

2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA 2023)

**Bangalore, India
8-9 September 2023**



**IEEE Catalog Number: CFP23N53-POD
ISBN: 979-8-3503-1056-6**

**Copyright © 2023 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:	CFP23N53-POD
ISBN (Print-On-Demand):	979-8-3503-1056-6
ISBN (Online):	979-8-3503-1055-9

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

2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA)

Table of Contents

Technical Papers

Scalable Model-Based Decentralized Applications in the Cloud Using Certificates and Blockchains1

Felix Härer

Cryptographic Challenges and Security in Post Quantum Cryptography Migration: A Prospective Approach.....9

Anoop Kumar Pandey, Aashish Banati, Balaji Rajendran, S D Sudarsan, K K Soundra Pandian

Enhancing PKI Security in Hyperledger Fabric with an Indigenous Certificate Authority...17

Gayathri Santhosh M, Reshmi T R

Hash-based Digital Signatures- A tutorial review22

P V Andana Mohan

Cryptographic Validation of Lightweight Block ciphers and Hash Functions.....30

UmaDevi, Abey Jacob

An Architecture for Risk-Based Authentication System in a Multi-Server Environment...40

Pramila R M , Samiksha Shukla

An ECC based Anonymous Authentication Protocol for Internet of Things.....45

Appala Naidu Tentu, Renuka Cheeturi

FPGA Implementation of the AES Algorithm with Lightweight LFSR-Based Approach and Optimized Key Expansion51

Samruddhi Purohit, Vaishnavi Deshpande, Vaishali Ingale

Lightweight Certificate-less Digital Signature Scheme for WSNs57

Rhithick Murali, Vivek Arunachalam, Jeevanantham S, Venkatesan C, Rebekka B