ISBN : 978-81-995461-3-4

Secure IoT Device Design Using Lattice-Based Post-Quantum CRYPTOGRAPHY

Shweta Murkute
Akanksha Dubey

SECURE IOT DEVICE DESIGN USING LATTICE-BASED POST-QUANTUM CRYPTOGRAPHY

Authors

Shweta Murkute
(MA, PGDCA, MSc., B.Ed., B.Sc.)

Akanksha Dubey
PhD in Mathematics
Department of Mathematics
Shri Rawatpura Sarkar University
Raipur, Chhattisgarh

Publisher :
Aditi Publication, Raipur, Chhattisgarh, India
Ph.: +91 9425210308

Secure IoT Device Design Using Lattice-Based Post-Quantum Cryptography

Year: **2026**
Edition - **01**

Authors
Shweta Murkute
Akanksha Dubey
Raipur, Chhattisgarh, India

ISBN : **978-81-995461-3-4**

Price: Rs. **799/-**

Publisher & Printer:
Aditi Publication,
Opp. New Panchajanya Vidya Mandir
Near Tiranga Chowk
Kushalpur, Raipur, Chhattisgarh, INDIA
+91 9425210308

Shweta Murkute (MA, PGDCA, MSc., B.Ed., B.Sc.) *is an accomplished academician with 19 years of dedicated teaching experience in higher education. With a strong interdisciplinary background in science, arts, education, and computer applications, she brings a comprehensive and integrated perspective to academics. Her qualifications reflect her deep commitment to learning and professional growth, enabling her to blend theoretical knowledge with practical application. Over the years, she has consistently upheld high academic standards and contributed significantly to curriculum enrichment and student development. She is currently pursuing her Ph.D. as a Scholar at* ***Shri Rawatpura Sarkar University****.*

Her teaching philosophy centres on clarity of concepts, analytical thinking, and technology-enabled learning. She is passionate about adopting innovative pedagogical approaches that enhance student engagement and foster intellectual growth. Through her experience, she has mentored numerous students, encouraging them to develop critical thinking skills and academic confidence. As an author, Shweta Murkute aims to extend her educational insights beyond the classroom by contributing meaningful academic content that supports learners, educators, and researchers. Her professional journey reflects dedication, versatility, and a continuous pursuit of excellence in the field of education.

Dr. Akanksha Dubey is a distinguished mathematician, researcher, and academic leader with extensive experience in higher education. Holding a Ph.D. in Mathematics, she has devoted her career to advancing analytical thinking and fostering interdisciplinary learning among students. With substantial teaching experience at both undergraduate and postgraduate levels, she has delivered courses in Algebra, Analysis, Applied Mathematics, Mathematical Modelling, Optimization Techniques, and Computational Mathematics. Her teaching philosophy emphasises conceptual clarity, logical reasoning, and practical applications, adopting a student-centric approach that nurtures curiosity and critical thinking.

Her research encompasses both theoretical and applied mathematics, including Fixed Point Theory, Best Proximity Theorems, Cryptography, Optimization Models, Artificial Intelligence in Education, and mathematical modelling for technological and environmental systems. She integrates mathematics with data science, machine learning, operations management, and secure communication frameworks. Dr. Dubey has published widely in reputed journals, authored and co-authored academic books, and contributed to edited volumes. Actively engaged in conferences, curriculum development, mentoring, and quality assurance initiatives, she promotes holistic growth, combining intellectual excellence with emotional balance and innovative thinking.

Preface

The rapid expansion of the Internet of Things (IoT) has transformed modern life, connecting billions of devices across healthcare, agriculture, transportation, industry, smart cities, and critical infrastructure. From wearable medical sensors and automated manufacturing lines to intelligent traffic systems and smart grids, IoT devices now form the digital nervous system of our society. However, this unprecedented connectivity has introduced equally significant cybersecurity challenges. Many IoT systems rely on classical cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC), which are increasingly vulnerable to emerging quantum computing advances. The need for resilient, future-proof security mechanisms has never been more urgent.

Quantum computing represents both a technological breakthrough and a disruptive threat to existing public-key cryptographic systems. Algorithms such as Shor's algorithm demonstrate that sufficiently powerful quantum computers could break widely deployed encryption mechanisms, compromising decades of sensitive data. This "harvest-now, decrypt-later" risk is especially critical for IoT systems, which often operate with long device lifecycles and limited update capabilities. In this evolving landscape, lattice-based post-quantum cryptography has emerged as one of the most promising solutions, offering strong mathematical security foundations believed to withstand quantum attacks.

This book was written to bridge the gap between mathematical theory and practical IoT implementation. While much research discusses post-quantum cryptography at a theoretical level, real-world deployment—particularly in resource-constrained IoT environments—presents unique challenges. Memory limitations, battery life constraints, latency sensitivity, hardware diversity, and large-scale interoperability all require careful engineering consideration. Through a structured progression—from foundational cryptographic principles and lattice mathematics to hardware implementation strategies

and real-world case studies—this book provides a comprehensive roadmap for secure IoT device design using lattice-based techniques.

Ultimately, this work aims to support researchers, engineers, policymakers, and students in building secure, scalable, and sustainable IoT infrastructures prepared for the quantum era. The transition to post-quantum cryptography is not merely a technological upgrade; it is a strategic necessity for safeguarding critical infrastructure, protecting personal data, and sustaining digital trust. By combining theoretical rigor with practical deployment insights, this book aspires to contribute meaningfully to the development of resilient IoT ecosystems in a rapidly evolving cybersecurity landscape.

Content

Aditi Publication

Aditi Publication

Opp. New Panchjanya Vidya Mandir, Near Tiranga Chowk,
Kushalpur, Dist.- Raipur-492001, Chhattisgarh
shodhsamagam1@gmail.com, +91 94252 10308

ISBN : 978-81-995461-3-4

9 788199 546134

₹ 799