

2024 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA 2024)

**Bangalore, India
5-6 September 2024**



**IEEE Catalog Number: CFP24N53-POD
ISBN: 979-8-3503-5198-9**

**Copyright © 2024 by the Institute of Electrical and Electronics Engineers, Inc.
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:	CFP24N53-POD
ISBN (Print-On-Demand):	979-8-3503-5198-9
ISBN (Online):	979-8-3503-5197-2

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

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

Efficiency of Zero-Knowledge Proofs: a Thorough Review and Analysis.....	1
<i>Chitranjan Prasad Sah, Manjot Kaur, Gurwinder Singh</i>	
PKI-Enabled Authentication and Encryption for Enhanced Drone Communication.....	8
<i>Pavan Jadhav, Mohammed Misbahuddin, Shrikrishna S Chippalkatti, S D Sudarsan</i>	
Demonstration of Secure Key Management Solution with Use Case in Permissioned Blockchain	18
<i>Geetha Sivanantham, Gowshalya Shri A M, Reshmi T R</i>	
Approach to Post Quantum Cryptography Validation	24
<i>Smitha G Havanur, Abey Jacob</i>	
Experimenting Integration of Custom ECDSA Algorithm in OpenSSL.....	33
<i>Geetha Sivanantham, Akila Krishnan, Reshmi T R</i>	
Role of PKI in Securing AMQP Communication.....	39
<i>Sanjay Adiwai, S Shuaib Ahmed, Balaji Rajendran, Mohammed Misbahuddin, S D Sudarsan</i>	
Advanced QKD Protocols and Practical Challenges	47
<i>Mohit Rajpurohit, Kaustubh Moni Deka, Vaibhav Pratap Singh, Haribabu P</i>	
Distributed Estimation Based Public Key Infrastructure for In-Vehicle Network Security.....	55
<i>Karthika Venkatesan, Seshadhri Srinivasan, Padmapritha Thamodharan, Nimesh Nagar, Haribabu P, S D Sudarsan, K K Soundara Pandian</i>	
Comparative Analysis of Hybrid Cryptosystems for Secure Image Encryption.....	62
<i>Nidhi Bhatt</i>	
On the Comparative Study of Recent Information Set Decoding (ISD) Attacks for QC-LDPC Code-Based McEliece Cryptosystem.....	69
<i>Sourabh Biswas, Indivar Gupta, Debasish Bera</i>	
Efficient Implementation of Entity On-Boarding and Authentication in Zero-Trust Systems.....	77
<i>Jayashree Rana, Pramod Kumar Meher, Rojalina Priyadarshini, K Pratyush Rao</i>	

Author Index