iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology

2021
Vol.9 No.S1

Future of cyber security: rise of quantum cryptography

Mishu Sikka
Department MSc Information Security at Royal Holloway, University of London, UK.

Email: mishu.sikka.2021@live.rhul.ac.uk

Abstract

Statement of the Problem: Nearby future holds the unfolding of quantum computers, making classical computers obsolete. To highlight this breakthrough, a classical computer takes around 300 trillion years to break RSA-2048-bit encryption, whereas quantum computers will require just 8 hours (Ekera M. & Gidney C., 2019), as per ongoing advancements in quantum computing. Preparing for such shift, researchers within cyber security domain have been working on post-quantum cryptographic techniques that could resist classical and quantum attacks. This new focused research on Post-Quantum Cryptography (PQC) has gained widespread recognition.[1-] The purpose of this study is to identify future cryptographic techniques for standardization process in quantum-crypto world. Methodology & Theoretical Orientation: The National Institute of Standards and Technology (NIST) has been regulating a project to assess quantum cryptographic algorithms for quantum-future standardization. Alongside, companies such as Google and Microsoft have already started experimenting with PQC's deployment. At this moment, Isogeny-based cryptography has established itself as a promising PQC scheme candidate, that has small signature and key sizes amongst all. Findings: Best known protocol backing this isogeny-based quantum secure approach is Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol. The quantum secure scheme is based on presumed difficulties in finding isogenies between super singular elliptical curves. Although considered as the most promising scheme, SIDH algorithm reveals additional information, that holds potential to be exploited and SIDH be broken in polynomial time by quantum computers. Conclusion & Significance:

Due to current technological limitations, the above-mentioned findings are theoretical and couldn't be confirmed in practice. Rise of quantum computing will result into present cryptographic techniques being broken, thus exposing the security of our digitized world to malicious actors around the globe. It is imperative to identify and establish post-quantum cryptographic techniques for standardization process that could hold down attacks from advanced computers, aka quantum computers.

Biography

Dr. Mishu is an avid learner and a cyber-security enthusiast with learning technical and management skills relevant to security domain. Currently pursuing Masters degree in Information security from Royal Holloway, University of London where skills are being gained from various modules such as Legal and Regulatory Aspects of Information Security, Introduction to Cryptography and Secure Systems, Security Management and being implemented into various coursework assignments and virtual programs such as Global Cyber Security Virtual Internship from Clifford Chance. Alongside, he's enrolled in remote certified internship where he's using security tools like OpenVAS, Harvester.py, Metasploit to find and exploit vulnerabilities, escalate privileges, completing assignments on Red teaming and Threat Hunting arenas. Currently, he's working on his MSc project on Improved torsion-point attacks on Isogeny based cryptosystems. Being industrial placement as an integral part of MSc Information Security with a year in industry, Mishu is open to placement opportunities relevant to cyber-security domain.