

2025 6th IEEE International Conference on Public Key Infrastructure and its Applications (PKIA 2025)

**Bangalore, India
3-4 September 2025**

IEEE Catalog Number:
ISBN:

CFP25N53-POD
979-8-3315-7478-9



Copyright © 2025, IEEE

All Rights Reserved

Copyright and Reprint Permissions:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

*** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.

IEEE Catalog Number:	CFP25N53-POD
ISBN (Print-On-Demand):	979-8-3315-7478-9
ISBN (Online):	979-8-3315-7477-2

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA

Phone:	(845) 758-0400
Fax:	(845) 758-2633
E-mail:	curran@proceedings.com
Web:	www.proceedings.com

TABLE OF CONTENTS

Lightweight and Efficient Module-LWE Identity-Based Encryption Scheme for Post-Quantum Security	1
<i>Kamna Sahu, Srinivasa KG, Satyanarayana Vollala</i>	
Extending Elliptic Curve Cryptography for Quantum Readiness	8
<i>Kunal Abhishek</i>	
Identity-Based Secure End-to-End Quantum-Safe MQTT Communication Using Ring-LWE	15
<i>Gunasekaran Raja, Sudhakar Theerthagiri, Santhosh Kumar T, Sangeetha Ramachandran, Nandini Babu</i>	
An HLS-driven Architectural Design for the PRESENT Lightweight Block Cipher	23
<i>Atul M., Diksha Shekhawat, Jugal Gandhi, M. Santosh, Jai Gopal Pandey</i>	
Cross-Platform Benchmarking of Shor's Algorithm for Quantum Cryptanalysis	28
<i>Noorul Hussain Ubaidur Rahman, Vanideve Jayavijayan, Muttukrishnan Rajarajan</i>	
Quantum Communication Applications: Beyond QKD	35
<i>Anoop Kumar Pandey</i>	
A Usable and Secure Authentication for Multi-server Environments to Enhance Digital Trust	48
<i>Mohammed Misbahuddin, S D Sudarsan, Ankur Sanda, Adilkhan H Kulkarni</i>	
Validation Framework for Module Lattice-Based Post-Quantum Digital Signature Scheme	56
<i>Smitha G Havanur, Rahul Kumar, Abey Jacob</i>	
Post-Quantum Hybrid Digital Signatures: Bridging Classical and Quantum-Resistant Cryptography	64
<i>Jitendra Kumar, Balaji Rajendran, Aashish Banati, K K Soundra Pandian, S D Sudarsan</i>	
Design and Implementation of a Post-Quantum Double Ratchet Using ML-KEM	72
<i>Akash Angom, Nirmalya Kar, Tribid Debbarma, Priyanka Biswas</i>	