

## **Title: Privacy-preserving Techniques in the Quantum Computing Era: Innovative Approaches for Enhanced Information Security**

Quantum computers present significant security concerns for traditional cryptography, prompting researchers and cryptographers to propose innovative methods for protecting data. This special session aims to explore privacy-preserving techniques that effectively secure sensitive data while ensuring robust security measures. The goal is to foster interdisciplinary collaboration and present cutting-edge research, case studies, and practical implementations that demonstrate the potential of privacy-preserving techniques in enhancing information security. This special session aims to make a significant contribution to the advancement of security solutions that are not only privacy-conscious but also fortified against potential threats from quantum computers, recognizing the crucial intersection between privacy and cybersecurity. The topics covered will include data privacy, information security, secure communication, image encryption, watermarking, digital signature, steganography, privacy preservation, AI and machine learning for cybersecurity, federated learning, chaos-based cryptography, homomorphic encryption, medical data security, secure multiparty computation, privacy-aware access control, blockchain security, biometric security, network security, Internet of Things (IoT) security, cloud security, forensic analysis, and privacy-preserving data sharing.

Session organizers:

[Dr Mujeeb Ur Rehman](#): With over ten years of experience, I am an experienced educator with cutting-edge teaching and research expertise in AI, Machine Learning, Cybersecurity, and IoT, having worked in academic, research, and industry environments. My contribution to the research community includes co-authoring more than 28 research papers, published in leading international journals (IEEE and IET Transactions) and peer-reviewed international conference (Best Paper Awards) proceedings. In recognition of my contributions to the field of Artificial Intelligence and Cybersecurity, I was awarded the Global Talent status by the UK Research and Innovation Body and the Royal Academy of Engineering in 2022. I am a member of the UKRI Talent Peer Review College. I also serve as the editor for numerous journals such as [PLOS One](#), [STEM](#) and European Scientific Journal, etc. Moreover, I have organized several special issues as a lead guest editor, including the [CMC journal Impact factor 3.86](#), [Intelligent Automation & Soft Computing \(Impact factor 3.7\)](#) and [MDPI Axioms \(Impact factor 2.0\)](#), among others. Furthermore, I have served as a technical committee member in several IEEE conferences including ICSC2023, San Antonio, USA, CGVC 23, Wales, UK, GlobConPT, New Delhi, India and ICAISC 23, Jeddah, Saudi Arabia etc. Additionally, I am a reviewer for numerous high-impact factor journals.

School of Computer Science and Informatics, De Montfort University, Leicester, UK.

**Interests:** Cybersecurity, Artificial Intelligence, Machine Learning, Information security, Multimedia encryption, IoT.

[Dr Aminu Usman](#)

School of Computer Science, University of Sunderland, UK

Interests: Cybersecurity, Information security, Artificial Intelligence, Medical data security

[Dr Arslan Shafique](#)

School of Biomedical Engineering, University of Glasgow, UK

Interests: Multimedia encryption, Cybersecurity, Artificial Intelligence, Deep Learning

[Abdulrazaq Abba](#)

School of Architecture, Computing and Engineering, University of East London,

Information Security and Software Engineering

Call for Conference Special Session – for session’s promotion.

We invite submissions for a special session on the profound challenges posed by quantum computers to conventional cryptography. As the security landscape undergoes a transformative shift, researchers and cryptographers are compelled to devise innovative approaches to safeguard sensitive data. This special session is dedicated to exploring privacy-preserving techniques that not only protect data effectively but also ensure robust security measures in the quantum era.

The primary objective of this special session is to encourage interdisciplinary collaboration and present state-of-the-art research, case studies, and practical implementations showcasing the potential of privacy-preserving techniques in fortifying information security. By focusing on the crucial intersection of privacy and cybersecurity, we aim to make meaningful contributions to the development of privacy-aware and enhanced security solutions amidst the advent of quantum computers.

We invite submissions on a wide range of topics, including but not limited to:

Data and information security

Secure communication

Image encryption and watermarking

Digital signature and steganography

Privacy preservation

AI and machine learning for cybersecurity

Federated learning

Chaos-based cryptography

Homomorphic encryption

Medical data security

Privacy-preserving AI and machine learning

Secure multiparty computation

Privacy-aware access control

Blockchain security

Biometric security

Network security

Internet of Things (IoT) security

Cloud security,

Forensic analysis

Privacy-preserving data sharing

Join us in shaping the discourse on privacy and cybersecurity in the quantum era by sharing your insights, research findings, and practical implementations. Let us collectively explore the cutting-edge solutions that will define the future landscape of information security. Submit your contributions and be part of this transformative dialogue at our upcoming conference special session.