IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 3 May 2024, accepted 13 June 2024, date of publication 12 July 2024, date of current version 22 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3427268

RESEARCH ARTICLE

A Secure and Privacy-Preserving Signature Protocol Using Quantum Teleportation in Metaverse Environment

PANKAJ KUMAR[1], VIVEK BHARMAIK[1], SUNIL PRAJAPAT[1], (Member, IEEE), GARIMA THAKUR[1], ASHOK KUMAR DAS[2,3], (Senior Member, IEEE), SACHIN SHETTY[4], (Senior Member, IEEE), AND JOEL J. P. C. RODRIGUES[5,6], (Fellow, IEEE)

[1]Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala 176215, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Telangana, Hyderabad 500032, India
[3]Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA
[4]Virginia Modeling, Analysis and Simulation Center, Department of Computational Modeling and Simulation Engineering, Old Dominion University, Suffolk, VA 23435, USA
[5]Amazonas State University, Manaus, Amazonas 69475-000, Brazil
[6]Lusófona University, 1749-024 Lisbon, Portugal

Corresponding authors: Pankaj Kumar (pkumar240183@gmail.com) and Ashok Kumar Das (iitkgp.akdas@gmail.com)

This work was supported in part by the DoD Center of Excellence in AI and Machine Learning (CoE-AIML) with the U.S. Army Research Laboratory under Contract W911NF-20-2-0277, in part by the National Science Foundation under Grant 2219742 and Grant 2131001, in part by Virginia Innovation Partnership Corporation under Grant 230849, and in part by Brazilian National Council for Scientific and Technological Development—CNPq under Grant 306607/2023-9.

ABSTRACT The burgeoning concept of the metaverse as an interconnected virtual space represents the forefront of the next-generation internet. Quantum teleportation, known for its prowess in ensuring secure and reliable communications, stands poised to revolutionize interactions within this immersive digital realm. In this context, we propose a comprehensive interaction protocol tailored for the metaverse environment. The designed protocol entails two fundamental components: first, the interaction between a user and their avatar, facilitated by a secure seven-qubit entangled state; and second, the interaction between two avatars, enabled through an efficient two-qubit entangled state. To fortify the protocol's resilience, quantum key distribution (QKD) is employed for secure key sharing, while a trusted certificate authority serves as an essential entity for signature verification. Through rigorous safety and efficiency analysis, we demonstrate the protocol's robustness and performance, ensuring adherence to fundamental security properties such as unforgeability, undeniability, verifiability and traceability. By seamlessly integrating quantum teleportation principles with the metaverse environment, our protocol not only enhances security but also unlocks novel avenues for interaction and exploration within this digital frontier.

INDEX TERMS Metaverse, quantum teleportation, secure interactions, quantum signature, entangled states.

I. INTRODUCTION

The metaverse is a futuristic internet concept that enables the convergence of virtual reality, augmented reality, and the internet in an integrated shared space. It embodies a virtual reality space where users can interact with immersive digital environments and other users in real-time. This multidimensional virtual world is made up of a broad spectrum of interconnected virtual places rather than being restricted to a single platform or technology [1]. The metaverse is a place where new cultures, values, and commercial activities emerge from the interaction between the real and virtual worlds. It offers immersive experiences that transcend space and time. Users take the form of avatars, embodying their virtual identities and engaging in real-time communication with others [2].

The term ''metaverse'' finds its roots in early virtual reality experiments and science fiction literature, gaining

The associate editor coordinating the review of this manuscript and approving it for publication was Abdel-Hamid Soliman.

widespread recognition with Neal Stephenson's ''Snow Crash,'' which envisioned a virtual reality environment where individuals interacted through avatars [3]. The metaverse has emerged from the environments of fiction into reality as a result of technological developments, greater computational capacity, and the convergence of multiple technologies.

Several methods have been developed to facilitate network communication for metaverse applications, yet the delay in network transmission presents a significant challenge. Techniques such as data streaming, network-level optimization in 5G networks, and enhancements in multimedia coding and quality perception are essential for the broader and more effective expansion of the metaverse [4].

The metaverse relies on diverse multimedia content, requiring various methods to support efficient and high-quality creation, generation, transmission, and visualization of this content. Additionally, integrating different fields such as artificial intelligence (AI), network communication, and virtual reality hardware is crucial for delivering a comprehensive solution. Despite significant progress over the past decade, there is still a need to extend the immersive digital world to a broader audience and enhance interactive and immersive experiences simultaneously [4].

The metaverse holds immense potential to revolutionize various aspects of our lives. One such area is remote collaboration in virtual environments, where virtual offices and conference rooms offer enhanced productivity and collaboration beyond traditional video conferencing methods [5]. The influence of the gaming industry has been instrumental in shaping the metaverse, blurring the lines between fiction and reality and enabling interactive storytelling, entertainment, and cooperative learning experiences. Moreover, the metaverse presents new opportunities for virtual commerce, challenging traditional notions of ownership and fostering economic growth through the production, exchange and sale of digital assets. Businesses and educational institutions are actively exploring the metaverse for immersive training and education, utilizing virtual classrooms and simulations for practical instruction and skill development. Privacy and digital identity considerations are crucial for the responsible adoption and expansion of the metaverse, while global social interaction is facilitated through virtual events and gatherings. Subsequently, the metaverse's potential applications extend to healthcare, design, and various other industries, representing a paradigm shift in how we perceive and interact with digital spaces [6]. By converging virtual and physical realities, the metaverse creates a digital space for interaction and collaboration, interacting with various aspects of our lives. Some basic elements of the metaverse are users, avatars, platform servers *PS*s and certificate authorities (*CA*). They have different roles and responsibilities depending on various system models. However, challenges related to security, privacy, and inclusiveness must be addressed for responsible development. Securing personal information and preventing unauthorized access is important for user privacy. Robust security is needed to protect virtual transactions and users from financial and identity-related threats. A secure foundation is necessary for user confidence and seamless communication [1]. Traditional security measures may face challenges in this dynamic realm. Here, the introduction of quantum teleportation (QT) can revolutionize security by providing unprecedented protection against data breaches, unauthorized access, and malicious activities [7].

Using the properties of entangled particle correlations and classical communication, QT is a method for processing quantum information that allows the transfer of an unknown state. This technique is based on the entanglement properties of quantum particles using the laws of quantum physics. Subsequent measurements are executed until the final operation on the receiver's particle replicates the original information. Authentication and signatures are two widely used concepts in QT to satisfy security properties [8]. Everyday life applications for quantum signatures include electronic commerce, electronic banking, electronic voting, and electronic payment systems. To improve communication security, several signature types can be employed based on the intended usage [9]. A reliable third party is involved in the signature and message verification process using arbitrated quantum signatures. The possibility of integrating QT into the metaverse is already being explored; this could lead to faster and more reliable communication in between metaverse interactions. Apart from preserving a secure channel, using QT in the metaverse can lead to new discoveries and advancements in technology [10]. This concept has gathered significant attention and interest in recent years, driven by advancements in technology, connectivity, and the growing popularity of virtual experiences.

A. MOTIVATION AND CONTRIBUTIONS

With the advancements in metaverse technologies, it is vital to focus on securing communications in metaverse environments. Although there have been some frameworks to authenticate the identities of participants [11], to capture full body motion of users [12], convergence of IoT-Metaverse [13], to transmit semantic information using quantum states [14], and blockchain based authentication [15]. Still, the convergence of the metaverse and quantum technology has not been achieved. Exploring the potential of quantum mechanics can bring about an evolution in the manner in which interactions occur in the metaverse environment. Therefore, by combining the two systems, we introduce a fully fledged interaction scheme based on QT for the metaverse environment.

The contributions to the suggested work are as follows.

1) The designed protocol is divided into two parts: in the first part, we introduce a protocol for interaction between the user and its avatar using trusted *CA*, and the second part focuses on decentralised avatar-avatar interactions in the metaverse environment. The protocol leverages seven qubit-entangled states and two qubit-entangled states for QT. The reliability

of the complete protocol is ensured using a quantum signature and a coding rule for obtaining quantum states.
2) Second, we project the scheme to various security attacks, including anti-quantum attacks, inter-resend attacks, and entangle and measure attacks. The protocol satisfies the safety properties, including unforgeability, undeniability, traceability and verifiability. The security analysis explains the strength of the proposed scheme, based on the principles of the quantum world.
3) At last, we use ''efficiency analysis'' and ''security comparison'' to highlight the reliability and uniqueness of the proposed protocol. These analyses demonstrate the adaptability of our protocol across diverse environments.

B. OUTLINE

The rest of this article is sketched as follows. Section II provides a detailed background on the related work in the metaverse environment. The basic preliminaries required for discussing the proposed scheme in this work are provided in Section III. The proposed scheme in the metaverse environment has been proposed in Section IV which is a secure and privacy-preserving signature protocol using quantum teleportation. Section V discusses the security and efficiency analysis of the proposed scheme. The concluding remarks are then provided in Section VI.

II. RELATED WORK

The term ''metaverse'' was coined by Neal Stephenson in 1992 in his novel Snow Crash [3]. Snow Crash is a cyberpunk novel that examines the notion of the metaverse. It occurs in a utopian future where individuals flee into a real-life world called the metaverse. It is accessed through special goggles and gloves [16]. The hero, Hiro Hero, is a pizza delivery driver in the real world and a skilled hacker in the metaverse. He investigates a virus that threatens both the real world and the metaverse. Ever since its beginning, the definition of the metaverse has differed, incorporating ideas such as a multiverse, a reflection world, and the manifested Internet. Second Life was a virtual world launched in 2003 by Philip Rosedale [17] where alternative life away from the physical world was offered. It allowed users to create a digital avatar and live in a world called the ''grid''. Residents were able to interact with each other, socialize, and also participate in activities with groups. Players had the facility to build and trade digital property. The experience it provided was equivalent to what companies like Meta offer to represent metaverse ambitions.

The rise of quantum cryptography is attributed to the limitations of classical cryptographic methods as a result of advancements in quantum computing. Quantum teleportation, a quantum-based branch of cryptography, is a technique evolved through successive developments over the past few decades that started with the introduction of the Quantum Key Distribution protocol [18] in the 1980s. It was a key sharing protocol where Alice and Bob adopted a protocol to securely share the key with the use of quantum principles. The next evolution came in 1993, when Bennett et al. [19] brought about the concept of QT in their work, where Alice and Bob shared an entangled Einstein, Podolski, and Rosen (EPR) pair to proceed with the transmission of quantum particles [20]. With the opening of a new field, new sub-fields split from it. The models were suggested to use it as a cryptographic tool, incorporating techniques such as authentication, signature, encryption, etc. One such protocol to incorporate quantum proxy signatures into QT was proposed by Mambo et al. [21] to delegate signing authority to another authorised user. Since then, a remarkable amount of work has been done in the field of QT incorporating various signatures and advanced encryption methods [22], [23], [24], [25], [26], [27], [28]. Chehimi and Saad, in their article, explore the potential of quantum technologies to improve the metaverse and overcome its challenges [10]. They reviewed quantum information and discussed three main areas: quantum computing and optimization, quantum machine learning, and quantum communications, and provided a vision of the technology's role in the immersive metaverse.

A comprehensive understanding of quantum information is crucial for overcoming challenges in the metaverse. Over the years, researchers have worked to converge the applications of quantum communication in a metaverse environment. Cui [29] explores the metaverse and blockchain technology's role in digital identity and economic systems. They proposed a cross-chain protocol for the metaverse architecture, incorporating QT and quantum time locks for secure communication. The paper highlights the importance of decentralized blockchain, smart contracts, and consortium blockchain in the metaverse governance model. The paper evaluates the security and efficiency of a quantum-resistant cross-chain protocol, highlighting its potential impact on classical cryptosystems. Khalid et al. [14] explored the possible advantages of combining variational quantum computing and quantum anonymous communication to create quantum semantic communication, where they aspired to allow metaverse users to engage with virtual surroundings more safely and reliably. Semantic communication is a method using artificial intelligence to transmit semantic meanings, not complete raw information. It is gaining popularity in metaverse applications like meta-healthcare and meta-transportation. An anonymous quantum semantic (QSC) system for metaverse applications was developed, integrating quantum detection, variational quantum computing, embedding, and quantum machine learning. This study significantly contributed to the development of secure semantic communication, taking advantage of QT and thus enhancing immersive metaverse experiences, despite limited research in this field. QT is only partially explored in real-world and virtual-world applications. However, there is a consistent attempt by scientists to leverage the benefits of the integration of the quantum internet and the metaverse realm.

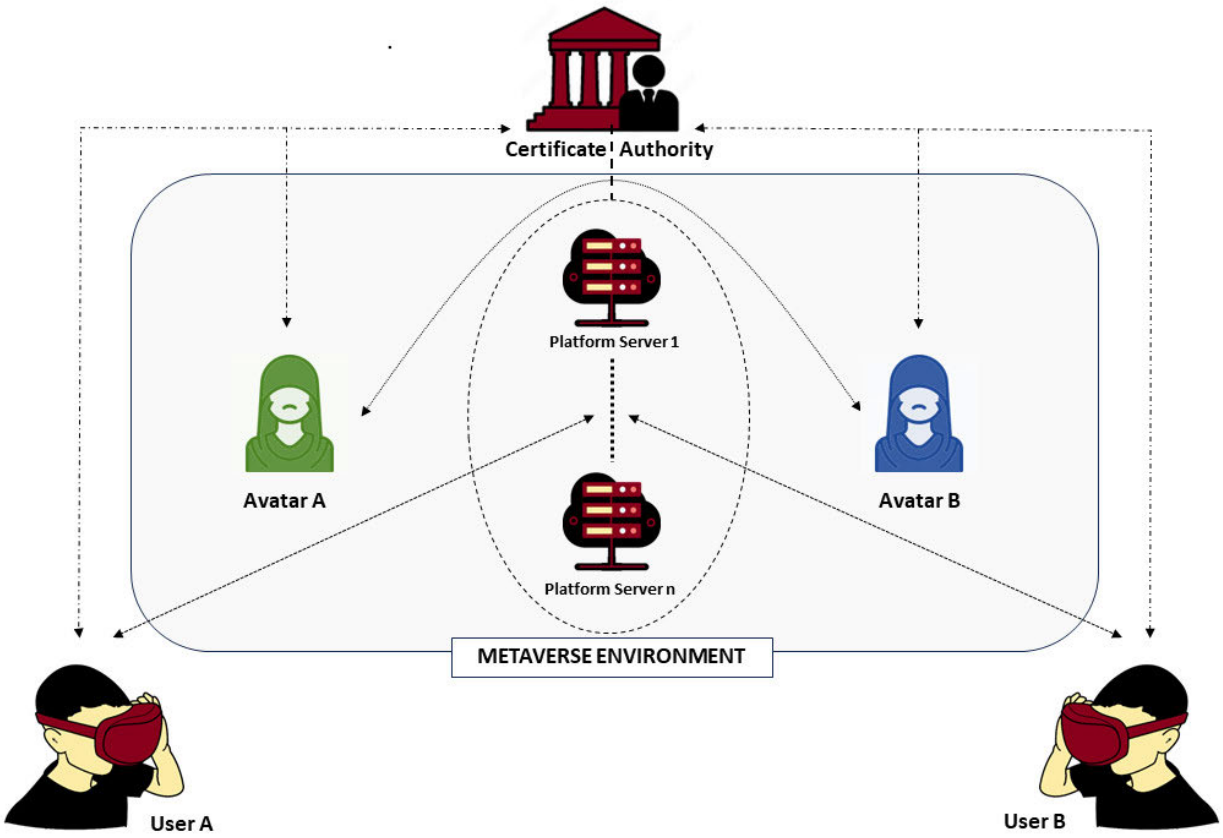

FIGURE 1. System Model.

III. PRELIMINARIES

In this section, we discuss the following basic preliminaries that are needed for discussing and analyzing the proposed scheme and other relevant existing schemes.

A. ENTANGLED STATE

Quantum entanglement is a unique state shared by multiple particles where the individual properties of particles are not defined until a measurement is made. This state is unique to the quantum domain because it allows a variety of possibilities among particles. Entangled systems can be measured, transformed, and purified. They can act as channels for quantum data in computing and cryptographic techniques, which is not possible for classical systems. Quantum information theory studies how quantum systems process information. Quantum space entanglement affirms that the quantum particle systems at each point are interrelated and inseparable. The state of a composite system can be either pure or entangled if this quantum state cannot be represented as the direct product of the quantum states of two subsystems. When a mixed state cannot be non-linearly entangled and cannot be effectively described as different forms of a directly integrable state, it is deemed non-entangled. The data that is contained in entangled states is a remarkable instrument for quantum information processing and is crucial to modern quantum computations and communications, such as QT.

B. QUANTUM SIGNATURE

Signatures play a crucial role in cryptography, ensuring message authenticity and integrity. In our protocol, we employ a modified quantum analog of the digital signature, leveraging the exceptional properties of quantum physics. Proxy signature authorizes the original signer to delegate signing capabilities to a proxy entity. In the context of our work, quantum proxy signatures offer enhanced security and privacy in metaverse interactions. They enables avatars to perform actions without revealing the user's private key, ensuring security and preventing unauthorized actions. Additionally, they encode user intent and authorization levels, facilitating better auditing and accountability in the metaverse. Quantum proxy signatures are theoretically unlinkable, enhancing anonymity and mitigating identity theft risks in virtual environments.

C. SYSTEM MODEL

The proposed protocol provides an interaction procedure for the metaverse environment. QT is utilised to convey information from one party to another. For the user to interact with his/her avatar, he/she must have authorization to enter the metaverse environment. The mutual authentication between *CA* and the user is pre-assumed in the suggested protocol. After the user's authentication, he/she obtains login credentials from *CA* and is able to create a digital avatar to

interact in the metaverse environment. Hence, the user signs in with this generated avatar on his smart device to various *PS* whose services he intends to avail of. The parties involved in this process are users, certificate authorities, various platform servers and users' avatars. Fig. 1 shows the system model of the proposed work. These parties have different roles and responsibilities:

- **User:** The user sends their identity and personal information to the *CA* for identity verification to participate in the metaverse environment. Then, the user creates an avatar, registers with various *PS*s through credentials obtained from certificate authorities, and accesses different virtual services managed by the *PS*$'s$. Thus, the user can communicate with the other avatars, and one avatar can communicate with the other avatars in virtual spaces using QT.
- **Avatar:** Avatar is a digital representation of the user and uses its credentials to generate the avatar to participate in the metaverse. Avatar has diverse roles, including interacting with other avatars and virtual entities; accessing a range of metaverse services. The user can have either a single avatar for all *PS*$'s$ or one avatar per *PS* depending on the metaverse environment.
- **Certificate Authority:** *CA* is a key player in the metaverse ecosystem. It authenticates player's true identities and provides login credentials so users can register in the metaverse. The user's identity information is received and authenticated by the *CA*. In this protocol, *CA* acts as the signature-verifying authority.
- **Platform Server:** *PS*s ensure transparency and trustworthiness in content transmissions, contributing to a safer metaverse environment. A user registers himself using his avatar with the *PS*. The information processed by the user is signed by *PS*s on the user's behalf. *PS*s provide virtual space for activities like education, gaming, learning, shopping, and healthcare.

The suggested framework has two parts:

- **Part 1:** The interaction between the user and his avatar;
- **Part 2:** The interaction between two avatars;

IV. PROPOSED METAVERSE INTERACTION SCHEME

In this section, we discuss various phases related to the proposed metaverse interaction scheme. Table 1 denotes the notations used in this communication process.

A. USER TO AVATAR INTERACTION

The user-avatar interaction process in metaverse is completed with the help of four parties:

- User (U_i), who creates his digital avatar and transmits information to its avatar
- Avatar (A_i), who receives the message and complete the communication process
- *PS*, who serves as a proxy signer and platform provider for users to interact and
- *CA*, who verifies the signature and provides valid credentials to participants

TABLE 1. Notations and their significance.

Notation	Description
w	Bit string of message transmitted by User (Part 1)
w'	bit string of message received by Avatar (Part 1)
a	Bit string of message transmitted by Avatar (Part 2)
ζ_{U_i}	Particle measurements obtained by User
ζ_{P_i}	Particle measurements obtained by Platform Server
ζ_{C_i}	Particle measurements obtained by Certificate Authority
ζ_{A_i}	Particle measurements obtained by Avatar A_i
$K_{U_iA_i}$	Shared Key of User and Avatar
$K_{A_iA_j}$	Shared Key of Avatars A_i and A_j
K_{U_iP}	Shared Key of User and Platform Server
K_{U_iC}	Shared Key of User and Certificate Authority
$K_{P,C}$	Shared Key of Platform Server and Certificate Authority
K_{A_iC}	Shared Key of Avatar and Certificate Authority
$\|\psi\rangle$	Quantum state of system

1) TELEPORTATION MODEL

User carries the information he wants to transmit as $|\psi\rangle_w = (q\,|0\rangle + r\,|1\rangle)_w$ where $|r|^2+|s|^2 = 1$. The complete state of the system can be described as $|\psi\rangle_{w1234567}$ [30], which consists of particles w and (1, 2, 3, 4, 5, 6, 7), is written in Eq. (1).

$$
\begin{aligned}
&|\psi\rangle_{w1234567}\\
&= |\psi\rangle_w \otimes |\psi\rangle_{1234567}\\
&= (q\,|0\rangle + r\,|1\rangle)_w \otimes |\psi\rangle_{1234567}\\
&= (q\,|0\rangle + r\,|1\rangle)_w \otimes \frac{\sqrt{2}}{4}(|0000000\rangle_{1234567}\\
&\quad + |0000011\rangle_{1234567} + |0001101\rangle_{1234567}\\
&\quad + |0001110\rangle_{1234567} + |1110001\rangle_{1234567}\\
&\quad + |1110010\rangle_{1234567} + |1111100\rangle_{1234567}\\
&\quad + |1111111\rangle_{1234567})\\
&= \frac{\sqrt{2}}{4}[q\,|00000000\rangle_{1234567} + q\,|00000011\rangle_{1234567}\\
&\quad + q\,|00001101\rangle_{1234567} + q\,|00001110\rangle_{1234567}\\
&\quad + q\,|01110001\rangle_{1234567} + q\,|01110010\rangle_{1234567}\\
&\quad + q\,|01111100\rangle_{1234567} + q\,|01111111\rangle_{1234567}\\
&\quad + r\,|10000000\rangle_{1234567} + r\,|10000011\rangle_{1234567}\\
&\quad + r\,|10001101\rangle_{1234567} + r\,|10001110\rangle_{1234567}\\
&\quad + r\,|11110001\rangle_{1234567} + r\,|11110010\rangle_{1234567}\\
&\quad + r\,|11111100\rangle_{1234567} + r\,|111111111\rangle_{1234567}] \qquad (1)
\end{aligned}
$$

2) INITIAL PHASE

- The user converts the message m that he wants to send to Avatar into a string of n bits:

$$w = \{w(1), w(2), \ldots, w(i), \cdots, w(n)\}.$$

- **QKD:** The parties use the QKD protocol to share the security keys.
  1) The key $\boldsymbol{K_{U_iA_i}}$ is shared between User U_i and his Avatar A_i,
  2) The key $\boldsymbol{K_{U_iP}}$ is shared between the U_i and *PS*,
  3) The key $\boldsymbol{K_{U_iC}}$ is shared between U_i and *CA*,
  4) The key $\boldsymbol{K_{PC}}$ is shared between *CA* and *PS* and
  5) The key $\boldsymbol{K_{A_iC}}$ is shared between A_i and *CA*.

TABLE 2. The process of generating the quantum states from message bit string.

$w(i)$	$\|\psi\rangle_{w(i)}$
0	$\|0\rangle$
1	$\|1\rangle$

- **Quantum Channel Generation:** CA generates n quantum states by using the seven qubit entangled state $|\psi\rangle_{1234567}$; and CA goes on to distribute these 7 entangled qubit particles to the concerned parties.

$$\begin{aligned}|\psi\rangle_{1234567} = \frac{\sqrt{2}}{4}(&|0000000\rangle_{1234567} + |0000011\rangle_{1234567} \\ &+ |0001101\rangle_{1234567} + |0001110\rangle_{1234567} \\ &+ |1110001\rangle_{1234567} + |1110010\rangle_{1234567} \\ &+ |1111100\rangle_{1234567} + |1111111\rangle_{1234567})\end{aligned}$$

- *CA* sends n number particles of the following particles correspondingly, (1, 5) to the user, (3, 7) to PS, (2) to A_i and (4, 6) to himself.
- *CA* implements regular eavesdropping checks to ensure the efficacy of the network.

3) AUTHORISING AND SIGNING PHASE

- The user authorizes *CA* to be his proxy signer for the communication and sends a n-bit string of the message w to A_i encrypted with their secret key via the secure channel.
- The user generates n quantum states that correspond to n-bit strings. $\{|\psi\rangle_{w(1)}, |\psi\rangle_{w(2)}, \ldots |\psi\rangle_{w(i)}, \ldots, |\psi\rangle_{w(n)}\}$

$$M = |\psi\rangle_{w(i)} = (q\,|0\rangle + r\,|1\rangle)_{w(i)}, \tag{2}$$

  where $q = 1$ and $r = 0$ or $q = 0$ and $r = 1$corresponding to $w(i) = 0$ or $w(i) = 1$. This coding rule stated in Table 2 is unknown to other parties except User U_i and his avatar A_i.
- U_i performs three-particle Von Neumann measurements on his particles (w, 1, 5) and records these measurements as $\{\zeta_{U_i}\}$.
- He sends $\boldsymbol{K_{U_iP}}\{\zeta_{U_i}\}$ to *PS* and $\boldsymbol{K_{U_iC}}\{\zeta_{U_i}\}$ to *CA*.
- *PS* decrypts the encrypted values with $\boldsymbol{K_{U_iP}}$ to get $\{\zeta_{U_i}\}$, performs two-particle Bell measurements on particles (3, 7) and records these as $\{\zeta_{P_i}\}$. It sends the signature $\boldsymbol{S\ \mathcal{D}\ K_{PC}}\{\zeta_{U_i}, \zeta_{P_i}\}$ to *CA*.

4) VERIFYING PHASES

- *CA* decrypts S and obtains $\{\zeta_{U_i}\}$ and $\{\zeta_{P_i}\}$ and for the signature verification, it individually matches the measurements $\{\zeta_{U_i}\}$ sent by U_i and *PS*. If the signature is not verified, the teleportation is aborted; otherwise, PS cooperates to complete QT.
- *CA* performs Bell measurements on (4, 6) particles, records these as $\{\zeta_{C_i}\}$ and sends $\boldsymbol{K_{A_iC}}\{\zeta_{U_i}, \zeta_{P_i}, \zeta_{C_i}\}$ to A_i.
- A_i utilizes the secret key $\boldsymbol{K_{A_iC}}$ to decipher the encrypted information and obtain $\{\zeta_{U_i}\}$, $\{\zeta_{P_i}\}$ and $\{\zeta_{C_i}\}$.
- Based on these outputs, A_i performs appropriate logical operations on his particle (2) and retrieves a quantum state $|\psi\rangle_{w'(i)}$. Thereafter, all n qubit particles are operated on to finally obtain $|\psi\rangle_{w'}$.
- Respective to the coding rule in Table 2, he performs classical measurement on his quantum bits to produce the classical bit string w'.
- Finally, the message is verified by A_i if the two data points $w' \stackrel{?}{=} w$ match and the teleportation is deemed successful. Otherwise, Avatar A_i declares the communication protocol invalid. Fig. 2 illustrates the user-avatar interaction model of our work.

B. AVATAR TO AVATAR INTERACTION

QT could be used for avatar-to-avatar interaction in the metaverse. This involves encoding information into a qubit, entangling it with another qubit, and sending it to the receiver. The receiver then decodes the information and recreates the original message. The general protocol for qubit QT works as follows: The aim is to transfer the quantum state of the message from one avatar to another. Since avatar generation is conditional on the verification of users' identities, only authenticated users can have avatars, and a two-party teleportation protocol is sufficient. In the beginning of the protocol, *CA* generates two particle-maximum-entangled pairs for avatars such that each pair is for two avatars wanting to interact with each other and shares it with a pair of two avatars. Since an avatar is controlled by its user, the actions performed by it will follow the directions given by the user.

1) INITIAL PHASE

- Avatar converts the message m that he wants to send to Avatar into a string of n bits:

$$a = \{a(1), a(2), \cdots, a(i), \cdots, a(n)\}.$$

- **QKD:** The parties use the QKD protocol to share the security keys.
  - Key $\boldsymbol{K_{A_iA_j}}$ is shared between Avatar A_i and another Avatar A_j,
  - The key $\boldsymbol{K_{A_iP}}$ between the A_i and *PS*, and $\boldsymbol{K_{A_jP}}$ between the A_j and *PS* are already shared in the previous part of the scheme.
- **Quantum Channel Generation:** *CA* generates n quantum states by using the two qubit maximal entangled state $|\psi\rangle_{XY}$; and goes on to distribute these entangled particles to the concerned parties.

$$|\psi\rangle_{XY} = \frac{1}{\sqrt{2}}(|00\rangle_{XY} + |11\rangle_{XY}) \tag{3}$$

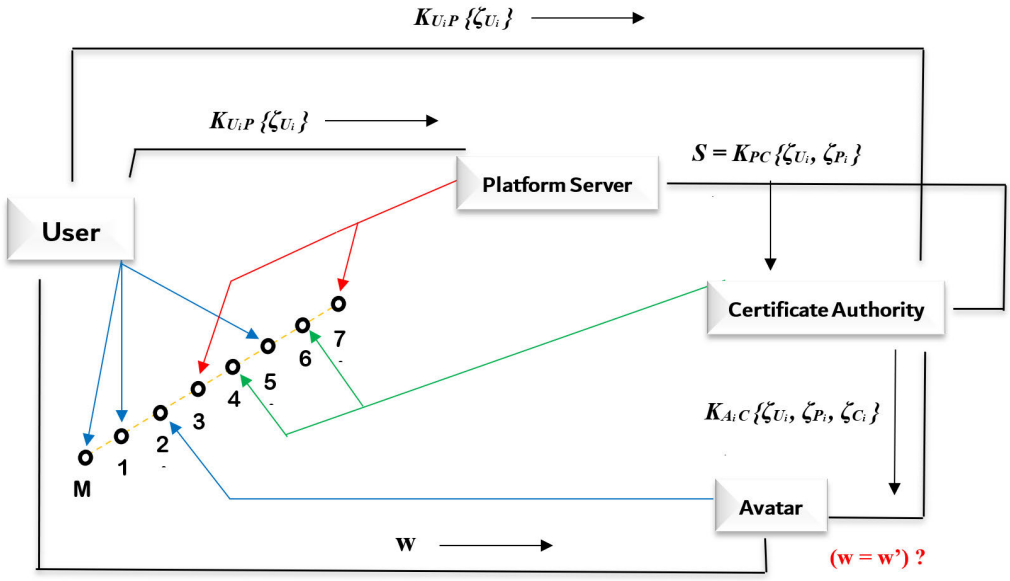

FIGURE 2. User-Avatar Interaction Model.

- *CA* sends n number particles of the following particles, correspondingly, $(X_i)'s$ to Avatar A_i and $(X_j)'s$ to Avatar A_j.
- *CA* implements regular eavesdropping checks to ensure the efficacy of the network.

2) COMMUNICATION PHASE

- Avatar A_i performs two-particle Bell measurements on his particles (a, X) and records these measurements as $\{\zeta_{A_i}\}$.
- The user generates n quantum states corresponding to n-bit strings; $\{|\psi\rangle_{a(1)}, |\psi\rangle_{a(2)}, \ldots |\psi\rangle_{a(i)}, \ldots, |\psi\rangle_{a(n)}\}$, where

$$P = |\psi\rangle_{a(i)} = (s\,|0\rangle + t\,|1\rangle)_{a(i)}, \tag{4}$$

  where $s = 1$ and $t = 0$ or $s = 0$ and $t = 1$corresponding to $a(i) = 0$ or $a(i) = 1$.
  This coding rule is similar to the one we used in the previous part of the scheme.
- A_j decrypts the encrypted values with $K_{A_iA_j}$ to get $\{\zeta_{A_i}\}$.
- Based on these measurements, A_j performs appropriate logical operations on his particle (Y) and retrieves a quantum state $|\psi\rangle_{a(i)}$. Thereafter, all n qubit particles are operated on to finally obtain $|\psi\rangle_a$.
- According to the coding rule in Table 2, performs classical measurement on his quantum bits to produce the classical bit string a.
- Finally, the message is received by A_j and the teleportation is declared successful. Fig. 3 illustrates the avatar-avatar interaction model of our work.

V. SECURITY AND EFFICIENCY ANALYSIS

To begin with, we conduct a safety analysis of protocol, including attacks, in this section. After that, the efficiency of our scheme is evaluated.

A. CORRECTNESS PROOF

In the following, we provide the correctness proofs for both the phases, namely Phase 1 and Phase 2.

- **Phase 1:** The entanglement properties of the entangled state aid in proving the correctness of the protocol. The user performs Von Neumann measurements on particles $(w, 1, 5)$. The user relays the encrypted measurements PS. Thereafter, PS performs the Bell measurements on particles $(3, 7)$. The encrypted measurements are forwarded to CA who performs another Bell measurement on $(4, 6)$ and sends their encrypted values to Avatar. Respective to the measurements, Avatar measures particles (2) to retrieve the quantum state of message w. At last, Avatar verifies $w = w'$, and declares the signature valid.
- **Phase 2:** Avatar A_i performs Bell measurements on particles (a,X). The user relays the encrypted measurements to another Avatar, A_j. Respective to the measurements, Avatar A_j measures particles (Y) to retrieve the quantum state of message a and apply the coding rule to obtain the original message.

B. SECURITY ANALYSIS

In the propositions 1–8, we show that the proposed scheme is robust against various attacks.

Proposition 1: The proposed scheme resists anti-quantum attack.

Proof: The foundation of classical cryptography is mathematical complexity, making it vulnerable to attacks by quantum computing. But the main tools used in quantum cryptography are quantum entanglement, quantum no-deleting theorem and the quantum no-cloning theorem, which hypothetically prevent any attack from a quantum computer. In this procedure, the actual message quantum

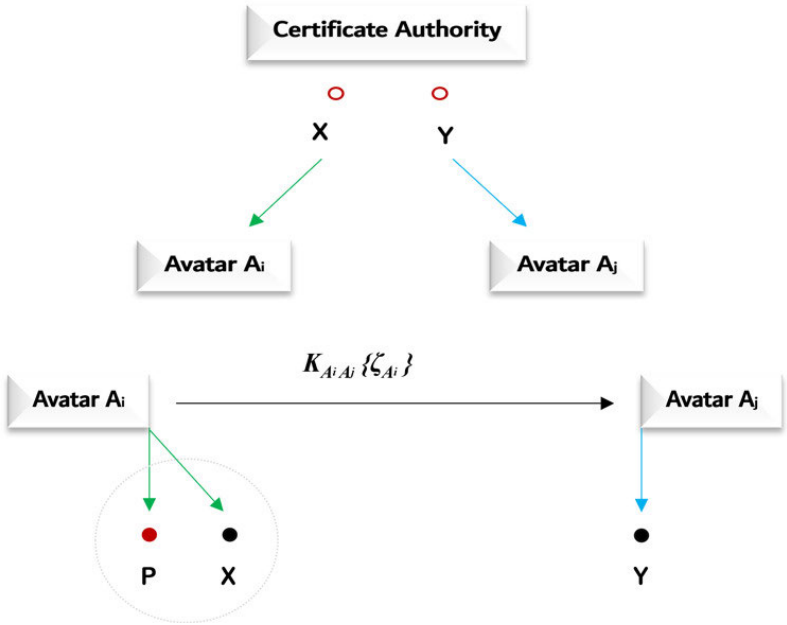

FIGURE 3. Avatar-Avatar Interaction Model.

states ψ_a and ψ_w containing information are obtained on the receiver's ends via the quantum correlation properties and do not go via the communication channel at all. The approach can thus achieve theoretical unconditional safety. □

Proposition 2: Privacy protection is provided in the proposed scheme.

Proof: In both the interactions between the user and his avatar and between two avatars, all the participants share entangled states, $|\psi\rangle_{1234567}$ (in the first case) or $|\psi\rangle_{XY}$ which make them the only authorised users to perform operations. This prevents external parties from intercepting any information exchanged during the two interactions. Hence, the information regarding the user's identity (in the first interaction) and the avatar's identity (in the second case) is retained exclusively in the secured environment of QT. □

Proposition 3: Unforgeability is supported in the proposed scheme.

Proof: In the first part, although the *PS* is a trusted party, if there is an internal forgery attempt by *PS*, the measurement mismatch of $\{\zeta_{U_i}\}$ during signature verification will reveal the forgery attack, and the protocol will be stopped and restarted. If there is an external forgery attack, that is, even if an external party gets access to any of the keys (which is also an impossible case, since the keys are shared through QKD protocol, making the key exclusive to those two participants who created the key, any outsider has to get access to the key before making a signature forgery attack, making the attack impossible to happen.), and somehow, if he/she is able to change the measurements and forward them, the message obtained in the last stage will not match the original message $w' \stackrel{?}{=} w$, and the protocol will be restarted.

In the second part, we have decentralized the communication process, involving only the two avatars intending to interact with each other. Therefore, internal forgery of measurements is not possible. The key $K_{A_iA_j}$ is shared between two avatars through QKD protocol, making any external party unable to determine the key. Therefore, unforgeability is ensured in both interactions by the correlation properties between the entangled particles. □

Proposition 4: Undeniability is supported in the proposed scheme.

Proof: All the parties are involved in both the interactions through QT, which makes the protocol dependent on the parties for its completion. Let's say that if an authorised party (say user) sends a message $\{x_i\}$ to another authorised party's avatar through the key $K_{U_iA_i}$ (i.e. user sends $K_{U_iA_i}\{x_i\}$ to his avatar), user has used his key $K_{U_iA_i}$ to encrypt the message to which only user and its avatar have access to and avatar can only decrypt the message by using the key $K_{U_iA_i}$. Therefore, once the user has sent the message, or the avatar has received the message, they can't deny their action. So if a sender sends the information to the intended receiver, the receiver is the confirmation of the fact that message was sent by the same user and vice-versa. As a consequence, the undeniability is not possible in the suggested protocol. □

Proposition 5: Verifiability is preserved in the proposed scheme.

Proof: The teleportation process in the first part involves the signature and the message, and their verification by the authorised parties. The signature $S = K_{PC}\{\zeta_{U_i}, \zeta_{P_i}\}$ is verified by the *CA* based on the string of measurements sent by User $\{\zeta_{U_i}\}$ and by the *PS* $\{\zeta_{U_i}, \zeta_{P_i}\}$. After the avatar obtains the information upon receipt of all the measurements on entangled particles, it matches the obtained output with the message received by it in the initial phase, $w' \stackrel{?}{=} w$ and hence, the message w is verified. □

TABLE 3. Security Comparison.

Parameter	Proposed scheme	Scheme in [31]	Scheme in [24]	Scheme in [30]
Quantum resource	genuine seven qubit entangled state	five-qubit maximally entangled state	three-particle GHZ-entangled state	genuine seven qubit entangled state
Encryption method	quantum one time pad (QOTP)	quantum fourier transform (QFT)	quantum one time pad (QOTP)	not used
Eavesdropping check	Yes	Yes	Yes	No
Efficiency	11.11% (Part 1) 100% (Part 2)	12.5%	14%	21.43%

Proposition 6: The proposed scheme supports traceability.

Proof: Virtual and physical traceability refers to the security property of being able to identify the origin of a teleported quantum state $|\psi\rangle$ i.e., to ensure the receiver can verify that the message originated from the sender and not from any unauthorized source trying to impersonate the sender. If a third party tries to impersonate the user's identity, quantum correlation prevents the third party from getting access to the user's entangled particle. Also, any unauthorised party attempting to get in the communication process can be traced through the identity information available to the *PS* and the *CA*. The verified access to QT protocol prevents the malicious party from accessing the digital identity of the user, which leaves his attempt and his original identity revealed. Thus, the traceability property is ensured, and the origin of the messages w and a can be traced back to the sender, user and avatar, respectively, in two parts of the scheme. □

Proposition 7: The proposed scheme resists intercept and resend attack.

Proof: This attack involves an eavesdropper attempting to intercept the communication between two parties, and attempting to resend these with their modified ones. As a result, the attacker might be able to pretend to be the user and undermine the legitimacy of the message. However, the presence of errors in the received information can alert the sender and receiver to a potential eavesdropper. To identify and address any inconsistency triggered by the eavesdropper's intervention, the two parties utilize the BB84 technique to share the key, which entails disclosing to the public a small piece of the data they received. This technique helps in detecting and eliminating any information the eavesdropper may have learned from successful guesses produced during the intercept-and-resend attack.

Proposition 8: Entangle and measure attack is resisted in the proposed scheme.

Proof: Another approach used by an eavesdropper to breach secure communication is an entangle-and-measure attack. In this property, the attacker entangles their measuring particle with the message-containing transported state. The message verification process employed in the first part of the scheme reflects any discrepancy created by the attacker, as the obtained message w and actual message w' won't match. If the attacking party entangles its own quantum particles, by the property of quantum mechanics, the previous shared entangled state will collapse, and the involved parties will gain knowledge. Also, contemporary QKD methods include measures like decoy states to identify and foil attempts at entangle-and-measure attacks. This makes the protocol safe against an entangle-and-measure attack. □

C. EFFICIENCY ANALYSIS

The efficiency of the proposed protocol can be determined using the definition [32]

1) PART 1 OF THE PROTOCOL

$$\eta = \frac{\mathcal{L}_s}{\mathcal{L}_q + \mathcal{L}_b},$$

Here, we do not need to consider the number of bits required for the eavesdropping check. $\mathcal{L}_s$ denotes the number of bits of the message. $\mathcal{L}_q$ denotes the number of qubits transmitted in the quantum channels, and $\mathcal{L}_b$ denotes the number of classical bits transmitted in the classical channels. In our scheme, the length of the message w is n bits. The quantum messages transmitted between participants are $n + n + 2n + 3n + n = 8n$ qubits. The classical messages transmitted between participants are n bits. Thus, we demonstrate the efficiency of this scheme as follows:

$$\eta = \frac{n}{8n + n} = \frac{n}{9n} = \frac{1}{9}$$

2) PART 2 OF THE PROTOCOL

$$\eta = \frac{\mathcal{L}_s}{\mathcal{L}_q + \mathcal{L}_b},$$

$\mathcal{L}_s$ denotes the number of bits of the message. a, $\mathcal{L}_q$ denotes the number of qubits transmitted in the quantum channels, and $\mathcal{L}_b$ denotes the number of classical bits transmitted in the classical channels.

In our scheme, the length of the message a is n bits. The quantum messages transmitted between participants are n qubits.Thus, we demonstrate the efficiency of this scheme as follows:

$$\eta = \frac{n}{n} = 1$$

VI. CONCLUSION

In this article, we introduced a new quantum signature secured metaverse interaction scheme, leveraging the principles of Quantum Teleportation (QT) and proxy signature. The proposed scheme consists of two parts, each harnessing the unique properties of 7-particle and 2-particle quantum

entangled states, respectively. The security of the protocol is ensured by the execution of quantum key distribution, entanglement correlations and proxy signature mechanisms. It facilitates the transmission of information from the users and their avatars, as well as between avatars in the metaverse environment. The proposed protocol satisfies safety properties, such as unforegeability, undeniability, verifiability, and traceability. In addition, the protocol is also robust to various security attacks, including intercept and resend attacks, entangle measure attack, and anti-quantum attack. The suggested model sets the template for the prospective integration of QT into the metaverse interactions. Therefore, our scheme is theoretically achievable and potentially implementable under an arranged teleportation setup.

REFERENCES

[1] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, "A survey on the metaverse: The State-of-the-art, technologies, applications, and challenges," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14671–14688, Aug. 2023.

[2] J. Oh, M. Kim, Y. Park, and Y. Park, "A secure content trading for cross-platform in the metaverse with blockchain and searchable encryption," *IEEE Access*, vol. 11, pp. 120680–120693, 2023.

[3] N. Stephenson, *Snow Crash* (Bantam Spectra Book). New York, NY, USA: Bantam Books, 1993. [Online]. Available: https://books.google.co.in/books?id=FU1bAAAAMAAJ

[4] S.-C. Chen, "Multimedia research toward the metaverse," *IEEE Multimedia Mag.*, vol. 29, no. 1, pp. 125–127, Jan. 2022.

[5] H.-J. Kwon, A. E. Azzaoui, and J. H. Park, "MetaQ: A quantum approach for secure and optimized metaverse environment," *Hum.-Cent. Comput. Inf. Sci*, vol. 12, p. 42, Jan. 2022.

[6] H. Yoon, Y. Lee, and C. Shin, "Avatar-based metaverse interactions: A taxonomy, scenarios and enabling technologies," *J. Multimedia Inf. Syst.*, vol. 9, no. 4, pp. 293–298, Dec. 2022.

[7] A. S. Badr and R. De Amicis, "An empirical evaluation of enhanced teleportation for navigating large urban immersive virtual environments," *Frontiers Virtual Reality*, vol. 3, Jan. 2023, Art. no. 1075811.

[8] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nat. Photon.*, vol. 9, no. 10, pp. 641–652, 2015.

[9] H. Zhang, Z. Ji, H. Wang, and W. Wu, "Survey on quantum information security," *China Commun.*, vol. 16, no. 10, pp. 1–36, Oct. 2019.

[10] M. Chehimi and W. Saad, "Quantum technologies for the metaverse: Opportunities and challenges," in *Metaverse Communication and Computing Networks: Applications, Technologies, and Approaches*. Hoboken, NJ, USA: Wiley, 2023, pp. 267–291.

[11] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, "Design of secure mutual authentication scheme for metaverse environments using blockchain," *IEEE Access*, vol. 10, pp. 98944–98958, 2022.

[12] K. Y. Lam, L. Yang, A. Alhilal, L.-H. Lee, G. Tyson, and P. Hui, "Human-avatar interaction in metaverse: Framework for full-body interaction," in *Proc. 4th ACM Int. Conf. Multimedia Asia*, Dec. 2022, pp. 1–7.

[13] R. Patan and R. M. Parizi, "Securing data exchange in the convergence of metaverse and IoT applications," in *Proc. 18th Int. Conf. Availability, Rel. Secur.*, Aug. 2023, pp. 1–8.

[14] U. Khalid, M. S. Ulum, A. Farooq, T. Q. Duong, O. A. Dobre, and H. Shin, "Quantum semantic communications for metaverse: Principles and challenges," *IEEE Wireless Commun.*, vol. 30, no. 4, pp. 26–36, Aug. 2023.

[15] M. Kim, J. Oh, S. Son, Y. Park, J. Kim, and Y. Park, "Secure and privacy-preserving authentication scheme using decentralized identifier in metaverse environment," *Electronics*, vol. 12, no. 19, p. 4073, Sep. 2023.

[16] J. Joshua, "Information bodies: Computational anxiety in neal Stephenson'sSnow crash," *Interdiscipl. Literary Stud.*, vol. 19, no. 1, pp. 17–47, Mar. 2017.

[17] M. Rymaszewski, *Second Life: The Official Guide*. Hoboken, NJ, USA: Wiley, 2007.

[18] G. Brassard and C. H. Bennett, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Sep. 1984, pp. 175–179.

[19] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Mar. 1993.

[20] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities," *Amer. J. Phys.*, vol. 58, no. 12, pp. 1131–1143, Jun. 1990.

[21] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. 79, no. 9, pp. 1338–1354, 1996.

[22] D. Lu, Z. Li, J. Yu, and Z. Han, "A verifiable arbitrated quantum signature scheme based on controlled quantum teleportation," *Entropy*, vol. 24, no. 1, p. 111, Jan. 2022.

[23] F.-L. Chen, Z.-H. Wang, and Y.-M. Hu, "A new quantum blind signature scheme with BB84-state," *Entropy*, vol. 21, no. 4, p. 336, Mar. 2019.

[24] J. Cao, X. Xin, C. Li, and F. Li, "Security analysis and improvement of a blind semi-quantum signature," *Int. J. Theor. Phys.*, vol. 62, no. 4, p. 87, Apr. 2023.

[25] Y. Jiang, L. Chen, X. Gong, Y. Zhu, and Y. Gao, "Quantum multi-party fair exchange protocol based on three-particle GHZ states," *Quantum Inf. Process.*, vol. 22, no. 9, p. 353, Sep. 2023.

[26] T.-T. Fan, D.-J. Lu, M.-G. You, and S.-J. Qian, "Multi-proxy signature scheme using five-qubit entangled state based on controlled quantum teleportation," *Int. J. Theor. Phys.*, vol. 61, no. 12, p. 273, Dec. 2022.

[27] Y. Xue, A. Yin, and K. Xing, "A quantum multi-proxy blind signature scheme based on D-dimensional GHZ states," *Int. J. Theor. Phys.*, vol. 62, no. 12, p. 265, Dec. 2023.

[28] J. Yu and J. Zhang, "Quantum (t,n) threshold proxy blind signature scheme based on bell states," *Int. J. Theor. Phys.*, vol. 61, no. 7, p. 207, Jul. 2022.

[29] Y. Cui, "A cross-chain protocol based on quantum teleportation for underlying architecture of metaverse," in *Proc. 7th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Apr. 2022, pp. 508–512.

[30] Z. Shao and Y. Long, "Circular controlled quantum teleportation by a genuine seven-qubit entangled state," *Int. J. Theor. Phys.*, vol. 58, no. 6, pp. 1957–1967, Jun. 2019.

[31] Y.-F. He and W.-P. Ma, "Quantum key agreement protocols with four-qubit cluster states," *Quantum Inf. Process.*, vol. 14, no. 9, pp. 3483–3498, Sep. 2015.

[32] A. Cabello, "Quantum key distribution in the Holevo limit," *Phys. Rev. Lett.*, vol. 85, no. 26, pp. 5635–5638, Dec. 2000.

PANKAJ KUMAR received the M.Sc. degree from CCS University, Meerut, India, in 2005, and the Ph.D. degree from Galgotias University, in 2020. He has been an Assistant Professor with the Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala, India. He has published over 40 academic research articles on information security and privacy preservation. His current research interests include cryptography, blockchain, wireless network security, information theory, and network coding.

VIVEK BHARMAIK received the Graduate degree from Himachal Pradesh University, Shimla, and the master's degree from the Central University of Himachal Pradesh, Dharamshala, India. His research interest includes quantum signature.

SUNIL PRAJAPAT (Member, IEEE) received the M.Sc. degree in mathematics from the Central University of Himachal Pradesh, Dharamshala, India, where he is currently pursuing the Ph.D. degree with the Srinivasa Ramanujan Department of Mathematics. His research interests include quantum cryptography and post-quantum cryptography, coding theory, blockchain, and various applications of cryptographic primitives in the real world. He is a renowned Reviewer for numerous IEEE, Taylor and Francis, MDPI, PLOS One, Elsevier, and Springer journals. He is a CSIR Fellow.

GARIMA THAKUR received the M.Sc. degree from the Central University of Himachal Pradesh, Dharamshala, India, where she is currently pursuing the Ph.D. degree. Her research interests include authentication, post-quantum cryptography, the IoT, and blockchain technology.

ASHOK KUMAR DAS (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently a Full Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India, and also a Visiting Research Professor with Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. His current research interests include cryptography, system and network security, including security in smart grids, the Internet of Things (IoT), the Internet of Drones (IoD), the Internet of Vehicles (IoV), cyber-physical systems (CPS) and cloud computing, intrusion detection, blockchain, AI/ML security, and post-quantum cryptography. He has authored over 420 papers in international journals and conferences in the above areas, including over 355 reputed journal articles. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has been listed in the Web of Science (ClarivateTM) Highly Cited Researcher, in 2022 and 2023, in recognition of his exceptional research performance. He was/is on the editorial board of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He also served as one of the Technical Program Committee Chairs for the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in June 2019, International Conference on Applied Soft Computing and Communication Networks (ACN'20), Chennai, India, in October 2020, second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, in October 2020, and International Conference on Applied Soft Computing and Communication Networks (ACN'23), Bengaluru, India, in December 2023. His Google Scholar H-index is 87 and i10-index is 264 with over 21,900 citations.

SACHIN SHETTY (Senior Member, IEEE) received the Ph.D. degree in modeling and simulation from Old Dominion University, in 2007. He was an Associate Professor with the Electrical and Computer Engineering Department, Tennessee State University, USA. He is currently a Professor with Virginia Modeling, Analysis and Simulation Center, Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. He has authored or co-authored over 185 research articles in journals and conference proceedings and two books. His research interests include the intersection of computer networking, network security, and machine learning. He was a recipient of the DHS Scientific Leadership Award. He has served as the Technical Program Committee Member of ACM CCS, IEEE INFOCOM, IEEE ICDCN, and IEEE ICCCN.

JOEL J. P. C. RODRIGUES (Fellow, IEEE) is currently a Professor with COPELABS, Lusófona University, Lisbon, Portugal. He is also the Leader of the Next Generation Networks and Applications Research Group (CNPq), the Director for Conference Development—IEEE ComSoc Board of Governors, an IEEE Distinguished Lecturer, the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the Scientific Council at ParkUrbis—Covilhã Science and Technology Park, the Past Chair of the IEEE ComSoc Technical Committee on eHealth, the Past Chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee Member of the IEEE Life Sciences Technical Community and the Publications Co-Chair, and a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is the Editor-in-Chief of the *International Journal on E-Health and Medical Communications* and an editorial board member of several high-reputed journals. He has been the General Chair and the TPC Chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He has authored or coauthored over 1000 papers in refereed international journals and conferences, three books, two patents, and one ITU-T recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. He is a member of the Internet Society and a Senior Member of ACM.