CAMBRIDGE INSTITUTE OF TECHNOLOGY
An Autonomous Institution

NAAC A+
ACCREDITED BY GRADE

PRE-CONFERENCE TUTORIAL

Organized as Part of

Second International Conference on
"Next-Gen Semiconductor Devices, Materials & Smart Computing Applications"

(ICNGSMCA-2026)

TRACK 1
Quantum Computing for Post-Quantum Security

TRACK 2
SOC Design (From RTL to GDS II)

TRACK 3
Cybersecurity in the Modern Digital Era

Date: 23 July 2026 | Time: 9:30 AM – 4:30 PM

REGISTER NOW

*Registration Deadline: July 17, 2026

In Association with

Taylor & Francis Group an informa business

CRC Press Taylor & Francis Group

Note:

- *Registration is limited to 50 participants per track.*
- *The registration fee is* ₹ **1,000** *per participant, which includes the tutorial kit and lunch.*
- *Participants may register for only one track.*

engg.cambridge.edu.in

TRACK 1: - Quantum Computing for Post-Quantum Security

Introduction:

The rapid advancement of quantum computing is expected to revolutionize computation, optimization, and cryptographic analysis. While quantum technologies offer transformative opportunities in science, engineering, and communication systems, they also pose significant threats to classical cryptographic algorithms widely used in digital security infrastructures. Algorithms such as RSA, ECC, and Diffie–Hellman are vulnerable to quantum attacks enabled by Shor's algorithm and Grover's search techniques. The Pre conference Tutorial will provide a balanced blend of theoretical concepts, quantum algorithms, cryptographic migration strategies, and practical insights into implementing quantum-resilient systems.

Objectives of pre-conference Tutorial:

1. To provide participants with foundational knowledge of quantum computing principles and their impact on modern cryptographic systems.
2. To introduce post-quantum cryptographic techniques, quantum-safe protocols, and emerging security architectures for future computing systems.
3. To explore current research directions, hardware challenges, quantum communication security, and standardization efforts initiated by organizations such as National Institute of Standards and Technology for next-generation secure communication frameworks.

Outcomes and Takeaway:

Designing and implementing quantum-resilient security frameworks for next-generation computing and communication systems.

Schedule

Session	Topic	Brief Description
Session 1	Fundamentals of Quantum Computing	Introduction to qubits, superposition, entanglement, quantum gates, quantum circuits, and quantum computational models. Overview of current quantum hardware platforms and research trends.
Session 2	Quantum Algorithms and Security Threats	Understanding Shor's Algorithm, Grover's Algorithm, and their implications on classical encryption systems such as RSA, ECC, and hash-based security mechanisms.
Session 3	Post-Quantum Cryptography (PQC)	Detailed introduction to lattice-based cryptography, code-based cryptography, multivariate cryptography, hash-based signatures, and quantum-safe encryption methods.
Session 4	Quantum-Secure Systems and Future Research Directions	Practical implementation strategies for quantum-safe systems, secure communication architectures, hybrid cryptographic models, standardization activities, and future research opportunities in quantum cybersecurity.

Pre-requisites for the Tutorial:

Basic understanding of computer science fundamentals and cybersecurity concepts, Familiarity with elementary mathematics, including linear algebra and probability, Basic knowledge of cryptography concepts such as encryption, decryption, and security protocols, Awareness of modern computing systems and networking fundamentals.

Who can attend?

UG / PG students, Faculty, Industry professionals, Research Scholars.

Sessions handled by Industry experts and Research Scientists

Coordinator

Dr. Pushpalatha H L

HOD and Professor
Department of Physics

+91-99458 90111 | 89701 16368

hod.phy@cambridge.edu.in

TRACK 2: - SOC Design (From RTL to GDS II)

Introduction:

Semiconductor design and fabrication are the foundation of modern electronics, communication, and computing systems. With the increasing emphasis on Atmanirbhar Bharat (self-reliant India) and the national focus on semiconductor ecosystem development, there is a strong need to build skilled manpower capable of handling end-to-end ASIC design and verification processes.

Through this workshop, participants will gain practical exposure to the complete digital ASIC design flow using SCL 180nm technology, aligning directly with the C2S (Chip to Startup Program) vision of developing a skilled semiconductor workforce and promoting indigenous chip design capabilities.

Objectives of pre-conference Tutorial:

1. To introduce participants to the end-to-end digital VLSI design flow and EDA tool usage.
2. To develop hands-on skills in Verilog coding, simulation, synthesis, and verification.
3. To perform synthesis, floorplanning, placement, routing, and physical verification using industry-standard tools.
4. To understand post-layout analysis and timing closure for tape-out readiness.
5. To generate and verify the final GDS II layout for fabrication submission to SCL (Semiconductor Laboratory), India. (Considering processor case study)

Outcomes and Takeaway:

RTL-to-GDS II Design Flow with Submission to SCL 180 nm Fabrication Facility.

Schedule

Session	Topic	
Session 1	RTL Design and Simulation Introduction to case study: Processor Verilog coding conventions Testbench creation and functional verification.	Verified synthesizable Verilog code and functional testbench.
Session 2	Logic Synthesis and Quality Checks Synthesis flow setup Timing, power, and area analysis Gate-level simulation.	Optimized netlist meeting design constraints.
Session 3	Floor planning, Placement and Routing Import synthesized netlist Design constraints and IO planning Placement and routing automation.	Completed layout with timing-closed routed design.
Session 4	Physical Verification and Post-Layout Analysis Design Rule Check (DRC), Layout vs Schematic (LVS) Post-layout timing and power analysis.	Verified layout meeting DRC/LVS requirements.
Session 5	GDSII Generation and Documentation GDSII extraction and verification Design documentation for submission Wrap-up and evaluation	Fabrication-ready GDSII file and design documentation.

Pre-requisites for the Tutorial:

Basic understanding of Digital Electronics and VLSI Design, Familiarity with Verilog HDL or equivalent hardware description language, Prior exposure to Linux environment and command-line tools, Knowledge of logic synthesis and timing concepts is beneficial (not mandatory).

Who can attend?

UG / PG students, Faculty, Industry professionals, Research Scholars.

Sessions handled by Industry experts and Research Scientists

Coordinator

Dr. Girish H

Professor
Department of ECE

+91-97411 22667 | 97426 95276

girish.ece@cambridge.edu.in

TRACK 3: – Cybersecurity in the Modern Digital Era

Introduction:

The rapid growth of digital technologies, including cloud computing, artificial intelligence (AI), the Internet of Things (IoT), and Industry 4.0, has revolutionized the way we live and work. At the same time, cyber threats have become more sophisticated, making cybersecurity a critical requirement for protecting digital assets, privacy, and critical infrastructure. This tutorial provides an overview of modern cybersecurity concepts, emerging threats, defense strategies, and best practices, along with practical insights into securing today's interconnected digital ecosystem. It is designed to equip participants with the knowledge and skills needed to understand, identify, and mitigate cyber risks in the modern digital era.

Objectives of pre-conference Tutorial:

1. Understand the fundamental concepts, principles, and significance of cybersecurity in the modern digital landscape.
2. Explore the evolving cyber threat landscape and modern defense strategies, including security technologies, frameworks, and best practices.
3. Develop practical knowledge of cybersecurity tools and techniques for vulnerability assessment, penetration testing, incident response, and secure computing.

Outcomes and Takeaway:

Understand the role of AI, cloud computing, and IoT in modern cybersecurity and awareness of emerging cybersecurity trends and future challenges in the digital era.

Schedule

Session	Topic	Expected Outcome
Session 1	Fundamentals of Cybersecurity	Introduction to Cybersecurity Cybersecurity Principles (Confidentiality, Integrity, Availability) Cyber Threat Landscape Common Cyberattacks and Attack Vectors mportance of Cyber Hygiene.
Session 2	Cyber Threats and Defense Mechanisms	Malware, Ransomware, Phishing, and Social Engineering Advanced Persistent Threats (APTs) Network Security and Endpoint Security Identity and Access Management (IAM) and Multi-Factor Authentication (MFA) Zero Trust Security Model.
Session 3	Merging Technologies and Secure Systems	Cloud Security Fundamentals AI in Cybersecurity IoT and Industry 4.0 Security Challenges Vulnerability Assessment and Penetration Testing Incident Response and Digital Forensics (Overview).
Session 4	Practical Cybersecurity and Future Trends	Hands-on Demonstration of Security Tools Case Studies of Major Cyberattacks Cybersecurity Standards and Compliance (ISO 27001, NIST, GDPR, PCI DSS) Best Practices for Individuals and Organizations Future Trends in Cybersecurity and Interactive Q&A.

Pre-requisites for the Tutorial:

- Basic knowledge of computers, operating systems, and the Internet.
- Familiarity with computer networks and common web applications.
- Interest in cybersecurity and digital technologies.

Who can attend?

UG / PG students, Faculty, Industry professionals, Research Scholars.

Sessions handled by Industry experts and Research Scientists

Coordinator

Dr. Vasantha M

Associate Professor
Department of CSE(IoT)

+91-98863 54457 | 89715 33373

vasantha.cse@cambridge.edu.in

CAMBRIDGE
INSTITUTE OF TECHNOLOGY
An Autonomous Institution

Approved by AICTE & UGC, New Delhi | Autonomous Institute Affiliated to VTU, Belagavi
| NAAC A+ & NBA Accredited | An ISO 9001:2015 Certified | UGC 2(f) Certified | Recognized by Govt. of Karnataka
| NIRF Ranked Innovation Institute 2023 | National Research Development Corporation
| Recognized as SIRO by DSIR, Govt. of India | Recognized as Host Institute by Ministry of MSME, Govt. of India

K R Puram, Bengaluru - 560 036 | +91-80-25618798/99 | principal@cambridge.edu.in | engg.cambridge.edu.in