (CHEN *et al.*, 2016).

Além disso, o impacto geopolítico dessa evolução tecnológica é igualmente significativo. Países e entidades que possuem ou desenvolvem tecnologia quântica podem obter vantagens estratégicas em termos de segurança, transmissão e processamento de dados, o que pode redefinir as dinâmicas de poder no cenário internacional, como visto no caso de Edward Snowden reportado por Landau (2014).

2.1.3 Computação Quântica Na Segurança Nacional

A história comprova que nações dotadas de tecnologia de ponta em inteligência de sinais desempenham um papel de extrema relevância ao salvar vidas e influenciar os resultados de conflitos bélicos e questões geopolíticas. Durante a Segunda Guerra Mundial, um marco significativo na história da criptografia foi estabelecido por Alan Turing com sua contribuição para a decifração da máquina Enigma. Esta máquina era utilizada pelos nazistas para cifrar suas comunicações militares e representava um desafio extraordinário, devido à sua complexidade e

a capacidade de gerar cifras aparentemente inquebráveis.

Turing contribuiu não só para a área de segurança, mas com toda a área de computação, durante seu trabalho com o exército britânico, juntamente com seu time, ele desenvolveu a máquina *Bombe*, um dispositivo capaz de interpretar e decifrar as mensagens gerada pela máquina Enigma, o que foi fundamental para a vitória dos seus aliados. Uma análise aponta que, caso os aliados não tivessem sido capazes de decifrar as comunicações criptografadas do eixo por meio da sofisticada máquina Enigma, estima-se que mais de 14 milhões de vidas teriam sido ceifadas no decorrer da Segunda Guerra Mundial (ALMEIDA, 1998).

Quatro décadas após os eventos que marcaram a Segunda Guerra Mundial, em 5 de setembro de 1983, o presidente dos Estados Unidos, Ronald Reagan, dirigiu-se à nação em um discurso que abalou as estruturas geopolíticas da época. Na ocasião, Reagan apresentou à população americana comunicações interceptadas das forças armadas soviéticas, o que forneceu evidências contundentes de que o abate do voo Korean Air 007 não foi um mero acidente, mas sim um ato intencional por parte dos soviéticos. Graças a essa divulgação pública, o presidente pôde expor e responsabilizar os soviéticos pelo ato hostil que resultou na perda de vidas inocentes, e repercutiu não só no âmbito da discussão política internacional, mas também na relação entre as potências da época. Esse episódio evidenciou mais uma vez a importância tanto da criptografia quanto da decifração das mensagens, e como esses podem ser fatores essenciais na determinação de eventos históricos cruciais (REAGAN'S, 2011).

Assim, a relevância dos decifradores de códigos da Enigma não se encerrou com o término da Segunda Guerra Mundial, mas sinaliza os desafios iminentes que organizações e nações enfrentarão quando a computação quântica se tornar uma ameaça à segurança. Durante o conflito, os Aliados guardaram em sigilo sua habilidade de quebrar os códigos da Enigma, e isso resultou na continuidade do uso dessas máquinas por governos ao redor do mundo por décadas, ao acreditar erroneamente na inviolabilidade de sua segurança. Nesse ínterim, as agências de inteligência do Reino Unido e dos Estados Unidos conseguiram interceptar e monitorar as comunicações de outros países em um período crucial da Guerra Fria. Contudo, as revelações sobre a quebra dos códigos da Enigma permaneceram sob sigilo até a década de 1970, quando especialistas da Sede de Comunicações do Governo da Grã-Bretanha expuseram o trabalho e as conquistas dos decifradores britânicos da Segunda Guerra Mundial (SINGH, 2001).

Desse modo, a criptografia é uma ferramenta essencial para proteger dados sensíveis e comunicações confidenciais, para garantir a segurança e a privacidade das informações (KUROSE; ROSS, 2013). No entanto, com o avanço da computação quântica e a possibilidade da criptoanálise quântica se tornar prática, como foi feito por Yan *et al.* (2022), surgem novos desafios e preocupações em relação à segurança dos sistemas de criptografia atuais. Logo, o impacto da computação quântica na segurança nacional tem se tornado uma preocupação cada vez mais relevante. Em suma, é necessário destacar a revolução que a computação quântica representa em relação à computação clássica, graças à capacidade dos *qubits* de operar em superposição e emaranhamento quântico (GALVÃO, 2007). Essa capacidade possibilita resolver

problemas de forma muito mais eficiente do que os computadores clássicos, o que denota um avanço tecnológico.

Conforme discutido por Grobman (2020), o diretor de tecnologia da McAfee, muitas vezes, acredita-se que os algoritmos de criptografia existentes serão capazes de resistir a ataques quânticos quando a computação quântica se tornar uma realidade. No entanto, deve-se considerar que mesmo hoje, sem a computação quântica plenamente funcional, os adversários geopolíticos, especialmente a China e os EUA, podem desviar dados criptografados que serão desbloqueados no futuro, quando a criptoanálise quântica se tornar prática.

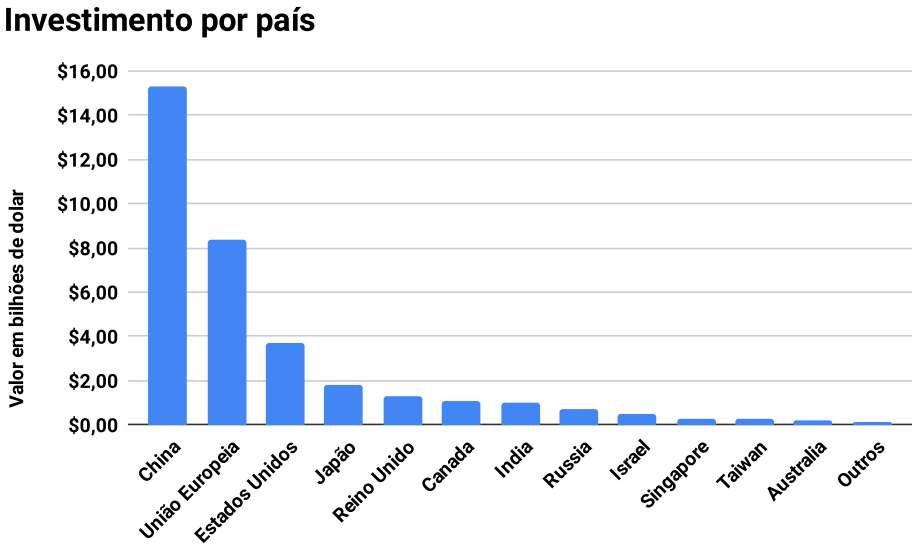
Um exemplo interessante sobre a segurança atemporal é o fato de que documentos relacionados ao assassinato de Kennedy, ocorrido há quase 60 anos, ainda estão sob sigilo devido a questões de segurança nacional (MATZA, 2023). Isso demonstra a importância da durabilidade dos segredos nacionais, especialmente quando envolvem informações sensíveis sobre fontes e métodos de coleta de inteligência.

Portanto, como elaborado por Grobman (2020), Mosca (2018) e Overbeck e Sendrier (2009), é crucial que o risco quântico atual não seja subestimado e que a sociedade em geral esteja ciente de que possíveis atacantes podem explorar vulnerabilidades em sistemas de criptografia, mesmo antes da criptoanálise quântica se tornar uma realidade. Deve-se estar preparado e adotar medidas proativas para fortalecer a segurança dos dados e comunicações mais confidenciais, além de garantir a proteção de informações críticas para a segurança nacional e a defesa de interesses estratégicos. É necessário um alerta em relação aos desafios e riscos que a computação quântica traz para a segurança nacional, especialmente no que diz respeito à criptografia, pois atualmente, muitos sistemas de segurança e métodos de criptografia dependem da inquebrabilidade dos algoritmos matemáticos, sobretudo o RSA. No entanto, a computação quântica pode em algum momento com facilidade quebrar esses algoritmos, o que coloca em risco a confidencialidade e integridade dos dados, especialmente em infraestruturas críticas como sistemas de energia, comunicações e defesa.

De forma global, a ascensão da China na computação quântica representa um desafio significativo para a liderança dos Estados Unidos e uma preocupação mundial nesse campo. O governo chinês tem como objetivo se tornar líder global em tecnologias emergentes e quânticas, com prioridade em aplicações militares e comerciais. A busca por autonomia tecnológica é impulsionada pela memória histórica da dominação estrangeira e subordinação sofrida pela China ao longo do século XIX e início do século XX. Diante disso, a China incluiu a computação quântica como parte essencial de suas estratégias de desenvolvimento tecnológico, com investimentos expressivos e metas ambiciosas para alcançar a liderança mundial até 2030 (KANIA; COSTELLO, 2018).

A China direciona vultosos recursos financeiros e humanos para impulsionar pesquisas e avanços em computação quântica. Estima-se que os investimentos chineses na área superem os US$15 bilhões, valor que ultrapassa as iniciativas dos Estados Unidos e de outras nações (QURECA, 2023). É possível observar um gráfico comparativo Figura 2 entre os esforços chineses

Figura 2 — Mapa de investimento em computação quântica em bilhão de dólares.



Fonte: Adaptado de (QURECA, 2023)

em relação aos outros países, no qual seria necessário todos os países juntos para ultrapassar o valor investido pela China. Desse modo, ressalta-se que os esforços nacionais chineses incluem pesquisas em comunicação quântica, computação quântica e metrologia quântica, ações e investimentos que refletem uma abordagem abrangente e estratégica para liderança tecnológica global.

Os EUA, por outro lado, em colaboração com o NIST também seguem desenvolvendo novas tecnologias no segmento, como a competição de padronização de criptografia pós-quântica, conduzida pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST), é um esforço significativo para selecionar algoritmos de criptografia capazes de resistir aos ataques de computadores quânticos. Na primeira etapa do projeto, um total de 69 algoritmos foram submetidos para avaliação (NIST-SUBMISSION, 2017). Dentre esses, foram selecionados quatro algoritmos: CRYSTALS-Kyber para criptografia geral, e CRYSTALS-Dilithium, FALCON e SPHINCS+ para assinaturas digitais. A escolha desses algoritmos é resultado de um processo de seis anos coordenado pelo NIST, que envolveu criptógrafos e especialistas em segurança de várias partes do mundo (BOUTIN; NIST, 2022).

Além disso, o NIST realizou a 5ª Conferência de Padronização de Criptografia Pós-Quântica em abril de 2024 para discutir os algoritmos selecionados e obter um parecer para informar as decisões de padronização. Este evento foi uma oportunidade crucial para o avanço da criptografia pós-quântica e para garantir a segurança da informação digital contra ameaças futuras (NIST, 2024).

A competição na computação quântica entre China e Estados Unidos vai além do aspecto tecnológico, de segurança nacional e cibernética. A quebra da segurança criptográfica

por computadores quânticos representa um desafio à privacidade, à proteção de dados sensíveis e à integridade das redes de comunicação. A corrida tecnológica entre as potências globais sinaliza uma disputa por supremacia tecnológica, normativa e regulatória, que pode reconfigurar as relações de poder no ciberespaço global (GROBMAN, 2020).

O avanço da China na computação quântica desencadeia reflexões sobre governança internacional, interoperabilidade de sistemas e proliferação de tecnologias avançadas. A busca pela liderança chinesa nesse campo motiva a revisão das estratégias de inovação, segurança cibernética e cooperação internacional por parte dos Estados Unidos e demais atores globais. A competição tecnológica entre China e Estados Unidos delineia não apenas uma disputa por avanços tecnológicos, mas também divergências quanto à governança da internet, segurança cibernética e liberdade na rede (KANIA; COSTELLO, 2018).

É fundamental compreender que a competição na computação quântica entre China e Estados Unidos moldará o futuro da tecnologia, da segurança cibernética e das relações internacionais. A cooperação e a competição entre as duas potências terão impactos significativos no equilíbrio de poder global, na governança digital e na proteção dos dados sensíveis. A corrida tecnológica na computação quântica representa um ponto crucial no cenário geopolítico contemporâneo, além de exigir uma análise cuidadosa dos desdobramentos e implicações dessa dinâmica para a segurança e estabilidade globais.

Nesse sentido, Grobman (2020) ressalta a importância de antecipar essa ameaça e investir em soluções de segurança pós-quântica, pois este trata-se de um problema e preocupação para hoje, não para o amanhã. Isso envolve o desenvolvimento de algoritmos de criptografia resistentes à computação quântica, assim como a elaboração de planos de contingência e estratégias de mitigação de riscos. A colaboração entre empresas, governos, instituições acadêmicas e a comunidade de segurança cibernética é fundamental para garantir a eficácia e a implementação dessas soluções.

A transição para a segurança pós-quântica não será simples nem rápida, exige esforços contínuos em pesquisa, inovação e educação sobre computação quântica e suas implicações para a segurança nacional. Também é necessário a conscientização e a colaboração são essenciais para enfrentar os desafios que a computação quântica representa, e assim garantir a proteção dos dados e sistemas em um mundo pós-quântico. Desta forma, a ação proativa e a adaptação constante às novas ameaças são fundamentais para manter a segurança cibernética como uma prioridade em todas as esferas da sociedade (OVERBECK; SENDRIER, 2009).

3 MATERIAIS E MÉTODOS

Como apresentado na seção de Fundamentação Teórica, a computação quântica e a potencial quebra do RSA, embora atualmente não representem um perigo imediato, podem gerar grandes problemas para a segurança mundial com o avanço das pesquisas. Portanto, a partir da análise da evolução histórica e da intensificação das pesquisas, este trabalho visa demonstrar

que o tema continua muito ativo, dado o volume de artigos publicados por ano sobre o tema. Assim, reforça-se a necessidade de evoluir as defesas contra essa nova ameaça.

Para isso, levantou-se os periódicos a partir do qualis calculado a partir da ferramenta "Qualis Ciência da Computação"[1] que utiliza a base de dados da *Scopus* como referência para converter o fator de impacto e avaliações feitas no exterior para o fator qualis utilizado no Brasil. A partir dessa ferramenta foram filtrados somente os periódicos classificados com A1, A2 e A3 e possuíam a palavra-chave "*quantum*" na definição do periódico. As bases escolhidas como fontes principais possuíam 14374 artigos, conforme listado na Tabela 1.

Base	Quantidade de artigos
IEEE - *IEEE JOURNAL OF QUANTUM ELECTRONICS*	6840
Springer Link - *QUANTUM INFORMATION PROCESSING*	4486
Quantum - *QUANTUM*	1359
IOPScience - *QUANTUM SCIENCE AND TECHNOLOGY*	866
Nature - *NPJ QUANTUM INFORMATION*	823

Tabela 1 — Quantidade de artigos por periódicos.

Além disso, bases como: IEEE xplore, Elsevier, NIST, JSTOR bem como relatórios de grandes empresas como Google, Microsoft e IBM, foram consultadas para complementar o processo. A partir desses periódicos, foram filtradas as palavras chaves "computação quântica", "RSA", "criptografia" e "geopolítica", bem como suas variações na língua inglesa "*quantum computing*", "RSA", "*cryptography*", "*geopolitics*". A partir das bases citadas, foram realizadas buscas com as palavras-chave, conforme reportado na Tabela 2. A partir dos números obtidos, é possível perceber a baixa relevância dos termos pesquisados na língua portuguesa visto que majoritariamente os artigos são publicados na língua inglesa para as bases escolhidas.

Termo	Quantidade de artigos
RSA	128
cryptography	1513
quantum computing	3502
geopolitics	2
criptografia	0
computação quântica	0
geopolítica	0
total	5145

Tabela 2 — Quantidade artigos por palavra-chave

A partir desses artigos, foi definido o seguinte racional:

- Identificar artigos com título correlato ao tema;

[1] https://ppgcc.github.io/discentesPPGCC/pt-BR/qualis/

- A partir dos artigos selecionados, realizar leitura dos tópicos Resumo, Introdução;
- No caso do resumo e introdução tocarem nos temas de computação quântica, criptografia RSA e geopolítica, esses artigos foram separados para criar a revisão bibliográfica.

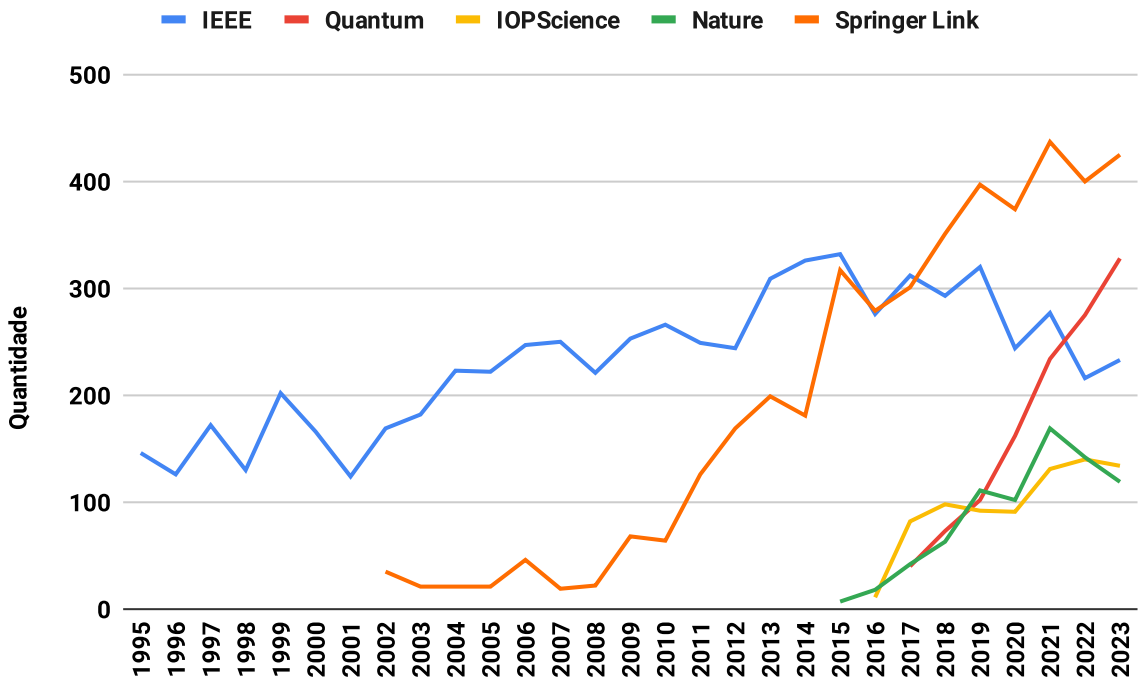
Por meio dessa abordagem metodológica, este estudo visa fornecer uma visão abrangente do estado atual da pesquisa sobre a segurança da informação em um contexto de computação quântica como foco na visão geopolítica do problema.

4 RESULTADOS E DISCUSSÕES

A partir do que foi discutido, é possível demonstrar o aumento na relevância do tema ao longo dos anos, ao destacar que a tecnologia está se tornando cada vez mais tangível. Além disso, é possível correlacionar o aumento nas publicações com os crescentes investimentos na área. E embora o algoritmo RSA não apresente risco iminente de quebra, é fundamental usar esse tempo para se preparar e desenvolver soluções de criptografia pós-quântica (PQC).

Ao avaliar a Figura 3, é possível verificar a visão histórica de publicações de artigo nos periódicos *IEEE - IEEE Journal Of Quantum Electronics, Springer Link - Quantum Information Processing, Quantum - Quantum, IOPScience - Quantum Science And Technology e Nature - NPJ Quantum Information*. Percebe-se que existe uma evolução nas quantidades anuais de artigos publicados sobre computação quântica aos longos dos anos. Esse aumento pode estar relacionado diretamente ao avanço tecnológico, quantidade de investimento e fatores históricos.

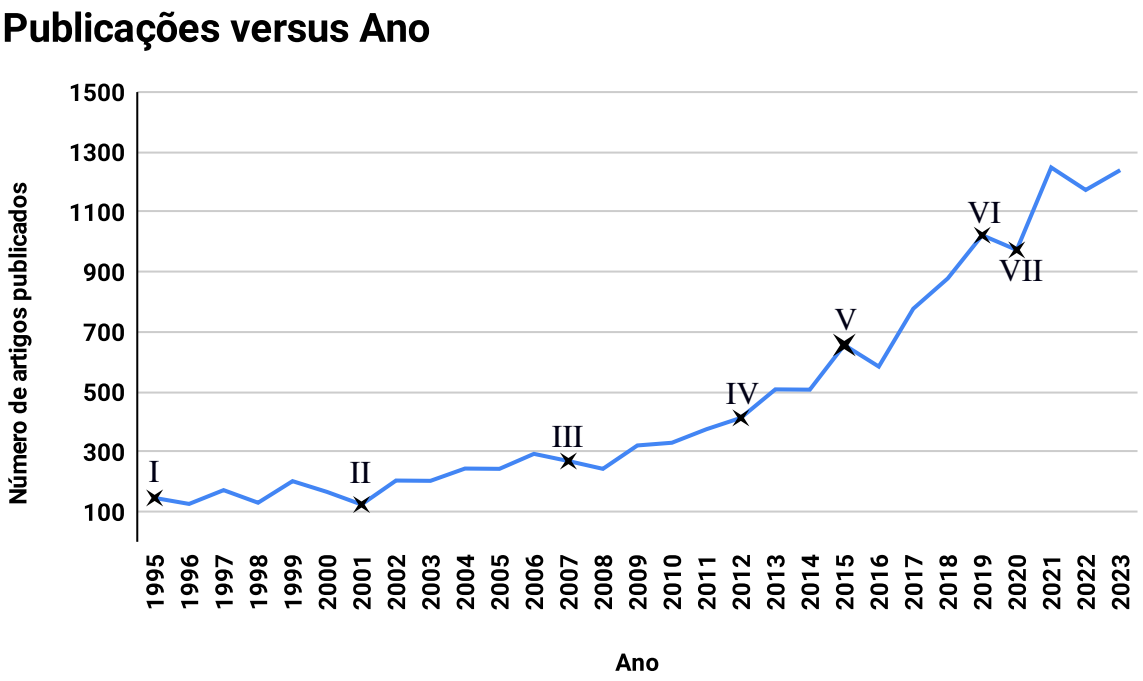
Figura 3 — Quantidade de artigos por ano por periódico.



Fonte: O autor.

Quanto aos investimentos, assim como levantado por McKinsey (2023) a partir de 2015, os valores aportados para empresas emergentes em computação quântica teve um grande salto, saindo de milhões para bilhões dólares em um curto período de tempo, e aumentou também a quantidade dessas empresas. Além disso, o período registrado das origens dos novos periódicos, como mostrado na Figura 3, também se dá no mesmo período onde os grandes investimentos começaram como é o caso da China em 2015 levantando por Kania e Costello (2018).

Figura 4 — Quantidade de artigos por ano, as estrelas representam fatores históricos.



Fonte: O autor.

Quando avalia-se a progressão das publicações é possível adicionar na visão, fatores históricos que podem estar relacionados com o volume de publicações, como, por exemplo:

I - 1994 - Peter Shor desenvolve o algoritmo de Shor (GALVÃO, 2007);

II - 2001 - Fatoração do número 15 semiprimo usando Shor em um computador quântico da IBM (DAVIS, 2022);

III - 2007 - Lançamento *D-Wave One* (ZAPAROLLI, 2019);

IV - 2012 - 1QBit lançada (1QBIT, 2024)

V - 2015 - Grande aporte Chinês declarado (KANIA; COSTELLO, 2018);

VI - 2019 - Google atinge a supremacia declarada (ARUTE *et al.*, 2019);

VII - 2020 - IBM *Quantum ROADMAP* (IBM, 2023).

Outro fator analisado foi a quantidade de publicações por periódico, conforme mostrado na Figura 3. Observa-se que os artigos publicados na IEEE não cresceram na mesma proporção que nas outras bases. Uma hipótese para isso é que, sendo uma das primeiras, a IEEE viu sua quantidade de publicações se dividir com o surgimento de novas bases específicas em computação quântica ao longo dos anos. Por outro lado, ao avaliar a quantidade total de artigos publicados, conforme Figura 4, percebe-se um crescimento constante acerca do tema. Os pontos marcados com estrelas indicam fatores históricos que, possível podem ter construído para o aumento das publicações.

Porém, ao analisar os artigos mais recentes referentes ao RSA, em 2021 os engenheiros da Google Gidney e Ekera (2021) postularam que seria necessário 20 milhões de *qubits* para quebrar o RSA, porém, logo no ano seguinte pesquisadores chineses Yan *et al.* (2022) criaram um algoritmo que dizia quebrar o RSA de 2048 com somente 372 *qubits*, o que gerou um grande impacto na comunidade acadêmica. Entretanto, em 2023 os pesquisadores da Google Khattar e Yosri (2023) reafirmaram a necessidade de milhões de *qubits* e geraram um artigo resposta inviabilizando o algoritmo gerado pelos pesquisadores chineses.

Esse fator demostra a evolução anual das pesquisas e, apesar de ainda não ser possível afirmar quem conseguirá implementar um computador quântico funcional, é fato que ele está cada vez mais próximo e assim como foi com o ENIAC *(Electronic Numerical Integrator and Computer)*, e não pode ser subestimado.

Com essa evolução, os algoritmos criptográficos como RSA e ECC, amplamente utilizados, são vulneráveis a ataques quânticos, o que torna necessária a adoção de algoritmos pós-quânticos (PQC). No entanto, essa transição é complexa, especialmente para países emergentes com recursos limitados. Assim como visto na Figura 2, na qual somente 7 países conseguem investir pelo menos 1 bilhão de dólares.

A migração para PQC enfrenta desafios consideráveis. A interoperabilidade entre dispositivos e sistemas legados é um desafio técnico relevante, assim como os custos e recursos necessários para implementação, que demandam investimentos significativos em pesquisa, desenvolvimento e infraestrutura. Além disso, a capacitação de profissionais qualificados é fundamental. A análise detalhada dos algoritmos PQC é fundamental para avaliar sua segurança e eficiência, identificando potenciais falhas e fortalecendo sua robustez. Os países emergentes também precisam desenvolver suas próprias soluções PQC, para evitar dependências externas e garantir a soberania digital (GROBMAN, 2020).

A cooperação internacional é outro aspecto essencial, permitindo a troca de conhecimento e colaboração para enfrentar a ameaça quântica de forma eficaz. No entanto, essa corrida contra o tempo coloca os países emergentes em desvantagem diante de potências como China e EUA, que investem maciçamente (GROBMAN, 2020).

Sem a preparação adequada, os países emergentes correm o risco de se tornarem alvos fáceis para ataques cibernéticos, o que poderia prejudicar seu desenvolvimento econômico e

tecnológico. Em resumo, a transição para algoritmos PQC é eminente, exige ação rápida e investimentos significativos em pesquisa, capacitação e cooperação internacional para garantir a segurança cibernética e evitar consequências desastrosas para a soberania e o desenvolvimento global.

Desse modo, seria ideal direcionar uma maior força de pesquisa não apenas para o desenvolvimento de computadores quânticos, mas também para a criptoanálise, na tentativa de desenvolver algoritmos pós-quânticos robustos e eficazes antes dos computadores quânticos se tornarem uma realidade efetiva. Esta atitude permitirá uma transição mais suave e preparada para a era quântica, e minimizaria os riscos (OVERBECK; SENDRIER, 2009).

5 CONSIDERAÇÕES FINAIS

A pesquisa analisou o impacto da computação quântica na segurança da informação, com foco na vulnerabilidade do algoritmo RSA e suas implicações para a segurança nacional. A revisão bibliográfica revelou um aumento significativo de pesquisas em computação quântica, o que evidencia a crescente preocupação com a ameaça que essa nova tecnologia representa à criptografia tradicional. A análise dos investimentos em pesquisa em computação quântica em diferentes países, especialmente China e Estados Unidos, mostrou uma corrida tecnológica intensa com implicações geopolíticas importantes. Os resultados da pesquisa reforçam a necessidade urgente de investir em pesquisa e desenvolvimento de soluções PQC para garantir a segurança em um mundo cada vez mais digitalizado.

Assim, como sempre foi, a criptografia desempenha um papel crucial na proteção de dados sensíveis e na garantia da privacidade das comunicações. No entanto, com os avanços da computação quântica e a possibilidade da criptoanálise quântica se tornar uma realidade, surge um novo cenário de desafios e preocupações em relação à segurança dos sistemas de criptografia tradicionais. Nesse contexto, o impacto da computação quântica na segurança internacional ganha relevância e destaque em estudos atuais, e reflete a necessidade iminente de adaptação e inovação para lidar com essa nova era tecnológica.

O movimento feito pela computação quântica em relação aos modelos de computação clássica se dá especialmente pela habilidade dos *qubits* de operarem em superposição e emaranhamento quântico, o que permite resolver problemas de maneira exponencial mais eficiente do que os computadores convencionais. Esse avanço tecnológico representa não apenas uma mudança paradigmática na computação, mas também um desafio à forma como tradicionalmente abordamos a segurança cibernética e a proteção de dados sensíveis.

Desse modo, para uma transição para a segurança pós-quântica será necessário esforços contínuos em pesquisa, desenvolvimento e educação sobre computação quântica e suas implicações para a segurança e a privacidade dos dados. A conscientização e a colaboração entre os diferentes setores da sociedade são essenciais para enfrentar os desafios impostos pela computação quântica, na tentativa de garantir a proteção dos sistemas e informações em um ambiente

pós-quântico.

Além disso, deve-se agir proativamente e adaptar-se às constantes novas ameaças no cenário da segurança cibernética tornam-se imperativos para manter a integridade e a confidencialidade das informações em um mundo digital em constante evolução. A segurança nacional deve ser tratada como uma prioridade estratégica em todas as esferas, envolvendo governos, empresas, instituições acadêmicas e a sociedade como um todo. A colaboração internacional e a troca de conhecimento se tornam ainda mais essenciais em um contexto global onde as fronteiras digitais se tornam cada vez mais tênues.

Diante desse cenário desafiador, é necessário estar atento e preparado para as mudanças que a era da computação quântica trará para a segurança cibernética e a proteção de dados sensíveis. A inovação, a pesquisa e o desenvolvimento de sistemas de segurança pós-quântica se apresentam como caminhos fundamentais para garantir a confiança e a robustez dos sistemas em um mundo interligado e digitalizado. É fundamental a união de esforços e a adoção de uma postura proativa para enfrentar os desafios impostos pela computação quântica, para construir um ambiente digital seguro e resiliente para as gerações futuras.

6 REFERÊNCIAS BIBLIOGRÁFICAS

1QBIT. **About Us**. [S.l.: s.n.], 2024. Disponível em: <https://1qbit.com/about/>. Acesso em: 28 abr. 2024.

ALMEIDA, José Maria Fernandes de. Alan Turing - A Bomba: a lógica, a matemática e a cifra. **Universidade do Minho**, Lisboa, fev. 1998. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/871/1/TURING.PDF>. Acesso em: 15 jan. 2024.

ARUTE, Frank et al. **Quantum supremacy using a programmable superconducting processor**. [S.l.: s.n.], 2019. Disponível em: <https://www.nature.com/articles/s41586-019-1666-5>. Acesso em: 28 abr. 2024.

BOUTIN, Chad; NIST. **Announces First Four Quantum-Resistant Cryptographic Algorithms**. [S.l.: s.n.], 2022. Disponível em: <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>. Acesso em: 28 abr. 2024.

CHEN, Lily et al. **NIST Internal Report 8105: Report on Post-Quantum Cryptography**. [S.l.: s.n.], 2016. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>. Acesso em: 28 abr. 2024.

DAVIS, Robert. **It's been 20 years since "15" was factored on quantum hardware**. [S.l.: s.n.], 2022. Disponível em: <https://www.ibm.com/quantum/blog/factor-15-shors-algorithm>. Acesso em: 28 abr. 2024.

FERRAIOLO, Hildegard; REGENSCHEID, Andrew. **Cryptographic Algorithms and Key Sizes for Personal Identity Verification**. [S.l.], 2023. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-78-5.ipd.pdf>. Acesso em: 28 abr. 2024.

GALVÃO, Ernesto F. **O que é computação quântica**. 1. ed. Rio de Janeiro: Vieira & Lent, 2007. ISBN 978-85-88782-43-3.

GIDNEY, Craig; EKERA, Martin. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. **QUANTUM**, 2021. Disponível em: <https://doi.org/10.22331/q-2021-04-15-433>. Acesso em: 13 abr. 2024.

GOOGLE LLC. **Google Transparency Report**. [S.l.: s.n.], 2024. Disponível em: <https://transparencyreport.google.com/https/overview>. Acesso em: 28 abr. 2024.

GROBMAN, Steve. Quantum Computing's Cyber-Threat to National Security. **PRISM**, v. 9, n. 1, p. 52–67, 2020. Disponível em: <https://www.jstor.org/stable/10.2307/26940159>. Acesso em: 20 mar. 2024.

GRUMBLING, Emily; HOROWITZ, Mark. **Quantum Computing: Progress and Prospects**. Edição: Engineering National Academies of Sciences e Medicine. Washington, DC: The National Academies Press, 2019. ISBN 978-0-309-47969-1. DOI: 10.17226/25196. Disponível em: <https://nap.nationalacademies.org/catalog/25196/quantum-computing-progress-and-prospects>. Acesso em: 28 abr. 2024.

IBM. **The IBM Quantum Roadmap**. [S.l.: s.n.], 2023. Disponível em: <https://www.ibm.com/roadmaps/quantum/>. Acesso em: 28 abr. 2024.

KANIA, Elsa B.; COSTELLO, John K. **QUANTUM HEGEMONY?: China's Ambitions and the Challenge to U.S. Innovation Leadership**. [S.l.], 2018. P. 6–13. Disponível em: <http://www.jstor.org/stable/resrep20450.6>. Acesso em: 28 abr. 2024.

KHATTAR, T.; YOSRI, N. **A comment on "Factoring integers with sublinear resources on a superconducting quantum processor."** [S.l.: s.n.], 2023. Disponível em: <http://arxiv.org/abs/2307.09651>. Acesso em: 13 abr. 2024.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down**. 6. ed. [S.l.]: Pearson Education do Brasil, 2013. ISBN 978-85-430-1443-2.

LANDAU, Susan. Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations. **IEEE Security & Privacy**, v. 12, n. 1, p. 62–64, 2014. DOI: 10.1109/MSP.2013.161.

MATZA, Max. **Kennedy: Milhares de arquivos sobre assassinato são abertos após 6 décadas pelo governo dos EUA**. [S.l.]: BBC, 2023. Disponível em: <https://www.bbc.com/portuguese/internacional-64002688>. Acesso em: 28 abr. 2024.

MCKINSEY. **Quantum Technology Monitor**. [S.l.: s.n.], 2023. Disponível em: <https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf>. Acesso em: 28 abr. 2024.

MOSCA, Michele. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? **IEEE Security & Privacy**, v. 16, n. 5, p. 38–41, 2018. DOI: 10.1109/MSP.2018.3761723.

NIST. **Fifth PQC Standardization Conference**. [S.l.: s.n.], 2024. Disponível em: <https://csrc.nist.gov/Events/2024/fifth-pqc-standardization-conference>. Acesso em: 28 abr. 2024.

NIST-SUBMISSION. **Post-Quantum Cryptography PQC: Round 1 Submissions**. [S.l.: s.n.], 2017. Disponível em: <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions>. Acesso em: 28 abr. 2024.

OVERBECK, Raphael; SENDRIER, Nicolas. Code-based cryptography. In: **Post-Quantum Cryptography**. Edição: Daniel J. Bernstein, Johannes Buchmann e Erik Dahmen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. P. 95–145. ISBN 978-3-540-88702-7. DOI: 10.1007/978-3-540-88702-7_4. Disponível em: <https://doi.org/10.1007/978-3-540-88702-7_4>. Acesso em: 28 abr. 2024.

QURECA. **Overview of Quantum Initiatives Worldwide 2023**. [S.l.: s.n.], 2023. Disponível em: <https://www.qureca.com/overview-of-quantum-initiatives-worldwide-2023/>. Acesso em: 21 abr. 2024.

REAGAN'S, Ronald. **President Reagan's Address to the Nation on the Soviet Attack on a Korean Airliner (KAL 007)**. [S.l.]: YouTube, 2011. Disponível em: <https://www.youtube.com/watch?v=9VA4W1wDMAk>. Acesso em: 28 abr. 2024.

SCHRÖDINGER, Erwin. Die gegenwärtige Situation in der Quantenmechanik. **Naturwissenschaften**, Springer, v. 23, p. 823–828, 1935.

SINGH, Simon. **The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography**. [S.l.]: Record, 2001. ISBN 978-0385495325.

WOOD, Georgia. Encryption and Security in a Post-Quantum World. **CSIS**, 2022. Disponível em: <https://www.csis.org/blogs/strategic-technologies-blog/encryption-security-post-quantum-world>. Acesso em: 15 mar. 2024.

YAN, Bao et al. **Factoring integers with sublinear resources on a superconducting quantum processor**. [S.l.: s.n.], 2022. arXiv: 2212.12372 [quant-ph]. Disponível em: <https://arxiv.org/pdf/2212.12372>. Acesso em: 28 abr. 2024.

ZAPAROLLI, Domingos. **A era dis qubits**. [S.l.: s.n.], 2019. Disponível em: <https://revistapesquisa.fapesp.br/a-era-dos-qubits/>. Acesso em: 28 abr. 2024.

ZHOU, Xin; TANG, Xiaofei. Research and implementation of RSA algorithm for encryption and decryption. In: PROCEEDINGS of 2011 6th International Forum on Strategic Technology. [S.l.: s.n.], 2011. v. 2, p. 1118–1121. DOI: 10.1109/IFOST.2011.6021216.