Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047669

ARTICLE

Chaotic Map-Based Authentication and Key Agreement Protocol with Low-Latency for Metasystem

Guojun Wang[1,2] and Qi Liu[3,*]

[1]School of Electronics & Information Engineering, Nanjing University of Information Science & Technology, Nanjing, 210044, China

[2]Yancheng Polytechnic College, Yancheng, 224000, China

[3]Jiangsu Province Engineering Research Center of Advanced Computing and Intelligent Services, School of Software, Nanjing University of Information Science and Technology, Nanjing, China

*Corresponding Author: Qi Liu. Email: qi.liu@nuist.edu.cn

Received: 13 November 2023 Accepted: 05 February 2024 Published: 26 March 2024

ABSTRACT

With the rapid advancement in exploring perceptual interactions and digital twins, metaverse technology has emerged to transcend the constraints of space-time and reality, facilitating remote AI-based collaboration. In this dynamic metasystem environment, frequent information exchanges necessitate robust security measures, with Authentication and Key Agreement (AKA) serving as the primary line of defense to ensure communication security. However, traditional AKA protocols fall short in meeting the low-latency requirements essential for synchronous interactions within the metaverse. To address this challenge and enable nearly latency-free interactions, a novel low-latency AKA protocol based on chaotic maps is proposed. This protocol not only ensures mutual authentication of entities within the metasystem but also generates secure session keys. The security of these session keys is rigorously validated through formal proofs, formal verification, and informal proofs. When confronted with the Dolev-Yao (DY) threat model, the session keys are formally demonstrated to be secure under the Real-or-Random (ROR) model. The proposed protocol is further validated through simulations conducted using VMware workstation compiled in HLPSL language and C language. The simulation results affirm the protocol's effectiveness in resisting well-known attacks while achieving the desired low latency for optimal metaverse interactions.

KEYWORDS

Metasystem; authentication and key agreement; chaotic map; secure communication

1 Introduction

With the arrival of 5G, the rapid development of artificial intelligence and cloud computing technology [1] has accelerated the realization of the metaverse. People can enter the virtual world and interact with others in the form of metaverse avatars [2] through virtual reality (VR) [3] headsets. This will change the organization and operation of existing societies by combining virtual reality. However, new challenges are also brought in protecting the privacy and security of the avatars. Different from the real world, the metaverse will not only face passive attacks and eavesdropping attacks but also

more active attacks will be launched to gain the benefits of the virtual world. Therefore, preserving the security and privacy of the avatar [4] is a current issue that needs to be addressed urgently.

Identity verification is an essential part of either the real world or the metaverse. In the real world, authentication is also applied in multiple environments. Under the industrial IoT environment [5], the user and sensing device authenticate and negotiate a session key for communication. In the metaverse, users represent themselves virtually by creating avatars and can access a variety of services through these avatars. However, in the current metaverse environment, any user has the freedom to create any avatar as their virtual representative. This property provides an avenue for malicious users to create avatars and cause serious security issues during metaverse interactions. Therefore, it is essential to design an AKA protocol that allows users to securely access available services in the metaverse and remain safe against other security threats. In the metaverse, meta-users and virtual devices verify each other's identity legitimacy and generate session key for communication transfer to protect the privacy of the users as well as the devices.

Although the metaverse can provide a variety of services, it is vulnerable to a variety of attacks that can threaten security. First, each communication in the metasystem may be maliciously attacked by an adversary. Attackers can illegally enter the virtual world of the meta-user or tamper with transmitted data by attacking the metasystem's communication channels. In addition, performance is a significant aspect of the user experience, besides the security aspect. Ryu et al. [6] presented a mutual authentication scheme using Elliptic Curve Cryptography (ECC) to offer secure communication between users and servers as well as secure interactions between avatars and avatars of the platform. Thakur et al. [7] proposed a secure ECC-based authentication scheme utilizing a fuzzy extractor for more secure user-server and avatar-avatar interactions. However, the high computational cost of the above literature makes them unsuitable for deployment into the metaverse.

1.1 Main Contributions

To solve the above problems, a chaotic mapping-based AKA protocol is proposed to protect the privacy of metaverse avatars, which can achieve secure communication between VR headset and tactile devices. Biometric of metaverse user is adopted as one of the authentication factors to improve the security of metaverse avatars which can resist malicious impersonation of the avatar. Further, user anonymity is achieved even if the tactile device is corrupted without any valid information. Finally, the proposed protocol is analyzed through experimental simulations and the experimental results show that it can be applied to privacy protection for metaverse avatars with better performance. The main contributions are summarized as follows:

1. User anonymity is considered to resist malicious attackers or corrupted tactile devices impersonating metaverse avatars when logging into a VR headset. To ensure the legitimacy of the avatar, the VR headset needs to verify the user's identity and complete collaboration with the tactile device. It means multi-party authentication needs to be completed between the user, headset, and tactile device before entering the metaverse. Based on the semi-group attribute of the Chebyshev polynomial, the session key is established after multi-party authentication. Malicious attackers cannot obtain user information from VR device communication even if launching Man-in-the-middle (MITM), impersonation, and forgery attacks.

2. The security of the session key established between the VR headset and tactile devices has been formally proven under the ROR model. Additionally, informal proofs substantiate its resilience against both passive and active attacks. This paper adopts the robust DY threat model to define the capabilities of the adversary. Malicious attacker not only has access to information stored locally

in sensor-based VR tactile devices through powerful analysis but also has absolute control over the information transmitted on the public channel. Without loss of generality, impersonation attacks on users, edge nodes, and tactile devices are analyzed in Section 5.1. The analysis results show that the proposed protocol can protect the security and privacy of metaverse avatars effectively despite strong attackers.

3. To further verify that the protocol can protect the privacy and security of the avatar effectively, security was further analyzed using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. To provide a robust level of security for the proposed protocol, rigorous testing was performed using the AVISPA tool. This tool allowed us to simulate active attacks and thoroughly evaluate the protocol's resistance to these attacks. The test results indicate that it provides efficient protection against replay and man-in-the-middle attacks. Based on the successful completion of these tests, it can be confidently asserted that the protocol is capable of withstanding a variety of active attacks and can offer a robust level of security for its intended use cases.

4. For security and performance, the proposed protocol is compared with related works and the result shows that the proposed protocol has better usability for Metasystem. The proposed protocol has undergone thorough analysis and comparison with other related works in terms of security and performance. The comparison results show that the proposed protocol has better usability, making it a more reliable and efficient means of authentication for secure communication in Metasystem. Overall, the comparison analysis highlights the strengths and advantages of the proposed protocol and confirms its potential as a leading solution in secure communication for Metasystem.

1.2 Related Works

Although the exploration and development of metaverse is still in the infancy phase, some works on metaverse [8,9] have already been proposed. Additionally, several works [10–14] have discussed security and privacy issues in the metaverse. As relevant technologies are deeply explored, research on the metaverse has involved multiple areas. Park et al. [15] discussed the three components involved in the metaverse and review representative applications in the metaverse in terms of user interaction, and implementation. Wang et al. [2] analyzed what security threats the metaverse will face in terms of security and privacy.

However, the issue of security in the metaverse has been of considerable concern. Rafique et al. [16] found that virtual reality systems work by presenting interactive views on head-mounted displays. To make virtual reality systems more secure, they also propose possible countermeasures. O'Brolcháin et al. [17] focused on two core ethical issues that may exist in virtual reality and social networks, namely threats to privacy (information printing, physical privacy, associative privacy) and threats to autonomy (freedom, knowledge, authenticity). They also proposed some countermeasures to address the threats to privacy. Falchuk et al. [18] concentrated on the technological underpinnings that contribute to an increased level of privacy for VR participants while immersed in social VR in their article.

Authentication is the first line of defense against access by illegal meta-users in the metaverse, which protects the meta-user's avatar [19] from unauthorized intrusion, therefore authentication is an integral part of the metaverse. Yang et al. [20] proposed a two-factor authentication framework based on chameleon signature and biometric authentication to suggest a secure meta-universe environment. In addition, the authentication framework is shown to guarantee the consistency and traceability of virtual identities after security analysis. Yu et al. [21] proposed a multi-server-based authentication key agreement to protect the user's private information, which can achieve user untraceability. Although

it reduced the communication and computation overheads compared to partially related works. However, it transmits 7 times, which cannot effectively guarantee the freshness of the message. Zheng et al. [22] proposed a three-party authentication key agreement based on chaotic mapping, considering the security needs of real applications, in which user anonymity is achieved.

2 Preliminaries

In this section, descriptions of the preliminaries are given and the notations are illustrated in Table 1.

Table 1: Notations

Notation	Description	Notation	Description
En	Edge node	ID_{Vtd_j}	Identifier of jth VR tactile device
Vh_i	ith VR headset	$\alpha, \beta_i, \gamma_i$	Long-term secret
Vtd_j	jth VR tactile device	$\|, \oplus$	Connection and exclusive-OR
ID_i	Identifier of ith meta-user	T_1, T_2, T_3	Timestamp
PW_i	Password of ith meta-user	ΔT	Maximum transmission delay
BIO_i	Biometrics of ith meta-user	$H(\cdot)$	One-way hash function

2.1 Fuzzy Extractor

Fuzzy extractor is widely accepted technique for extracting biometric characteristics. In this technique, it mainly contains generation and restoration functions. Now, we give the formal definitions of the two functions as follows:

$GEN(BIO) \rightarrow (\sigma, \tau)$: $GEN(\cdot)$ is the generating function of the fuzzy extractor. When the biometric BIO is input, the function outputs a secret value σ about the biometric and a recovery parameter τ.

$REP(BIO^*, \tau) \rightarrow \sigma$: $REP(\cdot)$ is the restoration function of the fuzzy extractor. When the biometric BIO^* and the recovery parameter τ are input, the function outputs the secret value σ^* about the biometric BIO^*.

2.2 Chebyshev Chaotic-Map

Chebyshev chaotic-map is a chaotic mapping function for generating a pseudo-random sequence of numbers. The formal definitions of Chebyshev chaotic-map are given as follows:

Definition 1: $T_r(p)$ represents the Chebyshev polynomial and is drawn up as $T_r(p) = cos\left(n \cdot cos^{-1}(p)\right)$, where r is randomly sampled in $\mathbb{Z}^+$ and $p \in [-1, 1]$. What's more, Chebyshev polynomials satisfy the following characteristic.

1. Recursiveness: $T_r(p) = 2pT_{r-1}(p) - T_{r-2}(p)$, where $r \geq 2$, $T_0(p) = 1$ and $T_1(p) = p$.

2. Semi-group: $T_m(T_r(p)) = cos\left(m \cdot cos^{-1}\left(cos\left(r \cdot cos^{-1}(p)\right)\right)\right) = cos\left(mr \cdot cos^{-1}(p)\right) = T_{mr}(p)$, where $m, r \xleftarrow{R} \mathbb{Z}^+$ and $p \in [-1, 1]$.

Definition 2: Chaotic-map discrete logarithm (CMDL): For a given number $p \in [-1, 1]$ and the related Chebyshev polynomial $T_r(p)$, the CMDL problem confirms that it is hard for probabilistic

polynomial time (PPT) adversary to compute r. In other words, the probability of an adversary A solving the CMDL problem in a finite time span is negligible.

$$Adv_A^{CMDL} = Pr[A(p, T_r(p)) = r] \leq \varepsilon \tag{1}$$

3 Formal Definition

3.1 System Model

Suppose a scenario exists where a patient has a sudden illness that requires surgery. However, specialized surgical treatment is not available where the patient is located. The relevant experienced physician can access the metasystem through the terminal and operate on the patient through the sensory device. Under the above scenario, there are three entities in the proposed metasystem communication network as shown in Fig. 1. The detailed description of each entity is given as follows.

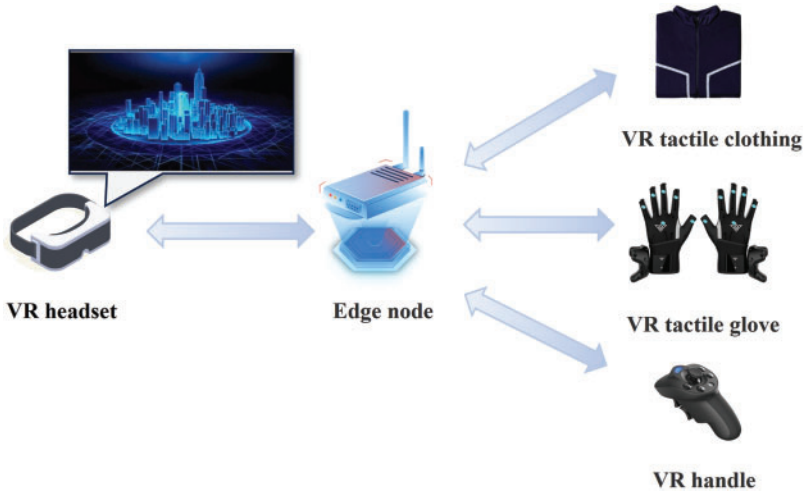

Figure 1: System model

Meta-user (Mu_i): Meta-users access the meta-system and connect VR tactile devices by logging in to their VR headset device Vh_i. Before Mu joined the metasystem, it needs to send registration information to the edge node to complete the registration through the secure channel. When the legitimate meta-user has successfully logged into the system, Vh_i sends an authentication message to the edge node over the public channel.

Edge node (En): In this paper, En is responsible for offline-registration of Vtd_j and online registration of Mu. When En received the authentication message from Vh_i, En verifies its legitimacy and computes a novel authentication message to send to Vtd_j. It is worth mentioning that edge node is assumed to be a trusted entity. This is sensible because the edge nodes are deployed by authorities in reality.

VR tactile device (Vtd_j): Offline-registration is required to be completed through En before Vtd_j can be deployed. When receiving an authentication message from En, Vtd_j verifies its legitimacy and generates a novel authentication message to send to Vh_i. Finally, the session key is generated between Vh_i and Vtd_j.

3.2 Adversary Model

In this paper, the popular DY adversary model is adopted, in which a strong adversary A is defined. The adversary has absolute control of the metasystem network under the DY model, specific capabilities are defined as follows.

Information transmitted over public channels can be obtained by adversaries, and even more can be deleted and modified. Notably, Vh_i and Vtd_j communicate on a public channel.

VR tactile devices in metasystem can be captured by A and information in the devices can be extracted by powerful analytical tool.

3.3 Security Model

We prove session key security under the widely-used ROR model, which is applied in formal proofs of many authentication protocols. The detailed description of the ROR security model is provided and shown as follows:

Participants. For better identification, the $\theta_1 th$, $\theta_2 th$ and $\theta_3 th$ of Mu_i, En and Vtd_j are defined as $P_{Mu_i}^{\theta_1}$, $P_{En}^{\theta_2}$ and $P_{Vtd_j}^{\theta_3}$.

Acceptance. A participant P^{θ} is accepted if it enters the accepted state after receiving the final intended protocol message. The links of communication messages constitute the session identifiers.

Partnering. Two participants P^{θ_1} and P^{θ_2} are partners if they both meet the following conditions. 1) P^{θ_1} and P^{θ_2} are in the accepted state. 2) P^{θ_1} and P^{θ_2} completed mutual authentication and shared an identifier. 3) P^{θ_1} and P^{θ_2} are mutual partners.

Freshness. If the session key between Mu_i and Vtd_j has not been obtained by an adversary A, the participants $P_{Mu_i}^{\theta_1}$ and $P_{Vtd_j}^{\theta_3}$ are fresh. A is assumed to have absolute control of the metasystem communication network. A can modify and delete information transmitted on the public channel and further access the following oracles.

Execute $\left(P_{Mu_i}^{\theta_1}, P_{En}^{\theta_2}, P_{Vtd_j}^{\theta_3}\right)$: A can obtain information about interactions between $P_{Mu_i}^{\theta_1}$, $P_{En}^{\theta_2}$ and $P_{Vtd_j}^{\theta_3}$ in public channel through this oracle. A can launch an eavesdropping attack with this query.

Reveal (P^{θ}): A can obtain sk generated between P^{θ} and its partner through this oracle.

Send (P^{θ}, m): A can send m to the participant P^{θ} through this oracle and can further obtain a response related to m. A can launch an active attack with this query.

Corruptheadset $\left(P_{Mu_j}^{\theta_1}\right)$: A can obtain all the parameters stored in the VR headset through this oracle. A can launch a VR headset device loss attack with this query.

Corruptheadset $\left(P_{Vtd_j}^{\theta_3}\right)$: A can obtain all the parameters stored in the VR tactile device through this oracle. A can launch a VR tactile device loss attack with this query.

Guess (P^{θ}): A can obtain the semantic security of sk between Mu_i and Vtd_j through this oracle. Before starting, a guess $g \in \{0, 1\}$ is output and sent to A. P^{θ} returns sk in case $g = 1$ or a random number in case $g = 0$ when sk is fresh. Otherwise, the output is $\perp$.

4 Proposed Protocol

There are four phases in our protocol. We will give the detailed construction of each phase in this section. Before adding an entity to the meta-system, initialization and entity registrations need to be

completed. Then, the session key is generated between the meta-user and the device after verifying each other's identities. The update of the authentication factor is additionally considered to prevent privacy breaches due to loss of passwords. The detailed construction of each stage is shown as follows.

4.1 Initial Phase

First of all, *En* will start to initiate the metasystem and pre-deploy for VR tactile devices. Vtd_j selects the device identifier ID_{Vtd_j} and generates random number c_j. Then, the pseudo-identifier $PVD_j = H\left(ID_{Vtd_j} \| c_j\right)$ is computed by Vtd_j and sent to *En*. For each PVD_j, *En* chooses a long-term secret γ_j and computes $H\left(\alpha \| \gamma_j\right)$, where α is *En*'s master key and $H\left(\alpha \| \gamma_j\right)$ is sent to Vtd_j as a response over the secure channel. Meanwhile, *En* stores $< PVD_j, H\left(\alpha \| \gamma_j\right), p >$ in local database, where p is the public parameter chosen by *En*.

4.2 Offline-Registration Phase

Meta-user access to the metaverse via a VR headset means that the legitimate meta-user needs to complete meta-user registration to gain permission. As shown in Fig. 2, the offline registration phase for meta-users can be divided into the following 3 steps.

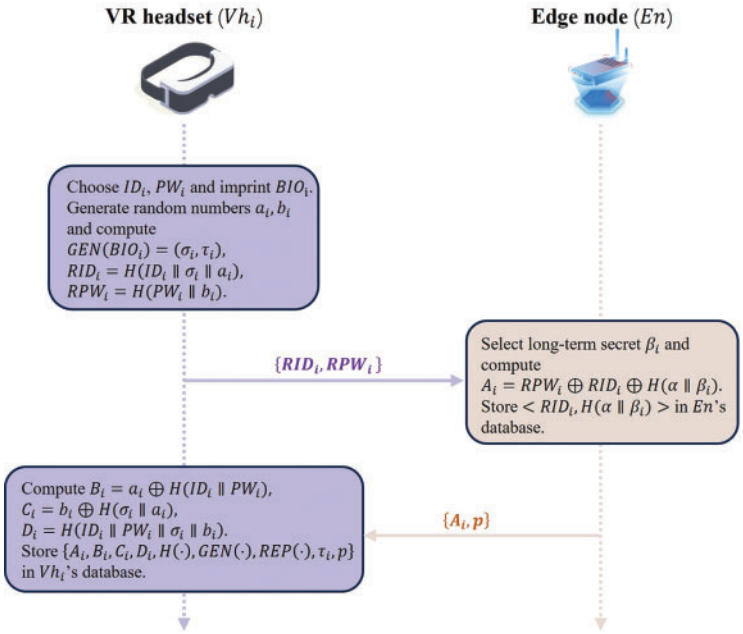

Figure 2: Meta-user registration

Step 1: Vh_i chooses ID_i, PW_i and reads retinal biometrics of meta-users BIO_i, after which the random numbers a_i and b_i are further generated. Then, Vh_i computes $GEN\left(BIO_i\right) = (\sigma_i, \tau_i)$, $RID_i = H\left(ID_i \| \sigma_i \| a_i\right)$ and $RPW_i = H\left(ID_i \| \sigma_i \| a_i\right)$. Meta-user registration information $\{RID_i, RPW_i\}$ is sent to *En* via the secure channel.

Step 2: After receiving the registration message from Vh_i, *En* selects the long-term secret β_i and computes $A_i = RPW_i \oplus RID_i \oplus H\left(\alpha \| \beta_i\right)$. As a registration response, $\{A_i, p\}$ is sent to Vh_i through the secure channel. Notably, $< RID_i, H\left(\alpha \| \beta_i\right) >$ is likewise stored in *En*'s database.

Step 3: Vh_i computes $B_i = a_i \oplus H(ID_i \| PW_i)$, $C_i = b_i \oplus H(\sigma_i \| a_i)$ and $D_i = H(ID_i \| PW_i \| \sigma_i \| b_i)$ when receiving A_i from En. Then, the information $\{A_i, B_i, C_i, H(\cdot), GEN(\cdot), REP(\cdot), \tau_i, p\}$ associated with ID_i is stored in Vh_i's database.

4.3 Login and Authentication Phase

Once the meta-user wants to access the metaverse and collaborate with the VR tactile devices, a secure session key needs to be established between Vh_i and Vtd_j. Before establishing the session key, authentication is required to prevent attackers from obtaining private information about the meta-user. As shown in Fig. 3, the login and registration phase can be divided into the following 7 steps.

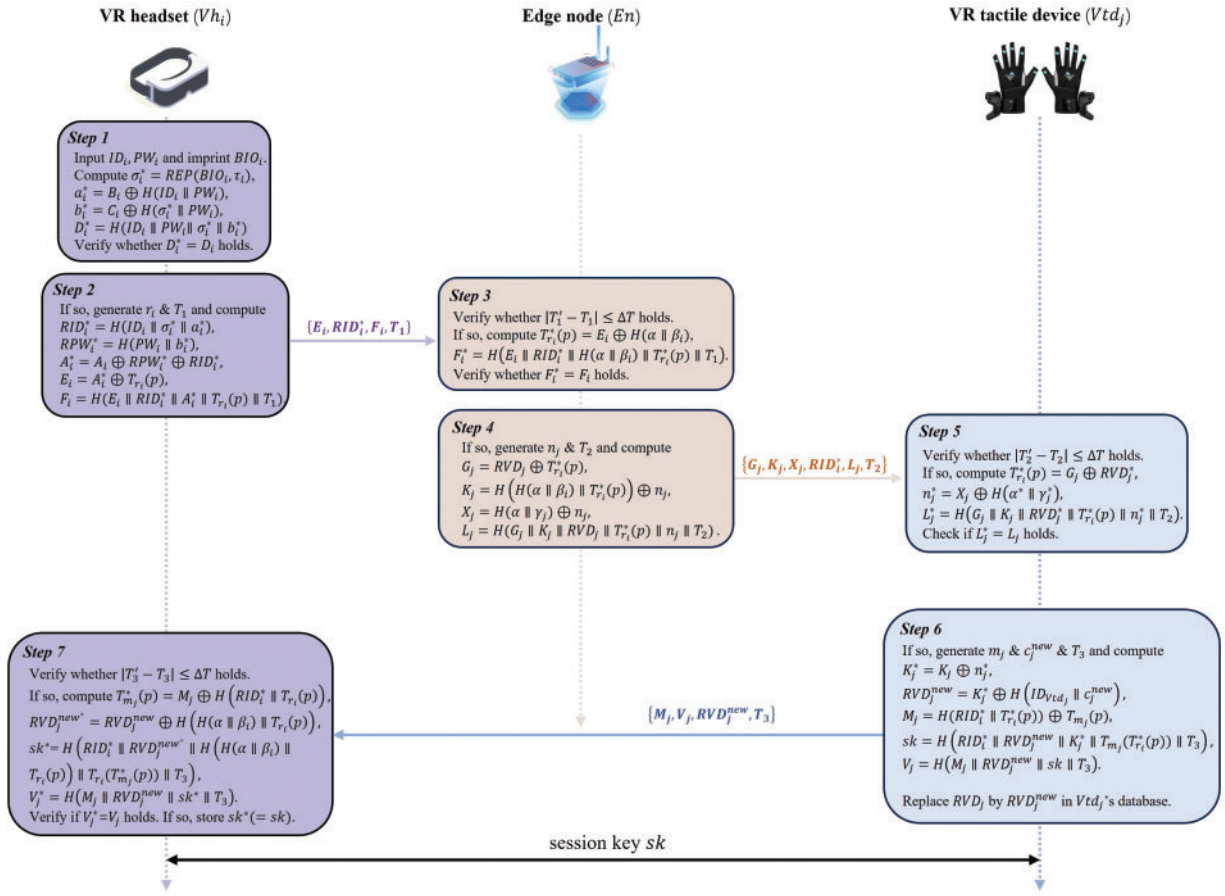

Figure 3: Login and authentication

Step 1: Vh_i computes $\sigma_i^* = REP(BIO_i, \tau_i)$, $a_i^* = B_i \oplus H(ID_i \| PW_i)$, $b_i^* = C_i \oplus H\left(\sigma_i^* \| PW_i\right)$ and $D_i^* = H\left(ID_i \| PW_i \| \sigma_i^* \| b_i^*\right)$, when meta-user inputs ID_i, PW_i and BIO_i. Vh_i verifies whether $D_i^* = D_i$ holds, where D_i is the information stored in Vh_i's database associated with ID_i.

Step 2: If the above equation holds, Vh_i computes $RID_i^* = H\left(ID_i \| \sigma_i^* \| a_i^*\right)$, $RPW_i^* = H\left(PW_i \| b_i^*\right)$, $A_i^* = A_i \oplus RPW_i^* \oplus RID_i^*$, $E_i = A_i^* \oplus T_{r_i}(p)$ and $F_i = H\left(E_i \| RID_i^* \| A_i^* \| T_{r_i}(p) \| T_1\right)$, where r_i is randomly chosen by Vh_i and T_1 is the timestamp. After the computation is completed, the authentication information $\left\{E_i, RID_i^*, F_i, T_1\right\}$ is sent to En through the public channel.

Step 3: *En* verifies whether $\left|T_1' - T_1\right| \leq \Delta T$ holds when receiving $\left\{E_i, RID_i^*, F_i, T_1\right\}$ from Vh_i. If the above equation holds, *En* computes $T_{r_i}^*(p) = E_i \oplus H(\alpha \| \beta_i)$ and $F_i^* = H\left(E_i \| RID_i^* \| H(\alpha \| \beta_i) \| T_{r_i}^*(p) \| T_1\right)$. Then, *En* verifies whether $F_i^* = F_i$ holds when F_i^* has been computed.

Step 4: If the above equation holds, *En* computes $G_j = RVD_j \oplus T_{r_i}^*(p)$, $K_j = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right) \oplus n_j$, $X_j = H(\alpha \| \beta_i) \oplus n_j$ and $L_j = H\left(G_j \| K_j \| RVD_j \| T_{r_i}^*(p) \| n_j \| T_2\right)$, where n_j is randomly chosen by *En* and T_2 is the timestamp. After the computation is completed, the authentication information $\left\{G_j, K_j, X_j, L_j, T_2\right\}$ is sent to Vtd_j through the public channel.

Step 5: Vtd_j verifies whether $\left|T_2' - T_2\right| \leq \Delta T$ holds when receiving $\left\{G_j, K_j, X_j, L_j, T_2\right\}$ from *En*. If the above equation holds, Vtd_j computes $T_{r_i}^*(p) = G_j \oplus RVD_j^*$, $n_j^* = X_j \oplus H\left(\alpha^* \| \gamma_j^*\right)$ and $L_j^* = H\left(G_j \| K_j \| RVD_j^* \| T_{r_i}^*(p) \| n_j^* \| T_2\right)$. Then, Vtd_j verifies whether $L_j^* = L_j$ holds when L_j^* has been computed.

Step 6: If the above equation holds, Vtd_j computes $K_j^* = K_j \oplus n_j^*$, $RVD_j^{new} = K_j^* \oplus H\left(ID_{Vtdj} \| c_j^{new}\right)$, $M_j = H\left(RID_i^* \| T_{r_i}^*(p)\right) \oplus T_{m_j}^*(p)$, $sk = H\left(RID_i^* \| RVD_j^{new} \| K_j^* \| T_{m_j}\left(T_{r_i}^*(p)\right) \| T_3\right)$ and $V_j = H\left(M_j \| RVD_j^{new} \| sk \| T_3\right)$, where m_j is randomly chosen by *En* and T_3 is the timestamp. After the above parameters have been calculated, Vtd_j replaces RVD_j by RVD_j^{new} in Vtd_j's database and sends $\left\{M_j, V_j, RVD_j^{new}, T_3\right\}$ to Vh_i through the public channel.

Step 7: Vh_i verifies whether $\left|T_3' - T_3\right| \leq \Delta T$ holds when receiving $\left\{M_j, V_j, RVD_j^{new}, T_3\right\}$ from Vh_i. If the above equation holds, Vh_i computes $T_{m_j}^*(p) = M_j \oplus H\left(RID_i^* \| T_{r_i}(p)\right)$, $RVD_j^{new^*} = RVD_j^{new} \oplus H\left(H(\alpha \| \beta_i) \| T_{r_i}(p)\right)$, $sk^* = H\left(RID_i^* \| RVD_j^{new^*} \| H\left(H(\alpha \| \beta_i) \| T_{r_i}(p)\right) \| T_{r_i}\left(T_{m_j}^*(p)\right) \| T_3\right)$, and $V_j^* = H\left(M_j \| RVD_j^{new} \| sk^* \| T_3\right)$. After the above parameters have been calculated, Vh_i verifies whether $V_j^* = V_j$ holds. If so, Vh_i stores sk^*.

4.4 Factors Update Phase

Considering the practical needs of users who have lost their passwords or whose biometrics need to be updated, factors update is also designed. As shown in Fig. 4, the factors update phase can be divided into the following 3 steps.

Step 1: Vh_i computes $\sigma_i^* = REP(BIO_i, \tau_i)$, $a_i^* = B_i \oplus H(ID_i \| PW_i)$, $b_i^* = C_i \oplus H\left(\sigma_i^* \| PW_i\right)$ and $D_i^* = H\left(ID_i \| PW_i \| \sigma_i^* \| b_i^*\right)$, when meta-user inputs ID_i, PW_i and BIO_i. Vh_i verifies whether $D_i^* = D_i$ holds, where D_i is the information stored in Vh_i's database associated with ID_i.

Step 2: Vh_i computes $GEN\left(BIO_i^{new}\right) = \left(\sigma_i^{new}, \tau_i^{new}\right)$, $B_i^{new} = B_i \oplus H(ID_i \| PW_i) \oplus H\left(ID_i \| PW_i^{new}\right)$ $A_i^{new} = A_i \oplus H\left(ID_i \| \sigma_i^{new} \| a_i\right) \oplus H(PW_i \| b_i) \oplus H\left(ID_i \| \sigma_i^{new} \| a_i\right) \oplus H\left(PW_i^{new} \| b_i\right)$, $C_i^{new} = C_i \oplus H(\sigma_i \| a_i) \oplus H(\sigma_i \| a_i)$ and $D_i^{new} = H\left(ID_i \| PW_i^{new} \| \sigma_i^{new} \| b_i\right)$.

Step 3: Replace A_i, B_i, C_i, D_i by A_i^{new}, B_i^{new}, C_i^{new} and D_i^{new} in Vtd_j's database when the above computation is completed.

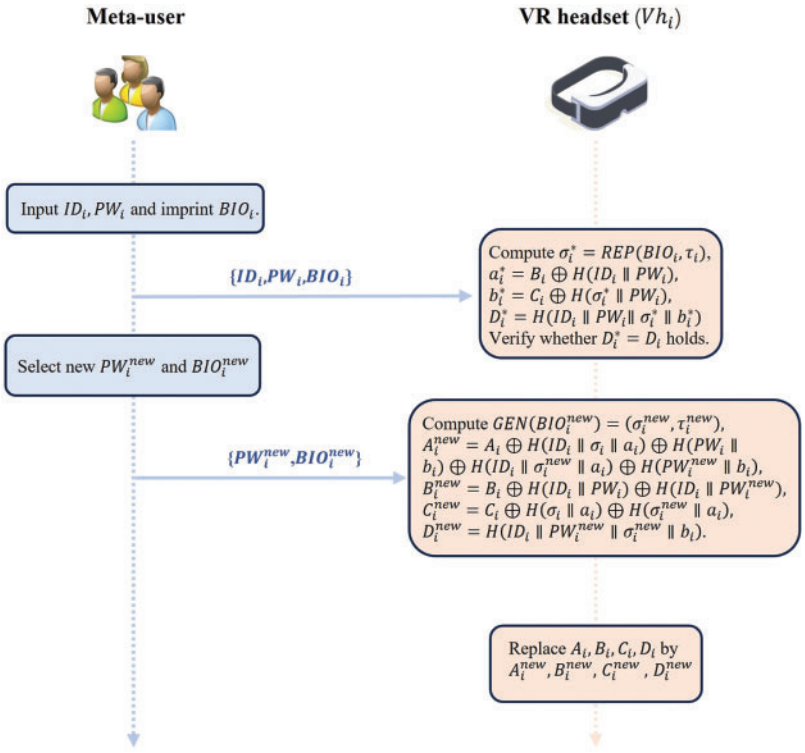

Figure 4: Factors update

5 Security Analysis

In this section, formal and informal proofs are given to prove security. The detailed proofs are described as follows.

5.1 Formal Proof

Assume that A is the PPT adversary to break our protocol. q_s, q_h, $|Hash|$, $|D|$, and l denote the number of *Send* query, the number of *Hash* oracle, the range space of $h()$, the size of the password dictionary D, and bits of σ_i, respectively.

Theorem 1: The advantage of A in breaking the *sk* security be shown as follows:

$$Adv_{\mathcal{A}}(PPT) \leq \frac{q_h^2}{|Hash|} + \frac{q_s}{2^{l-1} \cdot |D|} + 2Adv_A^{CMDL}(PPT) \tag{2}$$

Proof. We prove *Theorem 1* through five games, which are described in detail as follows.

$Game_0$: In $Game_0$, real attack is launched by A breaking our protocol under the ROR model. Then, the probability for A prevailing in $Game_0$ is summarized as follows:

$$Adv_{\mathcal{A}}(PPT) = \left|2Adv_{Game_0} - 1\right| \tag{3}$$

$Game_1$: $Game_1$ is simulated as an eavesdropping attack. In $Game_1$, A can obtain the authentication information $\{E_i, RID_i^*, F_i, T_1\}$, $\{G_j, K_j, X_j, L_j, T_2\}$ and $\{M_j, V_j, RVD_j^{new}, T_3\}$ transmitted over the public channel by accessing the $Execute(P_{Mu_i}^{\theta_1}, P_{En}^{\theta_2}, P_{Vtd_j}^{\theta_3})$. Then, A visits $Guess(P^{\theta})$ oracle to

verify whether sk established between Vh_i and Vtd_j is a session key or a random number, where $sk = H\left(RID_i^* \| RVD_j^{new^*} \| H\left(H\left(\alpha \| \beta_i\right) \| T_{r_i}\left(p\right)\right) \| T_{r_i}\left(T_{m_j}^*\left(p\right)\right) \| T_3\right)$, $RVD_j^{new} = K_j^* \oplus H\left(ID_{Vtd_j} \| c_j^{new}\right)$, $K_j^* = K_j \oplus n_j^*$, $K_j = H\left(H\left(\alpha \| \beta_i\right) \| T_{r_i}^*\left(p\right)\right) \oplus n_j$ and $T_{m_j}^*\left(p\right) = M_j \oplus H\left(RID_i^* \| T_{r_i}\left(p\right)\right)$. A needs to obtain $H\left(\alpha \| \beta_i\right)$, ID_{Vtd_j}, n_j and c_j^{new} to forge sk. However, the information exposed on public channels did not leak these parameters. Therefore, A will not increase the probability of winning through $Game_1$. Then, the probability for A prevailing in $Game_1$ is summarized as follows:

$$Adv_{Game_1} = Adv_{Game_0} \tag{4}$$

$Game_2$: In $Game_2$, A can access the $Send\left(P^\theta, m\right)$ and $Hash$ oracle compared to $Game_1$. It means that A can launch an active attack through these oracles in this game, attempting to fabricate messages to blind the participants. Although A can launch a hash query to verify the collision, each parameter contains random numbers, ID_i, PW_i and secrets associated with En. However, the information exposed on public channels did not leak these parameters. Therefore, A will not increase the probability of collision through $Game_2$. Then, the probability for A prevailing in $Game_2$ is summarized as follows:

$$\left|Adv_{Game_2} - Adv_{Game_1}\right| \leq \frac{q_h^2}{2\left|Hash\right|} \tag{5}$$

$Game_3$: In $Game_3$, A can access the $Corruptheadset\left(P_{Vtd_j}^{\theta_3}\right)$ oracle compared to $Game_2$. A can access information $\{A_i, B_i, C_i, H\left(\cdot\right), GEN\left(\cdot\right), REP\left(\cdot\right), \tau_i, p\}$ in Vh_i which is related to Meta-user, where $A_i = RPW_i \oplus RID_i \oplus H\left(\alpha \| \beta_i\right)$, $B_i = a_i \oplus H\left(ID_i \| PW_i\right)$, $C_i = b_i \oplus H\left(\sigma_i \| a_i\right)$ and $D_i = H\left(ID_i \| PW_i \| \sigma_i \| b_i\right)$. A needs to know the temporary secret a_i, σ_i and b_i to guess ID_i and PW_i. Assume that A can guess incorrectly at most q_s times and the probability for A prevailing in $Game_3$ is summarized as follows:

$$\left|Adv_{Game_3} - Adv_{Game_2}\right| \leq \frac{q_s}{2^l \cdot \left|D\right|} \tag{6}$$

$Game_4$: In $Game_4$, A tries to compute sk by analyzing the captured $\left\{E_i, RID_i^*, F_i, T_1\right\}$, $\left\{G_j, K_j, X_j, L_j, T_2\right\}$ and $\left\{M_j, V_j, RVD_j^{new}, T_3\right\}$ and solving the CMDL. A needs to get $T_{r_i}\left(T_{m_j}\left(x\right)\right)$ and $H\left(H\left(\alpha \| \beta_i\right) \| T_{r_i}\left(p\right)\right)$ to compute $sk = h\left(CID_j \parallel T_s\left(T_u\left(x\right)\right) \parallel TS_3 \parallel v^*\right)$, where r_i and m_j are respectively chosen by Vh_i and Vtd_j. It is clear from the above computations that A is difficult to compute $T_{r_i}\left(T_{m_j}\left(p\right)\right)$ without r_i and m_j even if it obtains p. Therefore, it requires A to solve the CMDL to obtain r_i and m_j from $T_{r_i}\left(p\right)$ and $T_{m_j}\left(p\right)$, respectively. Then, the probability for A prevailing in $Game_4$ is summarized as follows:

$$\left|Adv_{Game_4} - Adv_{Game_3}\right| \leq Adv_A^{CMDL}\left(PPT\right) \tag{7}$$

A makes a guess g after accessing $Guess\left(P^\theta\right)$ oracle. Then, the probability for A prevailing in $Game_4$ is summarized as follows:

$$Adv_{Game_5} = 1/2 \tag{8}$$

The probabilities from $Game_0$, $Game_1$ and $Game_4$ can be derived using the following expression:

$$\frac{1}{2}Adv_A\left(PPT\right) = \left|Adv_{Game_0} - 1/2\right| = \left|Adv_{Game_1} - Adv_{Game_4}\right| \tag{9}$$

Through the trigonometric inequality, we can obtain the following equation:

$$\left|Adv_{Game_2} - Adv_{Game_5}\right| \leq \frac{q_h^2}{2\,|Hash|} + \frac{q_s}{2^l \cdot |D|} + Adv_A^{CMDL}(PPT) \tag{10}$$

Finally, *Theorem 1* can be proved from the above equation and the final conclusion drawn.

$$Adv_{\mathcal{A}}(PPT) = 2\left|Adv_{Game_1} - Adv_{Game_4}\right| \leq \frac{q_h^2}{|Hash|} + \frac{q_s}{2^{l-1} \cdot |D|} + 2Adv_A^{CMDL}(PPT) \tag{11}$$

5.2 Informal Proof

Privileged-insider attack. In the meta-user registration phase, Vh_i sends RID_i, RPW_i to En to complete registration, where $RID_i = H(ID_i \parallel \sigma_i \parallel a_i)$ and $RPW_i = H(PW_i \parallel b_i)$. Assume that there exists an internal adversary A who has obtained RID_i, RPW_i, and that it is unable to obtain ID_i and PW_i from RID_i, RPW_i without a_i and b_i. Additionally, PW_i and σ_i are just as impossible to be stolen due to the one-way character of $H(\cdot)$. Overall, the proposed protocol will not leak any user-related information under the privileged-insider attack.

Anonymity and untraceability. As shown in Section 4.3, information $\{E_i, RID_i^*, F_i, T_1\}$, $\{G_j, K_j, X_j, L_j, T_2\}$ and $\{M_j, V_j, RVD_j^{new}, T_3\}$ exposed on the public channel without leaking credentials about meta-user. Similarly, the messages stored in the database of Vh_i have not disclosed the credentials of the meta-user. Assume that A can launch an eavesdropping attack to obtain $\{E_i, RID_i^*, F_i, T_1\}$, $\{G_j, K_j, X_j, L_j, T_2\}$ and $\{M_j, V_j, RVD_j^{new}, T_3\}$. However, A wants to get the ID_i which requires obtaining the secret $H(\alpha\|\beta_i)$, $H(\alpha\|\gamma_j)$ and the numbers r_i, n_j, m_j and c_j^{new} chosen randomly by Vh_i, En and Vtd_j. Finally, $\{E_i, RID_i^*, F_i, T_1\}$, $\{G_j, K_j, X_j, L_j, T_2\}$ and $\{M_j, V_j, RVD_j^{new}, T_3\}$ transmitted on the public channel is the result of the computation of $H(\cdot)$, and it is difficult for A to recover the ID_i. Therefore, the proposed protocol can achieve anonymity and untraceability.

Stolen headset attack. Assume the headset Vh_i of meta-user is stolen by A and the information $\{A_i, B_i, C_i, H(\cdot), GEN(\cdot), REP(\cdot), \tau_i, p\}$ stored in $Vh_i's$ database is captured, where $A_i = RPW_i \oplus RID_i \oplus H(\alpha\|\beta_i)$, $B_i = a_i \oplus H(ID_i\|PW_i)$, $C_i = b_i \oplus H(\sigma_i\|a_i)$, $D_i = H(ID_i\|PW_i\|\sigma_i\|b_i)$, $\{H(\cdot), GEN(\cdot), REP(\cdot)\}$ are one-way functions. From the above information, A who guesses the ID_i and PW_i correctly needs to know a_i and b_i. However, A wants to recover the correct a_i from B_i will need ID_i and PW_i. Therefore, A cannot guess ID_i and PW_i correctly from the information stored in Vh_i. In summary, the proposed protocol can resist stolen headset attack.

Replay attack. Assume A captures and replies the messages $\{E_i, RID_i^*, F_i, T_1\}$, where $E_i = H(\alpha\|\beta_i) \oplus T_{r_i}(p)$, $RID_i^* = H\left(ID_i\|\sigma_i^*\|a_i^*\right)$ and $F_i = H\left(E_i\|RID_i^*\|A_i^*\|T_{r_i}(p)\|T_1\right)$. However, timestamp T_1 will be verified by the setting threshold $\triangle T$ and A cannot calculate $sk^* = H\left(RID_i^*\|RVD_j^{new}\|H\left(H(\alpha\|\beta_i)\|T_{r_i}(p)\right)\|T_{r_i}\left(T_{m_j}^*(p)\right)\|T_3\right)$ without r_i, n_j, m_j and c_j^{new}. Therefore, it can resist replay attack.

MITM attack. Assume A can launch the MITM attack to capture information $\{E_i, RID_i^*, F_i, T_1\}$, $\{G_j, K_j, X_j, L_j, T_2\}$ and $\{M_j, V_j, RVD_j^{new}, T_3\}$ and attempt to impersonate a valid entity. In the case of $\{E_i, RID_i^*, F_i, T_1\}$, A modifies it in an attempt to trick En into believing that A is a legitimate user. It means that A needs to forge $E_i = H(\alpha\|\beta_i) \oplus T_{r_i}(p)$, $RID_i^* = H\left(ID_i\|\sigma_i^*\|a_i^*\right)$ and $F_i = H\left(E_i\|RID_i^*\|A_i^*\|T_{r_i}(p)\|T_1\right)$. Although A can select r_i^* and compute $T_{r_i^*}(x)$, A cannot forge $E_i = H(\alpha\|\beta_i) \oplus T_{r_i^*}(p)$ and $RID_i^* = H\left(ID_i\|\sigma_i^*\|a_i^*\right)$ without $H(\alpha\|\beta_i)$ and a_i^*. The same is true for other

authentication information, A entities cannot be authenticated without knowing the long-term secret values.

Mutual authentication. In metasystem, Vh_i, En and Vtd_j verify each other's legitimacy. First, En verifies the legitimacy of Vh_i by checking whether $F_i^* = F_i$ holds, where $F_i = H\left(E_i \| RID_i^* \| A_i^* \| T_{r_i}(p) \| T_1\right)$. Then, Vtd_j verifies the legitimacy of En by checking whether $L_i^* = L_i$ holds, where $L_i = H\left(G_j \| K_j \| RVD_j \| T_{r_i}^*(p) \| n_j \| T_2\right)$. Finally, Vh_i verifies the legitimacy of Vtd_j by checking whether $V_i^* = V_i$ holds, where $V_i = H\left(M_j \| RVD_j^{new} \| sk \| T_3\right)$.

Meta-user impersonation attack. Assume A steals the headset Vh_i of the meta-user and accesses the information $\{A_i, B_i, C_i, H(\cdot), GEN(\cdot), REP(\cdot), \tau_i, p\}$ in the local database through powerful analytical tools. Further, A intercepts $\left\{E_i, RID_i^*, F_i, T_1\right\}$ sent by Vh_i to En and tries to forge a valid message to fool En into believing it is a legitimate Meta-user. It means that A needs to forge $E_i = A_i^* \oplus T_{r_i}(p)$, $RID_i^* = H\left(ID_i \| \sigma_i^* \| a_i^*\right)$ and $F_i = H\left(E_i \| RID_i^* \| A_i^* \| T_{r_i}(p) \| T_1\right)$, where $A_i^* = H(\alpha \| \beta_i)$ and $a_i^* = B_i \oplus H(ID_i \| PW_i)$. Although A can generate r_i^* randomly and compute $T_{r_i^*}(p)$, the valid secret $A^* = H(\alpha \| \beta_i)$ and $PID_i^* = H\left(ID_i \| \sigma_i^* \| a_i^*\right)$ cannot be calculated without ID_i, σ, α and β_i. More importantly, the forged $H\left(\alpha^* \| \beta_i^*\right)$ cannot be verified by En. Therefore, it can resist Meta-user impersonation attack effectively.

Edge node impersonation attack. Assume A intercepts $\left\{G_j, K_j, RID_i^*, L_j, T_2\right\}$ sent by En to Vtd_j and tries to forge a valid message to fool Vtd_j into believing it is a legitimate edge node. It means that A needs to forge $G_j = RVD_j \oplus T_{r_i}^*(p)$, $K_j = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right) \oplus n_j$, $X_j = H\left(\alpha \| \gamma_j\right) \oplus n_j$ and $L_j = H\left(G_j \| K_j \| RVD_j \| T_{r_i}^*(p) \| n_j \| T_2\right)$, where $RVD_j = H\left(ID_{Vtd_j} \| c_j\right)$ and $n_j = X_j \oplus H(\alpha \| \gamma_i)$. Although A can generate n_j^* randomly, the valid secret $X_j = H\left(\alpha \| \gamma_j\right) \oplus n_j$ and $K_j = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right) \oplus n_j$ cannot be calculated without α, β_i, and γ_j. More importantly, the forged $H\left(\alpha^* \| \gamma_j^*\right)$ cannot be verified by Vtd_j. Therefore, it can resist Edge node impersonation attack effectively.

Tactile device impersonation attack. Assume A intercepts $\left\{M_j, V_j, RVD_j^{new}, T_3\right\}$ sent by Vtd_j to Vh_i and tries to forge a valid message to fool Vh_i into believing it is a legitimate tactile device. It means that A needs to forge $M_j = H\left(RID_i^* \| T_r^*\right)$, $K_j = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right) \oplus n_j$, $X_j = H\left(\alpha \| \gamma_j\right) \oplus n_j$ and $L_j = H\left(G_j \| K_j \| RVD_j \| T_{r_i}^*(p) \| n_j \| T_2\right)$, where $K_j^* = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right)$ and $RVD_j^{new} = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right) \oplus H\left(ID_{Vtd_j} \| c_j^{new}\right)$. Although A can generate m_j^* randomly and compute $T_{m_j^*}^*(p)$, the valid secret $K_j^* = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right)$ cannot be calculated without α, and β_i. More importantly, the forged $H\left(\alpha^* \| \beta_j^*\right)$ cannot be verified by Vh_i. Therefore, it can resist Tactile device impersonation attack effectively.

Session key security. The session key $sk = H\left(RID_i^* \| RVD_j^{new} \| K_j^* \| T_{m_j}\left(T_{r_i}^*(p)\right) \| T_3\right)$ is generated between Vh_i and Vtd_j. Assume A intercepts $\left\{M_j, V_j, RVD_j^{new}, T_3\right\}$ and attempts to compute $sk = H\left(RID_i^* \| RVD_j^{new} \| K_j^* \| T_{m_j}\left(T_{r_i}^*(p)\right) \| T_3^*\right)$ by generating c_j^* and T_3^*. However, A cannot recover the valid $RVD_j^{new} = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right) \oplus H\left(ID_{Vtd_j} \| c_j^{new}\right)$ and $K_j^* = H\left(H(\alpha \| \beta_i) \| T_{r_i}^*(p)\right)$ without α, β_i, r_i and ID_{Vtd_j}. Furthermore, $H(\cdot)$ is the collision-resistant one-way function. Therefore, the session key is secure in this paper.

6 Performance Analysis

In this section, detailed performance analyses are described from theoretical side, tool simulation and experimental analysis.

6.1 Comparison of Security and Overhead

We will analyze the security and theoretical overheads compared to the associated metaverse authentication protocols, respectively. First, the security is compared and the results are presented in Table 2. Ryu et al. [6] proposed a blockchain-assisted authentication protocol for metasystem. In their protocol, elliptic curve is employed to provide secure communication between the user and the platform server as well as avatar security. However, it is not able to resist real-world impersonation attacks and ensure session key security. Li et al. [23] proposed a server-assisted authentication method using chaotic mapping. However, it is also impossible to resist an impersonation attack. Zheng et al. [22] proposed an efficient session key establishment method between users through chaotic mapping. However, it still has information leakage when facing MITM attacks. From Table 2, it is easy to find that just Yu et al. [21] and ours can satisfy the full security requirements.

Table 2: Security comparison

Security	Ryu et al. [6]	Li et al. [23]	Yu et al. [21]	Zheng et al. [22]	Ours
Privileged-insider attack	√	√	√	√	√
Anonymity and untraceability	√	√	√	√	√
Stolen headset attack	√	√	√	×	√
Replay attack	√	√	√	√	√
MITM attack	√	×	√	×	√
Mutual authentication	×	×	√	√	√
Meta-user impersonation attack	√	×	√	√	√
Edge node impersonation attack	×	×	√	√	√
Device impersonation attack	×	×	√	√	√
Session key security	×	√	√	√	√

In terms of overhead, we compare and analyze the computation and communication overheads, respectively. From Table 3, We can find that our total cost is $18T_h + 4T_c$, where T_h is the time of hash operation and T_c is the time of chaotic mapping operation. Ryu et al. [6] implemented the security of avatars based on ECC and its total overhead is $25T_m + 31T_h + 8T_s$, where T_s is the time of symmetric encryption and decryption operation. Li 2016 implemented multi-party authentication using chaotic mapping and its total overhead is $19T_h + 6T_c$, which is higher than ours in terms of overhead. Meanwhile, Yu et al. [21] completed the three-party authentication using chaotic mapping and its total overhead is $19T_h + 4T_c$. However, it has the transmission count of 7, which will cause additional delay. Although Zheng et al. [22] and ours have the same total overhead, Zheng et al. only completed the two-party authentication. Finally, the analysis results show that the proposed protocol has high practicality in balancing security and computational overhead by comparing Tables 2 and 3.

Table 3: Cost comparison

Phase	Ryu et al. [6]	Li et al. [23]	Yu et al. [21]	Zheng et al. [22]	Ours
User side	$10T_m + 13T_h + 2T_s$	$7T_h + 3T_c$	$6T_h + 2T_c$	$10T_h + 2T_c$	$10T_h + 2T_c$
Edge node	$5T_m + 5T_h + 4T_s$	$8T_h + 1T_c$	$7T_h$	$8T_h + 2T_c$	$3T_h$
Device side	$10T_m + 13T_h + 2T_s$	$4T_h + 2T_c$	$6T_h + 2T_c$	/	$5T_h + 2T_c$
Total cost	$25T_m + 31T_h + 8T_s$	$19T_h + 6T_c$	$19T_h + 4T_c$	$18T_h + 4T_c$	$18T_h + 4T_c$
Transmission times	6	5	7	3	3

6.2 Tool Simulation

In order to analyze whether the protocol is resistant to man-in-the-middle and replay attacks, the popular AVISPA tool is employed to verify security. AVISPA is a tool for proving network security protocols and applications, which is integrated into the SPAN virtual machine through a virtual box. Our protocol is compiled in the HLPSL language and the validation result is shown in Fig. 5.

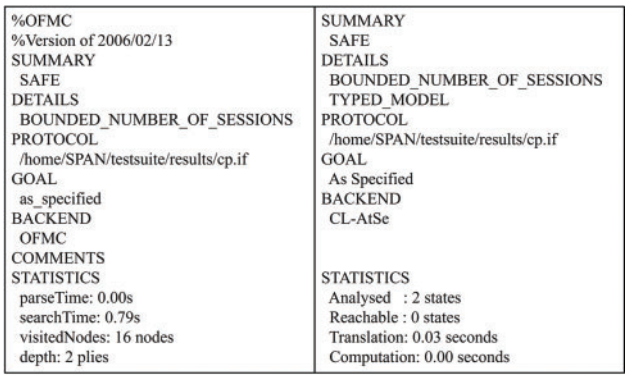

Figure 5: Simulation result

6.3 Experimental Analysis

To further compare the performance, the protocol was simulated with a VMware workstation at 2.7 GHz and 8 G RAM. We completed the experimental simulation using C based on PBC and GMP libraries. The computational and communication overhead results are shown in Figs. 6 and 7.

In [6], its runtime is 207.36 ms on the user side, 120 ms on the edge node side, 207.36 ms in the device side and transmission times is 6. Its total overhead is 534 milliseconds due to the high runtime of the power operation. In [23], its runtime is 53.54 ms in the user side, 19.66 ms in edge node side, 35.48 ms in the device side and transmission times is 5. In [21], its runtime is 36.12 ms in the user side, 2.24 ms in edge node side, 36.12 ms in the device side and transmission times are 7. In [22], its runtime is 37.4 ms in the user side, 36.76 ms in edge node side and transmission times is 7. Compared to the above protocol, our user-side runtime is 37.4 ms, node-side runtime is 0.96 ms and device-side runtime is 35.8 ms, which is the lowest total runtime. Importantly, we completed the session key establishment in the metasystem using only 3 rounds of transmission. This will reduce transmission delay and energy consumption in the metasystem.

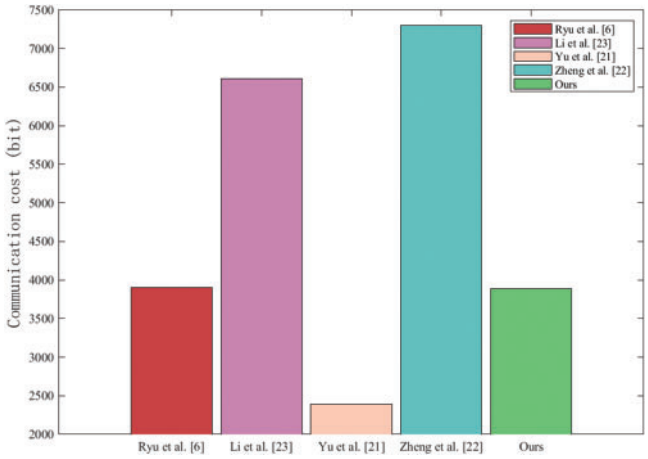

Figure 6: Computational overhead

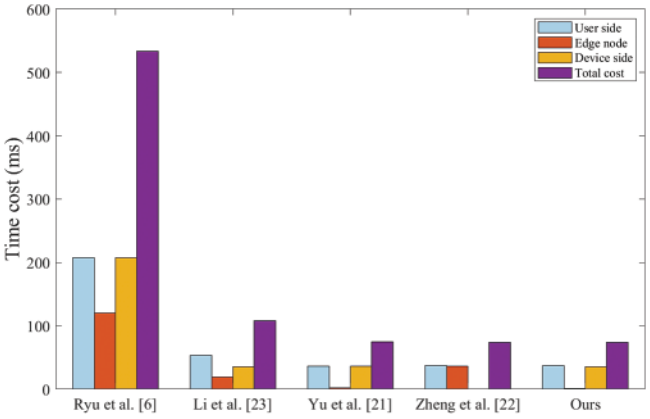

Figure 7: Communication overhead

7 Conclusion

In this paper, we proposed a chaotic map-based AKA protocol to secure the security of meta-users and avatars, which enables low-latency transmission of information in the metasystem. Considering the characteristics of the metasystem, meta-user biometrics are employed to strengthen session key security. Further, the functionality of updating passwords and biometrics through VR headsets by meta-users is considered. The security of the protocol is comprehensively analyzed through formal and formal security proofs. Finally, we simulated the performance of the protocol through theoretical analysis, tool simulation, and experimental simulation which shows that it can effectively resist MITM and replay attacks without additional overhead compared to other related protocols. In future work, we will take into account the frequent dynamic updates of devices in the metasystem. Improvement of secret values in the proposed scheme to reduce communication overhead and enhance security. Therefore, designing an authentication scheme without locally stored secret values is the first step in our future work.

Acknowledgement: Not applicable.

Funding Statement: This work has received funding from National Natural Science Foundation of China (No. 42275157).

Author Contributions: The authors confirm their contribution to the paper as follows: study conception and design: Guojun Wang; data collection: Qi Liu; analysis and interpretation of results: Guojun Wang, Qi Liu; draft manuscript preparation: Guojun Wang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. E. M. Cayamcela and W. Lim, "Artificial intelligence in 5G technology: A survey," in *Proc. ICTC*, Jeju, Korea, 2018, pp. 860–865.

[2] Y. Wang *et al.*, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 1, pp. 319–352, 2022.

[3] C. Anthes, R. J. García-Hernández, M. Wiedemann, and D. Kranzlmüller, "State of the art of virtual reality technology," in *2016 IEEE Aerospace Conf.*, Big Sky, MT, USA, 2016, pp. 1–19.

[4] R. D. Pietro and S. Cresci, "Metaverse: Security and privacy issues," in *Proc. TPS-ISA*, Atlanta, GA, USA, 2021, pp. 281–288.

[5] D. Liu, Y. Zhang, W. Wang, K. Dev, and S. A. Khowaja, "Flexible data integrity checking with original data recovery in IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp.*, vol. 24, no. 2, pp. 2618–2629, 2023.

[6] 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.

[7] G. Thakur, P. Kumar, C. M. Chen, A. V. Vasilakos, Anchna and S. Prajapat, "A robust privacy-preserving ECC-based three-factor authentication scheme for metaverse environment," *Comput. Commun.*, vol. 211, pp. 271–285, 2023.

[8] H. Ning *et al.*, "A survey on the metaverse: The state-of-theart, technologies, applications, and challenges," *IEEE Internet Things*, vol. 10, pp. 14671–14688, 2023.

[9] N. A. Dahan, M. Al-Razgan, A. Al-Laith, M. A. Alsoufi, M. S. Al-Asaly and T. Alfakih, "Metaverse framework: A case study on e-learning environment (ELEM)," *Electron.*, vol. 11, no. 10, pp. 1616, 2022. doi: 10.3390/electronics11101616.

[10] T. Zhang, J. Shen, C. F. Lai, S. Ji, and Y. Ren, "Multi-server assisted data sharing supporting secure deduplication for metaverse healthcare systems," *Future Gener. Comput. Syst.*, vol. 140, no. 1, pp. 299–310, 2023. doi: 10.1016/j.future.2022.10.031.

[11] S. Qamar, Z. Anwar, and M. Afzal, "A systematic threat analysis and defense strategies for the metaverse and extended reality systems," *Comput. Secur.*, vol. 128, no. 6, pp. 103127, 2023. doi: 10.1016/j.cose.2023.103127.

[12] J. D. N. Dionisio, W. G. B. Iii, and R. Gilbert, "3D virtual worlds and the metaverse: Current status and future possibilities," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 1–38, 2013. doi: 10.1145/2480741.2480751.

[13] L. H. Lee *et al.*, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," arXiv preprint arXiv:2110.05352, 2021.

[14] H. Yang, P. Vijayakumar, J. Shen, and B. B. Gupta, "A location-based privacy-preserving oblivious sharing scheme for indoor navigation," *Future Gener. Comp. Syst.*, vol. 137, no. 3, pp. 42–52, 2022. doi: 10.1016/j.future.2022.06.016.

[15] S. M. Park and Y. G. Kim, "A metaverse: Taxonomy, components, applications, and open challenges," *IEEE Access.*, vol. 10, pp. 4209–4251, 2022. doi: 10.1109/ACCESS.2021.3140175.
[16] M. U. Rafique and S. C. S. Cheung, "Tracking attacks on virtual reality systems," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 41–46, 2020. doi: 10.1109/MCE.2019.2953741.
[17] F. O'Brolcháin, T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky and B. Gordijn, "The convergence of virtual reality and social networks: Threats to privacy and autonomy," *Sci. Eng. Ethics.*, vol. 22, no. 1, pp. 1–29, 2016. doi: 10.1007/s11948-014-9621-1.
[18] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 52–61, 2018. doi: 10.1109/MTS.2018.2826060.
[19] J. A. de Guzman, K. Thilakarathna, and A. Seneviratne, "Security and privacy approaches in mixed reality: A literature survey," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–37, 2019. doi: 10.1145/3359626.
[20] K. Yang, Z. Zhang, Y. Tian, and J. Ma, "A secure authentication framework to guarantee the traceability of avatars in metaverse," *IEEE Trans. Inf. Foren. Secur.*, vol. 18, pp. 3817–3832, 2023. doi: 10.1109/TIFS.2023.3288689.
[21] Y. Yu, O. Taylor, R. Li, and B. Sunagawa, "An extended chaotic map-based authentication and key agreement scheme for multi-server environment," *Math.*, vol. 9, no. 8, pp. 798, 2021. doi: 10.3390/math9080798.
[22] Y. Zheng *et al.*, "Design and analysis of a security-enhanced three-party authenticated key agreement protocol based on chaotic maps," *IEEE Access.*, vol. 8, pp. 66150–66162, 2020. doi: 10.1109/ACCESS.2020.2979251.
[23] X. Li *et al.*, "A novel chaotic maps-based user authentication and key agreement protocol for multi-server environments with provable security," *Wirel. Pers. Commun.*, vol. 89, no. 2, pp. 569–597, 2016. doi: 10.1007/s11277-016-3293-x.