OBJECTIVE

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.

Quantum computers pose a serious threat to today's digital security due to their ability to factor numbers into primes much faster than their classical counterparts. A number of approaches have been proposed for Post-quantum Public Key Cryptography, the new solution based on Quantum Key Distribution. Hash based and Lattice-based cryptographic constructions are the leading applicants for public-key post-quantum cryptography. Organizations and government agencies should already be preparing for Post Quantum cryptography and have all the required processes in place to assess the new cryptography standards when they become available and research in different parts of the world.

Topics being covered:

- Fundamentals of Classical Encryption Techniques
- Public Key Cryptography and Algorithms
  - ✓ RSA, Diffie – Hellman, DSS
- Overview of Quantum Cryptography
- Introduction to Post Quantum Cryptography and MQ based Systems
- Hardware Implementations of Post Quantum Candidates
- Subset Sum Problem
- Introduction to Quantum Random Oracles
- Hash Based Signatures

TARGET AUDIENCE:

Faculty members and Research Scholars from academic institutes, Personnel from DRDO, DAE& DAE (Aided Institutions), R & D organization and related Industries.

FACULTY:

Sessions will be handled by experienced faculty members from Kongu Engineering College, reputed institutions and Experts from DAE R & D organization and related Industries.

BOARDING AND LODGING:

Accommodation and boarding if required will be provided in the college campus on first-come-first serve basis.

REGISTRATION FEE DETAILS:

Registration Fee: Rs.200/- per Participant.

- The course fee includes lunch and refreshment.
- Boarding and Lodging will be provided to all the selected participants in the college campus.
- Registration for the course can be made by sending the duly filled registration form along with a DD for Rs.200/- in favour of "**Kongu Engineering College Grants"** Payable at Perundurai, or at Erode to the Chairman. Registration is limited to 50 participants and selected on first-come-first serve basis.

HOW TO APPLY

The applicants should send their applications in the specified format through their Principal / Sponsor to reach us on or before **28.08.2022.** If selected, they should confirm their participation in time.

SCHEDULED DATES

Last date for receipt of Applications : 28.08.2022
Intimation of Selection : 30.08.2022
Confirmation by participants :31.08.2022

KONGU ENGINEERING COLLEGE (AUTONOMOUS) PERUNDURAI, ERODE 638 060 TAMILNADU

DRDO Sponsored Two Day National Level Seminar On

"Role of Post Quantum Cryptography in Defence and Security of Future India"

(02.09.2022 to 03.09.2022)

APPLICATION FORM

Name :
Designation :
Organization :
Gender :
Age :
Educational Qualification:
Address for :
Communication

Mobile Number :
E-mail ID :
Experience :
Teaching : _____years
Others (Specify) : _____years
Need Accommodation : YES / NO
Signature :

DECLARATION

The above information is true to the best of my knowledge. I agree to abide by the rules and regulations governing the course. If selected, I shall attend the programme for the entire duration. I also undertake the responsibility to inform the Chairman in case I am unable to attend the course.

Place:
Date: Signature of the Applicant

SPONSORSHIP CERTIFICATE

Mr/Ms/Dr_____
_____

is an employee of our Institute / Organization and is hereby sponsored. He/She will be permitted to attend the programme in full, if selected.

Place: Signature of the Sponsoring Authority

Date: Office Seal

Application form completed in all respects is to be sent to:

Mr.S.Vinothkumar M.E
Assistant Professor
Co - Convener

DRDO Sponsored
Two Day National Seminar on
"Role of Post Quantum Cryptography in Defence and Security of Future India"

Department of Information Technology
Kongu Engineering College
Perundurai Erode-638 060 Tamilnadu
Contact Mobile – 9443034110, 8072545847, 9003683789
E-mail: vinoths.it@kongu.edu, vinoth21787@gmail.com

ABOUT THE COLLEGE

Kongu Engineering College, a leading research-oriented institution with excellent facilities, is run by Kongu Vellalar Institute of Technology Trust. The Programmes of the institute are accredited by NBA and the institute is accredited by NAAC with A++ grade. It consists of 167 acres of land richly endowed with beautiful Greenland. It is an autonomous institution affiliated to Anna University, Chennai. The college has completed 37 years of dedicated and excellent service to the people of India and abroad in the field of Technical Education. The college offers 17 UG Programmes, 15 PG Programmes and 15 Research Programmes in Engineering, Applied Sciences and Management. In National Institution Ranking Frame work (NIRF) survey 2019, the institution has bagged 164th rank among all engineering institutions in India including premier institutions like IITs, NITs etc. Ranked 3rd Position in Tamilnadu and 33rd position in India among 126 Engineering Institutes in India (including IITs and NITs) by outlook Magazine. It has an active industry institute partnership centre to interact with industries and also has a Technology Business Incubator (TBI), first of its kind in India, nurturing entrepreneurs in hi-tech areas.

ABOUT THE DEPARTMENT

The Department of Information Technology is offering B.Tech. Degree Programme in IT and MTech Degree Programme in Information Technology. The faculty of the department has vast experience in academia and industry. Besides teaching, the department is actively involved in industrial consultancy, and conducting training Programmes for students and practicing engineers. The department has implemented the project "Application of IT for Water Quality Management in water treatment plant" sanctioned by AICTE and "Speech to Text Synthesis in Tamil" sponsored by Tamil Virtual University, Chennai under TSDF scheme. The department has extensive computing facilities with latest software like MATLAB, ORCAD, Visual Studio .Net, IBM-DB2, WebSphere Application Server (WAS) etc

ABOUT THE LOCATION

The college is situated at Perundurai on the National Highway (NH 47) about 80 km from Coimbatore and 20 km from Erode.

Estd : 1984

DRDO Sponsored
Two Day National
Level Seminar On

"Role of Post Quantum Cryptography in Defence and Security of Future India"

(02.09.2022 to 03.09.2022)

Organizing Committee

Chairman
Dr.S.Varadhaganapathy M.E., Ph.D.,
Professor

Convener
Dr.R.Shanthakumari M.E., Ph.D.,
Associate Professor

Co-Convenor
Mr.S.Vinothkumar M.E.,
Assistant Professor (Senior Grade)

Department of Information Technology.
Kongu Engineering College
Perundurai – 638060, Erode, TamilNadu

Tel: 04294-226570
Fax: 04294-220087
E-mail: svg@kongu.ac.in, rsk_shan@kongu.ac.in
vinoths@kongu.ac.in
Website: www.kongu.ac.in