International Journal of Marketing and Technology
Vol. 14 Issue 9, Sep 2024,
ISSN: 2249-1058 Impact Factor: 8.469
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Quantum Computing: Transforming the Future of Cryptography

Nirupam Samanta | Cyber Security Professional
Rajiv Dewan | Cyber Security Professional

Quantum processors represent a groundbreaking advancement in the computing industry, redefining the limits of computational capability. With their immense processing power, these cutting-edge systems can solve highly complex calculations in a fraction of the time it would take even the most advanced classical supercomputers—some problems that would require over ten septillion years can now be tackled almost instantaneously. Designed with principles that leverage quantum mechanics, these processors are not just theoretical marvels but practical innovations that have the potential to revolutionize fields such as cryptography, materials science, artificial intelligence, and beyond. As quantum technology continues to evolve, it is poised to unlock new possibilities, transforming industries and driving unprecedented levels of efficiency and problem-solving capability. However, with the advancement of quantum computing, traditional cryptographic algorithms are under threat. Cryptography is the central unit of cyber security and the essential element for protecting secret information through encryption. Please read on to know more about the future of traditional cryptography in the light of quantum computing.

What is Quantum computing?

Quantum computing is a turning point in technology. It is based on quantum mechanics and is able to solve problems that traditional computing just cannot handle. In contrast to the usual computers, which calculate the information, involves only binary bits (0s and 1s); quantum computers need quantum bits, or qubits which can be in a lot of states at once through the help of things like superposition and entanglement. This is also the specific feature responsible for the fastest speed of computations.

The computational ability of quantum systems grows in an exponential way: a system with n qubits can exist in 2n2^n2n states simultaneously. Though the technology is still in its growing-up phase, but its effect on computational science and real-world applications is awaited to be transformational in the long run. As the quantum computing becomes a mass-production entity, its strong adaptability will bring a new dimension to the industrial process on the global level in the forthcoming decades.

Quantum Computing and Cryptographic Threats

Quantum computers pose a significant risk to current cryptographic systems:

1. **Asymmetric key Cryptography:** In asymmetric encryption, prime numbers are crucial components used to generate encryption keys, particularly in the widely used RSA algorithm. The security of the encryption algorithm is based on the complexity of factorizing the product of two large random prime numbers. This makes it computationally hard for unauthorized parties to decrypt data without the private key.

   Shor's algorithm which is developed by mathematician Peter Shor in 1994, is a groundbreaking quantum algorithm, specifically focused on the efficient factorization of large numbers, a task that is computationally infeasible for classical algorithms at scale. This innovation which represents a milestone in the evolution of quantum computing, demonstrate its potential to outperform classical systems in solving specific complex problems.

   Shor's algorithm has very significant consequences especially in cryptography, it exposes vulnerabilities in widely used encryption methods such as RSA which depend on the difficulty of factorization of large prime numbers.

2. **Symmetric key Cryptography**: Symmetric-key algorithms use the same cryptographic keys for both the encryption of plaintext and decryption of ciphertext.

   In quantum computing, Grover's algorithm speeds up the solution to unstructured data searches. It runs the search in fewer steps than any classical algorithm could.

   In the context of cryptography, Grover's algorithm poses a significant threat to symmetric encryption algorithms. As it can significantly speed up the process of brute-forcing a symmetric key by searching through the possible keys makes the symmetric key cryptography vulnerable. Increasing key size could be effective countermeasure.

Post-quantum cryptography

Post-quantum cryptography (PQC), the development of cryptographic algorithms, is currently thought to be secure against a cryptanalytic attack by a quantum computer. Quantum-safe technology is the main point of PQC, a practical and application-oriented field that examines quantum computing threats to traditional encryption. Large cloud providers, financial institutions and healthcare organizations are developing quantum safe technologies**.**

Standardization:

In 2024, the National Institute of Standards and Technology (NIST) proactively provided its recommendations (read here) for post-quantum encryption algorithms. These include solutions designed to resist attacks from quantum computers while being efficient and compatible with current systems. Key algorithms focus on public key encryption, digital signatures etc.

Challenges:

1. Governments and critical industries like finance, cloud providers, and healthcare are leading the adoption of PQC standards. Many are conducting risk assessments and implementing systems as part of their crypto-agility strategies. However, regulatory uncertainty and the rapid pace of quantum computing advancements make the timelines challenging.

2. Transitioning to PQC is a phased process with several challenges, such as updating hardware, software, and protocols like TLS and VPNs.

3. Attackers are taking "harvest now, decrypt later" strategy where attackers collect encrypted data to decrypt in the future with quantum capabilities. Efforts are underway to secure infrastructure against these threats. However, this makes the implementation of quantum-resistant systems urgent.

References

1. Shor, P. W. (1997). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. https://en.wikipedia.org/wiki/Shor%27s_algorithm.
2. Grover, L. K. (1996). *A Fast Quantum Mechanical Algorithm for Database Search*. https://dl.acm.org/doi/10.1145/237814.237866.
3. Bernstein, D. J., & Lange, T. (2017). *Post-Quantum Cryptography*. Nature, 549(7671), 188-194.
4. National Institute of Standards and Technology (NIST). (2024). *Post-Quantum Cryptography Standardization*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards