Crimson Publishers
Wings to the Research

Opinion

Quantum Computing and AI Revolutionizing Cryptography and Security

Utpal Chakraborty*

Chief Digital Officer, AI Researcher, Allied Digital Services Ltd, India

ISSN: 2832-4463

***Corresponding author:** Utpal Chakraborty, AI Researcher, Allied Digital Services Ltd, India

Submission: January 19, 2022

Published: February 16, 2022

Volume 1 - Issue 5

How to cite this article: Utpal Chakraborty*,Quantum Computing and AI Revolutionizing Cryptography and Security. COJ Rob Artificial Intel. 1(5). COJRA. 000522. 2022.
DOI: 10.31031/COJRA.2022.01.000522

Opinion

We will not go into the fundamentals of cryptography and quantum properties like superposition and interference or "Shor's Algorithm" in this article. We would rather briefly discuss the challenges that are emerging in the conventional cryptographic and security arena as quantum computers are adding up more qubits onto it and becoming more powerful.

Cryptographers have been working for years to prepare for the possible arrival of quantum computers by developing so called quantum-secure encryption methods. Fearful about the fact that quantum breakthroughs are imminent and threaten the sanctity of known encryption algorithms, cryptographers were seeking to develop quantum-resistant crypto that can withstand the intervention of a quantum computers.

It all started with the assumption that classical computers will never be powerful enough to crack AES and RAS. But all assumptions came under threat when quantum computers came into picture. Although AES-256 symmetric keys are believed to be quantum resistant, but if the quantum algorithm can run on a large-scale quantum computer it will be capable of cracking even such strong encryptions to the point where all your encrypted data at rest as well as transit are at risk. Of course, quantum computers will have to add more qubits onto itself before it can break a such fairly complex encryption. But that's just a matter of time because the speed it is advancing, the day is not far when it will be able to crack almost every encryption that is built using conventional methods.

Good news is, given the work already underway, researchers have started developing quantum secure cryptography before large quantum computers with large number of qubits become available to break RSA. Quantum computers are unlikely to pose a practical threat to symmetric cryptography and asymmetric cryptography at least for some years. The reason being the quantum behavior of subatomic particles qubits still do not remain stable for long enough. The "Shor Algorithm" used by a quantum computer with enough stable qubits to break through today's public-key cryptography still have some time, so there is no risk at least for now. However, the asymmetry of cryptography like RSA, on which we rely today, could be broken by the quantum computers.

Also called "quantum-resistant" or "post-quantum"; the next generation of cryptography is designed to withstand quantum computers are been developed in collaboration with the University of California, Berkeley, and the National Institute of Standards and Technology (NIST) in the United States. We will have to look at the post-quantum cryptography algorithm, which claims to be able to protect data even from the capabilities of quantum computers, called quantum attack. This type of mechanism is called Quantum secure cryptography.

The use of quantum cryptography now will not only provides immediate protection for your data, but also secures high-quality data and ensures that data with long shelf life is protected against future attacks. It is important that a protocol with information-theoretical

security means that security is not based on arithmetical assumptions and remains secure. In addition, the key management systems and protocols used are also inherently protected against attacks by quantum computers.

Faced with this looming threat, IT decision-makers should consider post-quantum cryptography, where a secure attack by a quantum computer would take place in the critical IT systems tomorrow. Today's public key cryptography has proven to be safe from mathematical attacks but not from quantum computers. The good side is, harnessing quantum computing and AI, it's going to bring very exciting opportunities in almost every field and industry. The massive parallelism of quantum computing brings to the table many possibilities to solve critical problems that we used to dismiss as unsolvable till now.