Patent Search

Invention Title	QUANTUM-RESISTANT ENCRYPTION SYSTEM AND METHOD FOR SECURE DATA TRANSMISSION IN NEXT-GENERATION NETWORKS
Publication Number	12/2025
Publication Date	21/03/2025
Publication Type	INA
Application Number	202541019471
Application Filing Date	04/03/2025
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMMUNICATION
Classification (IPC)	H04L0009080000, H04L0009320000, H04L0009300000, H04L0009400000, H04L0009000000

Inventor

Name	Address	Country
Mr. Gude Ramarao	Associate Professor, Department of Electronics and Communication Engineering, G. Pullaiah College of Engineering and Technology, Kurnool, Kurnool District, Andhra Pradesh, India, Pin Code: 518002	India
Dr. Parvathi Gorantla	Associate Professor in Physics, Department of Science & Humanities, Chalapathi Institute of Engineering & Technology, Guntur, Guntur District, Andhra Pradesh, India, Pin Code: 522036	India
Mrs. Ramineni Srilakshmi	Assistant Professor in Mathematics, Department of Science & Humanities, Chalapathi Institute of Engineering & Technology, Guntur, Guntur District, Andhra Pradesh, India, Pin Code: 522036	India
Mrs. Pallepogu Bhavani	Assistant Professor in Physics, Department of Science & Humanities, Chalapathi Institute of Engineering & Technology, Guntur, Guntur District, Andhra Pradesh, India, Pin Code: 522036	India
Ms. Priyanka Gomase	Ph. D Scholar, Department of Computer Science and Engineering, Madhyanchal Professional University, Bhopal, Madhya Pradesh, India, Pin Code: 462044	India
Dr. P. Deepa	Associate Professor, Department of Electronics and Instrumentation Engineering, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India, Pin Code: 600119	India
Mr. Ravishankar C. Bhaganagare	Assistant Professor, Department of CSE (AI&ML), Vishwakarma Institute of Technology, Pune, Maharashtra, India, Pin Code: 411037	India
Dr. Telagarapu Prabhakar	Professor, Department of Electronics and Communication Engineering, GMR Institute of Technology, Rajam, Vizianagaram District, Andhra Pradesh, India, Pin Code: 532127	India
Dr. K. G. S. Venkatesan	Professor & Head, Department of A.I & D.S, Shree Sathyam College of Engineering & Technology, Sankari, Selam District, Tamil Nadu, India, Pin Code: 637301	India
Dr. M. Lakshmiprasad	Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India, Pin Code: 500043	India

Applicant

Name	Address	Country
Mr. Gude Ramarao	Associate Professor, Department of Electronics and Communication Engineering, G. Pullaiah College of Engineering and Technology, Kurnool, Kurnool District, Andhra Pradesh, India, Pin Code: 518002	India
Dr. Parvathi Gorantla	Associate Professor in Physics, Department of Science & Humanities, Chalapathi Institute of Engineering & Technology, Guntur, Guntur District, Andhra Pradesh, India, Pin Code: 522036	India
Mrs. Ramineni Srilakshmi	Assistant Professor in Mathematics, Department of Science & Humanities, Chalapathi Institute of Engineering & Technology, Guntur, Guntur District, Andhra Pradesh, India, Pin Code: 522036	India
Mrs. Pallepogu Bhavani	Assistant Professor in Physics, Department of Science & Humanities, Chalapathi Institute of Engineering & Technology, Guntur, Guntur District, Andhra Pradesh, India, Pin Code: 522036	India
Ms. Priyanka Gomase	Ph. D Scholar, Department of Computer Science and Engineering, Madhyanchal Professional University, Bhopal, Madhya Pradesh, India, Pin Code: 462044	India
Dr. P. Deepa	Associate Professor, Department of Electronics and Instrumentation Engineering, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India, Pin Code: 600119	India
Mr. Ravishankar C. Bhaganagare	Assistant Professor, Department of CSE (AI&ML), Vishwakarma Institute of Technology, Pune, Maharashtra, India, Pin Code: 411037	India
Dr. Telagarapu Prabhakar	Professor, Department of Electronics and Communication Engineering, GMR Institute of Technology, Rajam, Vizianagaram District, Andhra Pradesh, India, Pin Code: 532127	India
Dr. K. G. S. Venkatesan	Professor & Head, Department of A.I & D.S, Shree Sathyam College of Engineering & Technology, Sankari, Selam District, Tamil Nadu, India, Pin Code: 637301	India
Dr. M. Lakshmiprasad	Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India, Pin Code: 500043	India

Abstract:

[031] The present invention discloses a quantum-resistant encryption system designed for secure data transmission in the post-quantum era, safeguarding sensitive from both classical and quantum computational threats. The system incorporates lattice-based, code-based, hash-based, and multivariate polynomial cryptographic to ensure robust encryption and secure key exchange. It features a hybrid encryption framework, forward secrecy mechanisms, and an adaptive cryptographic agility dynamically respond to evolving security challenges. The invention is applicable across finance, defense, healthcare, cloud computing, and IoT, providing long-term da protection and resilience against quantum decryption attacks. Additionally, the system integrates hardware-accelerated encryption and AI-driven optimizations to enl performance and scalability. With a focus on future-proof security, this invention addresses the urgent need for quantum-safe cryptographic solutions in the rapidly e digital landscape. Accompanied Drawing [FIGS. 1-2]

Complete Specification

Description:[001] The present invention relates to the field of cryptographic security, particularly post-quantum cryptography (PQC) designed to protect digital communications from quantum computing threats. More specifically, the invention provides a quantum-resistant encryption system and method that ensures secu transmission using advanced cryptographic techniques, including lattice-based, code-based, and hash-based encryption schemes. This invention applies to various such as secure communication networks, financial transactions, cloud computing, military-grade security, and healthcare data protection, where long-term data confidentiality is crucial.

BACKGROUND OF THE INVENTION

[002] The rapid advancement in quantum computing poses a significant threat to conventional cryptographic systems. Traditional public-key encryption schemes su RSA, ECC, and Diffie-Hellman rely on the computational difficulty of integer factorization and discrete logarithm problems, which quantum computers can efficiently using Shor's algorithm. As quantum computing capabilities progress, existing cryptographic security measures are increasingly at risk, necessitating the developmer quantum-resistant encryption methods that can secure digital communication in the post-quantum era.

[003] Current encryption techniques ensure security based on the assumption that certain mathematical problems are computationally infeasible to solve within a reasonable timeframe. However, quantum computers exploit superposition and entanglement to perform parallel computations, drastically reducing the time requ decrypt sensitive data. This vulnerability endangers confidential information in financial institutions, government agencies, and cloud-based platforms, making it im to develop cryptographic solutions that remain secure even in the presence of quantum adversaries.

[004] To mitigate the risks posed by quantum computing, the cryptographic community has been researching post-quantum cryptography (PQC) algorithms that rel

View Application Status

राष्ट्रीय मतदाता सेवा पोर्टल
NATIONAL VOTERS' SERVICES PORTAL