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

by

Dr. M. Prem Laxman Das, Senior Scientist, SETS, Chennai

Public key cryptography enables two strangers, 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 most common such signature scheme is guaranteed by the hardness of certain mathematical problems, like factoring and discrete log. But, 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.

About Speaker

Dr M. Prem Laxman Das has completed his Ph.D. in Mathematics from Indian Statistical Institute. He works broadly in the domain of algorithmic aspects of algebra and number theory. In cryptology, his interests include cryptanalysis of public key systems, pairing-based crypto with applications to cloud computing security and aspects of post-quantum cryptography.

Date: 31st July 2020 **Time: 11.00 to 12.30** **Duration: 1 Hour 30 Minutes**

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://bit.ly/3jWe2B4**

For more details:

Dr. P. Nageswara Rao
Coordinator
9884143131
nageswar@setsindia.net

Mr. S. Karthikeyan
Technical Coordinator
9884158528
karthikeyan@setsindia.net