A Report on One-day Guest lecture on
"Protocols for the Future: Post-Quantum Public Key Infrastructure Essentials"
Organised by Department of Computer Science & Technology
on 03.02.2024

Organized by: Mr. N Saikiran, Assistant Professor, Department of CST; Mr. N Junnu Babu, Assistant Professor, Department of CST
Submitted by: Mr. N Saikiran, Assistant Professor, Department of CST
Resource Person Details: Dr. R. Kabaleeshwaran, Assistant Professor, Department of CSE, IIITDM Kurnool.
Participants: III Year CST Students
Attendance: 70 participants
Venue: CST Department
Mode: Offline

Report Received on 13.02.2024
Department of Computer Science & Technology has organized **"**One-Day Guest Lecture on Protocols for the Future: Post-Quantum Public Key Infrastructure Essentials**"** on **03.02.2024**(Saturday)from 10:00 AM to 12:00 PM.

WELCOME ADDRESS:
The event commenced promptly at 10:00 AM with a warm and engaging welcome address to all by **Mr. N Junnu Babu**, **Assistant Professor, Department of CST,** Madanapalle Institute of Technology &Science **(**MITS), Madanapalle. The main objective of a guest Lecture on "Protocols for the Future: Post-Quantum Public Key Infrastructure Essentials" is essential as the rise of quantum computing poses significant challenges to the cryptographic algorithms that underpin PKI.
Quantum computing harnesses the principles of quantum mechanics to perform complex calculations exponentially faster than traditional computers. This unprecedented computational power threatens the security of widely used asymmetric cryptographic algorithms, such as RSA and ECC, which form the basis of PKI. Quantum computers can potentially break these algorithms, rendering current encryption methods vulnerable to attacks.

Resource Person Lecture:
Dr. R. Kabaleeshwaran, Assistant Professor, Department of CSE, IIITDM Kurnool started to explain about Post-Quantum Public Key Infrastructure.Quantum computing represents a paradigm shift in the realm of information processing, promising unprecedented computational power that could revolutionize various fields. As we embark on this journey into the future of computing, it becomes imperative to understand the fundamentals of quantum mechanics and how they enable the extraordinary capabilities of quantum computers.

Resource Person stated with Quantum Resistant Cryptography

To address the imminent threat posed by quantum computing, researchers have been actively developing Quantum-Resistant Cryptographic Algorithms. These algorithms are designed to withstand attacks from quantum computers and ensure the continued security of PKI. Promising candidates include lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate cryptography. These approaches rely on mathematical problems that are believed to be resistant to quantum algorithms. The core idea that

has perhaps changed the world in ways that are hard to comprehend is that of public key cryptography. We can give you a piece of information that is completely public (the *public key*), known to all our adversaries, and yet we can still securely communicate as long as we do not reveal our piece of extra information (the *private key*). With the private key, we can then efficiently solve mathematical problems that, without the secret information, would be practically unsolvable.

Further, he explained about the Key Exchange and Signature Schemes.

Key Exchange:

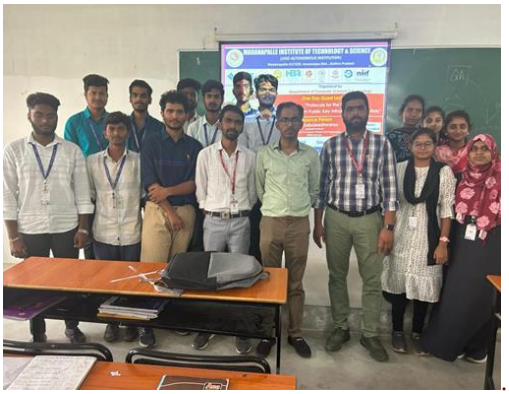
There are nine different suites of post-quantum key exchange algorithms still in the running in round three of the NIST Post-Quantum standardization project: Kyber, SABER, NTRU, and Classic McEliece (the "finalists"); and SIKE, BIKE, FrodoKEM, HQC, and NTRU Prime ("alternates"). These schemes have wildly different characteristics. This means that for step one, replacing the key exchange by post-quantum key exchange, we need to understand the differences between these schemes and decide which one fits best in TLS. Because we're doing ephemeral key exchange, we consider the size of the public key and the ciphertext since they need to be transmitted for every handshake. We also consider the "speed" of the key generation, encapsulation, and decapsulation operations, because these will affect how many servers, we will need to handle these connections.

Challenges and Road Ahead:

For our post-quantum signature scheme, we can draw a similar table. In TLS, we generally care about the sizes of public keys and signatures. In terms of runtime, we care about signing and verification times, as key generation is only done once for each certificate, offline. The round three candidates for signature schemes are: Dilithium, Falcon, Rainbow (the three finalists), and SPHINCS+, Picnic, and GeMSS.There are many signatures in a TLS handshake. Aside from the handshake signature that the server creates to authenticate the handshake (with public key in the server certificate), there are signatures on the certificate chain (with public keys for intermediate certificates), as well as OCSP Stapling (1) and Certificate Transparency (2) signatures (without public keys).

Furthermore, he discussed Challenges and Considerations as, implementing post-quantum cryptography presents several challenges. Firstly, there is a need to ensure backward compatibility with existing systems and infrastructure that rely on PKI. Additionally, the performance and efficiency of quantum-resistant algorithms need to be thoroughly evaluated to ensure they can handle the demands of modern computing environments.

Furthermore, the transition to post-quantum cryptography requires extensive testing, verification, and adoption by various stakeholders. It is crucial to establish trust and consensus in the security community regarding the new cryptographic algorithms to ensure their widespread acceptance and interoperability.



Vote of thanks:

The guest lecture formally concluded with a vote of thanks delivered by **Mr. N. Saikiran, Assistant Professor**, **Department of CST**. In his address, he expressed sincere gratitude to resource person for taking the time to share his expertise and inspired our students towards Post-Quantum Cryptography.

Outcomes:

At the end of Program, Students can able to,

1. Understand the Breakthroughs in Cryptography.
2. Exploring Advanced Techniques in Accelerated Optimization.
3. Understanding Post-Quantum Cryptography.
4. Illustrating the Challenges & Advancements in Security Analysis and Evaluation in the context of cyber-security and cryptography.
5. Outline of Research and Innovation in the Field of Information Technology.