Patent Search

Invention Title	QUANTUM COMPUTING ALGORITHM FOR OPTIMIZED CRYPTOGRAPHIC KEY DISTRIBUTION
Publication Number	40/2024
Publication Date	04/10/2024
Publication Type	INA
Application Number	202441070352
Application Filing Date	17/09/2024
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMMUNICATION
Classification (IPC)	H04L0009080000, H04L0009400000, H04L0009320000, G06N0010000000, G06N0010700000

Inventor

Name	Address	Country
Mrs.S.Madhavi	Assistant Professor, Department of ECE, St.Peter's Engineering College, Hyderabad, Telangana, India. Pin Code:500100	India
Dr.Inderpreet Kaur	Associate Professor, Department of Computer Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India. Pin Code:201306	India
Mrs.Vijaya Lakshmi Sannapureddy	Assistant Professor, Department of CSE, KKR & KSR Institute of Technology & Sciences, Guntur, Andhra Pradesh, India. Pin Code:522005	India
Dr.Padmavathi Vurubindi	Associate Professor, Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, Telangana, India. Pin Code:500075	India
Dr.Canavoy Narahari Sujatha	Professor, Department of ECE, Sreenidhi Institute of Science and Technology, Yamnampet, Medchal- Malkajgiri District, Telangana, India. Pin Code: 501301	India
Dr.M.Lakshmiprasad	Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India. Pin Code: 500043	India
Ms.B.Keerthi Samhitha	Assistant Professor, Department of Computer Science and Engineering, K L Deemed to be University, Vaddeswaram, Guntur District, Andhra Pradesh, India. Pin Code:522302	India
Ms.B.Sumathi	Assistant Professor, Department of Computer Applications, SNS College of Technology, Coimbatore, Tamil Nadu, India. Pin Code:641 035	India
Ms.Jacquelin Anushya.P	Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamil Nadu, India. Pin Code:641035	India
Mrs.A.Nagamani	Assistant Professor, Department of CSE, MLR Institute of Technology, Hyderabad, Medchal-Malkajgiri, Telangana, India. Pin Code:500043	India

Applicant

Name	Address	Country
Mrs.S.Madhavi	Assistant Professor, Department of ECE, St.Peter's Engineering College, Hyderabad, Telangana, India. Pin Code:500100	India
Dr.Inderpreet Kaur	Associate Professor, Department of Computer Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India. Pin Code:201306	India
Mrs.Vijaya Lakshmi Sannapureddy	Assistant Professor, Department of CSE, KKR & KSR Institute of Technology & Sciences, Guntur, Andhra Pradesh, India. Pin Code:522005	India
Dr.Padmavathi Vurubindi	Associate Professor, Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, Telangana, India. Pin Code:500075	India
Dr.Canavoy Narahari Sujatha	Professor, Department of ECE, Sreenidhi Institute of Science and Technology, Yamnampet, Medchal- Malkajgiri District, Telangana, India. Pin Code: 501301	India
Dr.M.Lakshmiprasad	Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India. Pin Code: 500043	India
Ms.B.Keerthi Samhitha	Assistant Professor, Department of Computer Science and Engineering, K L Deemed to be University, Vaddeswaram, Guntur District, Andhra Pradesh, India. Pin Code:522302	India
Ms.B.Sumathi	Assistant Professor, Department of Computer Applications, SNS College of Technology, Coimbatore, Tamil Nadu, India. Pin Code:641 035	India
Ms.Jacquelin Anushya.P	Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamil Nadu, India. Pin Code:641035	India
Mrs.A.Nagamani	Assistant Professor, Department of CSE, MLR Institute of Technology, Hyderabad, Medchal-Malkajgiri, Telangana, India. Pin Code:500043	India

Abstract:

The present invention relates to a quantum computing algorithm for optimized cryptographic key distribution, designed to enhance the security, efficiency, and scala secure communication systems. This algorithm utilizes quantum entanglement to establish a secure key exchange between communicating parties, ensuring that any intercept or measure the quantum states is detectable. The algorithm incorporates adaptive quantum error correction to mitigate the impact of noise and errors, and quantum-based authentication protocol to prevent unauthorized access and man-in-the-middle attacks. Additionally, a hybrid classical-quantum post-processing pha the raw keys through reconciliation and privacy amplification, ensuring the final cryptographic key is robust and confidential. The invention offers a scalable solution with both quantum and hybrid quantum-classical networks, providing a future-proof approach to secure data exchanges in various critical industries. Accompanied D [FIGS. 1-2]

Complete Specification

Description:[001] The present invention pertains to the field of cryptographic systems and secure communication protocols. Specifically, it focuses on cryptographic distribution mechanisms that leverage the principles of quantum computing and quantum mechanics to enhance security, efficiency, and scalability in secure communication networks. Quantum computing introduces a new paradigm in information security by providing methods that utilize the unique properties of quant states, such as superposition and entanglement, to achieve cryptographic goals that are theoretically resistant to attacks, including those posed by future quantum computers.

[002] This invention is directed towards addressing the limitations of classical cryptographic key distribution protocols, which are increasingly vulnerable to attacks a computational power advances. The advent of quantum computers presents a significant threat to classical encryption methods, as many of these methods, particu those based on factoring or discrete logarithm problems, may become easily breakable. In contrast, quantum key distribution (QKD) methods offer a solution by rel the laws of quantum mechanics to provide unbreakable security guarantees, even in the presence of adversaries with quantum computational capabilities.

[003] In particular, the invention focuses on the development of a quantum computing algorithm that optimizes the key distribution process, enhancing the overall efficiency and robustness of quantum key distribution. By incorporating quantum error correction, authentication protocols, and a hybrid classical-quantum post-p phase, the invention improves the reliability and scalability of secure communication networks, making it suitable for large-scale and distributed environments. This invention has applications in a wide range of secure communication scenarios, including but not limited to, financial transactions, military communications, and sec exchanges over the internet.

BACKGROUND OF THE INVENTION

View Application Status