Strategy and Synergy for Security

Society for Electronic Transactions and Security (SETS)

MGR Knowledge City, CIT Campus, Taramani, Chennai – 600 113
www.setsindia.in

Webinar On

Post Quantum Cryptography

Date: 29th March 2022

Time: 09.30 am to 5.30 pm

About the Webinar

Public key cryptography enables two communicators, who share no common secret information, to communicate securely over an open channel. Digital signatures are used mainly for ensuring authenticity and integrity of the message. The security of such most common signature scheme is guaranteed by the hardness of certain mathematical problems, like factoring and discrete log. However, these problems are easily broken by a quantum computer. It may be reasonable to assume that a large nation state would be able to afford a reasonably big quantum computer which threatens the present-day cryptography. Hence, it is prudent to plan for replacement of these most commonly used protocols. We shall sketch the challenges which a quantum-enabled adversary throws and possible solutions which would resist such quantum attacks.

Areas / Topic	Speaker
• Introduction to Post Quantum Cryptography and MQ Based Systems	Tapas Pandit *IISc, Bangalore*
• Hardware Implementations of Post Quantum Candidates	Debapriya Basu Roy *IIT Kanpur*
• Subset Sum Problem	Santanu Sarkar *IIT Madras*
• Introduction to Quantum Random Oracles	V Natarajan *SETS, Chennai*
• Hash Based Signatures	Samyuktha M *SETS, Chennai*
• Lattice Based Signatures	M Prem Laxman Das *SETS, Chennai*
Demonstration of Post Quantum Certificate Authority	

INSTRUCTIONS

Webinar Link: We will share the link for the webinar through the email for registered participants.

Note: Scientist/ Working Professionals/ Faculty / Research Scholars may attend the above said webinar

All are requested to register through the following link for the above webinar (No Registration Fee)

Registration Link: https://forms.gle/vfzPX44JaefpGQHo7 **For more details** https://setsindia.in/pqcwebinar

Acknowledgement: This webinar is supported under the sponsored project of Ministry of Electronics and Information Technology (MeitY), Government of India

Dr. P. Nageswar Rao
Coordinator
Mobile: 9884143131
eMail: workshop@setsindia.net

Dr. M. Prem Laxman Das
Senior Scientist
Mobile: 8939112742
eMail: prem@setsindia.net