Segurança da Informação: Computação Quântica e Criptografia Pós-Quântica

João Pedro Rodrigues Leite

4 de setembro de 2024

1 Introdução

Nos últimos anos, o campo da *Segurança da Informação* tem enfrentado grandes desafios devido ao avanço da tecnologia quântica. Empresas como IBM, Microsoft e Google estão envolvidas e empenhadas no desenvolvimento de computação quântica. O desenvolvimento de computadores quânticos, que utilizam princípios da física/mecânica quântica como a superposição e o emaranhamento, princípios nos quais não podem ser explorados na computação convencional. o princípio de superposição pode ser entendido por exemplo como a representação de um bit quântico ou qubit em vários estados, podendo então assumir valores como 0, 1 ou ambos ao mesmo tempo, já o emaranhamento cria uma interdepedência entre as partículas ou os qubits independentemente da distância entre eles, então ao fazer a medição do valor de um qubit imediatamente já será possível identificar o valor assumido pelo outro qubit que está interligado, com isso, os computadores quânticos podem realizar operações em paralelo, e ter o potencial de quebrar a criptografia convencional usada para proteger dados sensíveis nas comunicações digitais [4]. Esses sistemas representam uma ameaça significativa, pois, enquanto a criptografia convencional depende da complexidade computacional de realizar cálculos matemáticos, os computadores quânticos podem realizar operações paralelas em escala exponencial, comprometendo a segurança de muitos algoritmos de criptografia que são utilizados hoje.

2 Ameaças da Computação Quântica

Uma das principais ameaças que surgem com o desenvolvimento dos computadores quânticos é a estratégia conhecida como *store now, decrypt later* (armazenar agora, decifrar depois) [1]. Essa técnica consiste no armazenamento de dados criptografados com a esperança de que, no futuro, quando os computadores quânticos forem capazes de quebrar algoritmos criptográficos atuais utilizando algoritmos como o de Shor, esses dados possam ser decifrados. Esse cenário coloca em risco a integridade e confidencialidade das comunicações digitais.

3 Soluções Criptográficas Pós-Quânticas

Diante desse contexto, novas técnicas de *criptografia pós-quântica* (CPQ) estão sendo desenvolvidas para mitigar os riscos impostos pela computação quântica. A CPQ visa criar algoritmos que sejam resistentes a ataques baseados em computadores quânticos, utilizando métodos que permanecem permitem os dados sejam mantidos em segurança mesmo com a capacidade de processamento exponencial computadores quânticos [5].

4 Comparação entre Criptografia Clássica e Pós-Quântica

A diferença entre a criptografia clássica e a pós-quântica reside nos fundamentos matemáticos que protegem os dados. A criptografia clássica, como o RSA, que é amplamente utilizado na geração de chaves assimétricas como os certificados digitais, nas comunicações SSH para autenticação ou até mesmo na camada SSL/TLS para manter a comunicação segura, sua segurança baseia-se na complexidade da fatoração de números grandes e no logaritmo discreto, problema que é vulnerável a algoritmos quânticos como o algoritmo desenvolvido por Peter Shor em 1994 [6]. Há também outro algoritmo que foi desenvolvido por Lov Grover em 1996, e que também pode causar um impacto na criptografia convencial, especificamente nas que são baseadas em chaves simétricas como o AES, 3DES entre outros. Estima-se que esse algoritmo nas chaves simétricas reduziria a segurança delas pela metade, e uma das soluções encontradas para reduzir os impactos seria duplicar o tamanho

da chave para manter a segurança dos dados [3]. Em contrapartida, os algoritmos de criptografia pós-quântica são projetados para serem resistentes a esses tipos de ataques, garantindo a segurança das informações em um cenário de computação quântica [2].

5 Conclusão

Com o iminente avanço da computação quântica, a segurança da informação enfrenta um de seus maiores desafios. A adoção de algoritmos de criptografia pós-quântica é essencial para garantir a proteção dos dados nas comunicações digitais.

Referências

[1] Cameron R Argetsinger. The promise and peril of quantum computing and its implications for cyber insurance. *Journal of Emerging Issues in Litigation/Winter*, 4(1):65–73, 2024.

[2] Tim Callan. Quantum computing trends 2024. `https://www.siliconrepublic.com/machines/quantum-computing-trends-2024-sectigo-tim-callan`, 2024. Acessado em 05/08/2024.

[3] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[4] Saptarshi Mitra, Bappaditya Jana, Supratim Bhattacharya, Prashnatita Pal, and Jayanta Poray. Quantum cryptography: Overview, security issues and future challenges. In *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)*, pages 1–7. IEEE, 2017.

[5] S Nandhini, Harpreet Singh, and UN Akash. An extensive review on quantum computers. *Advances in Engineering Software*, 174, 2022.

[6] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.