REVISTA DA sbfoton
Vol. 5 - Dez/2024

Criptografia quântica e pós-quântica: evolução e perspectivas de uso em larga escala

Eduardo Mobilon e João Batista Rosolem
Fundação CPQD – Soluções de Conectividade
mobilon@cpqd.com.br, rosolem@cpqd.com.br

RESUMO: *A crescente demanda por transferência de dados segura e eficiente impulsiona o uso de sistemas de comunicação óptica e soluções criptográficas, essenciais para proteger informações sensíveis de ciberataques. Contudo, o avanço da computação quântica ameaça os métodos tradicionais de criptografia. Como resposta, surgem a criptografia quântica e a pós-quântica, que buscam fortalecer a segurança contra ataques futuros. Este artigo examina a evolução dessas tecnologias e suas aplicações potenciais, abordando suas vantagens e limitações. Também destaca o panorama global de pesquisa e desenvolvimento, incluindo a atuação brasileira em tecnologias quânticas e a importância da padronização para adoção em larga escala.*
Palavras-chave*: Criptografia quântica. Computação quântica. Distribuição quântica de chaves. Criptografia pós-quântica. Segurança da informação.*

ABSTRACT: *The increasing demand for secure and efficient data transfer drives the adoption of optical communication systems and cryptographic solutions, critical for protecting sensitive information from cyberattacks. Yet, advances in quantum computing threaten traditional cryptographic methods. In response, quantum and post-quantum cryptography emerge to strengthen security against future attacks. This paper explores the evolution and potential applications of these technologies, discussing their advantages and limitations. It also highlights global research and development efforts, including Brazil's contributions in quantum technologies and the importance of standardization for large-scale adoption.*
Keywords: *Quantum cryptography. Quantum computing. Quantum key distribution (QKD). Post-quantum cryptography (PQC). Information security.*

http://doi.org/10.5281/zenodo.14659440

INTRODUÇÃO

No cenário em constante evolução da comunicação moderna, a demanda por transferência de dados mais rápida, eficiente e segura levou à ampla adoção de sistemas de comunicações ópticas devido a sua elevada largura de banda e alcance, muito superiores quando comparadas a outros sistemas de comunicação existentes, como rádio, micro-ondas e cabos coaxiais. A informação transferida e armazenada tornou-se, de longe, o recurso global mais importante e valioso do mundo moderno, produzindo vários tipos de dados que precisam ser protegidos contra os ataques cibernéticos que geram prejuízos enormes a pessoas, organizações e países envolvidos. À medida que a informação atravessa as vastas redes de comunicação, a necessidade de proteger esses dados sensíveis torna-se crucial, de modo que a fragilidade dos canais de comunicações ópticas, em particular, apresenta desafios únicos para manter a privacidade e a segurança dos dados transmitidos. Nesse cenário, sistemas criptográficos desempenham um papel fundamental na garantia da confidencialidade e integridade das informações transmitidas ou armazenadas.

Por outro lado, o rápido avanço da tecnologia de computação quântica representa uma ameaça tangível e iminente à segurança desses sistemas. À medida que os computadores quânticos se aproximam da praticidade, os métodos de criptografia assimétrica clássica usados como parte das soluções de criptografia modernas podem ser comprometidos em algumas décadas, impulsionando o desenvolvimento das técnicas de criptografia quântica e pós-quântica que surgiram em resposta a esses desafios e ameaças significativas à segurança da informação. A primeira na verdade corresponde a métodos de distribuição de chaves e de geração de números aleatórios baseados em princípios da mecânica quântica, enquanto a segunda, corresponde a novos algoritmos clássicos rodando em processadores ou dispositivos clássicos que usam métodos matemáticos mais robustos e resistentes ao poder da computação quântica.

A implementação e uso desses novos tipos de criptografia, em particular as técnicas de distribuição quântica de chaves (*Quantum Key Distribution* – QKD) e os novos algoritmos de criptografia pós-quântica (*Post-Quantum Cryptography* – PQC), tornaram-se um tema de interesse nacional e internacional e a maioria dos países está tentando

ativamente desenvolver seus próprios produtos e redes, a fim de reduzir a dependência de soluções estrangeiras. No momento trava-se uma batalha de convencimento para uso dessas tecnologias e se uma delas é mais eficiente do que a outra.

Este artigo descreve a evolução desses dois tipos de criptografia e sua perspectiva de uso em larga escala.

SISTEMAS CRIPTOGRÁFICOS E A AMEAÇA DA COMPUTAÇÃO QUÂNTICA

Os sistemas criptográficos clássicos podem ser classificados em simétricos, assimétricos e híbridos. Os primeiros utilizam uma mesma chave criptográfica para cifrar e decifrar os dados e sua segurança reside na complexidade dessa chave. Com 256 bits, por exemplo, o espaço de chaves é de 2^{256} ou mais de 10^{77} possibilidades. Trata-se de um sistema ultra seguro, resistente inclusive à computação quântica. Porém, ele exige um mecanismo através do qual a chave seja compartilhada entre os nós Alice e Bob, conforme ilustrado na Figura 1.

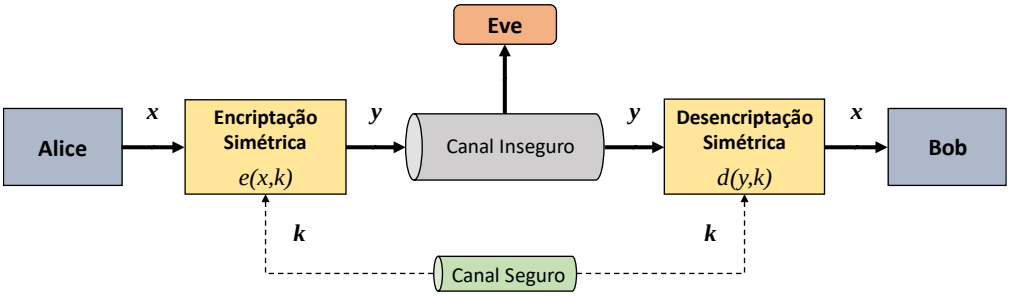

Figura 1 - Sistema criptográfico simétrico.

Esse problema do compartilhamento da chave foi resolvido na década de 1970, com o advento dos sistemas de criptografia de chaves públicas (*Public-Key Cryptography* – PKC) — uma ideia revolucionária proposta por Whitfield Diffie e Martin Hellman [1] com contribuições de Ralph Merkle [2] — nos quais os dados são cifrados com uma chave pública e decifrados com uma privada (de forma assimétrica), conforme ilustrado na Figura 2. Sua segurança é baseada em problemas matemáticos complexos como o do logaritmo discreto e o da fatoração de grandes números, os quais são difíceis de serem resolvidos por algoritmos da computação clássica.

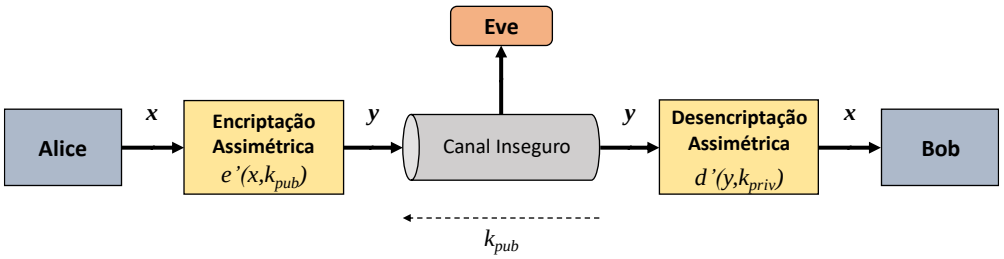

Figura 2 - Sistema criptográfico assimétrico.

No entanto, uma vez que os sistemas assimétricos chegam a ser mil vezes mais lentos que os simétricos, na prática utilizam-se os sistemas híbridos, nos quais os dados são protegidos pela criptografia simétrica (rápida, eficiente e segura) enquanto as chaves são trocadas entre Alice e Bob através da criptografia assimétrica.

A ameaça da computação quântica aos sistemas criptográficos modernos (clássicos) depende basicamente de dois fatores: a existência de um computador quântico especialmente projetado para atacar os sistemas criptográficos e algoritmos quânticos que sejam executados nesses computadores. O chamado *Q-Day* se refere a um evento futuro hipotético no qual a criptografia baseada em computadores clássicos será quebrada pela computação quântica. Em 1994, Peter Shor desenvolveu um algoritmo eficiente (o mais famoso e possivelmente o mais importante descoberto até hoje) para encontrar logaritmos discretos e fatorar inteiros com execução em tempo polinomial [3], destruindo a base de segurança para a maioria dos sistemas criptográficos de chave pública (assimétrica) implantados atualmente. Por sua vez, Lov K. Grover elaborou em 1996 um algoritmo de busca quântica que encontra a entrada esperada com uma aceleração quadrática de $\sqrt{N}$ passos [4], permitindo que um sistema criptográfico simétrico com chaves de 256 bits, por exemplo, seja atacado por força bruta com 2^{128} passos por um computador quântico, o que ainda é um esforço impraticável no atual estado da arte.

Apesar dos progressos significativos, diversos desafios tecnológicos ainda nos colocam distantes dessa realidade, entre os quais o problema da decoerência dos Qubits (*quantum bits*), que constituem a unidade básica de informação da computação quântica, e os erros induzidos por fatores ambientais, impedindo que os computadores quânticos atuais tenham o número de Qubits estáveis necessários para executar os algoritmos de Shor e Grover.

DISTRIBUIÇÃO QUÂNTICA DE CHAVES

Nesse cenário de ameaça à infraestrutura de criptografia clássica, a criptografia quântica surge como uma alternativa tecnológica capaz de alcançar a segurança teórica da informação explorando os princípios físicos da mecânica quântica, como exemplificado pelo teorema quântico de não clonagem e o princípio da incerteza de Heisenberg. Dessa maneira, é possível afirmar que sua segurança permanece indestrutível mesmo diante de avanços futuros do poder computacional.

Como uma das aplicações mais bem-sucedidas da criptografia quântica, a técnica de QKD [5] fornece segurança baseada na teoria da informação e é baseada nas leis da física quântica para distribuir chaves secretas simétricas entre um par de partes confiáveis. Essas chaves secretas podem então ser usadas por sistemas criptográficos simétricos para criptografar mensagens confidenciais a serem transferidas por um canal público. Sistemas QKD são usados, assim, como parte de um sistema criptográfico híbrido para garantir a confidencialidade dos dados transmitidos pelos sistemas de comunicação convencionais, com várias aplicações já sendo exploradas nas áreas de finanças e bancos, governo e defesa, nuvem e centros de dados, infraestrutura crítica, etc.

Conforme mostra a Figura 3, os elementos básicos de um sistema QKD são um transmissor (QKD-Tx) e um receptor (QKD-Rx), cada um dos quais denominado módulo QKD. Um enlace QKD — tipicamente formado por um canal quântico e outro clássico — conecta esses módulos e permite assim o compartilhamento das chaves criptográficas. O canal quântico é reservado para os sinais quânticos, como por exemplo o estado de luz coerente de nível de fóton único para transmitir sequências de bits aleatórias. O canal clássico, por sua vez, é reservado para sincronização e troca de dados necessários para o processo de seleção dos bits que formarão as chaves. Dessa forma, os módulos QKD geram chaves e as fornecem aos aplicativos que criptografam os dados para serem então transmitidos por qualquer enlace de comunicação em uma rede convencional.

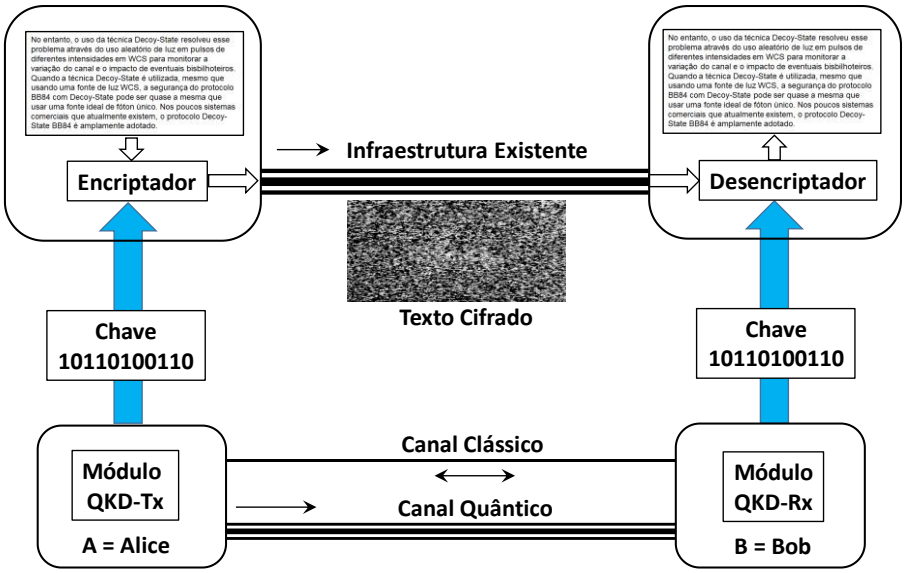

Figura 3 - Ilustração dos elementos de um sistema QKD.

Nos últimos anos, as tecnologias de QKD em enlaces ponto a ponto tiveram progressos significativos em termos de protocolos, dispositivos e sistemas, incluindo demonstrações em enlaces de fibras ópticas, fazendo uso de multiplexação por divisão de comprimentos de onda (*Wavelength Division Multiplexing* – WDM) e fibras especiais, bem como de transmissões por satélites de tecnologia quântica [5]. Adicionalmente, uma variedade de protocolos e dispositivos QKD foram desenvolvidos para melhorar o desempenho dessa técnica, sendo quantificados em termos de taxa da chave secreta, alcance e segurança.

O BB84 foi o primeiro protocolo QKD da história, proposto por Charles Henry Bennett e Gilles Brassard em 1984 [6], sendo então demonstrado com um protótipo experimental em 1992 [7]. Seus estudos são os mais abundantes em profundidade entre todos os protocolos QKD, o que garante sua alta segurança teórica. O protocolo BB84 original deve usar uma fonte ideal de fóton único, porém, como isso ainda não é prático e comercialmente viável, pode-se usar um laser semicondutor comum para preparar o que se chama de estado coerente fraco (*Weak Coherent State* – WCS) [5]. Tal abordagem alternativa é uma maneira prática e barata de criar probabilisticamente pulsos de fóton único e é amplamente empregada em sistemas de criptografia quântica para QKD, permitindo se aproximar de uma fonte ideal de fóton único. Entretanto, uma vez que a luz WCS contém vários fótons, isso abre a possibilidade de ocorrência de ameaças pelo ataque de divisão do número de fótons (*Photon Number Splitting* – PNS). Dessa forma,

sem algum complemento a taxa de chave segura para o protocolo BB84 usando WCS é bastante limitada.

A técnica *Decoy-State* [5] resolveu esse problema através do uso aleatório de luz em pulsos de diferentes intensidades em WCS para monitorar a variação do canal e o impacto de eventuais bisbilhoteiros. Quando ela é utilizada, mesmo com uma fonte de luz WCS a segurança do protocolo BB84 pode ser quase a mesma daquela usando uma fonte ideal de fóton único. Assim, nos poucos sistemas comerciais atualmente existentes, o protocolo *Decoy-State* BB84 é amplamente adotado [5].

Para a implementação de tais técnicas, o transmissor QKD deve preparar os estados quânticos como portadores de informações da chave. Tal processo, conhecido como preparação do estado quântico, consiste principalmente na seleção de bases, preparação de estados e modulação de intensidade de pulso (modulação *do Decoy-State*). Inicialmente, o transmissor e o receptor QKD selecionam dois conjuntos de bases ortogonais (base de codificação para Tx e base de medição para Rx), de modo que, uma vez que cada conjunto de bases contém dois estados quânticos ortogonais, quatro estados quânticos serão preparados no transmissor. O pulso curto emitido pela fonte WCS é usada como portadora de informação e é combinada com modulação de intensidade para atingir o *Decoy-State*. Nesse protocolo o pulso do estado quântico pode ser modulado em três intensidades diferentes que podem ser usadas como o estado do sinal, estado de isca e estado de vácuo, respectivamente. A codificação da informação é o processo no qual o transmissor carrega aleatoriamente o estado quântico utilizado para codificar as informações principais no pulso correspondente. De acordo com a sequência de números aleatórios, os estados quânticos que precisam ser codificados no pulso de luz são primeiro determinados através de uma correspondência convencionada com os dígitos binários (0, 1). Então, com base em determinada informação de estado quântico, o estado usado para codificar a informação da chave é modulado em um pulso correspondente, enquanto as informações dos bits são salvas.

A seguir, a transmissão de estado quântico é o processo no qual um transmissor envia um pulso de estado quântico carregado com informações importantes para o receptor através de um canal quântico, por exemplo via fibra óptica ou espaço livre. O transmissor registra a intensidade do pulso emitido e a informação da chave codificada,

enviando também sinais de sincronização ao receptor para permitir a detecção correta dos sinais do estado quântico.

Por fim, a medição do estado quântico pelo receptor consiste na aquisição da chave bruta nos processos de detecção e decodificação. O receptor primeiro seleciona aleatoriamente uma base de medição para medir os pulsos carregados com estados quânticos enviados pelo transmissor, detecta o sinal de fóton demodulado em detectores de fóton único e registra a resposta desses detectores para obter a chave bruta. O pós-processamento do protocolo BB84 é completado através da troca de informações entre as partes transmissoras e receptoras usando o canal clássico. Esse processo de destilação da chave usa autenticação para garantir a consistência e integridade das informações trocadas.

As empresas que hoje fornecem os equipamentos para QKD passaram por um longo processo de desenvolvimento laboratorial, testes em campo e testes pré-comerciais. Alguns desses produtos foram implementados pela indústria nos últimos anos, com destaque para empresas como a Toshiba e ID Quantique [8-9]. Já do ponto de vista da coexistência da tecnologia de QKD com a infraestrutura de telecomunicações existente, há inúmeros desafios a serem superados. As fibras ópticas instaladas são invariavelmente sujeitas a perturbações devido às mudanças nas condições ambientais e ao seu estresse físico, que por sua vez causam perturbações nos estados quânticos transmitidos. Elas também causam perdas de potência devido às emendas e curvas acentuadas. Adicionalmente, no uso compartilhado em sistemas WDM, o ruído existente provindo de amplificação óptica paralela também pode comprometer o desempenho da técnica de QKD.

Para avançar em larga escala de implantação comercial de sistemas QKD é necessário um extenso processo de padronização, que de fato vem ocorrendo. Atualmente, várias atividades de padronização em tecnologias quânticas estão em andamento em todo o mundo [10-11]. Todavia, apesar dos esforços dispensados por todos os atores envolvidos na iniciativa, ainda existem desafios significativos a serem superados para que o ecossistema integrado idealizado seja de fato estabelecido.

Em 2020 a Agência de Segurança Nacional dos EUA (*National Security Agency* – NSA) avaliou a usabilidade e as limitações técnicas atuais da criptografia quântica, em especial da técnica de QKD [12], listando cinco principais deficiências:

- QKD é somente uma solução parcial pois não possui um mecanismo de autenticação;
- QKD requer equipamento especial;
- QKD aumenta os custos de infraestrutura e os riscos de ameaças internas;
- Garantir e validar a QKD é um desafio significativo;
- QKD aumenta o risco de ataques de negação de serviço.

Uma publicação recente analisa e oferece caminhos para superar cada um desses problemas [13] e, dadas as suas propriedades complementares, o uso da técnica de QKD em combinação com os algoritmos de PQC parece fortalecer a estratégia de defesa pós-quântica.

CRIPTOGRAFIA PÓS-QUÂNTICA

De modo complementar, os novos algoritmos de PQC constituem uma resposta direta ao avanço da computação quântica e as suas implicações para a segurança dos sistemas criptográficos tradicionais. Alternativas começaram a ser exploradas desde os anos 2000, até que em 2016 o Instituto Nacional de Padrões e Tecnologia dos EUA (*National Institute of Standards and Technology* – NIST) lançou uma chamada formal para submissões de algoritmos de criptografia pós-quântica, iniciando uma competição global para identificar, analisar e padronizar algoritmos de criptografia que possam resistir à computação quântica.

As principais abordagens que utilizam problemas matemáticos de difícil solução tanto na computação clássica quanto na quântica são [14-15]:

- *Lattice-based Cryptography*: algoritmos baseados em problemas de redes, como o LWE (*Learning With Errors*) e o SIS (*Short Integer Solution*). Exemplos incluem Kyber e Dilithium;
- *Code-based Cryptography*: baseada em problemas de decodificação de códigos de correção de erros, como o esquema McEliece;
- *Hash-based Cryptography*: algoritmos que utilizam funções *hash* para assinatura digital, como SPHINCS+;

- *Multivariate Polynomial Cryptography*: algoritmos baseados na dificuldade de solução de sistemas de equações polinomiais multivariadas, como o Rainbow;
- *Isogeny-based Cryptography*: baseada na dificuldade de encontrar isogenias entre curvas elípticas, como o SIKE.

Em julho de 2022, o NIST anunciou quatro algoritmos principais que avançaram para a fase final de padronização [16]:

- *CRYSTALS–Kyber*: um algoritmo de criptografia de chave pública baseado em problemas de rede conhecido por sua eficiência e segurança;
- *CRYSTALS–Dilithium*: um algoritmo de assinatura digital projetado para ser robusto e eficiente, também baseado em problemas de rede;
- *SPHINCS+*: um algoritmo de assinatura digital baseado em *hash*, notável por sua abordagem sem suposições, o que significa que sua segurança não depende de suposições matemáticas específicas;
- *FALCON*: outro algoritmo de assinatura digital baseado em problemas de rede, conhecido por seu tamanho de assinatura pequeno e alta segurança.

Os três primeiros já possuem versões finais das padronizações FIPS (*Federal Information Processing Standard*) [17-19], publicadas em agosto de 2024. Outros quatro algoritmos candidatos seguem para uma quarta rodada de estudos e avaliação: BIKE, Classic McEliece, HQC e SIKE.

O governo americano está adotando diversas iniciativas para preparar seus sistemas de segurança nacional para a era da computação quântica, focando na migração para criptografia pós-quântica. Nesse intuito, o Conjunto de Algoritmos Comerciais de Segurança Nacional (*National Security Algorithm Suite* – CNSA) é uma seleção de algoritmos criptográficos promulgado pela NSA que serve como base criptográfica para proteger as informações dos sistemas de segurança nacional dos EUA até o nível ultrassecreto. Em setembro de 2022, a NSA anunciou o CNSA 2.0, que inclui suas primeiras recomendações para algoritmos criptográficos pós-quânticos (CRYSTALS-Kyber e CRYSTALS-Dilithium) e espera uma migração completa dos equipamentos de redes de comunicação até 2030. Em dezembro de 2022, o governo americano estabeleceu a Lei de Preparação para Segurança Cibernética de Computação Quântica, que exige que as agências federais “migrem sistemas para criptografia pós-quântica, que seja resiliente contra os ataques de computadores quânticos e computadores padrão”.

CRIPTOGRAFIA QUÂNTICA NO CPQD

Alinhado às iniciativas da comunidade científica mundial e às necessidades particulares do Brasil na área de segurança cibernética no domínio quântico, o CPQD vem articulando atividades de PD&I para exploração das tecnologias de geração quântica de números aleatórios, distribuição quântica de chaves e algoritmos de criptografia pós-quântica.

Espera-se ainda a montagem de um *testbed* a partir de soluções comerciais para integração dessas tecnologias, permitindo seu uso por empresas e universidades parceiras para a realização de experimentos com aplicações em áreas como *blockchain*, inteligência artificial, redes de comunicação, computação em nuvem, simuladores e dispositivos seguros para a Internet das coisas.

CONCLUSÃO

A PQC é considerada segura com base no conhecimento atual. Entretanto, diferentemente da técnica de QKD, não oferece segurança incondicional. Se novos algoritmos quânticos forem desenvolvidos no futuro com a capacidade de resolver de modo mais eficiente os problemas matemáticos nos quais os algoritmos PQC são baseados, ela poderia ser comprometida. Alternativamente, a técnica de QKD constitui a solução mais segura a longo prazo, uma vez que apresenta segurança incondicional garantida por princípios físicos fundamentais da mecânica quântica.

Embora no momento ocorra uma batalha de convencimento para uso dessas duas tecnologias e se uma delas é mais eficiente do que a outra, é possível que ocorra a convivência das duas abordagens por algum tempo e talvez até uma hibridização [20] na sua adoção.

REFERÊNCIAS

[1] W. Diffie and M. Hellman, “New Directions in Cryptography”. IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, November 1976. https://doi.org/10.1109/TIT.1976.1055638.

[2] Ralph C. Merkle, “Secure Communications Over Insecure Channels”. Communications of the ACM, vol. 21, no. 4, pp.294–299, 1978. https://doi.org/10.1145/359460.359473.

[3] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134, 1994. https://doi.org/10.1109/SFCS.1994.365700.

[4] Lov K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search”. Proceedings of the 28th ACM Symposium on Theory of Computing (STOC), pp. 212–219, 1996. https://doi.org/10.1145/237814.237866.
Updated version available at https://doi.org/10.48550/arXiv.quant-ph/9605043.

[5] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894, Secondquarter 2022. https://doi.org/10.1109/COMST.2022.3144219.

[6] Bennett, C. H. and Brassard, G., “Quantum Cryptography: Public Key Distribution and Coin Tossing”. Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India, pp. 175-17, 1984. https://doi.org/10.48550/arXiv.2003.06557.

[7] Bennett, C. H., Bessette, F., Brassard, G., et al., “Experimental Quantum Cryptography”. Journal of. Cryptology, vol. 5, pp. 3–28, 1992. https://doi.org/10.1007/BF00191318.

[8] R. Daws, “Toshiba and Orange demo quantum-secure fibre data transmission”, Telecoms Tech News, February 22, 2024, disponível em https://www.telecomstechnews.com/news/2024/feb/22/toshiba-orange-demo-quantum-secure-fibre-data-transmission/.

[9] R. Le Maistre, “SK Telecom, IDQ et al form Quantum Alliance”, TelecomTV, Mar 8, 2024, disponível em: https://www.telecomtv.com/content/security/sk-telecom-idq-et-al-form-quantum-alliance-49878/.

[10] Liu, R., et al.: Towards the industrialization of quantum key distribution in communication networks: a short survey. IET Quant. Comm. 3(3), 151– 163 (2022). https://doi.org/10.1049/qtc2.12044.

[11] Van Deventer, O., Spethmann, N., Loeffler, M. et al. Towards European standards for quantum technologies. EPJ Quantum Technol. 9, 33 (2022). https://doi.org/10.1140/epjqt/s40507-022-00150-1.

[12] National Security Agency (NSA). Quantum key distribution (QKD) and quantum cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[13] Renato Renner and Ramona Wolf, “The debate over QKD: A rebuttal to the NSA’s objections”. arXiv [quant-ph]. https://doi.org/10.48550/arXiv.2307.15116.

[14] Bernstein, D., Lange, T., “Post-Quantum Cryptography”. Nature, vol. 549, pp. 188–194, 2017. https://doi.org/10.1038/nature23461.

[15] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen (editors). Post-Quantum Cryptography. Springer Berlin, Heidelberg, ISBN 9783540887010, 2009. https://doi.org/10.1007/978-3-540-88702-7.

[16] NIST IR 8413-upd1. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8413-upd1.

[17] FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024. https://doi.org/10.6028/NIST.FIPS.203.

[18] FIPS 204. Module-Lattice-Based Digital Signature Standard. August 2024. https://doi.org/10.6028/NIST.FIPS.204.

[19] FIPS 205. Stateless Hash-Based Digital Signature Standard. August 2024. http://doi.org/10.6028/NIST.FIPS.205.

[20] D. Marchsreiter and J. Sepúlveda, “A PQC and QKD Hybridization for Quantum-Secure Communications”, 26th Euromicro Conference on Digital System Design (DSD), Golem, Albania, 2023, pp. 545-552, https://doi.org/10.1109/DSD60849.2023.00081