पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 09/2026	शुक्रवार	दिनांक: 27/02/2026
ISSUE NO. 09/2026	FRIDAY	DATE: 27/02/2026

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :16/02/2026
(21) Application No.202641017017 A
(43) Publication Date : 27/02/2026

(54) Title of the invention : Quantum-Resistant Cryptographic Authentication System

(51) International classification	:H04L 9/08, H04L 9/32, H04L 9/30, H04L 9/00, H04L 9/06
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No Filing Date	: :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Dr.L Sudha Rani
Address of Applicant :Associate Professor, Department of Computer science and Engineering, G Pulla Reddy Engineering college, College Address:G Pulla Reddy Engineering college(Autonomous), Kurnool- 518007, Andhra Pradesh, India. India Andhra Pradesh India
2)Amith Pradhaan
3)Shiny R M
4)Dr Nageswararao Sirisala
5)B.Rekhadevi
6)Debayan Bhowmik
7)Dr Hemantkumar Balasaheb Jadhav
8)Bappa Mondal
(72)**Name of Inventor :**
1)Dr.L Sudha Rani
2)Amith Pradhaan
3)Shiny R M
4)Dr Nageswararao Sirisala
5)B.Rekhadevi
6)Debayan Bhowmik
7)Dr Hemantkumar Balasaheb Jadhav
8)Bappa Mondal

(57) Abstract :
Quantum-Resistant Cryptographic Authentication System ABSTRACT: Quantum-resistant cryptography, often known as post-quantum cryptography, denotes a novel category of data security designed to safeguard information against quantum computers. Contemporary digital security solutions predominantly depend on mathematical problems that are not readily solvable by the majority of computers. For instance, two conventional encryption techniques, RSA and Elliptic Curve Cryptography (ECC), safeguard data by rendering it virtually infeasible for computers to ascertain the correct encryption key within a specified timeframe. Nonetheless, quantum computers present a novel challenge to these conventional security systems. To address this security issue, quantum-resistant encryption has been developed to endure the computing capabilities of quantum computers by utilizing distinct, more intricate mathematical challenges. Quantum-resistant encryption seeks to safeguard data security in anticipation of the widespread adoption of quantum computers. Quantum-resistant cryptography functions by substituting mathematical problems that quantum computers can efficiently resolve with novel, more complex forms of questions. These issues constitute the basis of numerous quantum-resistant cryptographic techniques. Lattice-based cryptography is a prevalent quantum-resistant technique and a favored alternative to conventional cryptographic methods. This approach depends on lattices, intricate mathematical constructs created by vector combinations, and necessitates computational resources to address challenges like identifying the shortest or nearest vector within the lattice. Examples of lattice-based algorithms specified by NIST are the ML-KEM (Module-Lattice-Based Key Encapsulation Mechanism) and ML-DSA (Module-Lattice-Based Digital Signature Algorithm). For outdated infrastructures, firms may necessitate updates to fully leverage modern solutions. A further problem is the long-term reliability of quantum-resistant methods. As quantum-resistant encryption progresses, so too may quantum computing, necessitating that cybersecurity researchers and developers consistently update and substitute methods. Nonetheless, despite obstacles, quantum-resistant encryption continues to serve as a viable short-term option for safeguarding against quantum attacks and holds potential for ensuring data security.

No. of Pages : 13 No. of Claims : 5