A Novel Approach for Analyzing the Cipher Algorithms of the Advanced Encryption Standard (AES) and Developing a New Quantum Algorithm in the Era of Quantum Computing and Quantum Cybersecurity

Abdalsalam, Mesk (School: Talae' Al-Amal Secondary Schools)

The purpose of this study is to investigate the susceptibility of the Advanced Encryption Standard (AES) algorithm to quantum computing-based attacks. Quantum computers possess the potential to solve certain mathematical problems significantly faster than classical computers, posing a potential threat to conventional cryptographic algorithms like AES. Rigorous quantum simulations and classical benchmarking techniques were employed to assess the effectiveness of quantum attacks against the AES algorithm. Quantum algorithms were implemented on a quantum computer simulator, and computational experiments were conducted to analyze the algorithm's resistance to quantum threats. Statistical methods, including hypothesis testing and confidence intervals, were utilized to quantify the level of risk posed by quantum attacks. The analysis successfully identified specific vulnerabilities in the AES algorithm when subjected to quantum computing-based attacks. Statistical significance testing demonstrated a notable increase in attack efficiency compared to classical methods. Additionally, a comparative analysis revealed the computational complexity and success rates of quantum attacks on AES. This study underscores the urgent need for developing post-quantum cryptographic solutions to safeguard sensitive data against emerging quantum threats. The findings highlight the potential risks associated with quantum computing in cryptographic applications and emphasize the importance of transitioning to quantum-resistant algorithms. Future research directions include exploring novel encryption schemes resilient to quantum attacks and integrating quantum-safe protocols into existing cryptographic systems.